

**PLAN ESTRATÉGICO DE TECNOLOGÍAS
DE LA INFORMACIÓN - PETI
2018 - 2021**

**UNIDAD PARA LA ATENCION Y REPARACION INTEGRAL A LAS VICTIMAS
UARIV**

Noviembre de 2018



GOBIERNO
DE COLOMBIA



UNIDAD PARA LAS VÍCTIMAS

**PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN
PETI – 2018**

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI

PROCESO: GESTIÓN DE LA INFORMACIÓN

CODIGO: 130,06,07-3

Versión:01

Fecha: 28/12/2018

Página 2 de 127

CONTROL DE CAMBIOS

Versión	Elaborado por	Revisado y Aprobado por	Fecha	Motivo
1	OTI – SRNDI – RNDI – OAC	Jhon Ricardo Morales - Jefe OTI	27-12-2018	Creación

TABLA DE CONTENIDO

INTRODUCCIÓN	6
1. OBJETIVOS.....	7
1.1. OBJETIVO GENERAL.....	7
1.2. OBJETIVOS ESPECÍFICOS	7
2. ALCANCE.....	7
3. MARCO NORMATIVO	8
3.1. ÁMBITOS Y LINEAMIENTOS DEL DOMINIO DE ESTRATEGIA DE TI.....	9
3.2. ROLES.....	9
4. RUPTURAS ESTRATÉGICAS.....	10
5. ANÁLISIS DE LA SITUACIÓN ACTUAL	11
5.1. ESTRATEGIA DE TI	11
5.1.1. MISIÓN DE LA UNIDAD PARA LAS VÍCTIMAS	13
5.1.2. VISIÓN DE LA UNIDAD PARA LAS VÍCTIMAS	13
5.1.3. OBJETIVOS ESTRATÉGICOS DE LA UNIDAD.....	13
5.1.4. ORGANIGRAMA DE LA ENTIDAD.	14
5.1.5. PLAN NACIONAL DE DESARROLLO	14
5.1.6. ESTRATEGIAS SECTORIALES.....	15
5.1.7. PLANES ESTRATÉGICOS INSTITUCIONALES	16
5.1.8. POLÍTICAS DE TI	16
5.2. USO Y APROPIACIÓN	16
5.3. SISTEMAS DE INFORMACIÓN.....	28
5.3.1. SISTEMAS DE INFORMACIÓN MISIONALES.....	29
5.3.2. ARQUITECTURA DE SISTEMAS DE INFORMACION.....	31
5.4. SERVICIOS TECNOLÓGICOS	38
5.5. GESTIÓN DE LA INFORMACIÓN	56
5.6. GOBIERNO DE TI.....	65
5.7. ANÁLISIS FINANCIERO COSTOS DE OPERACIÓN Y FUNCIONAMIENTO	67
6. ENTENDIMIENTO ESTRATÉGICO	70
6.1. MODELO OPERATIVO.....	70
6.1.1. MARCO INSTITUCIONAL	70
6.1.2. ESTRUCTURA ORGANIZACIONAL Y UBICACIÓN DE LA OTI.....	71

6.1.3. DESCRIPCIÓN DEL MAPA ESTRATÉGICO DE LA UNIDAD DE VÍCTIMAS.....	71
6.1.4. DESCRIPCIÓN DEL PLAN ESTRATÉGICO SECTORIAL	73
6.1.5. MISIÓN Y VISIÓN ESTRATÉGICA SECTORIAL.....	75
6.1.6. ESTRUCTURA DEL SECTOR INCLUSIÓN.....	76
6.1.7. PLAN ESTRATÉGICO SECTORIAL.....	76
6.1.8. MAPA DE PROCESOS - UNIDAD	78
6.1.9. PROCESO GESTIÓN DE LA INFORMACIÓN.....	79
6.1.10. POLÍTICAS DE TI	80
6.2. INTERCAMBIO Y NECESIDADES DE INFORMACIÓN	81
6.3. ALINEACIÓN DE TI CON LOS PROCESOS	81
7. MODELO DE GESTIÓN DE TI.....	83
7.1. ESTRATEGIA DE TI	83
7.1.1. PLANTEAMIENTO DE LA ESTRATEGIA GENERAL	84
7.1.2. ANÁLISIS DOFA Y ESTRATEGIAS ESPECIFICAS	86
7.1.3. ALINEACIÓN DE TI CON LA ESTRATEGIA DE LA UNIDAD PARA LAS VÍCTIMAS	90
7.1.4. MATRIZ OBJETIVOS ESTRATÉGICOS DE TI / DOMINIOS / INICIATIVAS	91
7.2. GOBIERNO DE TI.....	91
7.2.1. MARCO LEGAL Y NORMATIVO	91
7.2.2. POLÍTICAS DE TI	91
7.2.3. ESQUEMAS O INSTANCIAS PARA RELACIONAR O TOMAR DECISIONES.....	94
7.2.4. ESTRUCTURA ORGANIZACIONAL - ROLES Y PERFILES DE TI.....	94
7.2.5. RELACIONES CON OTRAS ÁREAS E INSTITUCIONES PÚBLICAS.....	94
7.2.6. MODELO DE GESTIÓN DE PROYECTOS.....	95
7.2.7. GESTIÓN DE PROVEEDORES y ANS.....	95
7.2.8. INDICADORES DE GESTIÓN DE TI.....	95
7.2.9. CADENA DE VALOR.....	96
7.2.10. GESTIÓN DE RIESGOS	96
7.3. GESTIÓN DE INFORMACIÓN	98
7.3.1. HERRAMIENTAS DE ANÁLISIS	99
7.3.2. ARQUITECTURA DE INFORMACIÓN.....	99
7.3.3. NECESIDADES DE INFORMACIÓN	99
7.4. SISTEMAS DE INFORMACIÓN.....	99
7.4.1. ARQUITECTURA DE SISTEMAS DE INFORMACIÓN.....	100

7.4.2. METODOLOGÍA DE DESARROLLO	103
7.5. MODELO DE GESTIÓN DE SERVICIOS TECNOLÓGICOS	103
7.5.1. ARQUITECTURA DE SERVICIOS TECNOLÓGICOS	103
7.5.2. INFRAESTRUCTURA Y CRITERIOS DE CALIDAD	103
7.5.3. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	104
7.5.4. CONECTIVIDAD	106
7.5.5. SERVICIOS DE OPERACIÓN.....	110
7.5.6. MESA DE SERVICIOS.....	110
7.5.7. PROCEDIMIENTOS DE GESTIÓN	110
7.6. USO Y APROPIACIÓN	111
7.6.1. ESTRATEGIA PARA USO Y APROPIACIÓN	111
8. MODELO DE PLANEACIÓN	114
8.1. LINEAMIENTOS Y/O PRINCIPIOS QUE RIGEN EL PETI.....	114
8.2. ESTRUCTURA DE ACTIVIDADES ESTRATÉGICAS	114
8.2.1. DISEÑAR E IMPLEMENTAR LA ARQUITECTURA EMPRESARIAL	114
8.2.2. FORMULAR E IMPLEMENTAR LA ESTRATEGIA DE USO Y APROPIACIÓN.....	114
8.2.3. SUMINISTRAR LOS RECURSOS PARA LAS INICIATIVAS DE GESTIÓN DOCUMENTAL DE LA UNIDAD Y EXPEDIENTE ÚNICO DIGITAL.....	114
8.2.4. GESTIONAR BUS DE DATOS BIZTALK.	115
8.2.5. APLICAR PLAN DE SEGURIDAD DE LA INFORMACIÓN.....	115
8.2.6. INTEGRAR ESTRATEGIAS Y SERVICIOS DE INFORMACIÓN CON OTRAS ÁREAS DE LA UNIDAD.....	115
8.2.7. IMPLEMENTAR UN PLAN DE CONTINGENCIAS O RECUPERACIÓN DE DESASTRES.	116
8.3. ELABORAR Y EJECUTAR PLAN MAESTRO O MAPA DE RUTA.....	116
8.4. DEFINIR INDICADORES DE SEGUIMIENTO AL PETI	116
9. PLAN DE COMUNICACIONES.....	121

INTRODUCCIÓN

La Unidad para la Atención y Reparación Integral a las Víctimas, fue creada por el Gobierno Nacional, mediante la Ley 1448 de 2011, como una unidad administrativa especial con personería jurídica y autonomía administrativa y patrimonial, y adscrita por el Decreto 4157 de 2011 al Departamento Administrativo para la Prosperidad Social. Considerando que su misión está definida como **“Liderar acciones del Estado y la sociedad para atender y reparar integralmente a las víctimas, para contribuir a la inclusión social y a la paz”** y que su visión sea **“En el año 2021 haber logrado que las víctimas, reparadas integralmente, ejerzan su ciudadanía y aporten en la consolidación de la paz como resultado de la gestión efectiva y coordinada de la Unidad con los demás actores del Sistema”**, es necesario que la Oficina de Tecnologías de la Información formule el presente Plan Estratégico de Tecnología – PETI como estrategia para alinear la estrategia de TI a la misión, visión y objetivos estratégicos definidos en la Unidad.

El Plan Estratégico de Tecnologías de la Información – PETI está basado en el documento “G.ES.06 Guía Cómo Estructurar el Plan Estratégico de Tecnologías de la Información – PETI” versión 1.0 del 30 de marzo de 2016, contiene la proyección de la estrategia de tecnología formulada en el año 2018 con actualización anual y vigencia hasta año 2021, en razón a que la Unidad solo tiene vida jurídica hasta esa fecha. Sin embargo, puesto que de conformidad con la Ley 1448 de 2011 en su artículo 155 permite a la víctima presentar su declaración hasta dos años después del hecho, lo cual aplicaría hasta el año 2023 si se presentaran hechos en el año 2021; se deberá formular un nuevo PETI con vigencia hasta el año 2023. La dinámica institucional, los posibles cambios de la estrategia del sector y la evolución en las tendencias de las Tecnologías de la Información, hacen necesario que su actualización se realice cada año, manteniendo la alineación a la estrategia institucional y al modelo integrado de gestión y planeación, con el fin de habilitar las capacidades y servicios de tecnología necesarios para impulsar las transformaciones en el desarrollo del sector y la eficiencia y transparencia del Estado.

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Establecer la estrategia de TI que será implementada durante el cuatrienio (2018-2021) en la Unidad para la Víctimas para planificar, definir y direccionar planes, programas y proyectos tecnológicos, implementando las iniciativas respectivas hacia el logro de objetivos estratégicos institucionales, generando valor público en la institución y en sus grupos de interés.

1.2. OBJETIVOS ESPECÍFICOS

- Determinar el estado actual de la información, las tecnologías de la información y las comunicaciones de la Unidad, en el marco de los modelos de planeación MIPG (Modelo Integrado de Planeación y Gestión), SIG (Sistema Integrado de Gestión), PAA (Plan Anual de Adquisiciones) y PA (Plan de Acción), con el fin de acercar a las víctimas para brindarles una oferta pertinente, eficaz, sostenible y oportuna soportada en elementos de TI.
- Fortalecer la integración de información e interoperabilidad entre las dependencias de la UNIDAD ADMINISTRATIVA PARA ATENCION Y REPARACION INTEGRAL A LAS VÍCTIMAS – UARIV y así mismo, entre la Unidad y las entidades del Sistema Nacional de Atención y Reparación Integral a las Víctimas SNARIV, a través de los sistemas de información y las tecnologías, para favorecer la atención a las víctimas, en procura de fomentar la cultura de confianza, colaboración e innovación para garantizar una atención digna, respetuosa y diferencial.
- Determinar el estado actual de cada dominio del Modelo IT4+ (Estrategia TI, Gobierno TI, Sistemas de Información, Servicios Tecnológicos y Uso y Apropiación), con el fin de desarrollar la Arquitectura Empresarial de la UNIDAD PARA LAS VÍCTIMAS bajo los criterios de la Política y Estrategia de Gobierno Digital.
- Fortalecer los componentes de seguridad de información de todos los dominios de la Arquitectura Empresarial como marco de referencia definido por el MINTIC.
- Establecer la situación objetivo o deseada para cada uno de los dominios del Modelo de Gestión IT4+, en el marco de desarrollo de la Arquitectura Empresarial
- Establecer el Modelo de Planeación del PETI formulando el mapa de ruta de las iniciativas o proyectos para alcanzar la situación deseada, en relación con los dominios del Modelo de Gestión IT4+ en el marco de desarrollo de la Arquitectura Empresarial.

2. ALCANCE.

El Plan Estratégico de Tecnologías de la Información (PETI) tiene una vigencia desde el año 2018 hasta el 2021, con actualización anual e inicia con el establecimiento de la situación actual, análisis de necesidades de la Unidad, estableciendo planes, programas y proyectos en función de los dominios de Modelos de Gestión IT4+ (Estrategia de TI ,Gobierno de TI, Gestión de la

Información, Sistemas de Información, Modelo de Gestión de Servicios Tecnológicos, Uso y Apropiación) y finaliza con la formalización del mapa de ruta de la estrategia de TI para el cuatrienio.

3. MARCO NORMATIVO

La Ley 1448 de 2011 *“Por la cual se dictan medidas de atención, asistencia y reparación integral a las víctimas del conflicto armado interno y se dictan otras disposiciones”* a través del artículo 166, creó la Unidad para la Atención y Reparación Integral a las Víctimas como una unidad administrativa especial con personería jurídica y autonomía administrativa y patrimonial, y adscrita por el Decreto 4157 de 2011 al Departamento Administrativo para la Prosperidad Social

El Decreto 4802 de 2011 *“Por el cual se establece la estructura de la Unidad Administrativa Especial para la Atención y Reparación Integral a las Víctimas”*, en su artículo 7 numeral 23, asigna a la Dirección General entre otras funciones la referida a: *“1: Crear, organizar y conformar comités, comisiones y grupos internos de trabajo, teniendo en cuenta la estructura interna, las necesidades del servicio y los planes y programas trazados para el adecuado funcionamiento de la Unidad”*

Ley 1712 de 2014, *“Por la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”*, señala que sus sujetos obligados deberán observar lo establecido por la estrategia de Gobierno en Línea en cuanto a la publicación y divulgación de información pública”.

Decreto 415 de 2016 del Departamento Administrativo de la Función Pública, a través del cual se definen los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones a ser acatados por las entidades del Estado del orden nacional y territorial, los organismos autónomos y de control, de tal forma que en su artículo 2.2.35.3 numeral 1 enuncia que deberán: *“Liderar la gestión estratégica con tecnologías de la información y las comunicaciones mediante la definición, implementación, ejecución, seguimiento y divulgación de un Plan Estratégico de Tecnologías de la Información – PETI que este alineado a la estrategia y modelo integrado de gestión.*

Subsiguiente en el artículo 2.2.35.3 numeral 2 el mencionado define entre otros aspectos que también deberán : *“ Liderar la definición, implementación y mantenimiento de la arquitectura empresarial de la entidad y/o sector en virtud de las definiciones y lineamientos establecidos en el marco de referencia de arquitectura empresarial para la gestión de Tecnologías de la Información y las Comunicaciones (TIC) del Estado, la estrategia GEL y según la visión estratégica, las necesidades de transformación y marco legal específicos de su entidad o sector.”*

El Decreto 1008 de 2018 del Ministerio de las Tecnologías y las Comunicaciones establece los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de

la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones". La política de Gobierno Digital antes Gobierno en Línea tiene como estructura dos componentes TIC PARA EL ESTADO y TIC PARA LA SOCIEDAD, además enmarca tres estándares o lineamientos ARQUITECTURA, SEGURIDAD Y PRIVACIDAD y SERVICIOS CIUDADANOS DIGITALES, dentro del lineamiento Arquitectura se ordena la directriz relacionada con la formulación e implementación del Plan Estratégico de Tecnología siguiendo la guía definida por el Ministerio de las Comunicaciones

3.1. ÁMBITOS Y LINEAMIENTOS DEL DOMINIO DE ESTRATEGIA DE TI

La siguiente tabla muestra los principales ámbitos y lineamientos de Arquitectura Empresarial - Gobierno Digital que se relacionan con el Plan Estratégico de Tecnologías de la Información - PETI:


Ámbito	Lineamiento
Entendimiento estratégico	<ul style="list-style-type: none"> • Entendimiento estratégico. LI.ES.01 • Documentación de la estrategia de TI en el PETI. LI.ES.05
Direccionamiento estratégico	<ul style="list-style-type: none"> • Plan de comunicación de la estrategia de TI. LI.ES.06

Tabla 1. Ámbitos y Lineamientos definidos por MINTIC para estructurar el PETI

3.2. ROLES

La lista de cargos y roles que intervienen en la elaboración del Plan Estratégico de Tecnologías de la Información son:

- Jefe de la Oficina de Tecnologías de la Información – OTI o quien haga sus veces
- Líder de Gestión Presupuestal de la OTI
- Líder Enlace de Planeación de la OTI
- Líder de Sistemas de Información
- Líder de Servicios Tecnológicos de la OTI
- Líder de Infraestructura de la OTI
- Líder de Uso y Apropiación de la OTI
- Líder de la Seguridad de la Información de la OTI
- Delegado de la Oficina Asesora de Comunicaciones
- Delegado de la Subdirección Red Nacional de Información
- Delegado de la Subdirección de Valoración y Registro

	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN		
	PETI – 2018		
	OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
PROCESO: GESTIÓN DE LA INFORMACIÓN			
CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018	Página 10 de 127

4. RUPTURAS ESTRATÉGICAS

Las rupturas estratégicas permiten resolver la pregunta “Cómo las tecnologías de la información generan valor a través de la implementación de nuevos servicios que faciliten acercar el estado a la víctima para lograr su condición como ciudadano”. Las rupturas estratégicas deben comunicar un cambio en el enfoque estratégico, de forma que le permitan a la Gerencia de TI transformar, innovar, adoptar un modelo y permitir que la tecnología se vuelva un instrumento que genere valor.

Algunas de las rupturas estratégicas identificadas por la OTI son:

ALINEACIÓN DE TI CON ESTRATEGIA INSTITUCIONAL

La Unidad viene adelantando acciones cuyo propósito es articular la estrategia de TI con la estrategia institucional y sectorial acogiendo a las directrices definidas por el Ministerio de las Tecnologías y las Comunicaciones – MINTIC.

GOBERNABILIDAD DE TI

Fortalecer el liderazgo de la Oficina de Tecnologías de la Información – OTI, en el marco de una gerencia integral, que genere articulación con las otras dependencias de la entidad, dotándola de elementos que le permita afianzar la estructura de TI al interior de los procesos y la relación con otras áreas y entidades.

OPTIMIZACIÓN PERMANENTE DE METODOLOGÍAS PARA LA GESTIÓN DE PROYECTOS

La OTI debe procurar la mejora continua en la implementación de lineamientos y buenas prácticas en la gestión de proyectos, esto significa facilitar el cumplimiento de los objetivos institucionales, la capacidad de los integrantes de grupos de trabajo, el valor agregado y calidad de los productos obtenidos.

EQUIPO HUMANO CON LIDERAZGO E INNOVADOR

Fortalecer las capacidades técnicas del equipo involucrado en las tecnologías de la información y las comunicaciones, así como las capacidades analíticas en cuanto a herramientas, resultados y publicación

FORTALECER LA DISPONIBILIDAD DE LA INFORMACIÓN COMO UN BIEN PÚBLICO

La información como activo de valor para la entidad debe fluir en línea desde sus fuentes hacia las partes interesadas de forma oportuna en términos de calidad, confiabilidad, integridad, disponibilidad y confidencialidad

 	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN		
	PETI – 2018		
	OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
PROCESO: GESTIÓN DE LA INFORMACIÓN			
CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018	Página 11 de 127

INTEROPERABILIDAD

Pensamiento sistémico hacia un sistema integral de estándares, fuentes y herramientas. La interoperabilidad debe pasar de procesos por lotes a procesos en línea en tiempo real.

5. ANÁLISIS DE LA SITUACIÓN ACTUAL

El estado de la situación actual de las Tecnologías de la Información de la Unidad está determinado por el nivel de alineamiento que existe con el marco de los dominios de la Arquitectura Empresarial definida por el MINTIC, para cumplir los objetivos estratégicos y misionales. Los dominios de la Arquitectura Empresarial objeto de este análisis son:

- DOMINIO ESTRATEGIA
- DOMINIO GOBIERNO
- DOMINIO INFORMACIÓN
- DOMINIO SISTEMAS DE INFORMACIÓN
- DOMINIO SERVICIOS TECNOLÓGICOS
- DOMINIO USO Y APROPIACIÓN

5.1. ESTRATEGIA DE TI

Hace referencia a realizar un diagnóstico y entendimiento claro y documentado del estado actual de la tecnología en la Unidad, para proporcionarle a la Jefatura de la OTI una orientación sobre el uso apropiado de la tecnología en el proceso de transformación institucional.



CONTEXTO ORGANIZACIONAL Y DEL ENTORNO

La Unidad para la Atención y Reparación Integral a las Víctimas junto con el ICBF y el Centro de Memoria Histórica pertenecen al Sector Inclusión cuya cabeza es el Departamento de Prosperidad Social. Mediante la Ley 1448 de 2011, en su artículo 166, se creó la Unidad para la Atención y Reparación Integral a las Víctimas como una unidad administrativa especial con personería jurídica y autonomía administrativa y patrimonial, y adscrita por el Decreto 4157 de 2011 al Departamento Administrativo para la Prosperidad Social. De otra parte, mediante el Decreto 4802 de 2011 el Departamento Administrativo de la Función Pública establece la estructura de la Unidad Administrativa Especial para la Atención y Reparación Integral a las Víctimas, asignando las siguientes funciones:

1. Aportar al Gobierno Nacional los insumos para el diseño, adopción y evaluación de la Política Pública de Atención y Reparación a las Víctimas garantizando el enfoque diferencial.
2. Promover y gestionar con las entidades que conforman el Sistema Nacional de Atención y Reparación Integral a las Víctimas la flexibilización y articulación de la oferta institucional para

la atención, asistencia y reparación de las víctimas.

3. Coordinar con el Ministerio de Hacienda y Crédito Público y el Departamento Nacional de Planeación, la asignación y transferencia a las entidades territoriales de los recursos presupuestales requeridos para la ejecución de los planes, proyectos y programas de atención, asistencia y reparación a víctimas según lo dispuesto en la Ley 1448 de 2011.
4. Coordinar la relación Nación territorio, para efectos de atención y reparación de las víctimas en los términos de la Ley 1448 de 2011, para lo cual participará en los Comités Territoriales de Justicia Transicional.
5. Implementar los mecanismos y estrategias para la efectiva participación de las víctimas, con enfoque diferencial, en el diseño de los planes, programas y proyectos de atención, asistencia y reparación.
6. Ejercer la Secretaría Técnica del Comité Ejecutivo para la Atención a las Víctimas.
7. Desarrollar estrategias en el manejo, acompañamiento, orientación, y seguimiento de las emergencias humanitarias y atentados según el artículo 168 de la Ley 1448 de 2011.
8. Implementar, de acuerdo con sus competencias, acciones para generar condiciones adecuadas de habitabilidad en caso de atentados terroristas donde las viviendas han sido afectadas, en coordinación con las entidades competentes.
9. Entregar la asistencia y ayuda humanitaria a las víctimas en los términos de los artículos 47, 64 y 65 de la Ley 1448 de 2011 y en las normas que la reglamenten.
10. Coordinar la creación, implementación y fortalecimiento de los Centros Regionales de Atención y Reparación y gerenciarlos en los términos de la Ley 1448 de 2011 y en las normas que la reglamenten.
11. Implementar acciones para brindar atención oportuna en la emergencia de los desplazamientos masivos.
12. Realizar esquemas especiales de acompañamiento y seguimiento a los hogares víctimas y contribuir su inclusión en los distintos programas sociales del Gobierno Nacional.
13. Coordinar los retornos y/o reubicaciones de las personas y familias que fueron víctimas de desplazamiento forzado, de acuerdo con lo dispuesto por el artículo 66 de la Ley 1448 de 2011 y en las normas que la modifiquen, adicionen o reglamenten.
14. Implementar el Programa de Reparación Colectiva en los términos de los artículos 151 y 152 de la Ley 1448 de 2011.
15. Apoyar la implementación de los mecanismos necesarios para la rehabilitación comunitaria y social de las víctimas.
16. Diseñar e implementar el programa de acompañamiento para promover una inversión adecuada de los recursos que reciba la víctima a título de indemnización administrativa.
17. Administrar el Fondo para la Reparación de las Víctimas y pagar las indemnizaciones judiciales ordenadas en el marco de la Ley 975 de 2005.
18. Operar la Red Nacional de Información para la Atención y Reparación a las Víctimas, incluyendo la interoperabilidad de los distintos sistemas de información para la atención y reparación a las víctimas.
19. Implementar y administrar el Registro Único de Víctimas, garantizando la integridad de la

 	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018	Página 13 de 127

información.

20. Las demás que le sean asignadas conforme a su naturaleza

5.1.1. MISIÓN DE LA UNIDAD PARA LAS VÍCTIMAS

Liderar acciones del Estado y la sociedad para atender y reparar integralmente a las víctimas contribuyendo a la inclusión social y la paz.

5.1.2. VISIÓN DE LA UNIDAD PARA LAS VÍCTIMAS

Al 2021, habremos logrado que las víctimas reparadas integralmente ejerzan su ciudadanía y aporten en la consolidación de la paz como resultado de la gestión efectiva y coordinada de la Unidad con los demás actores del Sistema

5.1.3. OBJETIVOS ESTRATÉGICOS DE LA UNIDAD

A continuación, se presentan los objetivos estratégicos de la Unidad:

- **OBJETIVO ESTRATÉGICO 1.**

Trabajar conjuntamente con las víctimas en el proceso de reparación integral para la reconstrucción y transformación de sus proyectos de vida.

- **OBJETIVO ESTRATÉGICO 2.**

Acercar el estado a las víctimas para brindarles una oferta pertinente, eficaz, sostenible y oportuna

- **OBJETIVO ESTRATÉGICO 3.**

Definir con las entidades territoriales la implementación de la Ley 1448/11, sus decretos reglamentarios y sus Decretos Ley

- **OBJETIVO ESTRATÉGICO 4.**

Vincular de manera activa la sociedad civil y a la comunidad internacional en los procesos de reparación integral de las víctimas del conflicto

- **OBJETIVO ESTRATÉGICO 5.**

Fortalecer la cultura de confianza colaboración e innovación para garantizar una atención digna, respetuosa y diferencial

5.1.4. ORGANIGRAMA DE LA ENTIDAD.

Corresponde a la estructura definida de conformidad con el Decreto 4802 de 2011.



Grafica 1. Organigrama de la UNIDAD PARA LAS VÍCTIMAS
Fuente: UNIDAD PARA LAS VÍCTIMAS

5.1.5. PLAN NACIONAL DE DESARROLLO

El Plan Nacional de Desarrollo “Todos por un Nuevo País” contempla tres (3) pilares: Paz, Equidad y Educación, los cuales se encuentran alineados a las estrategias transversales definidas en la Planeación Estratégica Sectorial desde el año 2016, permitiendo cumplir la misión, para atender a las víctimas, las personas y las instituciones beneficiarias de los programas del sector.

El Departamento Administrativo para la Prosperidad Social – DPS, antes Acción Social, cabeza del sector de la inclusión social al cual pertenece la Unidad, fue creado por el Gobierno Nacional mediante el decreto 415 de 2011 y tiene como función principal de formular, adoptar, dirigir, coordinar y ejecutar las políticas, planes generales, programas y proyectos para la superación de la pobreza, la inclusión social, la reconciliación, la recuperación de territorios, la atención a grupos

vulnerables, población en condición de discapacidad y la reintegración social y económica y la atención y reparación a víctimas de la violencia.

5.1.6. ESTRATEGIAS SECTORIALES

A continuación, se presentan los objetivos sectoriales y su alineación con las Estrategias definidas en el Plan Nacional de Desarrollo - PND “TODOS POR UN NUEVO PAÍS, PAZ, EQUIDAD y EDUCACIÓN”, posteriormente los diferentes compromisos misionales y funcionales.



Objetivo Sectorial 1	Objetivo Sectorial 2	Objetivo Sectorial 3	Objetivo Sectorial 4
Objetivo Sectorial 1 Generar condiciones para la integración y reconciliación comunitaria	Objetivo Sectorial 2 Reducir las brechas urbanorurales para la inclusión social	Objetivo Sectorial 3 Superar las brechas de acceso y permanencia a la educación para la población vulnerable	Objetivo Sectorial 4 Fortalecer la implementación de las políticas de desarrollo administrativo en el Sector
Estrategia A Reconocimiento y reparación integral a las víctimas de la violencia	Estrategia A Articulación territorial de la oferta social del Estado para población vulnerable	Estrategia A Armonizar y articular los instrumentos para la caracterización de la población y los territorios	Estrategia A Articulación sectorial en la prestación del servicio a la ciudadanía
Estrategia B Generación de condiciones en la población y territorios que permitan la reconciliación y la no repetición	Estrategia B Movilización de oferta privada y de cooperación internacional hacia los territorios focalizados	Estrategia B Articulación de la oferta del sector y la demanda de la población para superar las barreras de acceso y permanencia al derecho a la educación	Estrategia B Optimización de recursos en la implementación del programa de Gestión Documental
	Estrategia C Intervención conjunta del sector en las zonas con mayor incidencia de pobreza		Estrategia C Aprovechamiento de sinergias para cumplir las metas de gobierno en línea

Gráfica 2. Estrategias Sectoriales

Fuente: Plan Estratégico Sector de inclusión social y reconciliación 2018

COMPROMISOS MISIONALES Y FUNCIONALES DEL SECTOR

- Objetivos de Desarrollo Sostenible – ODS 2016-2030
- Plan Nacional de Desarrollo - PND
- Plan de Fortalecimiento y Plan de Acción de Víctimas
- Postconflicto y articulación con los PDET
- Documentos CONPES de política, territoriales, económicos y de contratos Plan/paz
- Compromisos con comunidad y pueblos indígenas
- Compromisos con Negritudes, Afrodescendientes, Raizales y Palenqueros
- Compromisos con el Pueblo ROM
- Compromisos presidenciales (Regiones, Consejos de Ministros)

 GOBIERNO DE COLOMBIA  UNIDAD PARA LAS VÍCTIMAS	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018

5.1.7. PLANES ESTRATÉGICOS INSTITUCIONALES

En relación con el Nivel Estratégico, la Unidad tiene como insumos y compromisos externos las directrices del Departamento Nacional de Planeación a través del Plan Nacional de Desarrollo, Ministerio de las Tecnologías y las Comunicaciones, CONPES e internamente cuenta con el Modelo Integrado de Planeación y Gestión - MIPG, el Sistema Integrado de Gestión – SIG, y el Plan Estratégico de Recursos Humanos. Con base en este marco de instrumentos formula los proyectos a ejecutar que conforman el Plan de Acción Anual y las inversiones necesarias para su ejecución conformando el Plan Anual de Adquisiciones, cuyo seguimiento y monitoreo se realiza mensualmente.

5.1.8. POLÍTICAS DE TI

El Decreto 1008 de 2018 dispone que las entidades están obligadas al cumplimiento de las políticas y lineamientos de la Estrategia de Gobierno en Línea ahora Gobierno Digital, entre ellos los relacionados Seguridad y Privacidad de la Información, en este sentido la UNIDAD PARA LAS VÍCTIMAS cuenta con la Resolución 740 de Noviembre de 2014 mediante la cual se adoptan las Políticas de Seguridad de la Información las cuales están en proceso de revisión y actualización con enfoques y actividades transversales a los componentes de TIC para Servicios, TIC para el Gobierno Abierto y TIC para la Gestión, tendientes a proteger la información y los sistemas de información, del acceso, divulgación, interrupción o destrucción no autorizada.

De otra parte, se adoptaron los lineamientos relacionados con el uso y control de los recursos tecnológicos como reglas de uso de servicios tecnológicos y responsabilidades acerca de los recursos de tecnología, pero no están debidamente formalizados y oficializados por la Unidad. Actualmente, se adelanta la proyección de las Políticas de TI que da cobertura a todos los recursos y operaciones de tecnología para su posterior oficialización y socialización.

5.2. USO Y APROPIACIÓN

5.2.1. CONTEXTO

La Oficina de Tecnologías de la Información construyó un plan de divulgación en 2014 y ha venido generando acciones de Uso y Apropiación de las Tecnologías, ejecutando actividades en procura de adoptar el modelo de Gestión de TI “IT4+” dentro de la Estrategia de Gobierno en Línea determinada por MINTIC, hoy Gobierno Digital, con el ánimo de fortalecer las habilidades de los colaboradores a través de la difusión del conocimiento y promoción del manejo de las herramientas tecnológicas disponibles en la Unidad.

Conforme la Unidad se ha robustecido tecnológicamente, en productos y servicios TI, se han aportado insumos para el apoyo a la gestión de los usuarios internos, en procura de un desempeño eficiente en la entidad. Se han realizado entregas funcionales, acompañadas de actividades de expectativa, sensibilización, divulgación, socialización y apropiaciones, mediante recursos de comunicación, presenciales y sitios web



Gráfica 3. Acceso a través SUMA
Fuente: OTI – Uso y Apropiación

En esta misma línea de divulgación y promoción, se han adelantado actividades de instrucción respecto al licenciamiento de software del que dispone la Unidad:

- Herramientas ofimáticas
- Herramientas colaborativas
- Office 365
- Herramientas de apoyo en el análisis de información: Power BI
- Herramientas para el respaldo de la información: Azure
- Mesa de Ayuda
- Aplicaciones en Producción
- Herramientas de Desarrollo o Apoyo Administrativo
- Sistemas de Información

Para este último ítem en fases de implementación de las herramientas de software que apalancan procesos misionales o de apoyo, se socializan los respectivos manuales de usuario y se realizan jornadas de capacitación sobre su uso y funcionamiento.

Se presenta una muestra de actividades de Uso y Apropiación en términos de sensibilización, divulgación, para la gestión del cambio



Gráfica 4. Actividades de transferencia UARIV
OTI – Uso y Apropiación

Las siguientes son fotografías de una muestra de actividades de transferencia de conocimiento, mediante sesiones de divulgación y promoción.



Grafica 5. Capacitación y Apropiación
OTI – Uso y Apropiación

La apropiación de los productos tecnológicos ha permitido soportar de una forma estable diferentes jornadas dirigidas hacia usuarios externos que impactan directamente el beneficio de las víctimas del conflicto, como son el Ministerio Público y colombianos en el exterior. Algunas de estas actividades son: Toma en línea, la cual consistió en la toma de la declaración que realizan los funcionarios del Ministerio Público y Consulado a través de la herramienta proporcionada por la Unidad para la Atención y Reparación Integral a las Víctimas, en dicho aplicativo se graba la información de las declaraciones rendidas por la población víctima, a través del Uso del computador con acceso a Internet y/o mediante una funcionalidad off- line suministrada por la Entidad. El funcionario del Ministerio Público y Consulado ingresa al sistema en línea, el Ministerio Público y Consulado imprimen la declaración con el fin de obtener las firmas de quienes participan.



Grafica 6. Capacitación y Divulgación OTI – Uso y Apropiación

Aunque se han adelantado acciones de uso y apropiación de TI, con actividades como expectativas, sensibilizaciones, divulgaciones, socialización, apropiaciones, entrega de insumos que apoyan la gestión, es necesario adelantar la caracterización de los interesados en el uso de las herramientas y servicios.

5.2.2. DIAGNOSTICO ACTUAL DE USO Y APROPIACIÓN – ENCUESTA A USUARIOS

Para el siguiente diagnóstico se ha diseñado y aplicado una encuesta a funcionarios y contratistas directos del orden nacional y territorial usuarios de las diferentes herramientas y sistemas disponibles en la entidad, con el fin de estimar el nivel de conocimiento y apropiación que se tiene en la Unidad sobre las tecnologías de la información y las comunicaciones.

• POBLACIÓN OBJETIVO

El instrumento se aplicó a tres grupos de población caracterizados o definidos por el rol jerárquico que ocupan:

- Nivel Estratégico: Grupo comprendido por los Directores y Subdirecciones de la Unidad

- Nivel Táctico: Grupo comprendido por los Coordinadores, Jefes y Líderes de Oficina
- Nivel Operativo: Grupo comprendido por los Usuarios finales que maneja el grande de las actividades del negocio.

• **APLICACIÓN DE ENCUESTA GENERAL**

La encuesta fue diligenciada por 613 personas, tanto funcionarios como contratistas y de todos los perfiles establecidos. Se obtuvieron los siguientes resultados:

Preguntas 1 y 2: Tipo de Vinculación (Funcionario-Contratista) y Perfil Profesional (Estratégico / Táctico / Operativo)



Convenciones:

Func. OPE: Funcionario con perfil Operativo Func. EST : Funcionario perfil Estratégico
 Func. TAC : Funcionario perfil Táctico
 Contrat. OPE : Contratista con perfil Operativo Contrat. TAC : Contratista perfil Táctico

Grafica 7. Resultados de la encuesta pregunta 1
 OTI – Uso y Apropiación

Como se puede observar en la gráfica, el 54% de la población encuestada corresponde a Contratistas (30% tácticos, 24% operativos), por lo cual podemos inferir que la muestra es representativa, pues los perfiles y tipos de contrato están equilibrados.

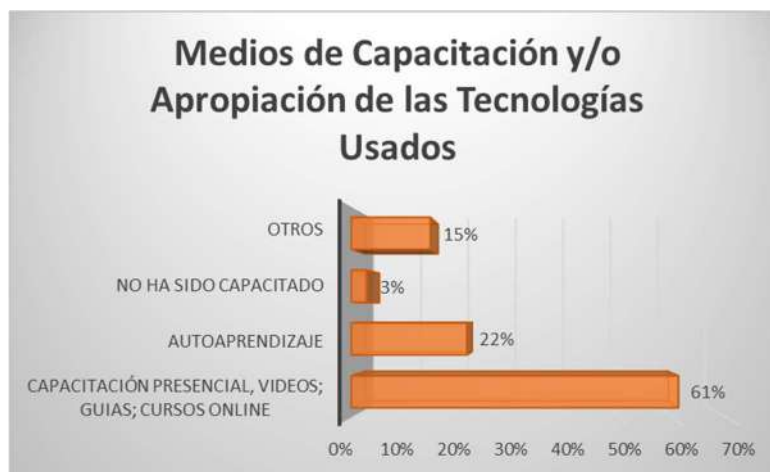
Pregunta 3: ¿Considera que las herramientas tecnológicas (Hardware y Software) suministradas por la Unidad le aportan al desarrollo de sus funciones a cabalidad?



Grafica 8. Resultados de la encuesta pregunta 3
OTI – Uso y Apropiación

En la gráfica encontramos: El 87% de la población encuestada considera que las herramientas suministradas por la Unidad son suficientes para cumplir con sus funciones a cabalidad, por lo tanto, la oferta de tecnología está bien enfocada, sin embargo, se debe profundizar en las necesidades específicas de ese 13% que no comparte la visión de la mayoría. Si bien la cifra es alta, la meta es que al menos el 95% de la población tenga las herramientas suficientes y necesarias para cumplir con sus funciones con la calidad, oportunidad y confiabilidad esperadas.

Pregunta 4: ¿Por cuáles medios se ha capacitado y/o apropiado de las tecnologías disponibles en la Unidad? Por favor indicar todas las que aplique



Grafica 9. Resultados de la encuesta pregunta 4
OTI – Uso y Apropiación

A pesar de que el 61% de la población encuestada manifiesta que ha sido capacitada, no se estableció exactamente que haya sido con programas implementados por la Oficina de Tecnologías. Sobre este ítem tenemos que profundizar en la problemática e implementar estrategias de capacitación más eficientes, debido a que también encontramos un 37% de la población que utiliza otros medios para el aprendizaje, cifra que nos enfrenta al gran reto de reenfoque, diversificar y masificar los programas de capacitación.

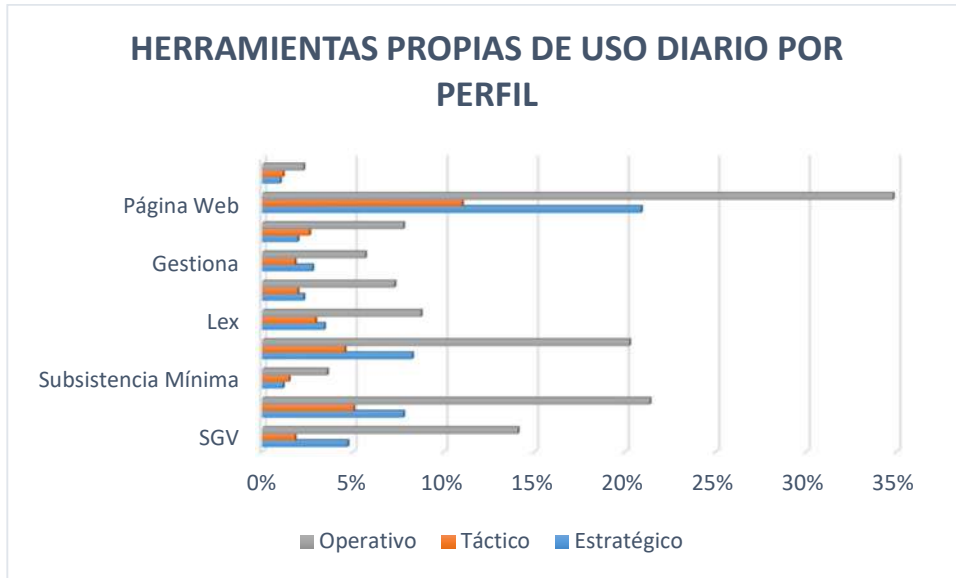
Pregunta 5: ¿Cuáles de las siguientes herramientas de Office 365 utiliza usted para el desempeño de sus funciones y con qué periodicidad aproximada?



Grafica 10. Resultados de la encuesta pregunta 5
OTI – Uso y Apropiación

Encontramos en promedio que el 50% de la población operativa encuestada usa a diario para el desarrollo de sus funciones, Outlook, Excel y Word, mientras que apenas el 17% de la población de perfil táctico las usa a diario. En cuanto al perfil estratégico, en promedio el 30% usa estas mismas herramientas a diario. Ahora bien, en cuanto al uso a diario Power Point, encontramos que sólo el 4% de la población táctica, el 6% de la estratégica y el 11% de la operativa. Al respecto se hace necesario indagar más acerca de las razones del poco uso de ésta última, con el fin de establecer acciones de mejora en el mediano plazo.

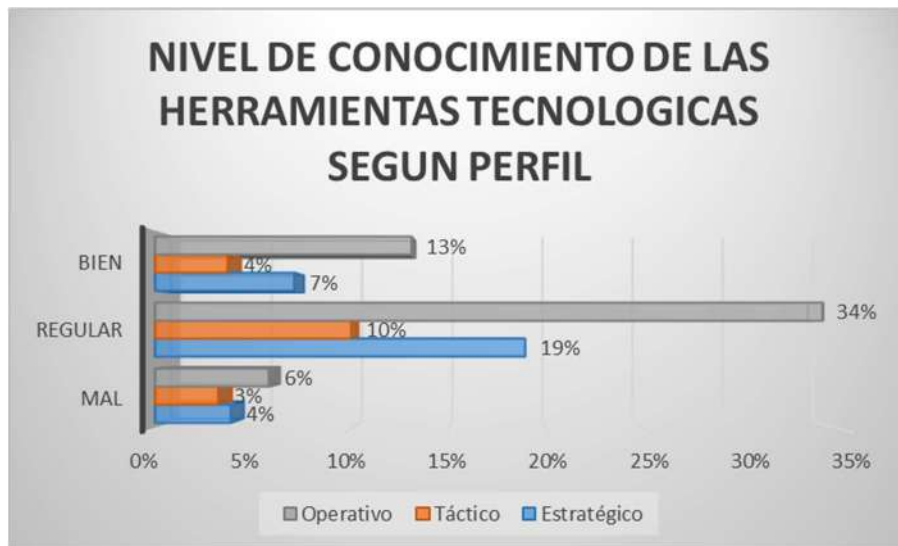
Pregunta 6: ¿Cuáles de los siguientes sistemas de información o aplicaciones conoce y con qué frecuencia los utiliza?



Grafica 11. Resultados de la encuesta pregunta 6 OTI – Uso y Apropiación

En cuanto a las herramientas propias, se observa que en todos los perfiles se usa con mayor frecuencia la Página Web y como veremos más adelante, a su vez lee informativo SUMA, lo que nos da una muy buena información sobre los canales de acceso a la información, esta fortaleza puede ser mejor aprovechada para llegar a todos los perfiles y optimizar de paso las estrategias.

Pregunta 7: De forma general, califique qué tanto conoce las herramientas tecnológicas con las que cuenta la Unidad (Sistemas de información institucionales, Aplicaciones ofimáticas, etc.), siendo 3 el mayor y 1 el menor.



Grafica 12. Resultados de la encuesta pregunta 7 OTI – Uso y Apropiación

Encontramos que apenas un 13% de la población operativa encuestada considera que tiene buen conocimiento de las herramientas, mientras que la población táctica y estratégica apenas tienen 4% y 7% respectivamente, por lo que se hace necesario fortalecer y reenfocar la estrategia de capacitación según los perfiles y la frecuencia de uso de las herramientas para el cumplimiento de las actividades propias de cada rol.

Pregunta 8: ¿Usted lee las divulgaciones y socializaciones tecnológicas publicadas en SUMA? como por ejemplo sobre Seguridad de la Información, gestión tecnológica y aplicaciones.



Grafica 13. Resultados de la encuesta pregunta 8
OTI – Uso y Apropiación

La población de nivel operativo es la que más lee SUMA, seguida por la estratégica que sumadas son el 84%, lo cual nos arroja una muy buena información acerca del uso de este canal.

Pregunta 9: ¿Ha recibido capacitaciones presenciales sobre productos tecnológicos como los Sistemas de Información institucionales, Seguridad de la Información, Office 365, Manejo de dotación tecnológica, etc.



Grafica 14. Resultados de la encuesta pregunta 9
OTI – Uso y Apropiación

En promedio el 63% de la población encuestada NO ha sido capacitada en el uso de las herramientas tecnológicas, puede deberse a la alta rotación de personal, especialmente los contratistas. Es una gran oportunidad de mejora.

Como se puede observar los encuestados afirman tener un conocimiento apropiado y suficiente sobre las herramientas y sistemas que utilizan para el desempeño de sus funciones y de otra se tiene un apropiado servicio de la mesa de soporte.

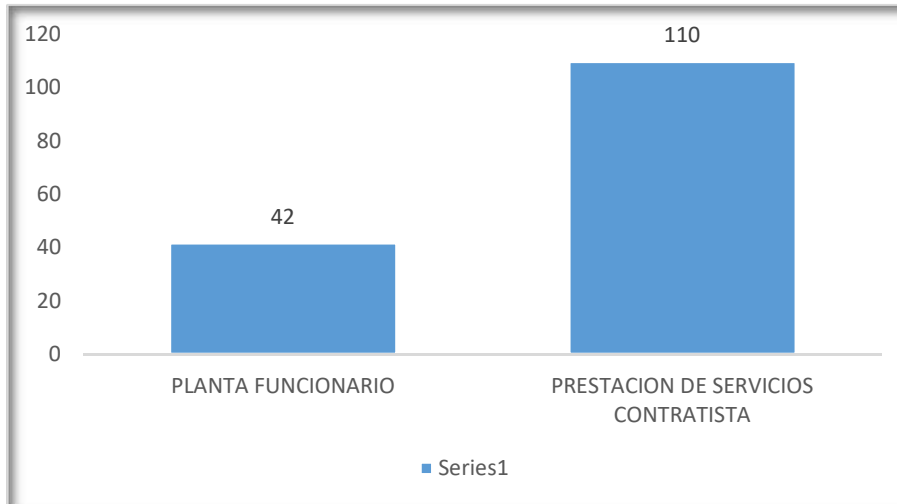
Sin embargo, al consolidar las respuestas a preguntas abiertas en donde el encuestado manifestó su opinión e interés, se tienen las siguientes conclusiones o necesidades:

- Mayor socialización en las funcionalidades de Office 365 que tiene contratada la Entidad.
- Divulgación presencial
- Multiplicar los esfuerzos en campañas de uso y apropiación de tecnologías
- Mayor participación en socializaciones a Direcciones Territoriales
- Unificar los sistemas de información
- Fortalecer el conocimiento en las herramientas Orfeo y el CRM

• **APLICACIÓN DE ENCUESTA ESPECÍFICA OFIMÁTICA**

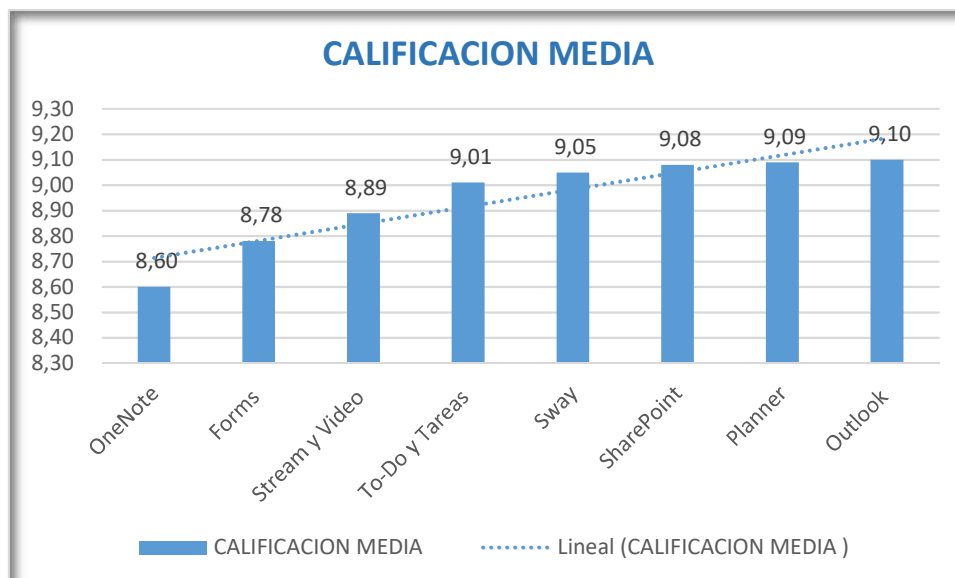
Encuesta aplicada a una población de 152 personas pertenecientes al personal de planta y contratistas de la Unidad, 42 funcionarios de planta y 110 contratistas.

Tema: OFFICE 365 en los servicios de OneDrive, Microsoft Teams, Yammer y Kaizala.



Grafica 15. Resultados de la encuesta Ofimática OTI – Uso y Apropiación

Respecto a las preguntas 3 a la 10, califique su nivel de interés respecto a una capacitación en las siguientes herramientas: SharePoint, OneNote, Sway, Outlook, Forms, Stream, Planner, To Do y Tareas siendo 10 el mayor y 1 el menor se obtuvo el siguiente resultado.



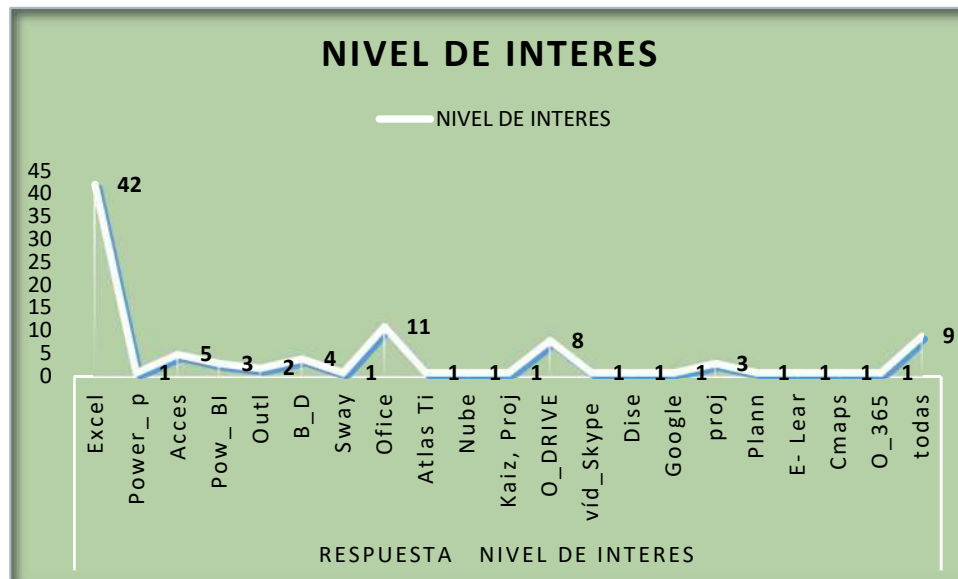
Grafica 16.

Resultados de la encuesta Interés en Capacitación OTI – Uso y Apropiación

En cuanto a la pregunta 11 ¿En cuáles otras herramientas tecnológicas considera que necesita

entrenamiento para el desempeño de sus actividades laborales?:

Excel, PowerPoint, Access, power BI, Outlook, Bases de Datos, Office, Atlas Ti, Nube, Kaizela, One Drive, Skype, Diseño, google, Project, Planner, E- Learning y Office 365, entre otras.



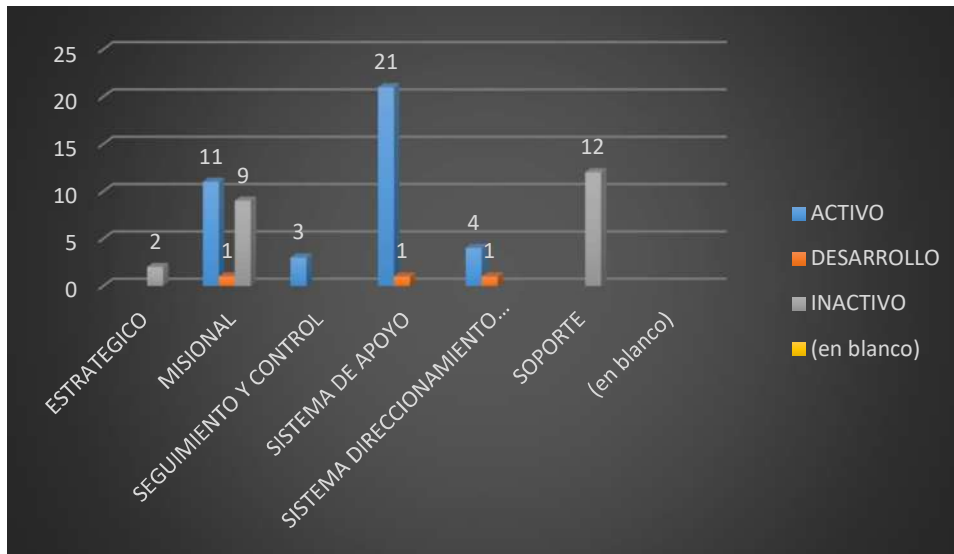
Grafica 17. Resultados de la encuesta Interés en Capacitación OTI – Uso y Apropiación

Como se puede observar los funcionarios de una parte tienen un conocimiento apropiado y suficiente sobre las herramientas y sistemas que utilizan para el desempeño de sus funciones y de otra se tiene un apropiado servicio de la mesa de soporte. Sin embargo, al consolidar las respuestas a preguntas abiertas en donde el encuestado manifestó su opinión e interés, se tienen las siguientes conclusiones o necesidades:

- Mayor divulgación y capacitación sobre fortalezas de Office 365 para
- Capacitación presencial
- Multiplicar los esfuerzos en campañas de uso y apropiación de tecnologías
- Mayor participación de socializaciones a Direcciones Territoriales
- Unificar los sistemas de información
- Capacitación de Orfeo para todos

5.3. SISTEMAS DE INFORMACIÓN

La entidad cuenta con 39 sistemas de información activos, según su ámbito de aplicación son clasificados en sistemas de soporte, sistemas misionales, sistemas estratégicos y sistemas de seguimiento y control, los procedimientos de formulación de requerimientos de desarrollo o mantenimiento para cada uno de ellos es liderado desde el punto de vista funcional por un área específica de la entidad y son implementados por equipos de ingenieros internos o proveedores externos.



Grafica 18. Sistemas de Información por Tipo de Proceso
OTI – Sistemas de Información

Los Sistemas de Información que se consideran de alta importancia o fundamentales son los siguientes:

- SISTEMA DE GESTIÓN PARA LAS VÍCTIMAS
- PORTAL VIVANTO
- MODELO SUBSISTENCIA MÍNIMA
- ORFEO
- LEX
- ACTOS ADMINISTRATIVOS - SUBSISTENCIA MÍNIMA
- RUV TEMPORAL
- INDEMNIZA - PAGO
- AHE
- ERP
- GESTIÓN DOCUMENTAL
- MAARIV

ANEXO – CATALOGO DE SISTEMAS DE INFORMACION

5.3.1. SISTEMAS DE INFORMACIÓN MISIONALES

Los sistemas de información se han construido y soportado en atención a los objetivos de cada área misiona y han sido caracterizados e incluidos en el Catálogo de Sistemas de información de la entidad, dicho documento se actualiza en forma permanentemente reflejando el estado del arte de los sistemas de información dando desarrollo al lineamiento LI.SIS.02 del ámbito de Planeación y gestión de los Sistemas de Información¹

Los sistemas de información de la Unidad han tenido diferentes orígenes, algunos fueron heredados de otras entidades, algunos fueron desarrollados a través de contratos con firmas desarrolladoras de software, otros desarrollados en forma por la Oficina de Tecnologías de la Información y otros desarrollados por las diferentes áreas misionales, ello hace que hoy conviva gran heterogeneidad de tecnologías, arquitecturas, lenguajes y plataformas sobre las cuales se realizan tareas de desarrollo y mantenimiento evolutivo.

Adicionalmente algunos aplicativos a manera de integración consumen la información contenida en el Modelo Integrado de Información creado por la Subdirección Red Nacional de Información, que es la instancia en la Unidad encargada de realizar el intercambio de información con otras entidades que conforman el SNARIV.

- **SERVICIOS WEB E INTEGRACIÓN**

La Unidad cuenta con un catálogo de servicios web caracterizados con la siguiente información:

- ✓ Nombre
- ✓ Descripción
- ✓ Sistemas de Información en los que ha implementado
- ✓ Dirección URL de alojamiento (Pública o Privada)
- ✓ Funcionario Responsable
- ✓ Métodos incorporados

En relación con la articulación de los servicios de información desarrollados por la OTI, existe un componente de consulta llamado Fuentes Externas cuyo objetivo es hacer un recorrido por diferentes aplicaciones claves que tienen datos de la víctima, para tomar la información necesaria que tiene cada sistema consultando por el número de identificación, de esta forma se busca la oportunidad y confiabilidad en la información, actualmente este componente es utilizado por los aplicativos (VIVANTO, SGV y LEX).

Además, como parte de las acciones de mejora para facilitar el intercambio de información se dispone de la herramienta BIZTALK mediante la cual se integrarán servicios web desarrollados por la OTI y por las otras áreas de la Unidad

¹ Catálogo de Sistemas de información, octubre de 2018

• **APLICATIVOS ADMINISTRATIVOS Y DE TALENTO HUMANO - ERP**

El término ERP se refiere a *Enterprise Resource Planning*, que significa “Sistema de Planificación de Recursos Empresariales”, es un conjunto de sistemas que permiten la integración de ciertas operaciones empresariales, como inventarios, nomina, contabilidad entre otros

La Unidad adquirió el licenciamiento del ERP para los siguientes módulos de gestión administrativa y talento humano:



- ✓ Nómina,
- ✓ Hojas de Vida,
- ✓ Carrera Administrativa,
- ✓ Viáticos,
- ✓ Salud Ocupacional,
- ✓ Bienestar Laboral
- ✓ Inventarios,
- ✓ Capacitación
- ✓ Portal Web de nómina

El licenciamiento se renueva cada año. Se cuenta con un contrato de mesa de soporte de nivel 1 y 2, en horario hábil.

El licenciamiento se ha estado renovando cada año y se tienen las siguientes versiones.

PRODUCTO	VERSION	ESTADO DE LA LICENCIA
SICOF.RRHH.Nomina	10.5.21	ACTIVA
SICOF.RRHH.Talento Humano	10.5.2.2	ACTIVA
SICOF.Administrativo.Compras e Inventarios	10.5.2.3	ACTIVA
SICOF.Viaticos	1.7	ACTIVA
SICOF.Portal del Empleado	1.0	ACTIVA
Apeon Application Server	3.0	ACTIVA

Grafica 19. Licenciamiento ERP
OTI – Sistemas de Información

 GOBIERNO DE COLOMBIA  UNIDAD PARA LAS VÍCTIMAS	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018
			Página 31 de 127

• SISTEMA DE INFORMACIÓN GEOGRÁFICA

La Unidad ha definido el procedimiento Sistema de Información Geográfica y cuenta con sistema de información geográfico ARCGIS, asegurando que los archivos de tipo geográfico que se comparten o solicitan, estén dentro del marco de interoperabilidad de Gobierno en Línea hoy Gobierno Digital, cumpliendo las disposiciones legales del MINTIC.

Algunas de las necesidades de información referentes a Sistemas de Información Geográfico:

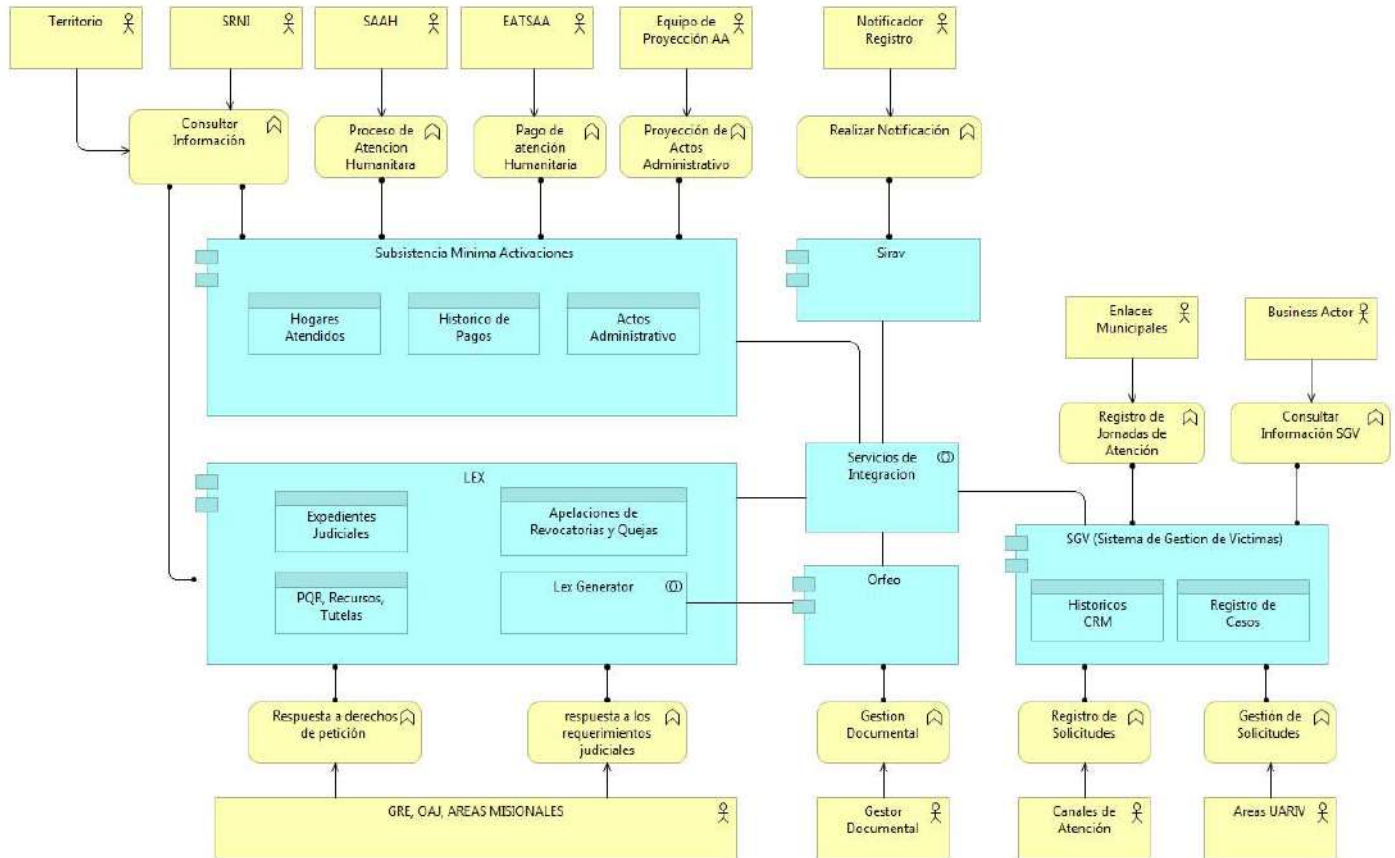
- Fondo de reparación de víctimas: Cartografía base de distintas escalas, información predial (R1 y R2) rural y urbano, cartas catastrales, Imágenes satelitales, fotografías aéreas.
- Subdirección de reparación colectiva: Cartografía base de distintas escalas, cartografía temática relacionada con dinámica del conflicto, características de población, aspectos ambientales y uso del suelo.
- Grupo de retornos y reubicaciones: Cartografía base de distintas escalas, información predial (R1 y R2) predial y urbano, cartografía temática relacionada con dinámica del conflicto, características de población, aspectos ambientales y uso del suelo.
- Subdirección prevención emergencias: Cartografía base de distintas escalas, cartografía temática relacionada con dinámica del conflicto, características de población, aspectos ambientales y uso del suelo, georreferenciación de información relacionada con la misión de la subdirección. Productos geoestadísticos
- Subdirección asistencia y atención: Cartografía temática con georreferenciación de información relacionada con la misión de la subdirección. Productos geoestadísticos
- Subdirección valoración y registro: Cartografía base de distintas escalas, información predial (R1 y R2) predial y urbano, cartografía temática relacionada con dinámica del conflicto, características de población, aspectos ambientales y uso del suelo
- Subdirección coordinación Nación – Territorio: Cartografía temática relacionada con georreferenciación de información relacionada con la misión de la subdirección.
- Subdirección general: Cartografía temática relacionada con georreferenciación de información relacionada con la misión de la subdirección. Productos geoestadísticos
- Dirección de Registro y Gestión de Información: Cartografía temática con georreferenciación de información relacionada con la misión de la subdirección.
- Grupo de Gestión de Talento Humano: Productos geoestadísticos.

5.3.2. ARQUITECTURA DE SISTEMAS DE INFORMACION

• ENFOQUE DE LA ARQUITECTURA

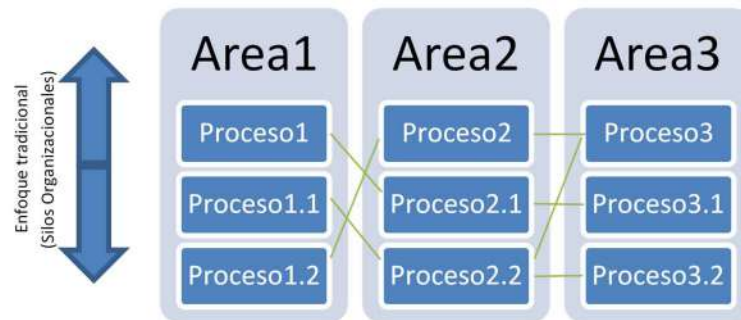
En general cada sistema de información posee su propia definición de arquitectura, ello debido a que se trata de sistemas que en muchas ocasiones fueron heredados a la Unidad por otras institucionalidades o que han sido fruto de la iniciativa aislada de los procesos internos La UNIDAD, dado que la entidad recoge información a través de diferentes canales de entrada que se han desarrollado de forma desarticulada y dada la alta demanda de solicitudes de atención para las víctimas

se cuenta con varias herramientas que se encargan de gestionar y producir nueva información para la operación diaria de la Entidad, adicionalmente la consolidación de la información se realiza en algunos casos mediante procesos no automatizados.



Gráfica 20 - Arquitectura Actual Sistemas Información
Fuente. OTI – Sistemas de Información

Hasta la fecha se han desarrollado aplicaciones con visión de proceso por lo que cada herramienta genera su propia información y por ende en ocasiones se tienen duplicadas entidades de información (personas, usuarios, geografías etc.) lo cual impacta la calidad de los indicadores y la consolidación de la información y requieren redundancia a nivel de infraestructura lo cual genera una carga adicional en la administración, mantenimiento, gobierno y costos de TI.



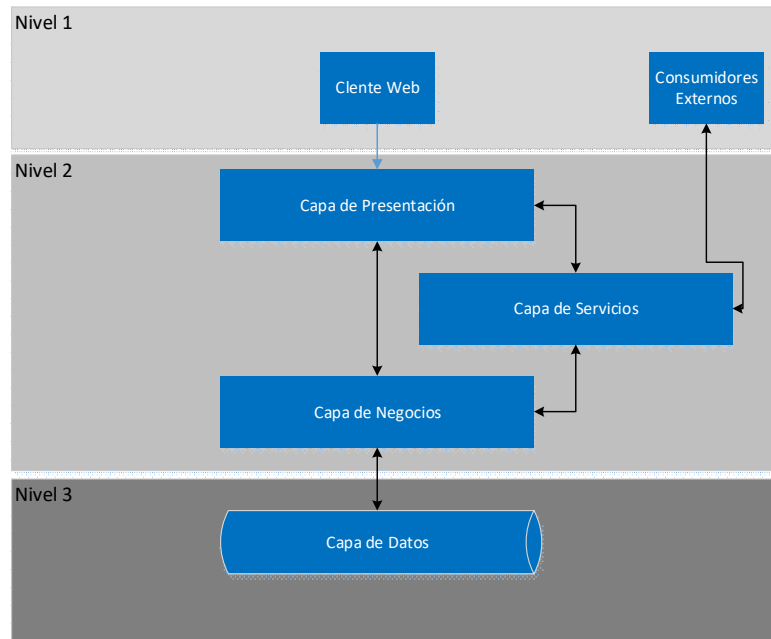
Gráfica 21. Enfoque de la Arquitectura tradicional – Silos Organizacionales
Fuente: Grupo de Sistemas de Información OTI - UNIDAD PARA LAS VÍCTIMAS

La existencia de sistemas por proceso ha dificultado además el intercambio de información dificultando la implementación de soluciones interoperables o únicas, sin embargo el intercambio de operación se logra de manera eficaz siendo necesario emprender acciones de mejora en atención a la necesidad de tener procesos más eficientes.

- **ARQUITECTURA ACTUAL DE APLICACIONES**

La Oficina de Tecnologías de la Información tiene la responsabilidad de apalancar los diferentes procesos presentes en las áreas misionales de la Unidad de Víctimas y por esta razón actualmente gestiona varios sistemas de información que han venido creciendo de forma desarticulada obteniendo como consecuencia un complicado flujo de información y que en el crecimiento organizacional con el tiempo ha venido reflejando pérdida de eficiencia.

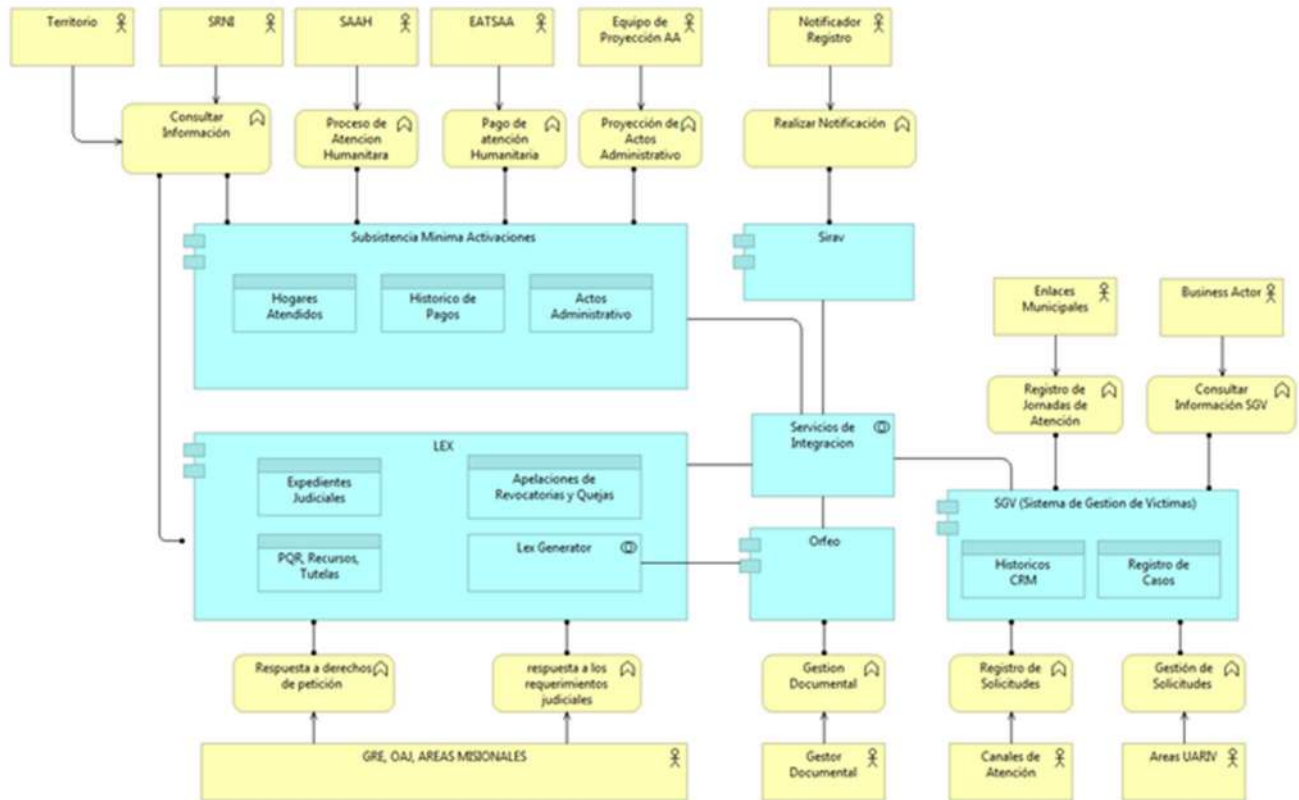
Las aplicaciones que actualmente gestiona la Oficina de Tecnologías de la información han sido diseñados y desarrollados en su mayoría bajo arquitectura N-Layer de tres (3) niveles



Gráfica 22. Diseño de Aplicaciones por Capas – Módulos Integrados

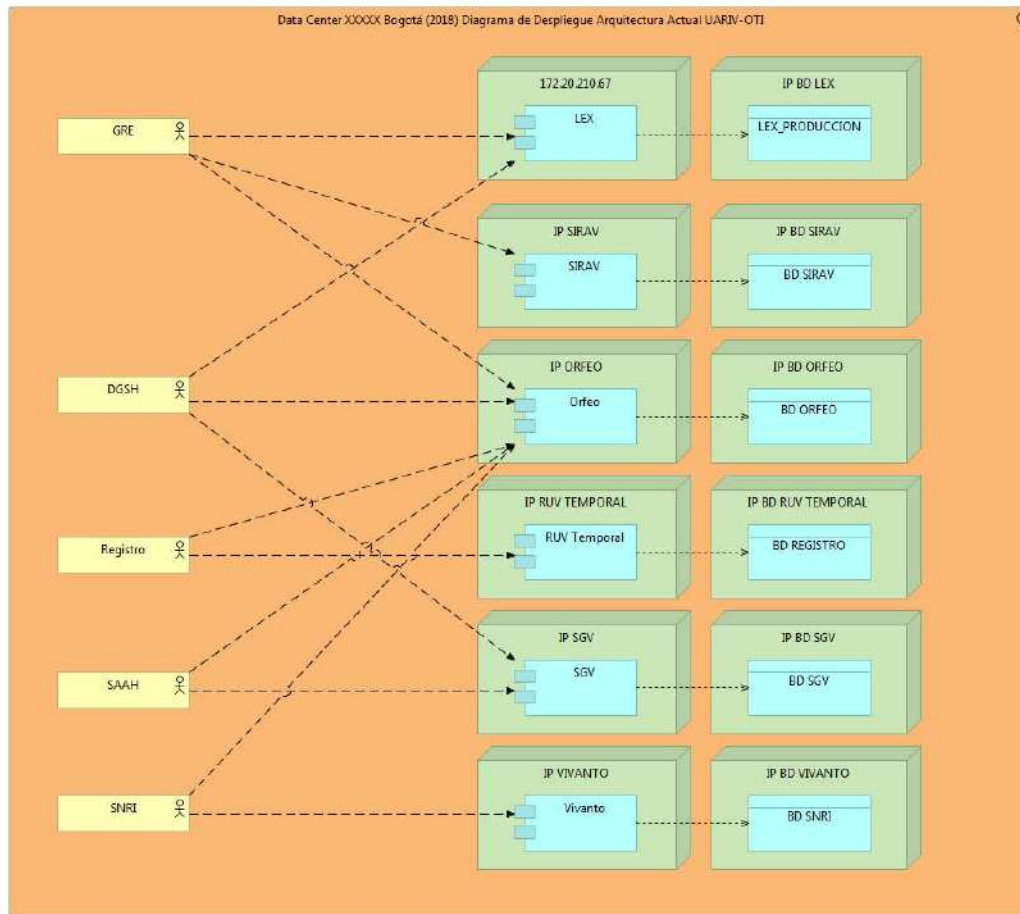
Fuente: Arquitectura AS-IS - Grupo de Sistemas de Información OTI - UNIDAD PARA LAS VÍCTIMAS

Actualmente los sistemas de información de la Unidad de Víctimas intercambian información a través de diferentes canales que se han desarrollado de forma desarticulada dada la alta demanda de solicitudes de atención para las víctimas contando con varias herramientas que se encargan de gestionar y producir nueva información para la operación diaria de la Unidad, adicionalmente la consolidación de la información se realiza mediante procesos manuales, ocasionando reprocesos y baja calidad. A continuación, el diagrama de Arquitectura Actual de los Sistemas de Información y el despliegue de la Arquitectura de Aplicaciones o Sistemas de Información



Gráfica 23 Arquitectura Actual de los Sistemas de Información

Fuente: Arquitectura de Referencia – Grupo de Sistemas de Información OTI



Gráfica 24. Arquitectura Despliegue de los Sistemas de Información

Fuente: Arquitectura de Referencia – Grupo de Sistemas de Información OTI - UNIDAD PARA LAS VÍCTIMAS

5.3.3. METODOLOGÍA DE DESARROLLO

Se ha definido un procedimiento en el Sistema Integrado de Gestión SIG para la implementación de soluciones llamado “**PROCEDIMIENTO DE DESARROLLO DE NUEVOS SISTEMAS DE INFORMACIÓN Y/O FUNCIONALIDADES EN SISTEMAS EXISTENTES**”, el cual tiene como alcance el diseño, desarrollo, pruebas y puesta en producción de herramientas tecnológicas.

Como metodología de desarrollo e implementación de proyectos de Sistemas de Información se viene trabajando en SCRUM (metodología de desarrollo ágil), de otra parte la administración del ciclo de vida de las aplicaciones y sus artefactos se realiza a través de plataforma Microsoft Team Foundation Server – TFS, que es un producto de Microsoft para la administración de código fuente, generación de informes, gestión de requisitos, administración de proyectos entre otros.

- **SOPORTE A LOS SISTEMAS DE INFORMACIÓN**



Se cuenta con el procedimiento **“SOPORTE A SISTEMAS DE INFORMACIÓN Y APLICACIONES”** respaldado por el SIG, cuyo alcance es la recepción de incidentes y requerimientos generados por usuarios, el diagnóstico de los mismos, las pruebas de requerirse, la documentación y la publicación de los ajustes sobre Sistemas de Información.

5.3.4. ANÁLISIS GENERAL DE LOS SISTEMAS DE INFORMACIÓN

La Oficina de Tecnologías de la Información tiene la responsabilidad de proveer a los diferentes procesos presentes en las áreas de la Unidad de Víctimas los sistemas de información adecuados para la gestión de sus tareas, se observa que los sistemas de información existentes ofrecen las facilidades para mantener la operación diaria de la Entidad y que las labores de mantenimiento sobre los sistemas permiten ofrecer mejoras en la automatización de procesos y ofrecer información entre procesos a través de servicios, con lo que se facilita la gestión y se mitiga la ausencia de información.

A pesar de lo anterior, existen opciones es necesario continuar los esfuerzos al interior de la Entidad y de la Oficina de Tecnologías de la información en pro de alinear los diferentes escenarios y equipos de desarrollo a un esquema unificado y estandarizado de operación, en la creación y mantenimiento de sistemas de información aún no se evidencia un gobierno efectivo sobre quienes deben realizar este tipo de tareas.

Se hace necesaria la definición de una arquitectura empresarial que motive la estructuración de los sistemas y soluciones informáticas con una visión empresarial y no solo de proceso, su ausencia dificulta identificar o alinear con claridad los diferentes componentes de las soluciones de sistemas y de información de la Unidad, y dificulta la adopción de modelos o metodologías apropiadas para el registro, procesamiento y entrega de resultados a los diferentes grupos de interés tanto internos como externos, lógicamente e hace necesario implementar u oficializar políticas, estándares y lineamientos haciéndolos extensivos a todos los equipos de trabajo que participan en la construcción de los sistemas de información..

 	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018
			Página 38 de 127

5.4. SERVICIOS TECNOLÓGICOS

La Unidad cuenta con líneas y servicios que dan cobertura para la atención del usuario final, todo mediante la adopción de tecnologías redundantes y en alta disponibilidad, soporte y Acuerdos de Nivel de Servicios - ANS definidos, los cuales permiten el soporte, la operación y administración de la infraestructura, los sistemas de información, servicios de intercambio, entre otros, todo bajo la experticia de la OTI.

Actualmente se cuentan con los siguientes procedimientos:

- Procedimiento Acceso Remoto a Servidores y Bases de Datos V1
- Procedimiento Creación de Usuarios en Sistemas de Información V1
- Procedimiento creación, modificación actualización y eliminación de buzones de correo institucional
- Procedimiento Dotación Tecnología Nueva Sede, Traslado de Sede y/o Adicionales V1
- Procedimiento Gestión de préstamo de Discos duros cifrados V1
- Procedimiento Gestión de Solicitudes de Dotación Tecnológica V1
- Procedimiento Solicitud de Servicios de Telefonía IP V1
- Procedimiento Soporte a Sistemas de Información y Aplicaciones V1
- Procedimiento Soporte Técnico a la Infraestructura Tecnológica V1
- Procedimiento Validación de Infraestructura e Inventario V1
- Procedimiento Creación de usuarios en sistemas de información V1
- Procedimiento Gestión de incidentes de seguridad de la información V2

5.4.1. ESTRATEGIA Y GOBIERNO

La gestión de los servicios tecnológicos se realiza de manera centralizada considerando los siguientes servicios y coberturas:

1. Dotación Tecnológica.

La OTI ofrece un servicio de dotación tecnológica con una cobertura nivel en modalidad de servicios por demanda. La Dotación tecnológica se conforma de una infraestructura TI dispuesta en cada sede y/o oficina de la unidad ofreciendo herramientas TI, equipos de cómputo, equipos de impresión y escáner, periféricos, cableado estructurado, centros de cableado, servicio integral de video conferencia todo con mantenimientos correctivos y preventivos

Para la entrega de un equipo, instalación e implementación de un puesto de trabajo o servicio de dotación tecnológica se sigue el procedimiento “Control de Solicitud de Dotación Tecnológica” el cual se gestiona a partir de una solicitud vía correo electrónico del jefe el área solicitante a la OTI o a la mesa de servicios el alcance real del servicio.

La dotación existente a la fecha es la siguiente:

SERVICIO DE DOTACIÓN TECNOLÓGICA								
LÍNEA DE SERVICIO	2012	2013	2014	2015	2016	2017	2018 a oct	TENDENCIA
PCS Y PORTATILES	440	1546	1986	2301	2384	2474	2647	
IMPRESORAS Y ESCANERS	56	160	201	224	237	261	267	
OFICINAS	20	31	36	40	40	42	39	

Tabla 2. Dotación Tecnológica
Fuente OTI – Servicios Tecnológicos

2. Soporte a Aplicaciones (Sistemas de Información, Aplicaciones)

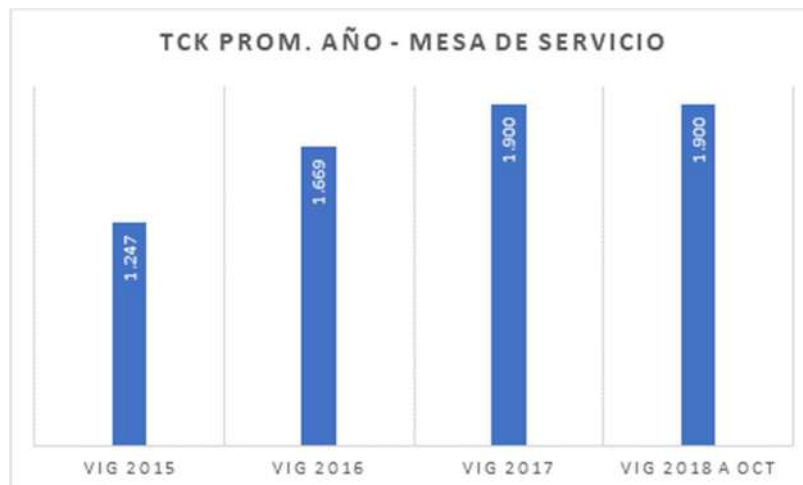
Este servicio va dirigido a garantizar el soporte técnico a incidentes y requerimientos de los sistemas información gobernados por la OTI y entregados a esta línea de servicio los cuales se asocian al recurso especializado de 2do y 3er nivel, dispuesto por la Unidad.

El procedimiento consiste en recibir una solicitud a través de la mesa de servicios (Nivel 1 – Mesa de servicios), clasificar la categoría correspondiente y escalar a través de un esquema multinivel al grupo Nivel 2- Soporte App. Este grupo se encarga de dar solución a la incidencia si se encuentra en su alcance o escalar a un nivel superior de ser necesario, correspondiente al grupo Nivel 3 – Desarrollo o infraestructura.

Se presta soporte a los Sistemas de Información que se encuentran en producción y en un nivel de madurez, desde la mesa de servicios centralizada, algunos de los sistemas son: Actos administrativos, Astrea, Auxilios funerarios, Buzón judicial, Comr, Lex, Orfeo, Subsistencia mínima, Vivanto y SGV entre otros.

3. Mesa de Servicios.

Es la primera instancia de atención a incidentes y requerimientos técnicos de los usuarios de la Unidad, estas solicitudes pueden corresponder a cualquiera de las líneas de servicios tecnológicos, es decir relacionadas con la dotación tecnológica, con el funcionamiento u operación de los sistemas de información, con la infraestructura, canales, conectividad y telefonía. Existe una mesa de servicios para todo el país con centro de operación en Bogotá la cual esta contratada en modalidad de servicio.



Grafica 25 Promedio mensual solicitudes tramitadas en la Mesa de servicios
Fuente OTI – Servicios Tecnológicos

Para la atención de las solicitudes y requerimiento se tiene dispuesto el siguiente esquema de atención de usuario final, la Mesa de Servicios de la Unidad, recibe las diferentes solicitudes de soporte a través de llamada al #5, a través de correos electrónicos enviados al buzón soporte.oti@unidadvictimas.gov.co o del link web

<http://unidaddevictimas.comware.com.co/uSDKV8/#/login>.

La Mesa de servicios realiza el diagnóstico inicial de las solicitudes, siendo esta el primer nivel de atención, se ejecutan acciones básicas de verificación; si la situación no fue solucionada, la mesa de servicios transfiere los casos al segundo nivel de soporte en sitio o soporte infraestructura. El horario de atención de la mesa de servicios es de lunes a viernes de 7:30 am a 7 pm.

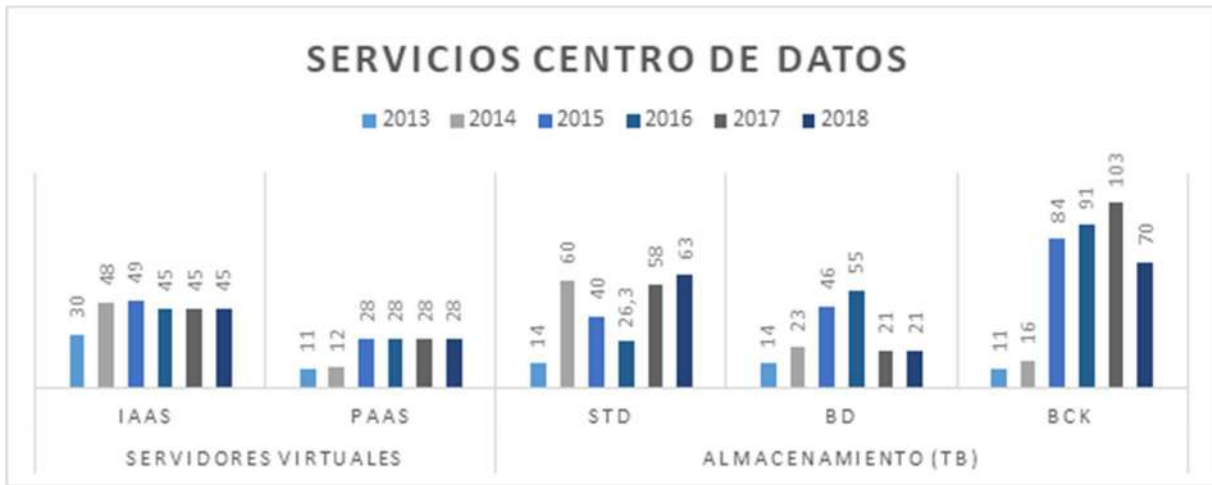
Para todas las solicitudes de soporte bien sea de dotación tecnológica, soporte en sitio o soporte de aplicaciones se lleva un registro en la herramienta de gestión (ARANDA) mediante la generación de un ticket por cada caso a solucionar, con él se realiza el seguimiento a todas las solicitudes informándole al solicitante el estado de su caso hasta la solución, momento en el cual se da el cierre del respectivo ticket con el diligenciamiento de la encuesta de satisfacción, esta encuesta permite medir el nivel de satisfacción de los usuarios.

4. Soporte en sitio:

Técnicos o tecnólogos funcionarios o contratistas de la Unidad que atienden servicios técnicos de segundo nivel directamente en las sedes de Bogotá y Medellín. Cuando el servicio es escalado y pertenece a una sede territorial el técnico de soporte en sitio se conecta remotamente a resolver el incidente o requerimiento asignado, si la solicitud es de hardware el caso es escalado a los proveedores quienes atienden y dan solución en cada sede de acuerdo a los ANS establecidos y si el servicio es de infraestructura se escala a este equipo.

5. Servicio de cómputo por demanda:

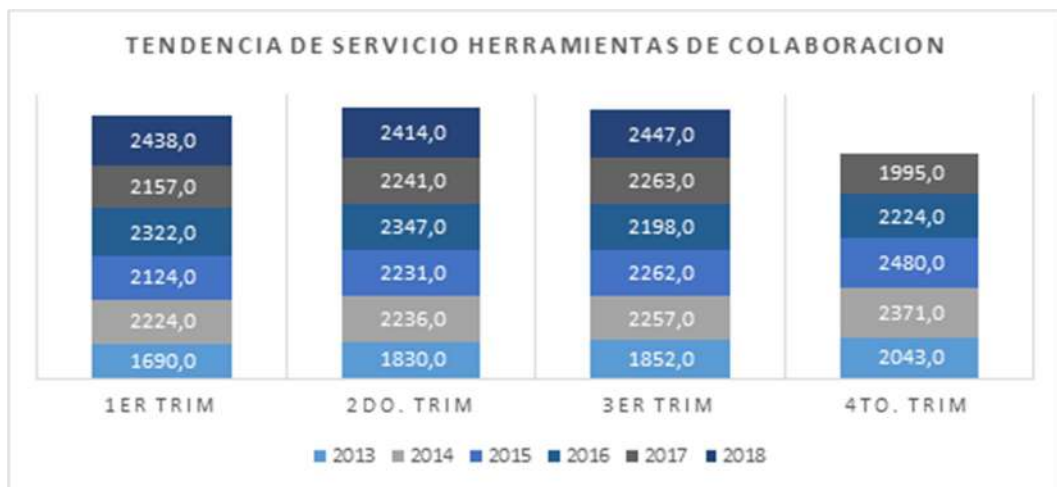
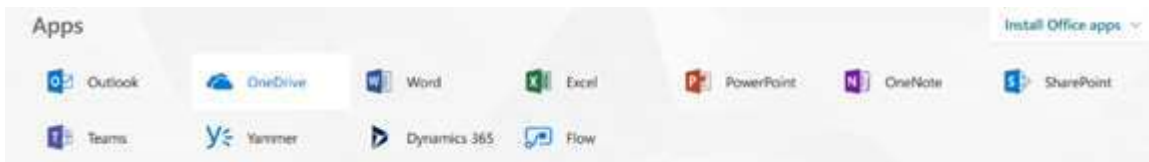
La Oficina de Tecnologías de la Información de la Unidad, brinda servicios de infraestructura virtual centralizada de cobertura nacional en la nube, bajo un esquema de cómputo por demanda, a través un servicio de Centro de Datos y servicio herramientas de colaboración. Dichos servicios son tercerizados, a través de Acuerdos Marco de precios, este servicio adquirido permite alojar, procesar, custodiar, disponer y asegurar los sistemas de Información estratégicos, misionales y apoyo, así como bases de datos e información para el registro, atención y reparación integral a las víctimas de la Unidad.



Gráfica 26. Servicios de Computo por Demanda
Fuente OTI – Servicios Tecnológicos

6. Herramientas Colaborativas

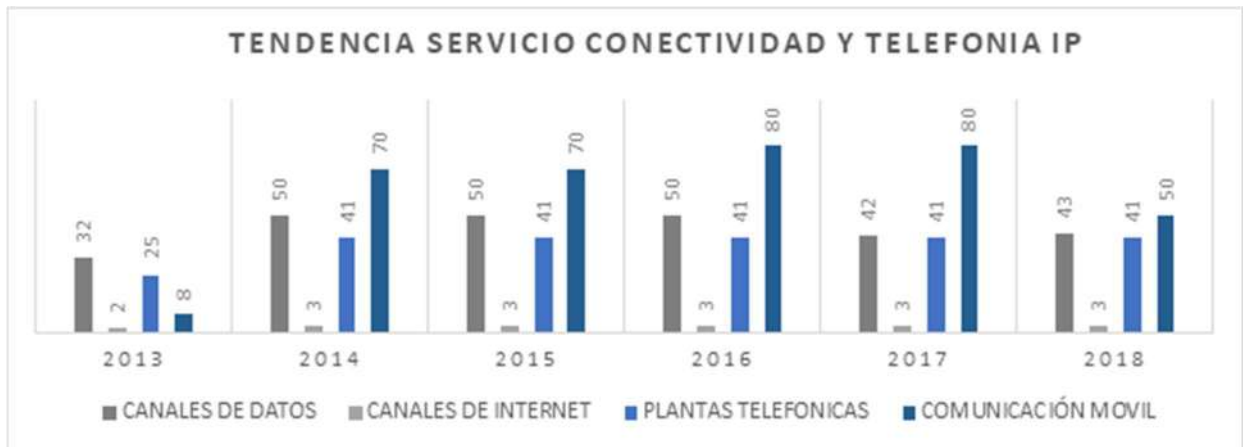
Servicio tercerizado a través de Acuerdos Marco de Precios servicios Microsoft, bajo plataforma unificada y acceso vía Web. Permitiendo entregar a la Unidad servicio de correo, Skype, almacenamiento por usuario, en un esquema de servicio por demanda. Las siguientes ilustraciones presentan las aplicaciones que la componen y la tendencia en la capacidad.



Gráfica 27. Tendencia de la capacidad de herramientas colaborativas
Fuente OTI – Servicios Tecnológicos

7. Servicios de conectividad y telefonía:

La OTI, a través de estos servicios interconecta las oficinas y el centro de datos de la Unidad, por medio de canales dedicados e internet, de forma tercerizada, centralizada y con una cobertura nacional a través de Acuerdos Marco de Precios. En cuanto los servicios de telefonía se brinda comunicación por medio de Telefonía Voz IP. A continuación, se presenta los servicios consolidados por vigencia.



Gráfica 28. Tendencia de los servicios de conectividad y telefonía

Fuente OTI – Servicios Tecnológicos

5.4.2. BUENAS PRACTICAS DE SOPORTE Y ACUERDOS DE SERVICIO

Toda la operación de soporte a los servicios tecnológicos tiende a ser sobre plataformas web, correo electrónico y en el marco de los lineamientos de buenas prácticas ITIL, de esta forma se contribuye a garantizar el mejoramiento continuo de todos los servicios. El proveedor de mesa de servicios dispuso de un grupo de expertos ITIL, para acompañar el diseño e implementación de los árboles de decisiones basada en prioridades y tiempo estimados de solución para atender los casos y solicitudes.

De otra parte, se han definido ANS con todos los actores en el proceso de soporte, es decir, proveedores, agentes de soporte en cada nivel, especialistas de aplicaciones y solicitantes, logrando así una importante cobertura hasta llegar a los operadores de procesos misionales que pueden llegar de 300 a 400 usuarios cada uno (call center). Se cuenta con acuerdos de niveles de servicio – ANS para los siguientes servicios tecnológicos:

- Servicio de Conectividad. ANS_AMP Conectividad II
- Servicio de Centro de Datos. ANS_AMP Nube Privada II
- Servicio de telefonía
- ERP – Sistema de Información
- Soporte a Aplicaciones

- Proveedores de equipos
- Soporte en sitio

5.4.3. INVENTARIO DE RECURSOS TECNOLÓGICOS

La Unidad cuenta con dos tipos de inventario, el que es propiedad de la Unidad que en su mayoría se encuentra en almacén y el que es suministrado en calidad de arrendamiento por diferentes proveedores como por ejemplo la dotación tecnológica. Para el control de los pc y portátiles en modalidad de arrendamiento se utiliza un gestor de inventario (Aranda) y el servicio @Remote Ricoh para control de impresoras y tóner, otro insumo para el inventario es la visita física que se realiza durante la ejecución de los mantenimientos preventivos y correctivos, otra forma es a través de correos a las Direcciones Territoriales o a las dependencias recordando la responsabilidad que tienen sobre el recurso asignado al área, todo ello conforma el procedimiento “Validación de la Infraestructura de Inventario Tecnológico”, que permite identificar el usuario responsable y los recursos asignados a cada uno.

5.4.4. IMPRESIÓN.

De acuerdo con los análisis de capacidad y necesidad, se cuenta con equipos multifuncionales en cada sede de la Unidad para ser compartidos por un número determinado de usuarios, quienes a través de una contraseña acceden al servicio y su administración es realizada por el soporte de infraestructura de la OTI. Se cuenta con el servicio de la aplicación @Remote de Ricoh para control de impresoras, hojas impresas, otra revisión es con las visitas a las sedes durante los mantenimientos preventivos y correctivos.

5.4.5. MANTENIMIENTO PREVENTIVO Y CORRECTIVO

Dentro del contrato con el proveedor de la Línea de Servicio Dotación Tecnológica están incluidos los mantenimientos preventivos y correctivos a la infraestructura contratada. Se realizan dos mantenimientos preventivos en todo el país, los cuales se programan en dos momentos del año, mayo/junio y noviembre/diciembre, cuya verificación y control es realizada por la Unidad en relación con el personal que el proveedor utiliza y los permisos de acceso a las diferentes sedes y recursos.

5.4.6. CONTROL DE ACCESO.

Se cuenta con control de acceso a las aplicaciones, servicios y componentes de la infraestructura de hardware y software, a través de módulos de seguridad en sistemas de información y mediante el uso del directorio activo existente en donde están las cuentas de usuario y contraseñas de todos los funcionarios, existe un solo directorio activo con copias en varios servidores en forma de réplica cuando se actualiza por la creación, modificación o eliminación de la información de un usuario, de otra parte a través del directorio activo se gestionan las políticas de seguridad en

computadores, claves fuertes, vigencia de claves, uso de contraseñas históricas, fondos de pantalla, bloqueo de sesiones no permitidas, etc.

5.4.7. INDICADORES DE GESTIÓN.

Mensualmente se generan indicadores sobre los servicios de soporte suministrados y el seguimiento al cumplimiento de los niveles de servicio ANS, esto incluye proveedores externos y usuarios internos de las áreas y aplicados a las diferentes modalidades de dotación tecnológica y soporte a aplicaciones; se recopilan las evidencias de cumplimiento y se determina el nivel de satisfacción del usuario final. Como control se informa a cada línea de servicio (sistemas de información, infraestructura, dotación tecnológica, etc.) el estado de los casos abiertos con el fin de solicitar su solución y cerramiento.

5.4.8. ESTRUCTURA ORGÁNICA – SERVICIOS TECNOLÓGICOS

Por cada servicio en operación se cuenta con un equipo de ingenieros y técnicos especializados en las diferentes áreas de la informática, los cuales garantizan la prestación del servicio la organización se muestra a continuación:



Gráfica 29. Diagrama del Equipo de Soporte Técnico
Fuente: Grupo de Servicios Tecnológicos OTI - UNIDAD PARA LAS VÍCTIMAS

ANEXO – CATALOGO DE SERVICIOS DE TI

5.4.9. INFRAESTRUCTURA

La Unidad cuenta con la infraestructura tecnológica en modalidad de servicio que permite soportar, administrar, alojar, procesar, custodiar y disponer de la información a nivel nacional y para soportar los sistemas de información y bases de datos en sus diferentes ambientes (desarrollo, pruebas y producción). Esta infraestructura es suministrada a través de un Acuerdo Marco de Precios por medio de una orden de compra específica compuesta por siguientes componentes:

- Infraestructura como Servicio – Servidores Virtuales – IaaS
 - Software como Servicio – SaaS
 - Sistemas de almacenamiento – SAN
 - Seguridad
 - Copias de respaldo
 - Otros servicios
- **SERVIDORES VIRTUALES**

Corresponde a los servidores y software para la operación de los sistemas de información (misionales, estratégicos y de apoyo), así como los servicios de red, unidades de almacenamiento de información y dispositivos de backup. Se tiene un total de 73 servidores, con la siguiente categorización:

Hardware	Descripción	Cantidad
TIPO DE SERVIDORES	USO BÁSICO	2
	USO INTERMEDIO	70
	USO ESTÁNDAR	1

Tabla 3. Inventario de Servidores por Tipo

Fuente. OTI – Servicios Tecnológicos

A continuación, la matriz detallada de servidores con identificación del servidor, aplicaciones residentes, tipo de servidor, tipo de procesador, memoria RAM y almacenamiento SAN optimizado y de alto rendimiento

IDENTIFICACION	APLICACIONES	TIPO DE SERVIDOR	Core	RAM	SAN AR	SAN OP	
162572	IFX01	DIRECTORIO ACTIVO PRIMARIO	Servidor Uso Basico	8	8		
162571	IFX02	DIRECTORIO ACTIVO SECUNDARIO	Servidor Uso Basico	8	8		
162580	TM52000005	RUV. ADMIN RUV	Servidor Uso intermedio	16	32		2300
162790	TM520200006	AHI. INDEMNIZA. POR. RUV TEMPORAL. SGI. SERVICIOS. SGS	Servidor Uso intermedio	16	32		800
162574	TM520200007	SIPOD - SIV - SIRA	Servidor Uso intermedio	16	32	700	500
162791	TM520200008	CONSULTA RUAJ. LIQUIDADOR. SIPOD2. WEBSERVICE	Servidor Uso intermedio	16	32		
162794	TM520200009	ORFEO	Servidor Uso intermedio	16	32		10340
162795	TM520200010	AHI. AHTRANSICION. ASTREA. BOTONAHE. GIC. ORA.	Servidor Uso intermedio	16	32		2600
162578	TM502200150	PAGINA WEB. RNI	Servidor Uso intermedio	16	32		200
162796	TM520200012	SIPOD - ADMIN SIPOD	Servidor Uso intermedio	16	24		400
162797	TM502200013	RELAY CORREO	Servidor Uso intermedio	16	24		100
162798	TM512200014	SERVIDOR DE ARCHIVOS Y FTP	Servidor Uso intermedio	16	24	200	7500
162769	TM512200015	ATENCION - AUDITORIA	Servidor Uso intermedio	24	36	1500	1200
162575	TM502200021	AHE. BIOCOTROL. INDICADORES PAT. LIQUIDADOR.	Servidor Uso intermedio	24	32	300	300
162799	TM520200026	APLICACIONES SUBSISTENCIA MINIMA. ERP	Servidor Uso intermedio	16	32		50
162800	TM501200034	SIV - SIRA	Servidor Uso intermedio	16	32		100
162770	TM200035	RUV BD	Servidor Uso intermedio	24	36	250	300
162801	TM501200037	ARCGIS SERVER	Servidor Uso intermedio	16	32		40
162802	TM520200038	ORFEO PRUEBAS. OTROS	Servidor Uso intermedio	16	32		350
162786	TM501200039	ACEDOC	Servidor Uso intermedio	16	24		2090
162787	TM508200011	INTRANET. TIERRAS. BIBLIOTECA. PARTICIPACION	Servidor Uso intermedio	16	32		40
162803	TM502200047	SGV APLICACION	Servidor Uso intermedio	16	32		2700
162576	TM502200048	SGV BASE DATOS	Servidor Uso intermedio	24	32	700	200
162771	TM502200052	BD DE DATOS PRUEBAS SIV. SIPOD. ORFEO. OAI. RUV. RNI.	Servidor Uso intermedio	24	32	2100	800
162780	TM502200064	INDEMNIZA (BD). EXPEDIENTE DIGITAL	Servidor Uso intermedio	24	32	500	1930
162781	TM502200065	MAARIV. FORMULARIO. SIGO. SIGESTION. OTRAS	Servidor Uso intermedio	24	32	800	1310
162804	TM502200066	SERVICIOS RNI. CAPTURADOR DINAMICO. TURNOS. MOVIL	Servidor Uso intermedio	16	24		150
162805	TM502200067	LEX	Servidor Uso intermedio	16	32		4600
162782	TM502200068	INDEMNIZA. MAARIV. PARI. CARACTERIZACION.	Servidor Uso intermedio	24	36	800	500
162806	TM502200069	VIVANTO V2.0 IN HOUSE	Servidor Uso intermedio	16	24		40
162807	TM500200072	VIVANTO DEFINITIVO	Servidor Uso intermedio	16	24		
162783	TM502200073	CRM - VIVANTO	Servidor Uso intermedio	16	24		
162579	TM502200076	POWER CENTER & DATA QUALITY	Servidor Uso Estandar	6	24		250
162573	TM502200077	BD ORACLE - FUENTES RNI	Servidor Uso intermedio	24	32	1300	750
162808	TM501200086	BANCO DE COSTOS. CHAT RNI. FORO RNI. POSI. MANTIS	Servidor Uso intermedio	16	24		40
162809	TM502200087	CRM OA RNI	Servidor Uso intermedio	16	24		20
162810	TM502200102	BPM PRUEBAS	Servidor Uso intermedio	16	24		
162811	TM502200103	SEDE ELECTRONICA PRUEBAS	Servidor Uso intermedio	16	24		
162812	TM502200104	DIGITALIZACION. GDOCWS. ESIGNA DIGITAL	Servidor Uso intermedio	16	24		20
162813	TM502200105	ALFRESCO PRUEBAS	Servidor Uso intermedio	16	24		20
162788	TM502200107	ALFRESCO PRODUCCION	Servidor Uso intermedio	16	24		500
162814	TM502200108	PARI 1 - BPM BALANCEO	Servidor Uso intermedio	16	32		
162815	TM502200109	SEDE ELECTRONICA	Servidor Uso intermedio	16	32		
162772	TM502200110	BD RNI STAGE. RNI DWH. RNI MEDICIONES	Servidor Uso intermedio	16	24		1350
162816	TM502200111	INVENTARIO FUENTES. SOLICITUD USR. CRUCES MASIVOS.	Servidor Uso intermedio	16	24		120
162817	TM502200113	DIGITALIZACION. GDOCWS. ESIGNA DIGITAL	Servidor Uso intermedio	16	32		
162818	TM502200119	CRM RNI	Servidor Uso intermedio	16	24		
162819	TM502200120	SHAREPOINT CRM RNI	Servidor Uso intermedio	16	24		
162820	TM502200128	PARI 2 - BPM BALANCEO	Servidor Uso intermedio	16	32		
162821	TM502200129	PARI 3 - BPM BALANCEO	Servidor Uso intermedio	16	32		
162822	TM502200130	PARI 4 - BPM BALANCEO	Servidor Uso intermedio	16	32		
162581	TM000135	CARACTERIZACION BD RNI	Servidor Uso intermedio	24	32	3000	1050
162773	TM520200137	MEDICION SUBSISTENCIA MINIMA	Servidor Uso intermedio	16	32	1000	700
162789	TM518200002	MOODLE - ENTIDAD CERTIFICADORA	Servidor Uso intermedio	16	24		100
162823	TM502200151	FQUTRAC	Servidor Uso intermedio	16	24		300
162824	TM520200152	ERV. SUBSISTENCIA MINIMA	Servidor Uso intermedio	16	24		350
162825	TM502200154	SIRAV	Servidor Uso intermedio	16	32		1500
162784	TM502200173	CRM. VIVANTO	Servidor Uso intermedio	24	24	200	250
162774	TM502200195	UNIDAD (RNI CRUCE. RNI CARACT. RNI GIC)	Servidor Uso intermedio	24	32	600	300
162832	TM502210197	VIVANTO V2.0 IN HOUSE (RNI - ADMON USR. RNI PAQ.	Servidor Uso intermedio	24	32	400	300
162775	TM502200198	LEX	Servidor Uso intermedio	32	32	350	300
162833	TM502200199	ORFEO	Servidor Uso intermedio	24	32	200	200
162776	TM502200200	BD PAARI Y SIG	Servidor Uso intermedio	32	64	2700	1000
162777	TM520200201	BD ERP. MCONSOLIDADO. PAARI. OTRAS	Servidor Uso intermedio	24	32	1400	400
162778	TM502200202	ERP. PCT. ASTREA. MAPA PROYECTOS. OTRAS	Servidor Uso intermedio	24	32	300	400
162785	TM502200203	BD VIVANTO DEFINITIVO	Servidor Uso intermedio	24	32		
162826	TM502200204	INFORMATION BUILDER (RNI)	Servidor Uso intermedio	16	24		300
162827	TM502200205	ACTOS ADMINISTRATIVOS	Servidor Uso intermedio	16	32		0
162828	TM520200207	NUOVA INTRANET	Servidor Uso intermedio	16	32		
162829	TM520200208	ACTOS ADMINISTRATIVOS. ASISTENCIA FUNERARIA.	Servidor Uso intermedio	16	32		
162830	TM520200209	GESTION DOCUMENTAL	Servidor Uso intermedio	16	32		
162577	TM520200210	REPORTING SERVICE APP	Servidor Uso intermedio	16	32	0	300
162831	TM502200063	VIVANTO APP	Servidor Uso intermedio	16	32		200
TOTALES				1294	2132	19300	52460

Gráfica 30. Inventario de Servidores de Centro de Datos

Fuente: Grupo de Infraestructura OTI

- **CENTRO DE DATOS – SOFTWARE**

Corresponde al sistema operativo, bases de datos y herramientas de desarrollo residentes en cada servidor:

Software	Cantidad
Windows Server 2008	34
Windows Server 2012	38
Windows Server 2008	1
Bases de Datos ORACLE	10 versión 11g
Bases de Datos SQLSERVER	- 1 / 2008 - 7 / 2012 - 1 / 2016

Tabla 4. Inventario de Servidores de Centro de Datos
Fuente: Grupo de Infraestructura OTI

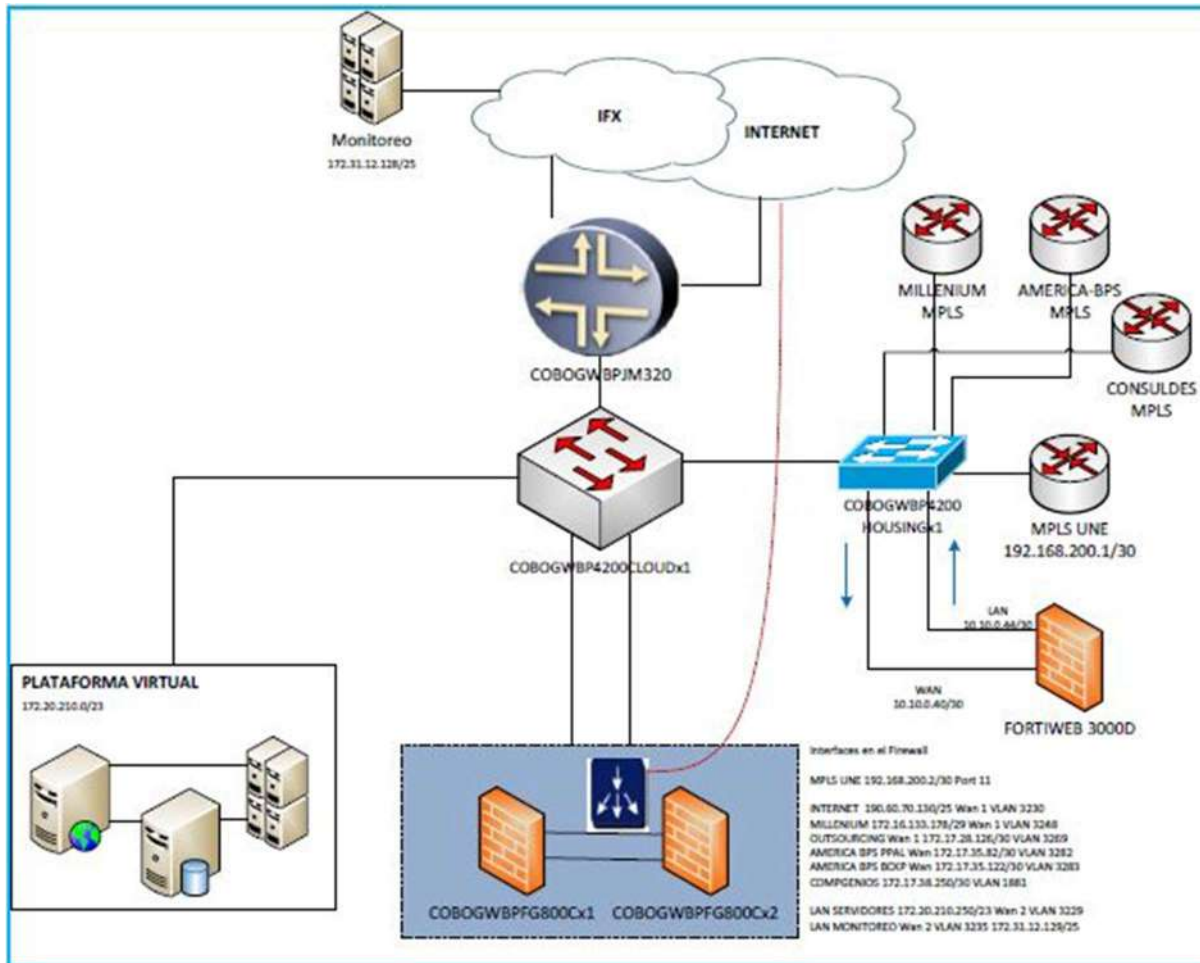
- **SISTEMAS DE ALMACENAMIENTO SAN.**

Se cuenta con una cantidad disponible aproximada de 81 TERAS distribuidas así:

- ALTO RENDIMIENTO 20.9 TERAS para bases de datos
- OPTIMIZADO 60.23 TERAS demás servicios

- **SEGURIDAD PERIMETRAL.**

A continuación el esquema de seguridad perimetral y elementos



Grafica 31. Esquema de red

Fuente: Grupo de Infraestructura OTI - UNIDAD PARA LAS VÍCTIMAS

- **COPIAS DE RESPALDO.**

Este servicio hace parte del contrato con el proveedor de centro de datos, las copias se realizan diariamente en modalidad de full diario con retención de cinco días y una copia de seguridad (base de datos) total mensual para guardar en centro de custodia. El software para copias y recuperación es VEEAM.

- **MONITOREO A LA INFRAESTRUCTURA**

Con el objeto de garantizar la operación y mantenimiento a la infraestructura tecnológica, se

utiliza el software de monitoreo Orión – SOLAR WIN que permite monitorear el estado de los servidores en cuanto a procesamiento, uso de memoria, almacenamiento en disco y canales de internet. Se ejecuta permanentemente para verificar el cumplimiento de los acuerdos de niveles de servicio generando el respectivo reporte de seguimiento.

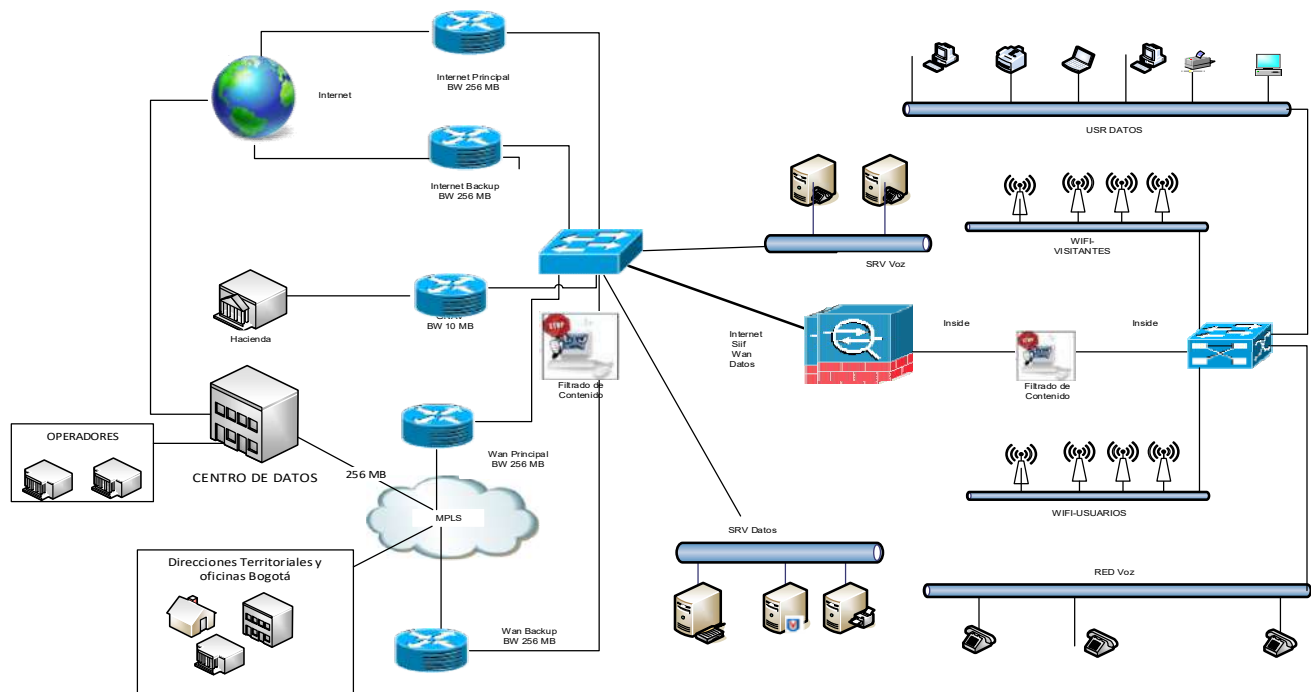
5.4.10. CONECTIVIDAD

La conectividad a distancia está basada en una red privada de comunicaciones MPLS mediante la cual se accede desde cualquiera de las sedes de la Unidad en el país, a las diferentes aplicaciones que se encuentran alojadas en los servidores del centro de datos.

Para la conectividad local cada sede o centro regional de la Unidad cuenta con un centro de cableado y una red local que conecta todos los computadores que se encuentran en operación.

Este esquema de comunicaciones y conectividad se gestiona mediante un Acuerdo Marco de Precios, en donde se definen y aplican los respectivos acuerdos de niveles de servicio – ANS, para garantizar la disponibilidad. La continuidad de la operación es responsabilidad del proveedor de comunicaciones. El cableado estructurado de la red LAN es categoría 6 A, cumpliendo con los estándares requeridos

A continuación, una ilustración de la topología de conectividad de la Unidad.



Grafica 32. Seguridad Perimetral

Fuente: Grupo de Infraestructura OTI – UNIDAD PARA LAS VÍCTIMAS

- **CANALES DE TELECOMUNICACIONES**

La Unidad dispone de un canal de Internet dedicado de 320 MB de ancho de banda con una solución de alta disponibilidad. Así mismo cuenta con una red WAN que permite la implementación de los servicios con que cuenta la Unidad.

Se cuenta con dos categorías de servicios contratados a través de Colombia Compra Eficiente

- Oro para sedes Bogotá
- Bronce para sedes de unidades territoriales

A continuación, la tabla de canales de comunicaciones (internet, MPLS) con capacidades asignadas por regional.

No	Código del servicio	Producto	Cantidad	Sede	Conexión	DEPARTAMENTO
3	IT-C-CT-2-76	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 1 - Nivel de servicio plata - Alta - NA - NA - BW: 10 Mbns - NA - Mes - CANTIDAD: 1	1	GNAP	GNAP	BOGOTA
4	IT-C-CT-2-132	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 1 - Nivel de servicio oro - Alta - NA - NA - BW: 256 Mbns - NA - Mes - CANTIDAD: 1	1	Avianca	MPLS BOGOTA	BOGOTA
5	IT-C-CT-2-132	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 1 - Nivel de servicio oro - Alta - NA - NA - BW: 256 Mbns - NA - Mes - CANTIDAD: 1	1	Centro de Datos	MPLS BOGOTA	BOGOTA
6	IT-C-CT-2-130	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 1 - Nivel de servicio oro - Alta - NA - NA - BW: 64 Mbns - NA - Mes - CANTIDAD: 1	1	Bavaria	MPLS BOGOTA	BOGOTA
7	IT-C-CT-2-131	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 1 - Nivel de servicio oro - Alta - NA - NA - BW: 128 Mbns - NA - Mes - CANTIDAD: 1	1	Afinsa	MPLS BOGOTA	BOGOTA
8	IT-C-CT-2-130	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 1 - Nivel de servicio oro - Alta - NA - NA - BW: 64 Mbns - NA - Mes - CANTIDAD: 1	1	Calle Real piso 9	MPLS BOGOTA	BOGOTA
9	IT-C-CT-2-128	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 1 - Nivel de servicio oro - Alta - NA - NA - BW: 40 Mbns - NA - Mes - CANTIDAD: 1	1	Fontibon	MPLS BOGOTA	BOGOTA
12	IT-C-CT-2-128	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 1 - Nivel de servicio oro - Alta - NA - NA - BW: 40 Mbns - NA - Mes - CANTIDAD: 1	1	Operador Registro	MPLS Operador	BOGOTA
13	IT-C-CT-2-128	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 1 - Nivel de servicio oro - Alta - NA - NA - BW: 40 Mbns - NA - Mes - CANTIDAD: 1	1	Operador - Cali CENTER	MPLS Operador	BOGOTA
14	IT-C-CT-2-38	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 1 - Nivel de servicio bronce - Alta - NA - NA - BW: 64 Mbns - NA - Mes - CANTIDAD: 1	1	Medellin	MPLS REGIONALES	ANTIOQUIA
15	IT-C-CT-2-33	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 1 - Nivel de servicio bronce - Alta - NA - NA - BW: 20 Mbns - NA - Mes - CANTIDAD: 1	1	Bogota	MPLS REGIONALES	REGIONALES
16	IT-C-CT-2-36	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 1 - Nivel de servicio bronce - Alta - NA - NA - BW: 40 Mbns - NA - Mes - CANTIDAD: 1	1	Cali	MPLS REGIONALES	VALLE
17	IT-C-CT-1-30	Enlaces de Conectividad Terrestre - Enlaces Dedicados a Internet - Región 1 - Nivel de servicio bronce - Alta - NA - NA - BW: 10 Mbns - NA - Mes - CANTIDAD: 1	1	Bucaramanga	INTERNET	SANTANDER
18	IT-C-CT-2-168	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 2 - Nivel de servicio bronce - Alta - NA - NA - BW: 10 Mbns - NA - Mes - CANTIDAD: 1	1	Pasto	MPLS REGIONALES	NARIÑO
19	IT-C-CT-2-30	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 1 - Nivel de servicio bronce - Alta - NA - NA - BW: 10 Mbns - NA - Mes - CANTIDAD: 1	1	Pereira	MPLS REGIONALES	RISARALDA
20	IT-C-CT-2-168	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 2 - Nivel de servicio bronce - Alta - NA - NA - BW: 10 Mbns - NA - Mes - CANTIDAD: 1	1	Popayan	MPLS REGIONALES	NARIÑO
21	IT-C-CT-2-30	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 1 - Nivel de servicio bronce - Alta - NA - NA - BW: 10 Mbns - NA - Mes - CANTIDAD: 1	1	C/gena	MPLS REGIONALES	BOGOTA
22	IT-C-CT-2-30	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 1 - Nivel de servicio bronce - Alta - NA - NA - BW: 10 Mbns - NA - Mes - CANTIDAD: 1	1	Santa Martha	MPLS REGIONALES	REGIONALES
23	IT-C-CT-2-30	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 1 - Nivel de servicio bronce - Alta - NA - NA - BW: 10 Mbns - NA - Mes - CANTIDAD: 1	1	Villavicencio	MPLS REGIONALES	META
24	IT-C-CT-2-30	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 1 - Nivel de servicio bronce - Alta - NA - NA - BW: 10 Mbns - NA - Mes - CANTIDAD: 1	1	B/quilla	MPLS REGIONALES	ATLANTICO
25	IT-C-CT-2-30	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 1 - Nivel de servicio bronce - Alta - NA - NA - BW: 10 Mbns - NA - Mes - CANTIDAD: 1	1	Valledupar	MPLS REGIONALES	CESAR
26	IT-C-CT-2-30	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 1 - Nivel de servicio bronce - Alta - NA - NA - BW: 10 Mbns - NA - Mes - CANTIDAD: 1	1	Monteria	MPLS REGIONALES	CORDOBA
27	IT-C-CT-2-168	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 2 - Nivel de servicio bronce - Alta - NA - NA - BW: 10 Mbns - NA - Mes - CANTIDAD: 1	1	Cúcuta	MPLS REGIONALES	NORTE DE SANTANDE
28	IT-C-CT-2-168	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 2 - Nivel de servicio bronce - Alta - NA - NA - BW: 10 Mbns - NA - Mes - CANTIDAD: 1	1	Quibdó	MPLS REGIONALES	CHOCO
29	IT-C-CT-2-168	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 2 - Nivel de servicio bronce - Alta - NA - NA - BW: 10 Mbns - NA - Mes - CANTIDAD: 1	1	Florencia	MPLS REGIONALES	CAQUETA
30	IT-C-CT-2-30	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 1 - Nivel de servicio bronce - Alta - NA - NA - BW: 10 Mbns - NA - Mes - CANTIDAD: 1	1	Barrancabermeja	MPLS REGIONALES	SANTANDE
31	IT-C-CT-2-168	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 2 - Nivel de servicio bronce - Alta - NA - NA - BW: 10 Mbns - NA - Mes - CANTIDAD: 1	1	Sincelejo	MPLS REGIONALES	SUCRE
32	IT-C-CT-2-309	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 3 - Nivel de servicio bronce - Alta - NA - NA - BW: 20 Mbns - NA - Mes - CANTIDAD: 1	1	Apartado	MPLS REGIONALES	ANTIOQUIA
33	IT-C-CT-2-30	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 1 - Nivel de servicio bronce - Alta - NA - NA - BW: 10 Mbns - NA - Mes - CANTIDAD: 1	1	Ibagué	MPLS REGIONALES	HUILA
34	IT-C-CT-2-30	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 1 - Nivel de servicio bronce - Alta - NA - NA - BW: 10 Mbns - NA - Mes - CANTIDAD: 1	1	Neiva	MPLS REGIONALES	HUILA
35	IT-C-CT-2-30	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 1 - Nivel de servicio bronce - Alta - NA - NA - BW: 10 Mbns - NA - Mes - CANTIDAD: 1	1	Manizales	MPLS REGIONALES	CALDAS
36	IT-C-CT-2-30	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 1 - Nivel de servicio bronce - Alta - NA - NA - BW: 10 Mbns - NA - Mes - CANTIDAD: 1	1	Yopal	MPLS REGIONALES	CASANARE
37	IT-C-CT-2-168	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 2 - Nivel de servicio bronce - Alta - NA - NA - BW: 10 Mbns - NA - Mes - CANTIDAD: 1	1	Riohacha	MPLS REGIONALES	GUAJIRA
38	IT-C-CT-2-306	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 3 - Nivel de servicio bronce - Alta - NA - NA - BW: 10 Mbns - NA - Mes - CANTIDAD: 1	1	Armenia	MPLS REGIONALES	QUINDIO
39	IT-C-CT-2-30	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 1 - Nivel de servicio bronce - Alta - NA - NA - BW: 10 Mbns - NA - Mes - CANTIDAD: 1	1	Tunja	MPLS REGIONALES	BOYACA
40	IT-C-CT-2-303	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 3 - Nivel de servicio bronce - Alta - NA - NA - BW: 4 Mbns - NA - Mes - CANTIDAD: 1	1	Mocoa	MPLS REGIONALES	PUTUMAYO
41	IT-C-CT-2-303	Enlaces de Conectividad Terrestre - Enlaces Dedicados entre Puntos - Región 3 - Nivel de servicio bronce - Alta - NA - NA - BW: 4 Mbns - NA - Mes - CANTIDAD: 1	1	Arauca	MPLS REGIONALES	ARAUCA
42	IT-C-CS-2-153	Enlaces de Conectividad Satelital - Enlace a Internet Satelital VSAT - Región 4 - Nivel de servicio bronce - NA - BW: 6 Mbns - BW: 3 Mbns - Re-uso: 1:4 - NA - Mes - CANTIDAD: 1	1	Puerto Carreño	MPLS REGIONALES	VICHADA
43	IT-C-CS-2-153	Enlaces de Conectividad Satelital - Enlace a Internet Satelital VSAT - Región 4 - Nivel de servicio bronce - NA - BW: 6 Mbns - BW: 3 Mbns - Re-uso: 1:4 - NA - Mes - CANTIDAD: 1	1	San José del Guaviare	MPLS REGIONALES	GUAVIARE
44	IT-C-CS-2-111	Enlaces de Conectividad Satelital - Enlace a Internet Satelital VSAT - Región 3 - Nivel de servicio bronce - NA - BW: 6 Mbns - BW: 3 Mbns - Re-uso: 1:4 - NA - Mes - CANTIDAD: 1	1	Vaupes	MPLS REGIONALES	VAUPES
45	IT-C-CS-2-153	Enlaces de Conectividad Satelital - Enlace a Internet Satelital VSAT - Región 4 - Nivel de servicio bronce - NA - BW: 6 Mbns - BW: 3 Mbns - Re-uso: 1:4 - NA - Mes - CANTIDAD: 1	1	Puerto Inirida	MPLS REGIONALES	GUAINIA
47	IT-C-CT-10-3	Enlaces de Conectividad Terrestre - Traslado de Enlace Fuera del Perímetro de la Entidad - Región 1 - Nivel de servicio oro - NA - NA - NA - NA - Enlace - CANTIDAD: 2	2			BOGOTA
48	IT-C-CT-4-125	Enlaces de Conectividad Terrestre - Ampliación Definitiva de Enlace Terrestre - Región 2 - Nivel de servicio oro - NA - NA - NA - BW: 64 Mbns - NA - Mes - CANTIDAD: 2	2			BOGOTA
49	IT-C-SC-02-1	Servicios Complementarios - Experto Senior: Redes - Comunicaciones - Región 1 - Nivel de Servicio Complementario - NA - NA - NA - NA - Hora - CANTIDAD: 500	500		FR-GDO-0007	BOGOTA

5.4.11. SERVICIOS DE OPERACIÓN

La Unidad para su operación cuenta con los siguientes servicios y/o recursos:

- **CORREO ELECTRÓNICO**

La Unidad utiliza el servicio de correo electrónico a través del producto de Microsoft Office 365, el cual se administra a través del esquema de directorio activo dentro del grupo de herramientas colaborativas.

- **TELEFONÍA**

Se cuenta con infraestructura y equipos tecnológicos que constituyen el sistema de telefonía de la entidad, dicho sistema permite las comunicaciones entre las diferentes dependencias y direcciones regionales. La red está conformada por telefonía análoga en regionales para llamadas locales y digital e IP a través de la cual se presta el servicio a través de la red MPLS para la comunicación entre sedes, se tienen 1139 extensiones. El sistema de telefonía central está compuesto servidor de telefonía SIEMENS en un nodo principal de referencia OpenScape Voice Simplex, con centrales de supervivencia en las sedes territoriales de referencia OpenScape Branch y teléfonos de referencia OpenStage

Ítem	Denominación Unidad de Víctimas	Sede	Teléfonos Registrados en OSB
1	Dirección Territorial Urabá	Apartadó	8
2	Dirección Territorial Arauca	Arauca	10
3	Dirección Territorial Eje Cafetero	Armenia	10
4	Dirección Territorial Magdalena Medio	Barrancabermeja	17
5	Dirección Territorial Atlántico	Barranquilla	20
6	Dirección Territorial Central	Bogotá - Cundinamarca	17
7	Dirección Territorial Central	Bogotá – Avianca	388
8	Dirección Territorial Central	Bogotá – Afinsa	105
9	Dirección Territorial Central	Bogotá - Parque Santander P4	53
10	Dirección Territorial Central	Bogotá - Edificio Bavaria	1
11	Dirección Territorial Central	Bogotá - Edificio Calle Real	41
12	Dirección Territorial Central	Bogotá - Parque Santander P3	88
13	Dirección Territorial Central	Bogotá – Fontibón	11
14	Dirección Territorial Santander	Bucaramanga	8
15	Dirección Territorial Valle	Cali	39
16	Dirección Territorial Bolívar	Cartagena	14
17	Dirección Territorial Norte de Santander y Arauca	Cúcuta	16

Ítem	Denominación Unidad de Víctimas	Sede	Teléfonos Registrados en OSB
18	Dirección Territorial Caquetá y Huila	Florencia	11
19	Dirección Territorial Central	Ibagué	11
20	Dirección Territorial Eje Cafetero	Manizales	11
21	Dirección Territorial Antioquia	Medellín	48
22	Dirección Territorial Meta y Llanos Orientales	Mitú	4
23	Dirección Territorial Putumayo	Mocoa	12
24	Dirección Territorial Córdoba	Montería	9
25	Dirección Territorial Caquetá y Huila	Neiva	14
26	Dirección Territorial Nariño	Pasto	12
27	Dirección Territorial Eje Cafetero	Pereira	18
28	Dirección Territorial Cauca	Popayán	19
29	Dirección Territorial Meta y Llanos Orientales	Puerto Carreño	5
30	Dirección Territorial Meta y Llanos Orientales	Puerto Inírida	4
31	Dirección Territorial Chocó	Quibdó	8
32	Dirección Territorial Cesar y Guajira	Riohacha	7
33	Dirección Territorial Meta y Llanos Orientales	San José del Guaviare	11
34	Dirección Territorial Magdalena	Santa Marta	15
35	Dirección Territorial Sucre	Sincelejo	15
36	Dirección Territorial Central	Tunja	17
37	Dirección Territorial Cesar y Guajira	Valledupar	9
38	Dirección Territorial Meta y Llanos Orientales	Villavicencio	22
39	Dirección Territorial Meta y Llanos Orientales	Yopal	11
		Total	1139



Tabla 6. Inventario de Telefonía por Regional
Fuente: Grupo de Infraestructura OTI - UNIDAD PARA LAS VÍCTIMAS

- **DHCP – DNS – DIRECTORIO ACTIVO**

En algunas regionales se encuentran servidores que prestan servicios de comunicaciones entre los cuales está DHCP, DNS, directorio activo – DA y servicios de impresión. La Unidad cuenta con un dominio el cual se encuentra replicado en varios controladores de dominio, donde están registradas las cuentas de usuario, contraseñas y políticas definidas por la Unidad. Entre las políticas de seguridad en computadores, claves fuertes, vigencia de claves, uso de contraseñas históricas, fondos de pantalla y bloqueo de sesiones no permitidas.

- **ANTISPAM.**

Este servicio está incluido dentro del paquete de Office 365 contratado.

 	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018
			Página 54 de 127

- **ANTIVIRUS**

El antivirus usado para los servidores del centro de datos es TREND MICRO el cual es suministrado y administrado por el proveedor de Centro de Datos. Para los servidores y equipos que no hacen parte del centro de Datos se cuenta con el antivirus McAfee.

- **ADMINISTRACIÓN DE LOS SISTEMAS DE INFORMACIÓN**

Los sistemas de información, aplicaciones y servicios web se encuentran alojados en los servidores del centro de datos contratado y son administrados por los funcionarios responsables de la infraestructura computacional de la unidad.

- **AMBIENTES COMPUTACIONALES**

Para cumplir las diferentes etapas del ciclo de desarrollo de sistemas de información se han definido los siguientes ambientes computacionales:

- Ambiente de producción
- Ambiente de preproducción
- Ambiente de desarrollo
- Ambiente de pruebas
- Ambiente de reportes
- Ambiente de capacitación

Aunque se cuenta con estos ambientes computacionales de trabajo, no todos se utilizan para todas las aplicaciones, es decir, dependiendo de la necesidad, complejidad y uso de una aplicación se utilizan unos ambientes u otros, por ejemplo:

- LEX requiere ambientes de producción, capacitación, reportes y pruebas.
- SISCOD y SIRAV un solo ambiente porque no son objetos de modificación.

La disposición de los ambientes de trabajo no parte de análisis basados en criterios técnicos o modelos de decisión como cargas y concurrencia, sino de estimaciones basadas en la experiencia y conocimiento de los desarrolladores y/o los administradores.

MANTENIMIENTO A BASES DE DATOS



El mantenimiento a las bases de datos es continuo, el cual incluye afinamiento a sentencias (tunning), recreación de índices., ejecución de estadísticas, control de espacios, entre otros, tanto de Oracle como de SQL Server.

SOPORTE A INFRAESTRUCTURA

El soporte a la infraestructura y sus componentes de hardware y comunicaciones se realiza a

partir de solicitudes que se reciben en su mayoría a través de correo electrónico o por las diferentes herramientas que permiten el monitoreo, a continuación los servicios disponibles :

- SOPORTE A SERVIDORES
- SOPORTE A BASES DE DATOS
- SOPORTE A CORREO ELECTRÓNICO
- SOPORTE A APLICACIONES
- SOPORTE A CANALES DE COMUNICACIONES
- SOPORTE A LA RED INALÁMBRICA
- SOPORTE A SERVICIOS DE RED – DNS DHCP
- SOPORTE A LA ADMINISTRACIÓN DE EQUIPOS DE SEGURIDAD Y COMUNICACIONES

 	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018	Página 56 de 127

5.5. GESTIÓN DE LA INFORMACIÓN

Al respecto de la gestión de información la Subdirección Red Nacional de Información que pertenece a la Dirección de Registro y Gestión de la Información es el área directamente responsable de dicha gestión en cuanto que coordina todo lo relacionado con la información del Sistema Nacional de Atención y Reparación Integral a las Víctimas – SNARIV , la cual reúne a todas las entidades de gobierno nacional y territorial que participan y colaboran con la ruta de prevención, asistencia y reparación a las víctimas del conflicto.

5.5.1. FUENTES DE DATOS

La Subdirección de la Red Nacional tiene como una de sus misiones gestionar y proveer insumos para la aplicación de la política pública, en relación con la información recopila toda la información que las diferentes entidades del SNARIV tienen sobre las víctimas, la ordena y dispone para que sea consumida por todas las entidades del Estado, de tal forma que puedan tomar decisiones para dar aplicación a la política pública de víctimas, la otra misión por ley es coordinar y articular la Red Nacional de Información.

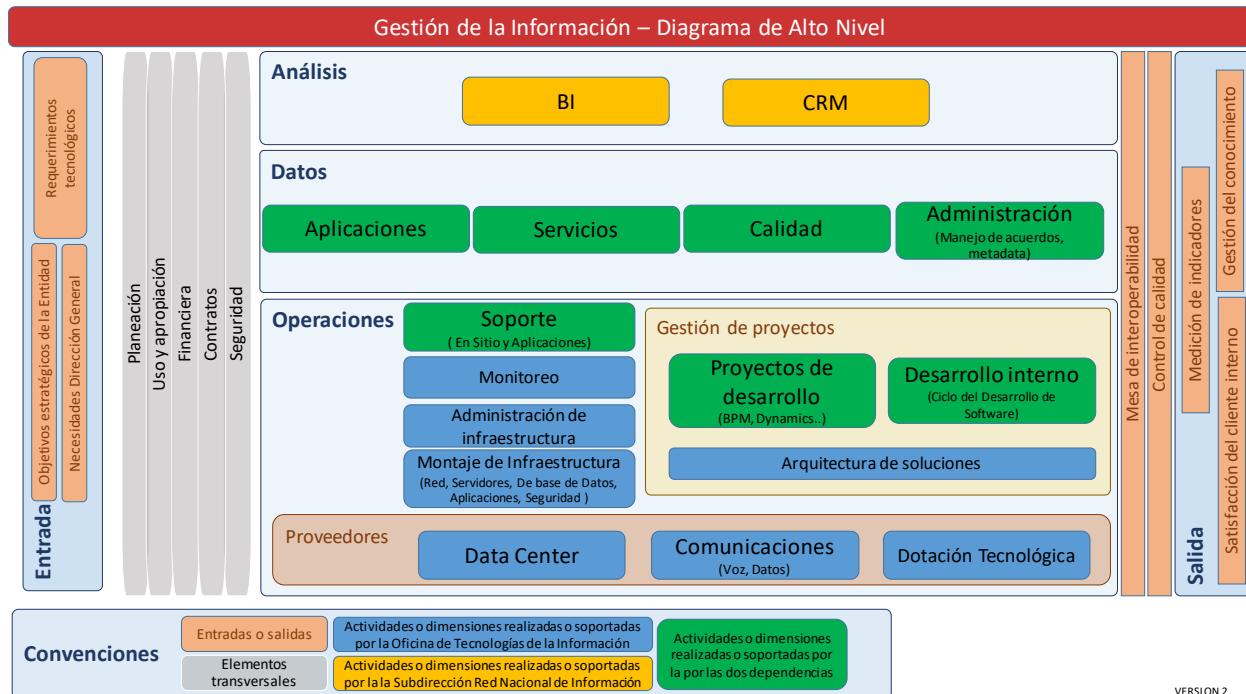
Otra fuente de información es la que se recopila por cada una de sus Subdirecciones de la Unidad en el cumplimiento de su misión siguiendo el ciclo de información de la víctima, es decir, reparación, valoración, asistencia y reparación.

5.5.2. GOBIERNO DE DATOS

La UNIDAD PARA LAS VÍCTIMAS ha creado la Mesa de Gobierno Digital con participación de la OTI, las diferentes Direcciones Misionales, Oficina de control Interno y Oficina de Comunicaciones en donde se analiza y define todo lo relacionado con el gobierno de datos y el intercambio de información que debe darse entre las diferentes entidades. Desde hace 5 años que MINTIC dio los lineamientos de Gobierno en Línea (hoy Gobierno Digital), se venía trabajando en dos espacios que eran el Subcomité Técnico de Sistemas de Información y la Mesa de Interoperabilidad con presencia solo de la SRNI por parte de la Unidad, ahora todos los temas relacionados serán abordados y tratados en el Mesa de Gobierno Digital

5.5.3. ARQUITECTURA DE INFORMACIÓN

En relación con este componente la UNIDAD PARA LAS VÍCTIMAS se encuentra en el proceso de formular e implementar su Arquitectura Empresarial siguiendo los lineamientos definidos por MINTIC en cumplimiento de la política de Gobierno Digital, en este sentido y como insumo para la formulación de la arquitectura, se presenta a continuación un diagrama de alto nivel que esquematiza la gestión de la Información en cada una de las capas estructurales, es decir, capa de proyectos, desarrollo y soporte, capa de datos donde se encuentran aplicaciones y servicios que los procesan y capa de análisis donde se presentan herramientas generadoras de información detallada y consolidada.



Gráfica 33. Diagrama de Alto Nivel – Gestión de la Información
Fuente: Grupo de Sistemas de Información OTI - UNIDAD PARA LAS VÍCTIMAS

5.5.4. CALIDAD DE DATOS

La Subdirección de Registro y Valoración adelanta un proyecto relacionado con la depuración de la información del registro de la víctima, consiste en verificar la información que históricamente se ha recopilado de otras instituciones y de la transcripción directa de los documentos diligenciados por las mismas víctimas, en los sitios donde presentan sus declaraciones y solicitudes (procuraduría, alcaldías, defensorías). En el documento elaborado por la Subdirección de Registro y Valoración “CALIDAD DE DATOS EN LA DIRECCIÓN DE REGISTRO” que se anexa, se presenta el análisis de la situación actual y avances del proyecto Calidad de Datos 2017-2018, ejecutado por dicha Subdirección. Este tema será abordado por la Mesa de Gobierno Digital.

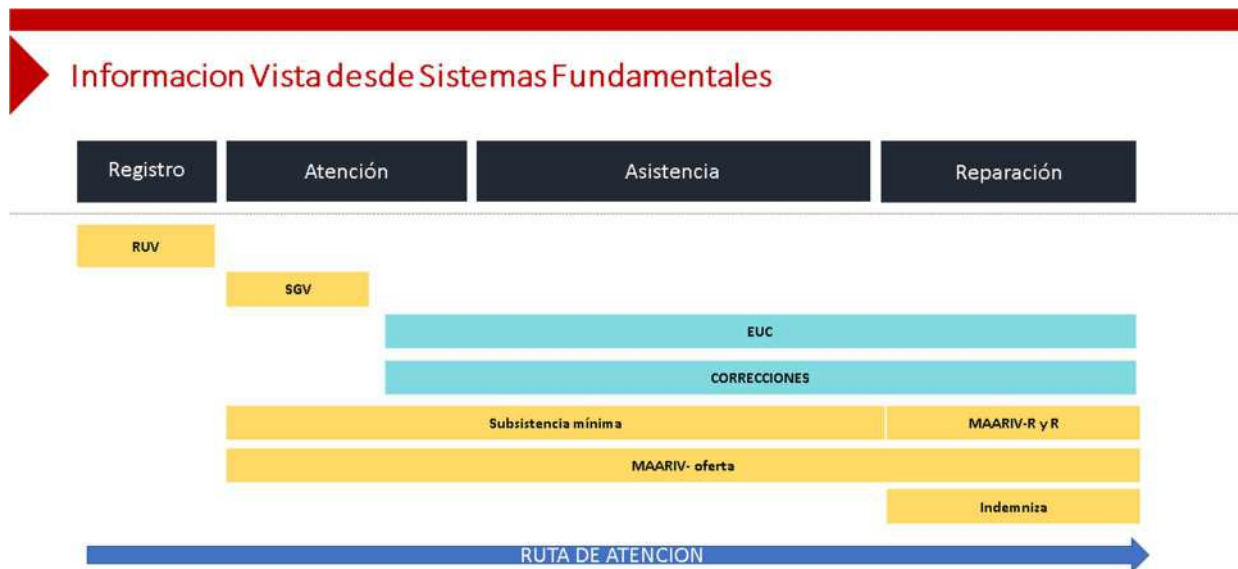
5.5.5. FLUJOS DE INFORMACIÓN Y GOBIERNO DE DATOS

La Red Nacional de Información tiene un diccionario de datos que es el conjunto organizado de variables de la información de las víctimas, que se dispone en las bases de datos de MINTIC bajo los estándares propuesto por ese Ministerio, cumpliendo con los lineamientos definidos para el gobierno de datos. También se tiene un directorio de servicios de información ya validados y registrados en el portal de intercambio de información del MINTIC para el consumo por parte de las diferentes entidades.

Se tiene un catálogo de datos abiertos y se está trabajando en la estrategia para la publicación de estos datos. Se tiene el propósito de conformar un comité conformado por la OTI, la SRNI, la OAP, la OAC y la OAJ para publicar lo pertinente en el portal de datos abiertos del MINTIC, a tales efectos, se ha participado en los talleres ofrecidos por el MINTIC para socializar las políticas y lineamientos sobre datos abiertos.



El Modelo Integrado de Información desarrollado por la SRNI es un instrumento para unificar las tablas de datos de las diferentes Subdirecciones de la Unidad que recopilan, procesan y generan información, el propósito es generar un solo repositorio de tablas que puedan ser consumidas por todas las dependencias, buscando lograr una sola fuente de datos, con tablas de datos no solo de las diferentes dependencias de la Unidad sino también de las diferentes entidades de la SNARIV.

En relación con los sistemas de información desarrollados y/o administrados por la OTI, la siguiente gráfica es un esquema conceptual del flujo de información general en el proceso de registro, valoración y reparación a la víctima. Se observa la participación de los diferentes aplicativos implementados para soportar la gestión misional de cada una de las áreas, así como las aplicaciones transversales que dan el soporte complementario necesario en temas de gestión documental (Aplicativo Orfeo), registro jurídico (LEX) y servicio de notificación (Notificaciones).



Gráfica 34. Diagrama de Ruta de Información vista desde los Sistemas Fundamentales
Fuente: OTI UNIDAD PARA LAS VÍCTIMAS

*RUV. Entiéndase como los sistemas heredados por la anterior institucionalidad (SIPOD, SIV, SIRAV, RUV_T, Portal de Consulta VIVANTO)

 GOBIERNO DE COLOMBIA  UNIDAD PARA LAS VÍCTIMAS	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018

Considerando los diferentes aplicativos o módulos o sistemas de información que desarrollan otras Subdirecciones de la Unidad se creó la Mesa de Interoperabilidad de manera oficial cuyo objetivo es identificar las diferentes fuentes de información para unificar criterios de administración y procesamiento de información. Estos temas serán abordados y tratados por la Mesa de Gobierno Digital

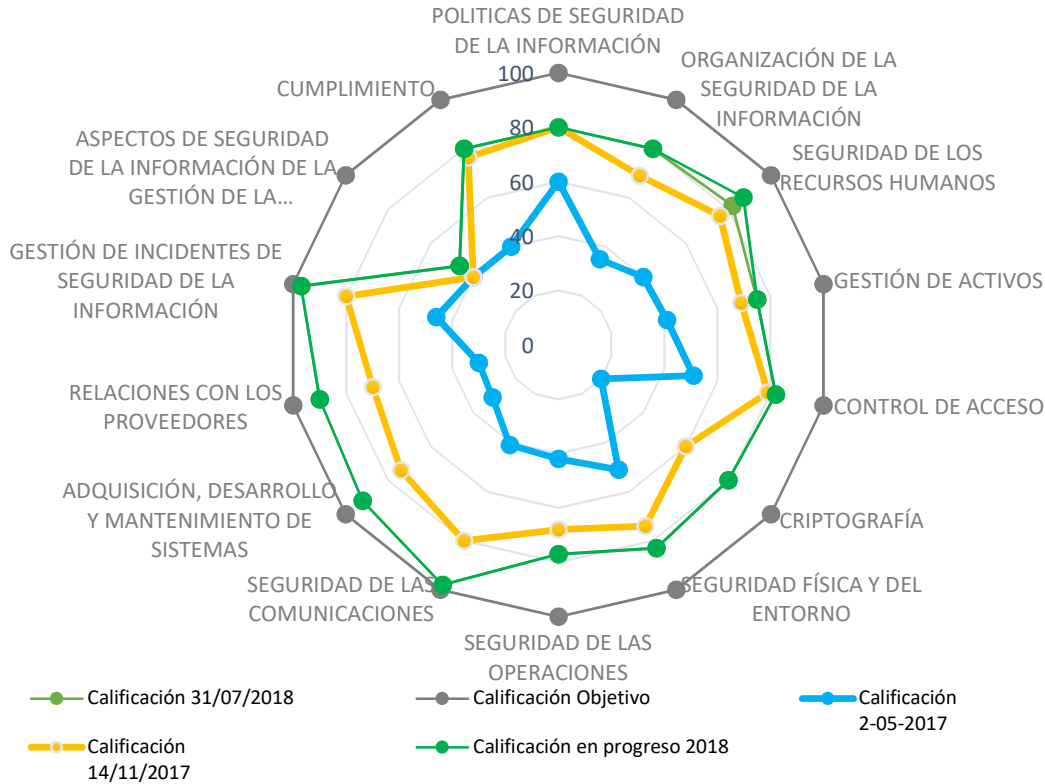
5.5.6. SEGURIDAD DE LA INFORMACIÓN.

Dentro del marco de las buenas prácticas de la Norma ISO27001:2013, la Unidad para la Atención y Reparación Integral a las Víctimas implementa el Modelo de Seguridad y Privacidad del MinTIC, teniendo en cuenta sus siguientes dimensiones:

- ✓ Política general de seguridad de la información
- ✓ Aspectos organizacionales de la seguridad de la información
- ✓ Seguridad de los recursos humanos
- ✓ Gestión de activos
- ✓ Control de acceso
- ✓ Cifrado o criptografía
- ✓ Seguridad física y del entorno
- ✓ Seguridad de las operaciones
- ✓ Seguridad de las comunicaciones
- ✓ Adquisición, desarrollo y mantenimiento de sistemas
- ✓ Relaciones con los proveedores
- ✓ Gestión de incidentes de seguridad de la información
- ✓ Aspectos de seguridad de la información de la gestión de continuidad de negocio
- ✓ Cumplimiento

Con relación al cumplimiento del Modelo, a 31 de octubre de 2018, la Unidad ha avanzado en un 82%, según la herramienta de diagnóstico del MinTIC:

BRECHA ANEXO A ISO 27001:2013



Gráfica 35. Comportamiento Dominio de Seguridad de la Información
 Fuente: OTI – Seguridad de la Información

No.	Evaluación de Efectividad de controles						EVALUACIÓN DE EFECTIVIDAD DE CONTROL
	DOMINIO	Calificación 2-05-2017	Calificación 14/11/2017	Calificación 31/07/2018	Calificación en progreso 2018	Calificación Objetivo	
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	60	80	80	80	100	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	35	69	80	80	100	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	40	76	82	87	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	41	69	75	75	100	GESTIONADO
A.9	CONTROL DE ACCESO	51	79	82	82	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	20	60	80	80	100	GESTIONADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	51	74	83	83	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	42	68	77	77	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	41	80	98	98	100	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	31	74	92	92	100	OPTIMIZADO
A.15	RELACIONES CON LOS PROVEEDORES	30	70	90	90	100	OPTIMIZADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	46	80	97	97	100	OPTIMIZADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	40	40	47	47	100	EFFECTIVO
A.18	CUMPLIMIENTO	40	76,5	80	80	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		41	72	82	82	100	OPTIMIZADO

Tabla 7. Cumplimiento del Modelo de Seguridad y Privacidad de la Información del MinTIC a corte 31 de octubre de 2018

Fuente OTI – Seguridad de la Información

Adicionalmente, la Unidad cuenta con el plan de seguridad y privacidad de la información aprobado por el Comité Institucional de Gestión y Desempeño, en la sesión del 30 de julio de 2018, donde se definen las siguientes actividades:

No.	Actividad	Responsable	Cobertura	Plan	Fecha Inicio	Fecha Final
1	Actualizar inventario de activos de información	Procesos a nivel central	NACIONAL	Plan de Acción / SIG	01/07/2018	31/08/2018
2	Diseñar y socializar el plan de sensibilización de seguridad de la información	Oficina de Tecnologías de la Información	NACIONAL	SIG	01/04/2018	30/05/2018
3	Socializar al interior de cada proceso los productos presentados en el marco de los encuentros de enlaces SIG y/o los boletines o flash informativos que se generen en materia de seguridad de la información	Procesos a nivel central	NACIONAL y TERRITORIAL	Plan de Acción / SIG	01/05/2018	31/12/2018
4	Identificar inventario de proveedores críticos	Procesos a nivel central	NACIONAL	Plan de Acción / SIG	01/04/2018	30/06/2018
5	Identificar, valorar, definir plan de tratamiento y realizar seguimiento de riesgos de activos críticos	Procesos a nivel central	NACIONAL	Plan de Acción / SIG	01/04/2018	31/12/2018
6	Gestionar el respaldo de la información almacenada en equipos de cómputo	Procesos a nivel central	NACIONAL	SIG	01/05/2018	30/09/2018

No.	Actividad	Responsable	Cobertura	Plan	Fecha Inicio	Fecha Final
	asignados al usuario, teniendo en cuenta Onedrive o servidor de archivos Totoro					
7	Realizar etiquetado de documentos por medio de Enterprise Mobility and Security de Microsoft- EMS	Procesos a nivel central	NACIONAL	SIG	01/09/2018	31/12/2018
8	Documentar Protocolo de contacto con autoridades	Oficina de Tecnologías de la Información	Oficina de Tecnologías de la Información	Plan de Acción	01/04/2018	31/05/2018
9	Inventario de certificados de sitio seguro SSL asociados a la aplicación correspondiente indicando su vigencia.	Oficina de Tecnologías de la Información	Oficina de Tecnologías de la Información	Plan de Acción	01/05/2018	30/06/2018
10	Identificar software autorizado por la Oficina de Tecnologías de la Información.	Oficina de Tecnologías de la Información	Oficina de Tecnologías de la Información	Plan de Acción	01/09/2018	31/12/2018

Tabla 8. Cronograma – Plan de Seguridad y Privacidad de la Información - UARIV 2018
Fuente OTI – Seguridad de la Información

Adicionalmente, en el equipo de Seguridad y Riesgo Informático de la Oficina de Tecnologías de la Información, se plantean los siguientes roles:

- Rol: Líder de la Seguridad de la Información de la OTI
- Rol: Analista de riesgos de seguridad de la información.
- Rol: Analista para la seguridad informática.

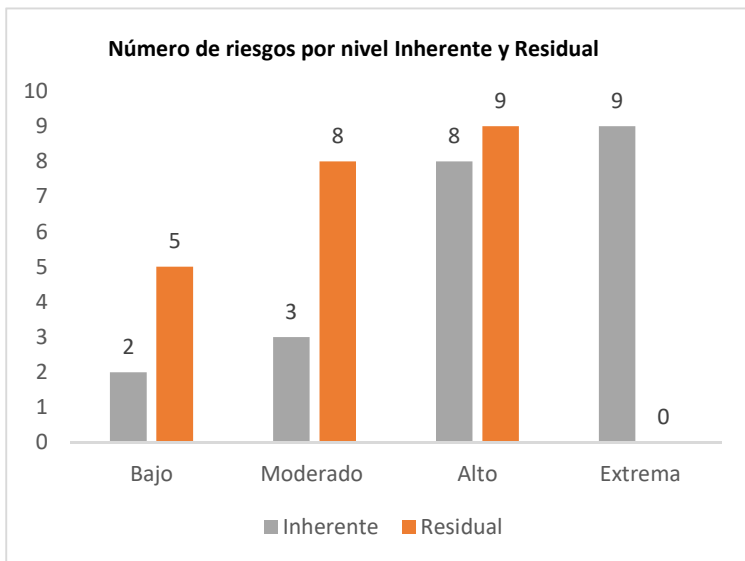
En relación con el recurso humano, las personas actualmente contratadas cuentan con especialización relacionada en Seguridad de la Información. Así mismo, han asistido a las

sesiones de divulgación del Modelo de Seguridad y Privacidad de la Información realizadas por el MINTIC y a jornadas de capacitación del CSIRT Gobierno.


Desde la Oficina de Tecnologías de la Información en articulación con el Grupo de Gestión Documental, se lidera la actualización del inventario de activos de información en cumplimiento no solamente del mencionado modelo, sino que además aporta en el cumplimiento de Ley 1712 de 2014, llamada Ley Transparencia.

Adicionalmente, en el marco del Subsistema de Gestión de Seguridad de la Información, se gestiona la identificación, análisis, valoración y tratamiento de riesgos de seguridad de la información en los procesos de nivel central de la Entidad. Actualmente, el equipo de seguridad y riesgo informático adelanta el seguimiento a los controles y planes de tratamiento de los riesgos de los procesos de la Entidad.

Es importante mencionar que, de los 18 procesos de la Entidad, 13 tienen asociados activos críticos (Direccionamiento Estratégico, Gestión de la Información, Prevención de hechos victimizantes, Registro y Valoración, Gestión para la Asistencia, Reparación Integral, Participación y Visibilización de las Víctimas, Gestión Jurídica, Gestión de Talento Humano, Gestión Financiera, Evaluación Independiente, Control Interno Disciplinario y Servicio al Ciudadano). Los 5 procesos restantes no tienen activos críticos asociados (Comunicación Estratégica, Gestión Administrativa, Gestión Documental, Gestión Contractual y Gestión Interinstitucional)



Gráfica 36. Comparativo Niveles de Riesgo
Fuente OTI – Seguridad de la Información

	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018	Página 64 de 127

Con relación con la estructura de procedimientos recomendada por las buenas prácticas en materia de seguridad de la información, en el marco de la mejora continua, se debe definir los siguientes protocolos o procedimientos:

- Procedimiento de intercambio de información
- Gestión de Certificados Digitales en Sistemas de Información.
- Gestión de verificación cumplimiento de políticas
- Controles criptográficos
- Gestión de cambios (En construcción)
- Gestión de capacidad
- Gestión de aseguramiento de servicios de red
- Gestión de controles de seguridad en el desarrollo de software
- Gestión de continuidad
- Gestión de recuperación ante desastres

DERECHOS DE AUTOR

Se incluyen en los contratos firmados con el personal de desarrollo y terceros, cláusulas relacionadas con la propiedad de los derechos de autor de los sistemas de información, , sin embargo se debe mejorar en el registro de derechos de autor de los sistemas de información diseñados y construidos al interior de la Entidad.

ETHICAL HACKING



La Unidad ha realizado ejercicio sobre análisis de vulnerabilidades, pero se debe mejorar en la creación del procedimiento o protocolo que permita su gestión de manera repetible y periódica.

SEGURIDAD EN LA INTEROPERABILIDAD

La Unidad cuenta con acuerdos de intercambio de información con las Entidades del SNARIV, los cuales formalizan la articulación e intercambio de datos por diferentes mecanismos. Sin embargo, se debe mejorar en la identificación y documentación de los diferentes flujos de información al interior de la Entidad y con terceros, tanto por la RNI como por la OTI, para fortalecer la implementación y documentación de los controles respectivos para robustecer la seguridad existente.

SEGURIDAD DE SERVICIOS EN LA NUBE

La Unidad cuenta con servicios tipo nube contratados bajo la modalidad del Acuerdo Marco de Precios de Colombia Compra Eficiente, el cual incluye aspectos transversales de seguridad, sin embargo, en la gestión de riesgos se deben incluir los relacionados con este tipo de almacenamiento de información.

 	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018	Página 65 de 127

5.6. GOBIERNO DE TI

ESTRUCTURA ORGANIZACIONAL Y TALENTO HUMANO



La OTI desarrolla acciones enmarcadas dentro del proceso estratégico “Gestión de la Información”, cuyo objetivo es orientar las gestiones de la tecnología de la información y las comunicaciones TIC articuladas con las estrategias misionales generando valor en el marco de las políticas y lineamientos establecidos por el Gobierno Nacional.

La estructura organizacional y de gobierno de TI en la UNIDAD PARA LAS VÍCTIMAS está conformada por una Jefatura de la Oficina de Tecnologías de la Información, 11 funcionarios de planta y 37 en la modalidad de prestación de servicios, adicionalmente por parte de los diferentes proveedores de servicios se cuenta con 6 colaboradores.

Cuenta con perfiles especializados para liderar cada una de las diferentes líneas de servicio o instancias de apoyo táctico a la Jefatura Proyectos de Gobierno, Gestión Presupuestal, Enlace de Planeación, Sistemas de Información, Servicios Tecnológicos y Uso y Apropiación.

Mediante el Decreto 4802 de 2011 se asignan las siguientes funciones a la Oficina de Tecnologías de la Información:

1. Diseñar y proponer la política de uso y aplicación de tecnologías, estrategias y herramientas para el mejoramiento continuo de los procesos de la Unidad.
2. Garantizar la aplicación de buenas prácticas y principios para el manejo de la información institucional, siguiendo los lineamientos y directrices del Gobierno Nacional.
3. Diseñar e implementar un modelo de interoperabilidad de sistemas y gestión de información misional, con el fin de permitir el acceso a la información por parte de entidades y actores, de manera ordenada e integrada que facilite la toma de decisiones.
4. Vigilar que en los procesos tecnológicos de la Unidad se tengan en cuenta los estándares y lineamientos dictados por las entidades competentes, y en especial, por el Ministerio de las Tecnologías de la Información y las Comunicaciones que permitan la aplicación de las políticas que en materia de información expidan las entidades competentes.
5. Administrar una plataforma unificada de los sistemas de información de la Unidad que permita articular las diferentes fuentes de información en una sola herramienta de gestión y efectuar análisis de información con procesamiento en tiempo real.
6. Elaborar el mapa de información que permita contar de manera actualizada y completa con los procesos de producción de información de la Unidad.
7. Informar al Director General y a las dependencias de la Unidad, sobre la gestión informática que realicen entidades del Estado relacionadas con la atención, asistencia y reparación integral de las víctimas, y proponer mejoras para la mayor eficiencia en los procesos misionales de la Unidad.
8. Proponer al Director General planes, estrategias y proyectos que en materia de Tecnologías

 GOBIERNO DE COLOMBIA  UNIDAD PARA LAS VÍCTIMAS	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018

de la Información se deban adoptar.

9. Analizar los sistemas e instrumentos de gestión de la información de la Unidad, y proponer mejoras al Director General.

10. Dirigir, orientar y participar en el desarrollo de los contenidos y ambientes virtuales requeridos para el cumplimiento de las funciones y objetivos de la Unidad.

11. Proponer a la Dirección General las estrategias de coordinación de los sistemas de información con las entidades involucradas en el proceso de atención, asistencia y reparación de las víctimas.

12. Proponer las especificaciones técnicas para la administración, la recepción y la entrega de la información según protocolos de intercambio de esta.

13. Implementar las metodologías y procedimientos que adopte la Unidad para el desarrollo, instalación, administración, seguridad y uso de la infraestructura tecnológica, teniendo en cuenta los lineamientos que en la materia generan las entidades competentes.

14. Administrar los sistemas de información, equipos, redes y herramientas tecnológicas y brindar el soporte técnico para su funcionamiento adecuado.

15. Realizar el seguimiento, control y evaluación a la ejecución de los planes, programas y proyectos en tecnologías de la información de la Unidad.

16. Ejecutar los programas y proyectos relacionados con las tecnologías de la información adoptados por la Unidad en coordinación con las demás dependencias.

17. Definir con las entidades competentes la arquitectura de los sistemas de información, la infraestructura tecnológica, los sistemas de gestión y monitoreo y los esquemas de seguridad y confidencialidad de la información de la Red Nacional de Información.

18. Apoyar el desarrollo y sostenimiento del Sistema Integrado de Gestión Institucional y la observancia de sus recomendaciones en el ámbito de su competencia.

19. Las demás inherentes a la naturaleza y funciones de la Dependencia

A continuación, la lista de posiciones de los funcionarios vinculados directamente a la UNIDAD PARA LAS VÍCTIMAS:

DENOMINACIÓN DEL EMPLEO	CÓDIGO	FUNCION - ROL	GRADO
Jefe Oficina	137	JEFE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN	22
Profesional Especializado	2028	LIDER SISTEMAS DE INFORMACION	24
Profesional Especializado	2028	LIDER SERVICIOS TI • Soporte en sitio, Soporte aplicaciones	24
Profesional Especializado	2028	LIDER DE USO Y APROPIACION	24
Profesional Especializado	2028	LIDER FINANCIERO - CONTRACTUAL	21
Profesional	2044	• Planes de acción • Enlace OCI • seguimiento Plan de acción y	9
Analista de sistemas	3003	• Soporte en sitio	18
Analista de sistemas	3003	LIDER CONCEPTUAL Y DE APOYO a la gestión de desarrollo	18
Analista de sistemas	3003	LIDER CONCEPTUAL Y DE APOYO a la gestión de desarrollo	18
Analista de sistemas	3003	•Apoyo tareas administrativas, contratos y financiero.	18
Técnico	3100	• Apoyo administrativo.	16

Tabla 9. Lista de Cargos de la Oficina de Tecnologías de la Información
Fuente: Oficina de Tecnologías de la Información OTI - UNIDAD PARA LAS VÍCTIMAS

5.7. ANÁLISIS FINANCIERO COSTOS DE OPERACIÓN Y FUNCIONAMIENTO

La Oficina de Tecnologías de la Información cuenta con un Proyecto de Inversión cuyo código en el Banco de Proyectos de Inversión es BNP 201411000409 vigencia 2018. A partir de la asignación anual de recursos se establece el Plan Anual de Adquisiciones conformado por proyectos, servicios y soluciones tecnológicas. El valor asignado para la vigencia de 2018 es de Treinta y un mil millones de pesos (\$31.000.000.000), la siguiente tabla muestra la distribución por rubros:

PRESUPUESTO DE INVERSIÓN POR RUBRO

RUBRO	PRESUPUESTO EN MILLONES	PORCENTAJE
SERVICIOS DE COMPUTO POR DEMANDA	\$ 6.258	20,18 %
SERVICIOS DE CONECTIVIDAD	\$ 1.685	5,44 %
SERVICIOS DE DOTACIÓN TECNOLÓGICA	\$ 17.700	57,10 %
SERVICIOS DE SISTEMAS DE INFORMACIÓN	\$ 5.357	17,28 %
TOTAL	\$ 31.000	

Tabla 10. Inversión por rubro

Fuente: Grupo de Gestión Presupuestal OTI – UNIDAD PARA LAS VÍCTIMAS

PRESUPUESTO DE INVERSIÓN POR TIPO DE PROCESO DE CONTRATACIÓN

TIPO DE PROCESO	PLANEADO	CDP	RP	OBLIGADO
ACUERDO MARCO PRECIOS	\$ 5.933	\$ 4.939	\$ 4.936	\$ 1.946
AGREGACION DE DEMANDA	\$ 780	\$ 780	\$ 423	\$ -
CONTRATACION DIRECTA	\$ 20.210	\$ 19.356	\$ 18.404	\$ 9.292
MENOR CUANTIA	\$ 157	\$ 156	\$ -	\$ -
SELECCIÓN ABREVIADA MENOR CUANTIA	\$ 300	\$ 300	\$ -	\$ -
SUBASTA INVERSA ELECTRONICA	\$ 800	\$ 800	\$ -	\$ -
TRASLADO AREA	\$ 1.864	\$ 1.864	\$ 14	\$ 14
TRASLADO PROYECTO	\$ 823	\$ 823	\$ -	\$ -
VIATICOS & TICKETS	\$ 129	\$ 101	\$ 99	\$ 21
SUBTOTAL	\$ 30.998	\$ 29.120	\$ 23.877	\$ 11.273

Tabla 11. Inversión por Tipo de Proceso en millones de pesos - fecha de corte julio 2018

Fuente: Grupo de Gestión Presupuestal OTI – UNIDAD PARA LAS VÍCTIMAS

Mediante el seguimiento mensual se hace monitorea la ejecución de los recursos de inversión programados en el plan anual de adquisiciones. La siguiente ilustración presenta la ejecución a cierre de Julio la oficina de tecnologías a comprometido el 77% de la asignación de recursos.



Gráfica 37 Seguimiento mensual de recursos de inversión

Fuente OTI – Gestión de Presupuesto

Cada proceso contractual definido en el plan anual de adquisiciones cuenta con la debida supervisión según el manual establecido por el grupo de gestión contractual de la entidad.

LICENCIAMIENTO

Para la operación legal y autorizada de las diferentes herramientas de software (sistemas operativos, aplicaciones, utilitarios) se cuenta con el respectivo licenciamiento en diferentes modalidades: compra, compra y renovación, derechos de uso, donación, servicios de arriendo y suscripción de licencias de uso, como se presenta en el siguiente anexo.

ANEXO - INFORME DE LICENCIAMIENTO

CAPACIDAD

La capacidad instalada hace referencia a la disponibilidad de los siguientes recursos tecnológicos: servidores, equipos de cómputo, equipos de impresión y escáner, periféricos, cableado estructurado, centros de cableado, servicio integral de video conferencia, mesa de servicios de primer nivel, soporte técnico, mantenimientos correctivos y preventivos. El siguiente anexo presenta la disponibilidad de recursos y análisis de seguimiento.

ANEXO - GESTIÓN DE CAPACIDAD

6. ENTENDIMIENTO ESTRATÉGICO

Corresponde a un análisis del modelo de operación de la Unidad su organización, las necesidades de información y la alineación de la OTI con los procesos institucionales.

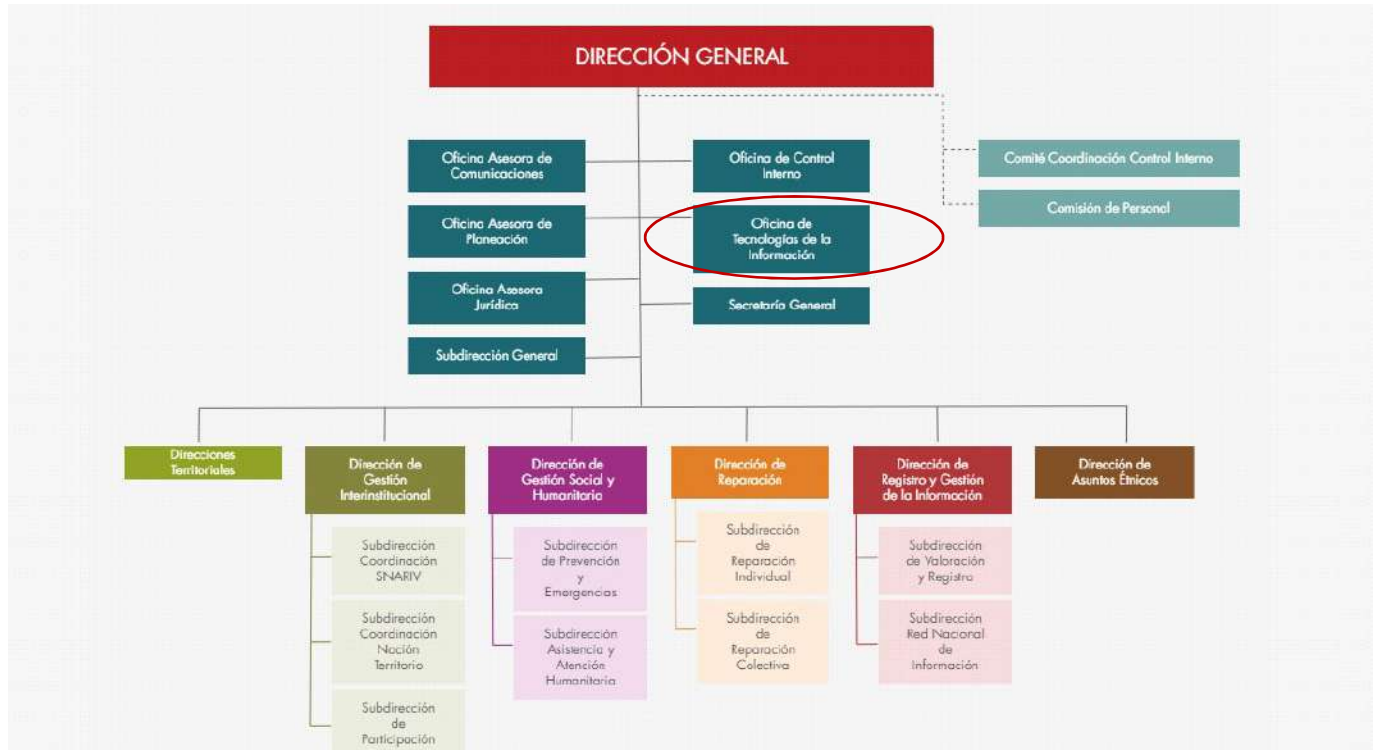
6.1. MODELO OPERATIVO

6.1.1. MARCO INSTITUCIONAL

El entendimiento de la Entidad como ejecutor de políticas públicas haciendo parte del sector social y al mismo tiempo entendida como ente coordinador del sistema nacional de atención a la población víctima SNARIV, hace que deba asumir diferentes roles y competencias, ello en virtud de que las entidades que hacen parte del sector y las del SNARIV no son necesariamente las mismas, o a que sus marcos legales o institucionales no se encuentran perfectamente alineados; por ello la organización ha creado una estructura que le permite atender los dominios a que hace referencia el plan asignando competencias a su Oficina de Tecnologías de la Información y a la Red Nacional de Información a fin de armonizar el desarrollo técnico.

Según lo anterior la OTI da desarrollo a los lineamientos de la arquitectura TI en lo que tiene que ver con los procesos misionales, de apoyo, estratégicos y de seguimiento en tanto correspondan a temas tecnológicos de manejo interno en la entidad que inciden en la atención y reparación de las víctimas y soportan sus procesos no relacionados con entidades del sector o el SNARIV, por otra parte la RNI da desarrollo al dominio de información en el marco del SNARIV, alineando dicho dominio en forma coordinada con las entidades del sector y el SNARIV siguiendo los lineamientos que para los demás dominios se lideran en la OTI

6.1.2. ESTRUCTURA ORGANIZACIONAL Y UBICACIÓN DE LA OTI





6.1.3. DESCRIPCIÓN DEL MAPA ESTRATÉGICO DE LA UNIDAD DE VÍCTIMAS

La UNIDAD PARA LAS VÍCTIMAS formuló el Plan Indicativo 2014-2018 a partir de los lineamientos del Plan Nacional de Desarrollo, la puesta en marcha de la Ruta Integral, la suscripción del Decreto 2569 de 2014, hoy incorporado en el Decreto Sectorial 1084 de 2015, y el Acuerdo Final de Paz para complementar la construcción de los indicadores a través de los cuales se medirá la gestión de la Entidad, alineándolos a las metas consignadas al Plan Nacional de Desarrollo.

La alineación estratégica se soporta y encuadra en dos pilares:

- El Plan Nacional de Desarrollo que incorpora aspectos fundamentales en materia de construcción de una paz sostenible y que se fortalecen con las acciones gubernamentales ejecutadas y en ejecución para implementar el Acuerdo Final de Paz.
- La Ley 1448 de 2011, decretos reglamentarios y decretos ley para comunidades étnicas, y el marco legal que impone la necesidad de garantizar un efecto transformador de la reparación a las víctimas, es decir, un impacto real en la consolidación de su proyecto de vida, una real participación, la recuperación de su ciudadanía y un ejercicio activo de sus derechos

 GOBIERNO DE COLOMBIA  UNIDAD PARA LAS VÍCTIMAS	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018

De otra parte, el Plan Nacional de Desarrollo plantea tres retos estratégicos a la Unidad para las Víctimas, a saber:

- Superar la situación de vulnerabilidad de las víctimas del conflicto armado: se refiere al reconocimiento del conflicto armado interno y de la existencia de los daños causados a las víctimas individuales y colectivas.
- Superar el estado de cosas inconstitucional decretados por la Corte Constitucional hace más de 10 años: corresponde a la consolidación de un proceso que promueva las condiciones de seguridad y de convivencia pacífica para la concreción de la paz y del posconflicto.
- Consolidar procesos de reparación integral tanto individuales como colectivos: indica la coherencia y concordancia entre la implementación de la política pública de atención y reparación integral y las políticas de desarrollo integral que potencien los territorios.

Adicionalmente se plantearon los objetivos estratégicos para la Unidad y para la OTI, alineados con los definidos por el Departamento de Prosperidad Social, cabeza del sector, como se presenta a continuación, los objetivos estratégicos de la OTI son objeto de actualización en el capítulo Modelo de Gestión de este documento.

OBJETIVOS ESTRATÉGICOS DEPARTAMENTO DE PROSPERIDAD SOCIAL	OBJETIVOS ESTRATÉGICOS UNIDAD PARA ALAS VÍCTIMAS	OBJETIVOS ESTRATÉGICOS OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
1. Formular lineamientos de política para reducción de la pobreza y la pobreza extrema y contribución a la consolidación de la clase media y la reconciliación	1. Trabajar juntamente con las víctimas en el proceso de reparación integral para la reconstrucción y transformación de sus proyectos de vida	1. Garantizar la prestación de los servicios de información para atender las necesidades de reparación integral a las víctimas del conflicto
2. Coordinar e implementar las acciones que contribuyan a la generación de condiciones para la equidad y la reconciliación en los territorios	2. Acercar el estado a las víctimas para brindarles una oferta pertinente, eficaz, sostenible y oportuna	2. Mantener los sistemas de información en un nivel eficaz y sostenible, para lograr que las Víctimas reciban oportunamente la integración y la reparación.
3. Articular y gestionar la oferta social de entidades públicas, socios privados, tercer sector e innovadores para la inclusión social de los hogares y las comunidades	3. Definir con las entidades territoriales la implementación de la Ley 1448/11, sus decretos reglamentarios y sus Decretos Ley	4. Mantener los recursos tecnológicos en un nivel eficaz y sostenible, para lograr que las Víctimas reciban oportunamente la integración y la reparación.
4. Mejorar la gestión de los procesos de soporte de la Entidad	4. Vincular de manera activa la sociedad civil y a la comunidad internacional en los procesos de reparación integral de las víctimas del conflicto	5. Desarrollar el buen gobierno de las tecnologías de la información, para cumplir con las disposiciones legales y garantizar el uso correcto de los recursos tecnológicos para reparar a las víctimas.
5. Fortalecer la comunicación estratégica y la participación ciudadana	5. Fortalecer la cultura de confianza colaboración e innovación para garantizar una atención digna, respetuosa y diferencial	5. Proporcionar a la comunidad herramientas y mecanismos de carácter técnico-social, para afianzar en la víctima el conocimiento sobre los beneficios, los derechos y los recursos tecnológicos disponibles.

Tabla 12. Alineación de Objetivo Estratégicos DPS – UNIDAD PARA LAS VÍCTIMAS - OTI

6.1.4. DESCRIPCIÓN DEL PLAN ESTRATÉGICO SECTORIAL

El Sector de Inclusión Social y Reconciliación está en cabeza del Departamento de Prosperidad Social, las entidades que conforman el Sector de Inclusión Social y Reconciliación y que están adscritas al Departamento Administrativo de la Presidencia de la República son:

1. El Departamento para la Prosperidad Social –DPS fue creado por el Gobierno Nacional

mediante el decreto 4155 de 2011 que transformó la antigua Agencia Presidencial para la ACCIÓN SOCIAL y la Cooperación Internacional – ACCIÓN SOCIAL. Su creación impuso al DPS como organismo principal de la administración pública del Sector Administrativo de Inclusión Social y Reconciliación, con la función principal de formular, adoptar, dirigir, coordinar y ejecutar las políticas, planes generales, programas y proyectos para la superación de la pobreza, la inclusión social, la reconciliación, la recuperación de territorios, la atención a grupos vulnerables, población discapacitada y la reintegración social y económica y la atención y reparación a víctimas de la violencia

2. El Instituto Colombiano de Bienestar Familiar –ICBF adscrito al DPS mediante Decreto 4156 de 2011, su objetivo principal es trabajar por el pleno desarrollo de la primera infancia y el bienestar de las familias, para ello promueve el desarrollo integral de los niños desde su gestación hasta los 6 años contribuyendo al logro de la equidad y la inclusión.
3. La Unidad Especial de Atención y Reparación de las Víctimas creada por la ley 1448 de 2011 y se encuentra adscrita al DPS mediante Decreto 4157 de 2011. El objetivo de la Unidad es responder por la atención y reparación integral de las víctimas del conflicto armado, coordinando políticas encaminadas a satisfacer los derechos de verdad, justicia y reparación.
4. El Centro de Memoria Histórica adscrito al DPS mediante Decreto 4158 de 2011, tiene como objetivo reunir y recuperar todo el material documental, testimonios orales y de otras características, relativos a las violaciones cometidas contra aquellas personas que individual o colectivamente hayan sufrido un daño por hechos ocurridos a partir del 1 de enero de 1985.



Gráfica 38. Objetivos del Sector
Fuente: Departamento de Prosperidad Social

6.1.5. MISIÓN Y VISIÓN ESTRATÉGICA SECTORIAL

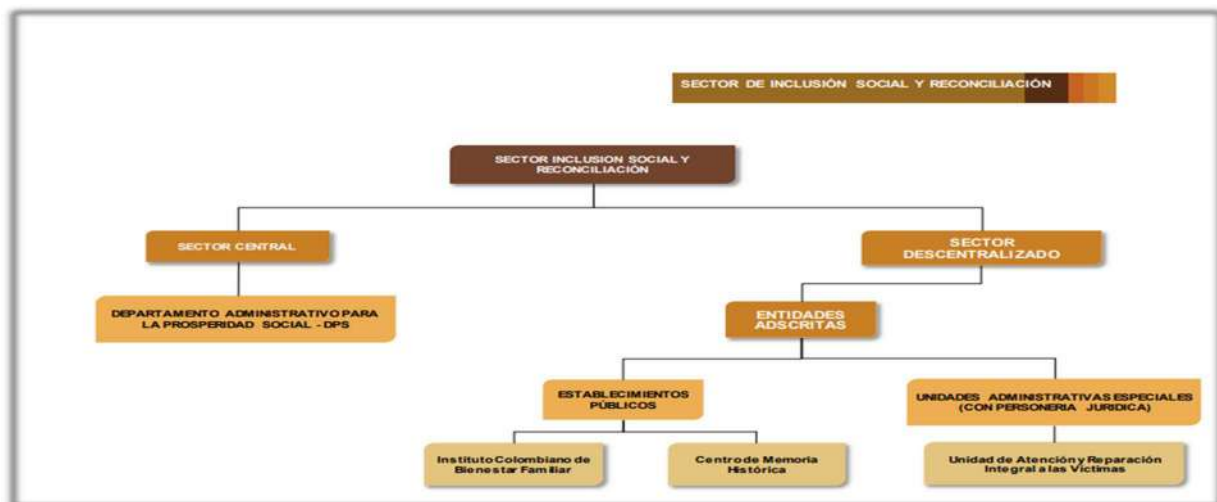
	DPS	ICBF	UARIV	CENTRO MEMORIA
M I S I O N	Diseñar, coordinar e implementar políticas públicas para la inclusión social y la reconciliación	Trabajar con calidad y transparencia por desarrollo y la protección integral de la primera infancia, la niñez, la adolescencia y el bienestar de las familias colombianas	Liderar acciones del Estado y la sociedad para atender y reparar integralmente a las víctimas para contribuir a la inclusión social y a la paz	Contribuir a la realización de la reparación integral y el derecho a la verdad del que son titulares las víctimas y la sociedad en su conjunto, así como al deber de memoria del estado con ocasión de las violaciones ocurridas en el marco del conflicto armado colombiano, en un horizonte de construcción de paz, democratización y reconciliación.
V I S I O N	Para el año 2025 se habrá erradicado la pobreza extrema y contribuido a la inclusión social y la reconciliación	Cambiar el mundo de las nuevas generaciones y sus familias, siendo referente en estándares e calidad y contribuyendo a la construcción de una sociedad en paz, próspera y equitativa	En el 2021 habremos logrado que las víctimas reparadas integralmente ejerzan su ciudadanía y aporten en la consolidación de la paz como resultado de la gestión efectiva y coordinada de la Unidad con los demás actores del sistema	A 2018 el Centro Nacional de Memoria Histórica será una plataforma de promoción, diálogo y articulación de las memorias plurales del conflicto armado, que garantiza la inclusión de diversos actores y poblaciones y contribuye a la reparación integral, reconocimiento histórico, las garantías de no repetición y la construcción de una paz sostenible

Tabla 13. Misión y Visión Estratégica Sectorial

Fuente: Plan Estratégico Sectorial de Inclusión Social y Reconciliación - DPS

6.1.6. ESTRUCTURA DEL SECTOR INCLUSIÓN

El Decreto 4155 del 3 de noviembre de 2011, transforma la Agencia Presidencial para la Acción Social y la Cooperación Internacional - Acción Social, en Departamento Administrativo para la Prosperidad Social, perteneciente al Sector Administrativo de Inclusión Social y Reconciliación, y se fija su objeto y estructura. El Decreto 2559 del 30 de diciembre 2015, fusiona la Agencia Nacional para la Superación de la Pobreza Extrema – ANSPE y la Unidad Administrativa Especial para la Consolidación Territorial – UACT en el Departamento Administrativo para la Prosperidad Social.



Gráfica 39 Diagrama de la Estructura del Sector Inclusión

Fuente: Departamento de Prosperidad Social

Como lo evidencia la gráfica anterior, la Unidad para las Víctimas pertenece al sector de la inclusión social y la reconciliación. La Entidad cabeza de sector es el Departamento de Prosperidad Social, quien formuló el Plan Sectorial de Inclusión Social y Reconciliación, el cual presenta como alcance estratégico sectorial “Por una paz estable y duradera, transformamos nuestro país en un territorio incluyente, con equidad y condiciones para la reconciliación, donde todas las personas gocen efectivamente de sus derechos”.

6.1.7. PLAN ESTRATÉGICO SECTORIAL

Tomando en consideración que durante la vigencia 2017 se expide el Decreto 1499 del 11 de septiembre de 2017 por parte del Departamento de la Función Pública por el cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015, se realiza ajuste al Plan Estratégico sectorial, así como la alineación del PND y el MIPG.

Así mismo se han definido : la Estrategia Sectorial transversal de Gobierno de Datos, el Plan

Anticorrupción,, la Administración de Riesgos, la Racionalización de Trámites, la Participación Ciudadana, la Rendición de Cuentas y los Mecanismos para la Transparencia y Acceso a la Información, nuevos elementos que de forma estratégica se integran al plan estratégico institucional y sectorial y que permiten realizar seguimiento a la gestión realizada para el cumplimiento de las actividades misionales.

A continuación la Matriz del Plan Estratégico Sectorial con sus dimensiones y políticas:

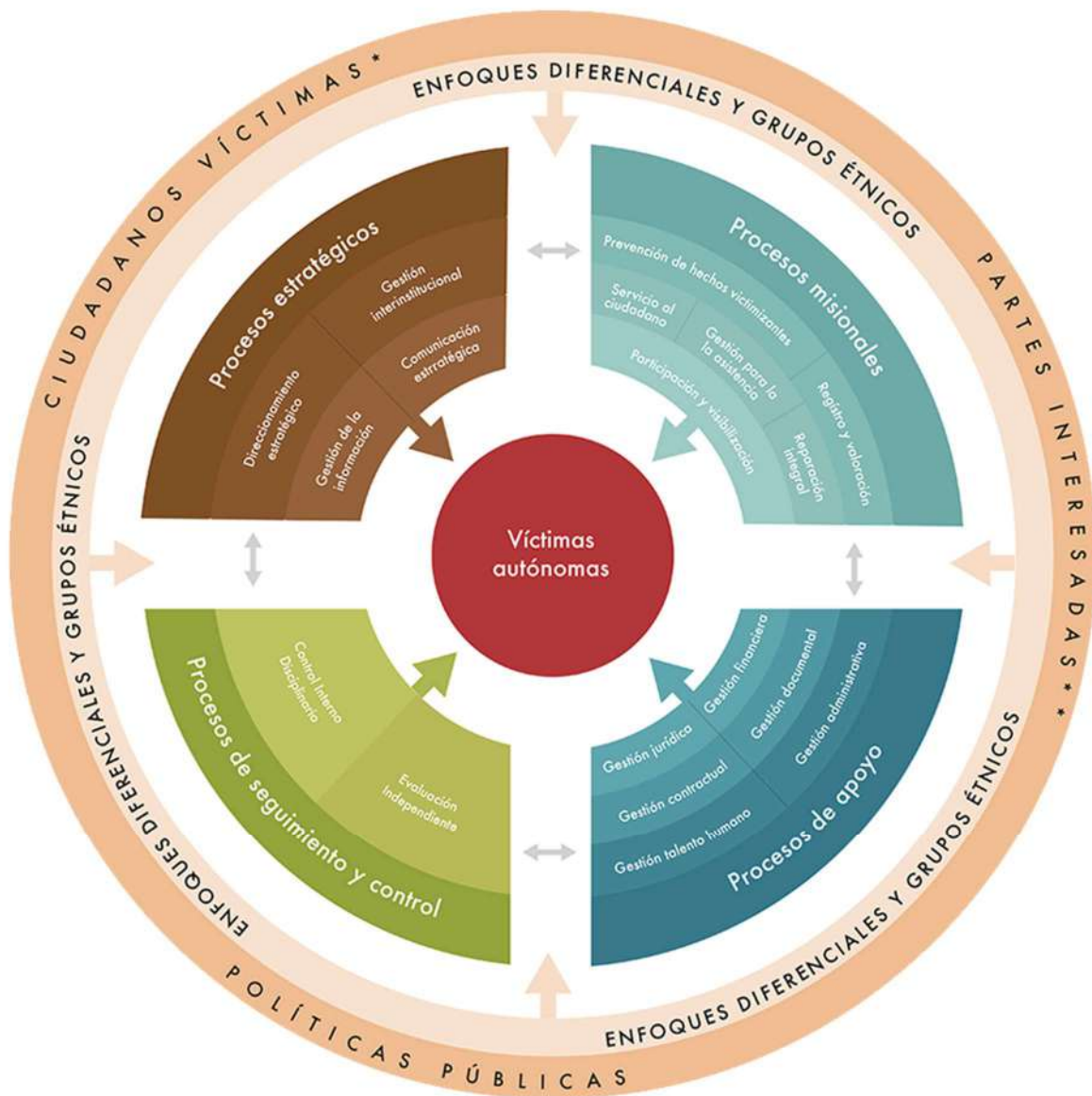
DIMENSIÓN		POLÍTICAS ASOCIADAS	
Talento Humano	Integridad		
	Gestión Estratégica del Talento Humano		
Direcciónamiento Estratégico y Planeación	Planeación Institucional		
	Gestión Presupuestal y Eficiencia del Gasto Público (programación)		
Gestión con valores para resultados	Ventanilla Hacia Adentro	Fortalecimiento institucional y simplificación de procesos	
		Gobierno digital (gestión)	
		Seguridad digital	
		Gestión Presupuestal y Eficiencia del Gasto Público (ejecución)	
	Defensa jurídica		
	Ventanilla hacia Afuera	Servicio al ciudadano	
		Gobierno digital (servicios y gobierno abierto)	
		Racionalización de trámites	
Participación ciudadana.			
Evaluación de resultados	Seguimiento y Evaluación del Desempeño Institucional		
Información y Comunicación	Gestión Documental		
	Transparencia y acceso a la Información pública y lucha contra la corrupción		
Gestión del Conocimiento y la Innovación	Gestión del Conocimiento		
Control Interno	Control Interno		

Gráfica 40 Diagrama del Plan Estratégico Sectorial
Fuente: Plan Estratégico Sectorial de Inclusión Social y Reconciliación

6.1.8. MAPA DE PROCESOS - UNIDAD



La Unidad en el Sistema Integrado de Gestión y el Modelo Integrado de Planeación y Gestión tiene definido un Mapa de Proceso con 18 procesos así:

4 procesos Estratégicos, 6 Procesos Misionales, 2 Procesos de Seguimiento y Control y 6 Procesos de Apoyo



Grafica 41. Mapa de Procesos

Fuente: Sistema de Gestión Integrado de la UNIDAD PARA LAS VÍCTIMAS

 GOBIERNO DE COLOMBIA  UNIDAD PARA LAS VÍCTIMAS	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018
			Página 79 de 127

6.1.9. PROCESO GESTIÓN DE LA INFORMACIÓN.

Desde el direccionamiento estratégico, las tecnologías de información y comunicaciones se definen como instrumentos fundamentales para lograr el cumplimiento de los planes y objetivos institucionales; en este sentido la alta dirección ubica al proceso de Gestión de la Información como un proceso estratégico en el marco del Modelo Integrado de Planeación y Gestión – MIPG y el Sistema Integrado de Gestión - SIG.

OBJETIVO.

Gestionar los servicios, gobierno y capacidad tecnológica que soporta la operación y las necesidades de la Unidad frente las tecnologías de la información y articular a las entidades que conforman la red nacional de información para facilitar el flujo eficiente de información que permita realizar el seguimiento a la implementación de la política pública para apoyar el cumplimiento de la misión y objetivos de la Unidad. Está conformado por los siguientes procedimientos:

- Acceso remoto a servidores y bases de datos
- Procedimiento Acceso Remoto a Servidores y Bases de Datos V1
- Procedimiento Creación de Usuarios en Sistemas de Información V1
- Procedimiento de creación, modificación o actualización y eliminación de buzones de correo institucional V2
- Procedimiento Desarrollo de Nuevos Sistemas de Información y/o Funcionalidades en Sistemas Existentes V1
- Procedimiento Dotación Tecnología Nueva Sede, Traslado de Sede y/o Adicionales V1
- Procedimiento Gestión de Incidentes seguridad V2
- Procedimiento Gestión de Préstamo de Discos duros cifrados V1
- Procedimiento Gestión de Solicitudes de Dotación Tecnológica V1
- Procedimiento Solicitud de Servicios de Telefonía IP V1
- Procedimiento Soporte a Sistemas de Información y Aplicaciones V1
- Procedimiento Soporte Técnico a La Infraestructura Tecnológica V1
- Procedimiento Validación de Infraestructura e Inventario V1
- Procedimiento Alistamiento de la Información V4
- Procedimiento Difusión y Aprendizaje V2
- Procedimiento Sistemas de Información Geográfica V1

ALCANCE.

El proceso inicia con la identificación de las necesidades de información, soluciones y servicios de TI, análisis e implementación según los requerimientos de la Unidad y finaliza con la generación de insumos en materia de información y el soporte a las necesidades tecnológicas.

CARACTERIZACIÓN DEL PROCESO GESTIÓN DE LA INFORMACIÓN.

En concordancia con el modelo de gestión en el ciclo PHVA se cumplen las siguientes actividades:



PLANEAR	HACER	VERIFICAR	ACTUAR
<ul style="list-style-type: none"> • Identificar la normatividad • Formular Plan de Acción y Proyecto de Inversión • Gestionar la capacidad de los recursos y servicios de TI • Formular lineamientos planes, estrategias y políticas para implementar proyectos de TI • Establecer el contexto estratégico identificando los factores internos y externos 	<ul style="list-style-type: none"> • Ejecutar el Plan de Acción • Identificar los riesgos de TI • Desarrollar los Sistemas de Información • Soportar los Sistemas de Información • Dotar tecnológicamente nuevas sedes • Gestionar las solicitudes de dotación tecnológica • Gestionar la infraestructura tecnológica • Gestionar el SGSI • Dar trámite a las solicitudes de Información SNRI • Alistar y disponer las fuentes y bases de datos de Información de la población víctima SNRI 	<ul style="list-style-type: none"> • Autoevaluar la gestión con seguimiento a indicadores • Monitorear y realizar el tratamiento a los servicios y /o productos no conformes 	<ul style="list-style-type: none"> • Formular e implementar acciones correctivas preventivas y de mejora

Tabla 14. Ciclo PHVA – Proceso de Gestión de la Información

6.1.10. POLÍTICAS DE TI

El Decreto 1078 de 2015 dispone que las entidades están obligadas al cumplimiento de las políticas y lineamientos de la Estrategia de Gobierno en Línea o Gobierno Digital, entre ellos los relacionados Seguridad y Privacidad de la Información, en este sentido la UNIDAD PARA LAS VÍCTIMAS cuenta con las Políticas de Seguridad de la Información que comprende enfoques y actividades transversales a los componentes de TIC para Servicios, TIC para el Gobierno Abierto y TIC para la Gestión, tendientes a proteger la información y los sistemas de información, del acceso, divulgación, interrupción o destrucción no autorizada, de otra parte, existen lineamientos relacionados con el uso y control de los recursos tecnológicos como reglas de uso de servicios tecnológicos y responsabilidades acerca de los recursos de tecnología, pero no están debidamente formalizados y oficializados por la Unidad.

De otra parte, se cuenta con la proyección de Políticas de TI que da cobertura a todos los recursos y operaciones de tecnología.

 	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018
			Página 81 de 127

6.2. INTERCAMBIO Y NECESIDADES DE INFORMACIÓN

Diseñar construir e implementar un estándar (políticas, procedimientos) de interoperabilidad entre todas las entidades del SNARIV , en temas de información gobierna la RNI, desde el 2017 se realizan talleres para mapear la información del sistema con 11 entidades que aportaron sus diccionarios de datos, con el fin buscar la estandarización de información dado que los conjuntos de variables son diferentes; de la misma manera se está trabajando para la construcción de un marco común para la homologación de variables y así lograr consistencia y confiabilidad en el dato. De otra aparte, en temas de políticas, procedimientos y métodos gobierna la OTI

• DATOS ABIERTOS.

Se está trabajando en la estrategia para publicación de datos abiertos siguiendo los lineamientos del DPS avalados por el MINTIC, con el ánimo de identificar nuevos conjuntos de datos susceptibles de ser publicados como datos abiertos de la UARIV. Actualmente se delegó en la mesa de Gobierno Digital el levantamiento de un inventario de información que complemente la información misional y de Registro que actualmente está publicada en el portal www.datos.gov.co.

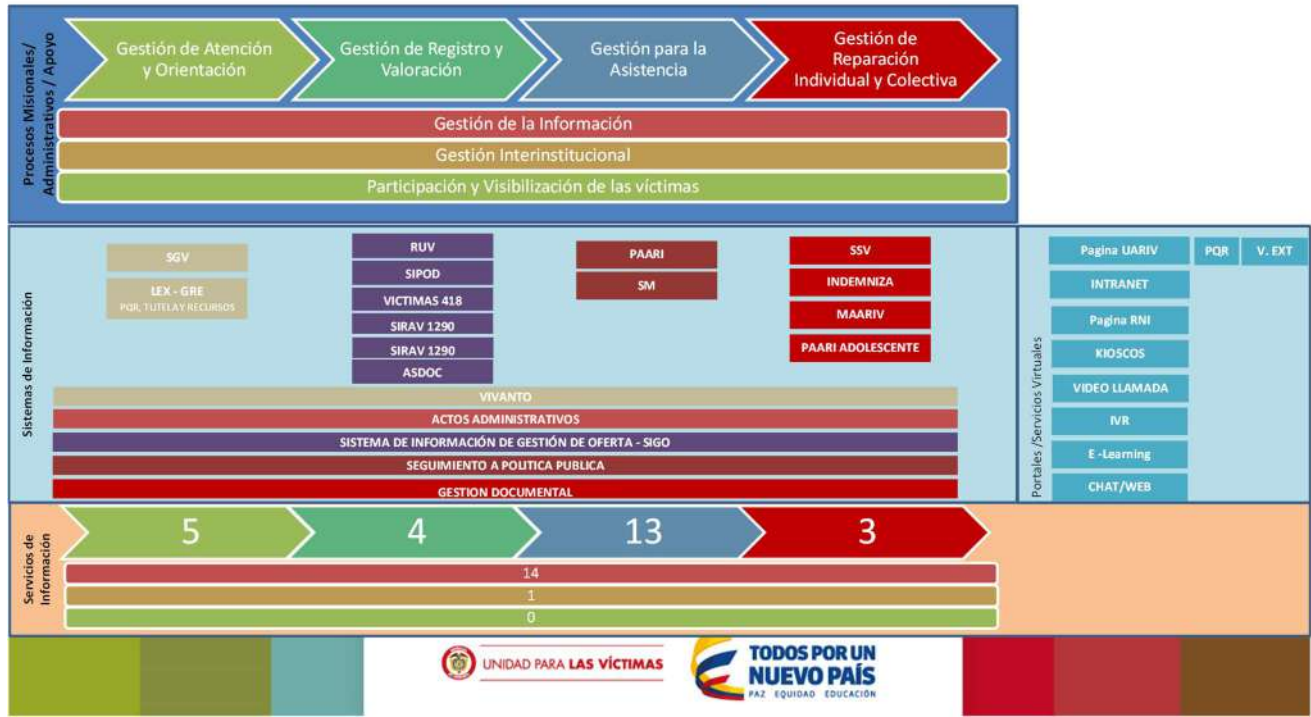
• MODELO INTEGRADO DE INFORMACIÓN.

Instancia para unificar las tablas de datos de las diferentes Subdirecciones de la Unidad que recopilan, procesan y generan información, el propósito es generar un solo repositorio de tablas que puedan ser consumidas por todas las dependencias, buscando lograr una sola fuente de datos, con tablas de datos no solo de las diferentes dependencias de la Unidad sino también de las diferentes entidades del SNARIV. El Sistema Nacional de Atención y Reparación Integral a las Víctimas – SNARIV – está constituido por el conjunto de entidades públicas del nivel gubernamental y estatal en los órdenes nacional y territoriales y demás organizaciones públicas o privadas; encargadas de formular o ejecutar los planes, programas, proyectos y acciones específicas, que tiendan a la atención y reparación integral de las víctimas, la coordinación de este sistema está a cargo de la Unidad y entre sus objetivos están:

1. Participar en la formulación e implementación de la política integral de atención, asistencia y reparación a las víctimas.
2. Adoptar las medidas de atención que faciliten el acceso y cualifiquen el ejercicio de los derechos a la verdad, justicia y reparación de las víctimas.
3. Adoptar las medidas de asistencia que contribuyan a restablecer los derechos de las víctimas, brindando condiciones para llevar una vida digna.
4. Adoptar los planes que garanticen el ejercicio efectivo de los derechos de las víctimas.

6.3. ALINEACIÓN DE TI CON LOS PROCESOS

A continuación, se presenta el esquema de relación entre los sistemas de información y los servicios de información de la OTI con las diferentes áreas/procesos de la Unidad.



Gráfica 42 Diagrama de relación Sistemas de Información / Procesos
 Fuente: Grupo Sistemas de Información OTI – UNIDAD PARA LAS VÍCTIMAS

7. MODELO DE GESTIÓN DE TI

7.1. ESTRATEGIA DE TI

De acuerdo con lo establecido en el marco de referencia de Gobierno Digital, en el dominio de estrategia de TI, se presentarán a continuación los principios con los que debe cumplir nuestra estrategia de TI.





Gráfica 43 Principios y valores Modelo de Gestión IT4+

Fuente: Modelo de Gestión IT4+ - MINTIC

Con base en los principios enunciados, la estrategia de TI tiene como propósito:

- Implementar la tecnología apropiada para ofrecer servicios de TI de alta calidad centrados en las víctimas, instituciones, grupos de interés y usuarios.
- Apoyar mediante TI la participación ciudadana y la gestión y eficiencia administrativa de la UNIDAD PARA LAS VÍCTIMAS, garantizando la seguridad y la privacidad de la información.
- Integrar el marco de referencia de arquitectura empresarial a la estrategia de TI para implementar las mejores prácticas, guías y estándares que facilitarán el uso adecuado de la tecnología para soportar los servicios de TI y el cumplimiento de nuestra misión y objetivos estratégicos.
- Planear, definir y mantener la estrategia de TI alineada con los objetivos estratégicos de la Unidad, el Plan Estratégico Sectorial y el Plan Nacional de Desarrollo.

 GOBIERNO DE COLOMBIA  UNIDAD PARA LAS VÍCTIMAS	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018
			Página 84 de 127

Para efectos de obtener conceso sobre la definición y estructura de la Estrategia de TI se realizaron los ejercicios que se desarrollan continuación:

- PLANTEAMIENTO DE LA ESTRATEGIA GENERAL
- ANÁLISIS DOFA
- DEFINICIÓN DE ESTRATEGIAS ESPECIFICAS

7.1.1. PLANTEAMIENTO DE LA ESTRATEGIA GENERAL

Considerando los principios enunciados, la Estrategia de TI de la Unida de Victimas consiste en:

“APLICAR LAS TECNOLOGÍAS DE LA INFORMACIÓN PARA ACERCAR EL ESTADO A LAS VICTIMAS EN PRO DE SU ATENCIÓN, REPARACIÓN INTEGRAL Y EJERCICIO CIUDADANO”.

Para este propósito se definen tres objetivos o ejes estratégicos alineados al marco de la Política y Estrategia de Gobierno Digital definida por el Gobierno Nacional, a través del Ministerio de las Tecnologías y las Comunicaciones

OBJETIVO ESTRATÉGICO 1. - SERVICIOS CIUDADANOS DIGITALES.

“Ofrecer soluciones tecnológicas para facilitar a las víctimas su interacción con la Unidad optimizando la gestión y el servicio.”

OBJETIVO ESTRATÉGICO 2. - OBJETIVOS DE DESARROLLO SOSTENIBLE – INNOVACIÓN TECNOLOGÍAS EMERGENTES.

“Generar sinergias con las entidades involucradas en la atención a la población víctima y con terceros para contribuir a la transformación digital del Estado”

OBJETIVO ESTRATÉGICO 3. - ARQUITECTURA DE TI – SEGURIDAD Y PRIVACIDAD

“Fortalecer la seguridad y la eficiencia de la gestión interna, a partir del mejoramiento de las capacidades TI”



Gráfica 44 Objetivo Estratégico 1
Fuente OTI – Jefatura



Gráfica 45 Objetivo Estratégico 2
Fuente OTI – Jefatura



Gráfica 46 Objetivo Estratégico 3
Fuente OTI – Jefatura

7.1.2. ANÁLISIS DOFA Y ESTRATEGIAS ESPECIFICAS

La formulación de la Estrategia y la definición de los Objetivos Estratégicos fueron el resultado del ejercicio-taller DOFA en donde se evaluaron las **Debilidades, Oportunidades, Fortalezas y Amenazas** como se presenta a continuación.

Con la participación de 40 funcionarios de diferentes dependencias que lideran procesos estratégicos, misionales y de apoyo, se conformaron tres grupos de análisis así:

- Servicios Tecnológicos
- Sistemas de Información
- Seguridad y Privacidad

A cada grupo se le asignó un objetivo estratégico específico para analizar, los integrantes de cada grupo estaban relacionados entre sí por las funciones que cumplen y el objetivo estratégico objeto de análisis. A continuación las matrices resultantes del análisis.

SERVICIOS TI _ DOTACION_INF	FORTALEZAS	DEBILIDADES
	1. Personal dedicado a la seguridad de la informacion	1. Mesa de servicios no atiende todos los servicios
	2. Permanencia del conocimiento dada la continuidad del personal	2. Alta vulnerabilidad en los sistemas de informacion
	3. Buena infraestructura tecnologica	3. Falta de actualizacion, capacitacion en tecnologia y crecimiento profesional
	4. Nueva direccion conoce la misionalidad de la entidad	4. No hay comunicación acertiva
	5. Contamos con recursos financieros	5. No contamos con personal tecnico en las DT
	6. Equipos autogestionados y autocontrolados	6. Falta de aprovechamiento de los recursos tecnologicos por desconocimiento
	7. Personal idoneo	7. No sabemos vender nuestros productos
	8. Somos proceso estrategico	8. Percepcion del cliente frente a la atencion de la mesa y de los servicios
		9. Alta rotacion mesa de servicio
	10. Incumplimiento en los tiempos de entrega de los servicios	
	11. No hay medicion de los servicios y productos ofrecidos.	
	12. No hay gobernabilidad sobre los servicios tecnologicos de la unidad.	
	13. Poco personal con diferentes roles asignados	
OPORTUNIDADES	ESTRATEGIAS	
1. Por la terceracion se accede a nuevas tecnologias	1. Alinear los servicios TI con Gobierno Digital	1. Plan para canalizar a través de la mesa de servicios el soporte de todas las herramientas de la unidad
2. Mejor aprovechamiento de los recursos y ahorro presupuestal a través de Colombia compra eficiente	2. Implementar 3 estrategias de innovacion al año, aprovechando la infraestructura y el personal	2. Implementar politicas de gobierno TI
3. Tener un plan de mejoramiento	3. Aprovechar _participar en las iniciativas y retos Mintic	3. Garantizar la oportunidad de los servicios TI mediante plan de seguimiento
4. Acompañamiento de Mintic	4. Implementar programa de capacitacion	4. Fortalecer y promover la comunicación interna.
5. Por la terceracion tenemos adquisicion de nuevos servicios		
AMENAZAS		
1. Cambio de administracion	1. Rediseñar los ANS	1. Buscar reconocimiento a nivel externo
2. Insatisfaccion de nuestros usuarios finales	2. Implementar nuevas herramientas y modelos de seguimiento	2. Buscar sinergias con otras entidades para mejorar la cobertura y atencion a las victimas.
3. Tiempos no cumplidos por proveedores	3. Implementar nuevas herramientas tecnologicas	3. Ampliar la cobertura de soporte en las DT.
4. Plazo ley de victimas		

SISTEMAS DE INFORMACION	FORTALEZAS	DEBILIDADES
	1. Talento Humano	1. Falta de estandares y procedimientos
	2. Oportunidad en respuesta TI	2. Falta de insumos tecnologicos
	3. Conocimiento del negocio, aptitud, respaldo presupuestal, mejoramiento de procesos internos ,	3. Falta de oportunidad en la entrega de informacion consolidada
	4. Metodologia de trabajo	4. Falta de comunicacionb, falta de colaboracion.
		5. Falta uso y apropiacion
		6. Percepcion negativa del area
	7. Multiples sistemas de informacion para la entrada de informacion, gobierno, control de personal.	
OPORTUNIDADES	ESTRATEGIAS	
1. Capacitaciones con entidades externas TI	1. Informacion tecnologica a traves de SI y nuevas tecnologias TI	1. Fomentar politicas y lineamientos en busca de establecer un gobierno SI con alcance a nivel unidad y en el sector TI
2. Articulacion para la definicion de requerimientos	2. Implementar lineas de trabajo de nuevas tecnologias.	2. Alinear los SI existentes con los dominios de arquitectura empresarial adaptado IT4+
3. Capacitacion de uso y apropiacion		3. Divulgar SI desarrollados/ implementados por la OTI
4. Adoptar metodologias de desarrollo por componenetes reutilizables		
5. Nuevas metodologias de optimizacion para desarrollo.		
6. Entrega oportuna de productos		
7. Gobierno TI		
8. Capacidad infraestructura		
9. Gobernabilidad entre entidades del sector		
10. Necesidad de informacion		
AMENAZAS		
1. Tiempo de respuesta operadores	1. Implementar metodologia para la gestion del conocimiento de SI	1. Definir ans que permitan la satisfaccion y continuidad del servicio mediante el uso de nuevas tecnologias orientadas a toma de desiciones.
2. Cambios organizacionales del estado	2. Capacitacion y adopcion de buenas practicas que permitan evolucionar metologias de desarrollo para una mayor oportunidad en la entrega de soluciones tecnologicas.	2. Buscar sinergias con otras entidades para mejorar la cobertura y atencion a las victimas.
3. Perdida, tercerizacion de desarrollo		
4. Falta de gobierno sistemas de informacion		
5. Cambios tecnologicos		
6. Finalizacion acuerdos marcos o contratos para contincidad de servicios		
7. Falta controles de seguridad		
8. Falta continuidad del personal contratado		

	FORTALEZAS	DEBILIDADES
SEGURIDAD	1. Evolucion del MSPi	1. Consolidacion de archivos parcializados
	2. Brindar informacion a traves de canalesindeminzacione en la	2. Falta de apropiacion sobre seguridad
	3. Seguimiento al comportamiento de los usuarios	3. Compartir informacion de la unidad a traves de canales no propios de launidad.
	4. Gestion de riesgos	4. Usar medios externos para acceso a los pc's de la unidad
	5. Conciencia de la importancia de la seguridad de la informacion	5. Uso de herramientas no oficiales de la unidad (software)
	6. Creacion de area de seguridad con roles definidos	6. Falta de apropiacion sobre seguridad
	7. Lineamientos y politicas definidas	7. Falta de lineamientos en desarrollo seguro de software pruebas.
	8. Planes de tratamietno al riesgo y riesgos asociados	8. Herramientas tecnologicas para el monitoreo de usuarios de todos los sistemas de informacion en tiempo real. Apropiacion del conocimiento.
	9. Instrumento T9SPI	9. Limitacion de la gestion por parte de las personas contratadas porel operador a causa del contrato.
	10. Personas responsables de implementar estrategias de seguridad	10. Ausencia de oficial de seguridad oficial
	11. Conciencia basica de la necesidad de seguir protocolos de seguridad en la unidad	11. SGSI unicamente liderada por la OTI
	12. Garantizar la seguridad de la informacion de las victimas	12. No hay gobernabilidad sobre los servicios tecnologicos de la unidad.
	13. Comunicacion efectiva ante amenazas externas	13. Control de acceso a la informacion fisico
	14. Alto conocimiento y respuesta de RR HH de infraestructura OTI	14. Falta de canales efectivos de comunicaci3n con DT
	15. Tecnologia adquirida en pro seguridad.	15. Monitoreo real de actividades fraudulentas y severidad en los castigos cuando hay una actividad fraudulenta.
	16. RR HH calificado, SGSI buenas practicas oficial y aprobado.	16. Activacion de politicas en el DLD
	17. Ejecuta procedimietno de monitoreo	17. Robo de bases de datos por parte de funcionarios
	18 Lineamientos de seguridad en la unidad.	18. Herramientas en excel para llevar temas misionales.
OPORTUNIDADES	ESTRATEGIAS	
1. Confiabilidad en los informes reportados a nivel nacional, confiabilidad a los datos dados de las victimas.	1. Definir el plan de contingencia para mitigar impacto por desastres naturales apoyo Mintic y CSLRT	1. Participar oportunamente en espacios, foros de ambiente gubernamental y privado actualizados.
2. Aumentar el alcance de nuestros SI a moviles para nuestras victimas	2. Diseñar e implementar el aseguramiento en seguridad de la informacion en DTS y puntos de atencion.	2. Articular con Csirt Gobierno
3. A nivel de la OTI tener amplio conocimiento de la arquitectura TI Colombia de Mintic	3. Fortalecer y capacitar el recurso humano para la gestion de incidentes de seguridad int.	3. Gestionar apoyo de Mintic (Recursos y apoyo, capacitacion.
4. Capacitaciones de Microsoft para hacer conocer todas las herramientas Office 365	4. Gestionar el aseguramiento de la informacion enviada a terceros o entres de control. intercambio de informacion	4. Participar en retos, concursos, competencias para mostrar lo hecho, reconocimiento y valoraci3n externa.
5. Gestion articulada con el CSIRT gobierno de incidentes de seguridad.	5. Fortalecer el control de activos para evitar fugas de informacion	5. Aprovechamiento de nuevas tecnologias
6. Apoyo de otras entidades con experiencias, casos de éxito	6. Gestion de la vulnerabilidad tecnica.	6. Crear y fomentar equipos de investigacion tecnologica/enfoque soluciones para las victimas.
7. Contamos con dinero		
8. Conciencia del gobierno sobre el tema.		
9. Inversion y apoyo gubernamental		
10. Apoyo CSIRT gobierno		
AMENAZAS	ESTRATEGIAS	
1. La unidad es atractiva para los hackers	1. Administracion efectiva, gestion de configuracion, segregacion de funciones de infraestructura de seg.	1. Actualizar politica, apoyo gubernamental, seguimiento de la implementacion
2. Funcionarios y contratistas que salen de la unidad, fenomenos naturales, recorte de recursos.	2. Implementar procedimientos de gestion de cambio en SI	2. Comunicaci3n, apropiacion, induccion, reinducc3n, multiplicadores.
3. Afectacion de la pagina por Hacking	3. Estrategia de continuidad de operaci3n.	3. Analisis en tiempo real para el monitor de eventos con tecnologia de punta y apoyo de Gobierno.
4. Constante alerta respecto a ataques de robo de informacion	4. Definir la instancia que cumple funciones como oficial de cumplimiento.	
5. Crecimiento exponencial de malware a nivel mundial		
6. Incremento de vulnerabilidades con el internet de todo (IOE)		
7. Suplantaci3n en el pago de la indemnizaci3n.		
8. Acceso indebido a la informacion		
9. Insuficiente conocimiento de los procesos de la unidad.		
10. No hay cultura del tema de seguridad a nivel de usuario filial.		

7.1.3. ALINEACIÓN DE TI CON LA ESTRATEGIA DE LA UNIDAD PARA LAS VÍCTIMAS

A continuación se observa la alineación de los objetivos estratégicos de la Unidad, los objetivos estratégicos de TI, los dominios del Marco de Referencia de Arquitectura Empresarial y los productos con los cuales se da cumplimiento.

OBJETIVOS ESTRATÉGICOS UNIDAD PARA LAS VÍCTIMAS	OBJETIVOS ESTRATÉGICOS DE TI	DOMINIOS AE	PRODUCTO
OBJETIVO 1. Trabajar juntamente con las víctimas en el proceso de reparación integral para la reconstrucción y transformación de sus proyectos de vida	OBJETIVO 1. • Ofrecer soluciones tecnológicas para facilitar a las víctimas su interacción con la Unidad optimizando la gestión y el servicio. OBJETIVO 3. • Fortalecer la seguridad y la eficiencia de la gestión interna, a partir del mejoramiento de las capacidades TI"	INFORMACIÓN • Implementar los recursos de Planeación y Gobierno a los datos para asegurar la oportunidad y la calidad de la información.	Arquitectura de Información Estructura de los Componentes de Información con calidad y seguridad
OBJETIVO 2. Acercar el Estado a las víctimas para brindarles una oferta pertinente, eficaz, sostenible y oportuna	OBJETIVO 1. • Ofrecer soluciones tecnológicas para facilitar a las víctimas su interacción con la Unidad optimizando la gestión y el servicio.	SISTEMAS DE INFORMACIÓN • Fortalecer la gestión de los Sistemas de Información	Arquitectura de Sistemas de Información Servicios de Intercambio de Información Implementados Sistemas de Información Optimizados
	OBJETIVO 3. • Fortalecer la seguridad y la eficiencia de la gestión interna, a partir del mejoramiento de las capacidades TI	SERVICIOS TECNOLÓGICOS • Fortalecer la gestión de los Servicios Tecnológicos	Arquitectura de Servicios Tecnológicos Plataforma Tecnológica eficiente para soportar los procesos
OBJETIVO 4. Definir con las entidades territoriales la implementación de la Ley 1448 de 2011, sus decretos reglamentarios y los Decretos de Ley	OBJETIVO 2. • Generar sinergias con las entidades involucradas en la atención a la población víctima y con terceros para contribuir a la transformación digital del Estado	GOBIERNO • Diseñar, implementar y mantener la Estrategia y el Gobierno de TI alineados a la Estrategia Institucional y del Sector Inclusión	Arquitectura Empresarial Implementar la Arquitectura Empresarial
OBJETIVO 5. Fortalecer la cultura de confianza colaboración e innovación para garantizar una atención digna respetuosa y diferencial	OBJETIVO 1. • Ofrecer soluciones tecnológicas para facilitar a las víctimas su interacción con la Unidad optimizando la gestión y el servicio. OBJETIVO 2. • Generar sinergias con las entidades involucradas en la atención a la población víctima y con terceros para contribuir a la transformación digital del Estado	USO Y APROPIACIÓN Diseñar, implementar y mantener el Uso y Apropiación de las Tecnologías de Información	Gestión de Cambio Cultural al interior y exterior de la Entidad Portafolio de productos y Servicios actualizado y disponible

Tabla 15. Correlación de Objetivos Estratégicos UNIDAD PARA LAS VÍCTIMAS y TI
Fuente. OTI - UNIDAD PARA LAS VÍCTIMAS

7.1.4. MATRIZ OBJETIVOS ESTRATÉGICOS DE TI / DOMINIOS / INICIATIVAS

La matriz de iniciativas definidas por cada uno de los objetivos estratégicos se presenta en el siguiente anexo.

ANEXO - MATRIZ DE INICIATIVAS.

7.2. GOBIERNO DE TI

Una vez definida la Estrategia de TI y los Objetivos Estratégicos de TI se establecen los elementos de control que conforman al Gobierno de TI para la situación objetivo o deseada (TO BE), a continuación se describen dichos elementos de control.

7.2.1. MARCO LEGAL Y NORMATIVO

La gestión de tecnología de la información y las comunicaciones de la Unidad tiene como marco legal las disposiciones del Estado a través del Ministerios de las Tecnologías de la Información y las Comunicaciones, en los siguientes y decretos:



- DECRETO 2482 / 2012 Artículo 3 sobre la implementación de “GEL” y “PETI”
- DECRETO 2573 / 2014 Artículo 3 definición de modelo de ARQUITECTURA EMPRESARIAL
- DECRETO 415/ 2016 Artículo 2.2.35.3 - OTROS LINEAMIENTOS PETI
- DECRETO 1008 / 2018 - Sobre transformación de GEL A GOBIERNO DIGITAL

7.2.2. POLÍTICAS DE TI

La Oficina de Tecnologías de la Información tiene definida de una parte la Política de Seguridad de la Información, sin embargo, es necesario cumplir con requerimientos de carácter nacional y universal, relacionados con políticas que den cubrimiento a los otros aspectos fundamentales de las tecnologías. En este sentido se define una política en el marco de la Estrategia Nacional de Gobierno Digital, cuyo alcance sea el grupo de ámbitos que conforman cada Dominio de la Arquitectura Empresarial.

ANEXO - POLITICAS DE TI

“POLÍTICA PARA LA IMPLEMENTACIÓN DE GOBIERNO DIGITAL QUE CONTRIBUYA A LA COMUNICACIÓN DIRECTA ENTRE LA UNIDAD PARA LAS VÍCTIMAS Y LAS VÍCTIMAS, LOS DIFERENTES ACTORES SOCIALES Y LAS PARTES INTERESADAS”.

  GOBIERNO DE COLOMBIA UNIDAD PARA LAS VÍCTIMAS	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018
			Página 92 de 127

1. CAPITULO - ESTRATEGIA DE TI

PROPÓSITO.

Direccionar el diseño, implementación y evolución de la Arquitectura Empresarial, así como asegurar su alineación con las estrategias y objetivos institucionales, sectoriales y nacionales.

LINEAMIENTOS

Para realizar una correcta implementación de esta política, es necesario aplicar lo relacionado con los siguientes lineamientos:

- Entendimiento estratégico
- Direccionamiento estratégico
- Implementación de la Estrategia TI
- Seguimiento y evaluación de la Estrategia TI

2. CAPITULO - GOBIERNO DE TI

PROPÓSITO

Definir las estrategias y prácticas apropiadas para la adopción del marco de la Arquitectura Empresarial y el gobierno de la gestión de TI requeridas por la Unidad.

LINEAMIENTOS

Para realizar una correcta implementación de esta política, es necesario aplicar lo relacionado con los siguientes lineamientos:

- Cumplimiento y alineación
- Esquema de Gobierno TI
- Gestión integral de proyectos de TI
- Gestión de la operación de TI

3. CAPITULO - GESTIÓN DE INFORMACIÓN



PROPÓSITO

Garantizar el apropiado diseño de los servicios de información, la gestión del ciclo de vida del dato el análisis de información y el desarrollo de capacidades para el uso estratégico de la misma.

LINEAMIENTOS

Para realizar una correcta implementación de esta política, es necesario aplicar lo relacionado con los siguientes lineamientos:

- Planeación y Gobierno de los Componentes de Información
- Diseño de los Componentes de Información
- Análisis y aprovechamiento de los Componentes de Información
- Calidad y Seguridad de los Componentes de Información

 	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018	Página 93 de 127

4. CAPITULO - SISTEMAS DE INFORMACIÓN

PROPÓSITO

Direccionar la planeación y diseño de la arquitectura de las aplicaciones así, como el ciclo de vida de los sistemas de información para garantizar el buen funcionamiento de los procesos institucionales de la Unidad.

LINEAMIENTOS

Para realizar una correcta implementación de esta política, es necesario aplicar lo relacionado con los siguientes lineamientos:

- Planeación y gestión de los Sistemas de Información
- Diseño de los Sistemas de Información
- Ciclo de vida de los Sistemas de Información
- Soporte de los Sistemas de Información
- Gestión de la calidad y seguridad de los Sistemas de Información

5. CAPITULO - SERVICIOS TECNOLÓGICOS

PROPÓSITO

Brinda la mayor eficacia y transparencia a la gestión de la infraestructura tecnológica que soporta los sistemas y servicios de información de la Unidad.

LINEAMIENTOS

Para realizar una correcta implementación de esta política, es necesario aplicar lo pertinente con los siguientes lineamientos:

- Arquitectura de Servicios Tecnológicos
- Operación de Servicios Tecnológicos
- Soporte de los Servicios Tecnológicos
- Gestión de la calidad y seguridad de los Servicios Tecnológicos

6. CAPITULO - USO Y APROPIACIÓN


PROPÓSITO

Crear una cultura de buen uso y apropiación de los recursos y procesos de tecnología de la Unidad por parte de los funcionarios y usuarios en general.

LINEAMIENTOS

Para realizar una correcta implementación de esta política, es necesario aplicar lo pertinente con los siguientes lineamientos:

- Definición de la Estrategia para el Uso y Apropiación de TI
- Gestión del cambio de TI
- Medición de resultados en el uso y apropiación

 	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018	Página 94 de 127

7.2.3. ESQUEMAS O INSTANCIAS PARA RELACIONAR O TOMAR DECISIONES

El Comité Directivo de la Unidad desarrolla temas relacionados con los servicios de tecnología necesarios para su gestión, de otra parte existe el Comité de Gestión y Desempeño Institucional con participación de las diferentes áreas de la entidad. En este escenario se deriva la Mesa de Gobierno Digital donde participan todas las áreas para abordar todos los temas tecnología de la Entidad, puesto que cada área es la propietaria de su proceso misional y la responsable de información que produce.

En relación con la OTI existen a manera de rol las funciones de nivel táctico representadas en los líderes de cada línea de servicio (Proyecto de Gobierno, Gestión Presupuestal, Sistemas de Información, Servicios Tecnológicos y Uso y Apropiación), es necesario formalizar una instancia de carácter táctico que complemente la línea de mando definida en los comités de instancias superiores. Este comité debe dar tratamiento a todos los temas de manera conjunta asignando responsabilidades por la línea de servicio y realizando seguimiento al cumplimiento de los requerimientos y compromisos.

7.2.4. ESTRUCTURA ORGANIZACIONAL - ROLES Y PERFILES DE TI

Como se presentó en el numeral 6.1.4 la estructura organizacional y de gobierno de TI en la UNIDAD PARA LAS VÍCTIMAS está conformada por una Jefatura de la Oficina de Tecnologías de la Información, 11 funcionarios de planta y 37 en la modalidad de prestación de servicios, adicionalmente por parte de los diferentes proveedores de servicios se cuenta con 6 colaboradores.



Al respecto y dado que las funciones están definidas de manera general y a veces diferentes a las actividades que se ejecutan, es necesario abordar un análisis sobre la estructura orgánica desde el punto de los roles asignados y las cargas de trabajo para cada línea de servicio.

Como aspecto importante es necesario realizar ejercicios para identificar problemáticas mediante ejercicios de Diagnóstico y Mejora de Clima Laboral.

7.2.5. RELACIONES CON OTRAS ÁREAS E INSTITUCIONES PÚBLICAS

Considerando los objetivos estratégicos de las entidades del sector, se ha creado una mesa de trabajo sectorial donde participa la OTI, con el propósito de realizar talleres coordinados por MINTIC a través de CINTEL (entidad contratada por el MINTIC para apoyar la implementación de la política de Gobierno Digital y sus modelos y lineamientos). Se han realizado algunos talleres para realizar ejercicios sobre la implementación de modelos de arquitectura empresarial y gestión de tecnologías dentro del marco de Gobierno Digital.

En relación con la SNARIV (Sistema Nacional de Atención y Reparación Integral a las Víctimas), se tiene como propósito la estandarización de información dado que los conjuntos de variables son diferentes entre las entidades, en este sentido se elaborará un documento de guía que

 	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018	Página 95 de 127

contemple la unificación de variables y de otra parte la definición de los lineamientos de referencia para protección de datos personales.

7.2.6. MODELO DE GESTIÓN DE PROYECTOS

La gestión presupuestal de la OTI tiene como marco de referencia el Modelo de Gestión de Proyectos de Inversión definido por el DNP, allí se da curso a las disposiciones de Gobierno Nacional en relación con la adquisición de productos, bienes y servicios, aplicando los Acuerdos Marco de Precios definido por el Estado, con base en los cuales también se realiza el seguimiento y monitoreo a todos los recursos adquiridos, es necesario definir una instancia que proporcione las directrices y lineamientos para la ejecución de los proyectos desde el punto de vista técnico y no solo de inversión, también elaborar o formalizar la metodología de evaluación de alternativas de solución y/o tendencias tecnológicas para la adquisición de servicios y/o soluciones de TI, cuando las adquisiciones no se tramitan por el Acuerdo Marco de Precios.

7.2.7. GESTIÓN DE PROVEEDORES y ANS

La OTI elabora un Plan Anual de Adquisiciones donde se registran todas las inversiones en materia de tecnología, es un solo proyecto debidamente registrado ante el DNP, conformado por actividades que son las inversiones por cada línea de servicios, la gestión de proveedores de cada una de las inversiones se realiza siguiendo las disposiciones del estado definidas en los Acuerdos Marco de Precios, allí se definen por cada bien o producto adquirido o contratado, los Acuerdos de Niveles de Servicios pertinentes y se realiza el seguimiento y monitoreo correspondiente elaborando mensualmente el reporte del estado de la gestión presupuestal, de otra parte la información relacionada con el proyecto es registrada en SISGESTION - Sistema para la Formulación y Seguimiento a la Planeación Institucional y en el SECOP – Sistema Electrónico de Contratación Pública.

Se tienen las siguientes modalidades de contratación:

- Acuerdo Marco de Precios
- Contratación Directa
- Prestación de Servicios
- Agregación de Demanda
- Traslado de Proyecto
- Traslado Área
- Selección Abreviada Menor Cuantía
- Subasta Inversa Electrónica

7.2.8. INDICADORES DE GESTIÓN DE TI

En relación con la gestión de la Oficina de Tecnologías de la Información se han definido y registrado en SISGESTION los siguientes indicadores:

- Porcentaje de ejecución mensual de proyectos TI con impacto misional ejecutados por demanda
- Porcentaje de solicitudes tecnológicas mensuales atendidas oportunamente
- Porcentaje de desarrollos mensuales por demanda priorizada de sistemas de información
- Porcentaje de cumplimiento de planes de trabajo para implementar ANS en la herramienta
- Nivel de implementación bimensual del plan estratégico de tecnologías de la información (PETI)
- Porcentaje de implementación mensual del Sistema de Gestión de Seguridad de la Información
- Porcentaje de cumplimiento del plan de migración a IPv6
- Numero de servicios de consulta y trámites de atención a la Víctima
- Inventario de activos de información actualizado.

Estos indicadores en general permiten medir el cumplimiento y uso de los recursos. Se deben definir indicadores relacionados con la calidad y satisfacción de los productos, servicios y proyectos de cada línea de servicio.

7.2.9. CADENA DE VALOR

Teniendo como foco principal la misión a cumplir y los objetivos estratégicos a lograr, la Cadena de Valor de TI considera el Sistema Integrado de Gestión y el enfoque definido por el Estado para el Gobierno Digital de las entidades, de esta forma va en procura de atender los requerimientos de la sociedad y del estado, para contribuir a la integración de las víctimas y a una informática de valor.





Gráfica 48 Cadena de Valor PETI
Fuente: OTI – Gobierno Digital

7.2.10. GESTIÓN DE RIESGOS

A partir de la metodología para la Administración de Riesgos definida en la Unidad, para la vigencia de 2018 se han identificado 10 riesgos para el Proceso Gestión de la Información cuya responsabilidad está distribuida de la siguiente de forma:

Riesgos 1 y 2 Oficina de Tecnologías de la Información
Riesgos 3 y 4 Subdirección Red Nacional de Información
Riesgos 5 al 10 Seguridad de la Información.

La matriz de riesgos y controles, las tablas de valoración de riesgos y las tablas de evaluación de

 GOBIERNO DE COLOMBIA  UNIDAD PARA LAS VÍCTIMAS	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018
			Página 97 de 127

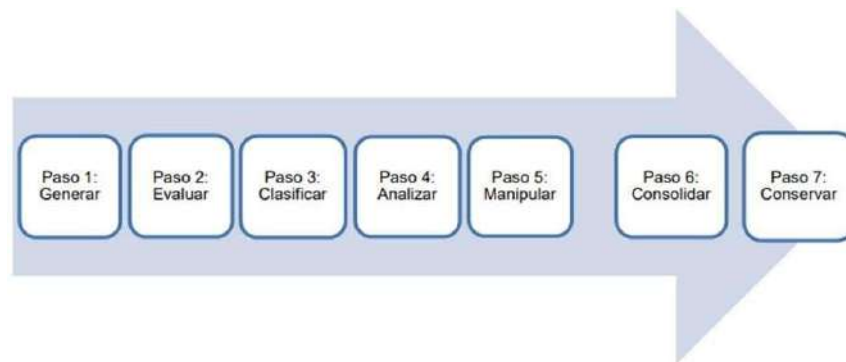
controles se encuentran en el siguiente anexo

ANEXO – MAPA DE RIESGOS

7.3. GESTIÓN DE INFORMACIÓN

Con el propósito de fortalecer la gestión de información y la calidad de datos, las actividades que en este sentido se han venido desarrollando, como son: la mesa de interoperabilidad de la RNI con otras entidades, la mesa de interoperabilidad de la OTI con otras dependencias de la Unidad, el proyecto de depuración de información que adelanta la Subdirección de Valoración y Registro, se deben alinear con los modelos definidos por el MINTIC, en relación con temas como Calidad de Datos evaluando el ciclo de vida del dato y los flujos que sigue, tanto a la información de la víctima como a la información de la Unidad.

Esta evaluación permite determinar en qué puntos es necesario aplicar la gestión de la calidad de los datos y la información como se observa en la siguiente gráfica:



Gráfica 49. Diagrama del Ciclo del Dato

Fuente: Guía Técnica de Información - Ciclo de vida del dato - MINTIC



En el paso 1 (Generar) se identifican las fuentes de información, en el paso 2 (Evaluar) se evalúa la pertinencia y calidad inicial del dato para gestionarla durante las etapas posteriores del ciclo de vida, se realiza la siguiente actividad dentro del plan de calidad:

- Evaluar criterios y campos críticos para calidad del dato.
- Evaluar situaciones que implican depuración del dato (apoyándose en herramientas de perfilamiento y en el conocimiento del negocio).
- Evaluar capacidad para gestión de calidad del dato.
- Enmascaramiento de datos: Evaluar situaciones que implican enmascaramiento del dato, en especial, debido a reglas de protección de información

En el paso 3 (Clasificar), se realiza una clasificación de los datos según el flujo de los procesos y por los criterios como si es alfabético, tiempo de publicación, acceso y modificación.

En el paso 4 (Analizar), se analizan los criterios, campos críticos, y necesidades de depuración pertinentes en la calidad para gestión del ciclo de vida

En el paso 5 (rediseño de procesos), se Implementan tareas para el aseguramiento y depuración de calidad durante el ciclo de vida del dato.

 GOBIERNO DE COLOMBIA  UNIDAD PARA LAS VÍCTIMAS	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018
			Página 99 de 127

En el paso 6 (consolidar), se cargan los datos teniendo en cuenta que la reducción de campos, tipos, y valores, no afecte las cifras ni variables tratadas en los consolidados.

Finalmente, el paso 7 (Conservar), se trata de mantener de forma consistente y completa la información para fines de continuidad, replicación y análisis histórico.

Adicionalmente se debe definir una política y procedimiento para la Gestión de Información.

7.3.1. HERRAMIENTAS DE ANÁLISIS

La Unidad cuenta con herramientas para análisis de información y gestión de bodegas de datos – inteligencia de negocios que no ha sido debidamente aprovechadas por las diferentes áreas y niveles de la Entidad, en ese sentido se debe fortalecer la sensibilización y motivación complementando el Plan Institucional de Capacitación. Se deben incluir temas y herramientas relacionadas, como Sistemas de Información Geográfica, herramientas para inteligencia de negocios como Power – BI.

7.3.2. ARQUITECTURA DE INFORMACIÓN

Durante el año 2017 la Unidad inició labores en torno al tema de arquitectura empresarial logrando un esquema general de flujos de información dando un primer paso hacia una arquitectura de información. Teniendo en cuenta que la estrategia es la de realizar ejercicios de arquitectura,

Se debe tener en cuenta que la formulación e implementación de la Arquitectura Empresarial es un ejercicio gradual y continuo, por lo tanto, se iniciará esta definición según las directrices estratégicas que se impartan desde la alta dirección.,

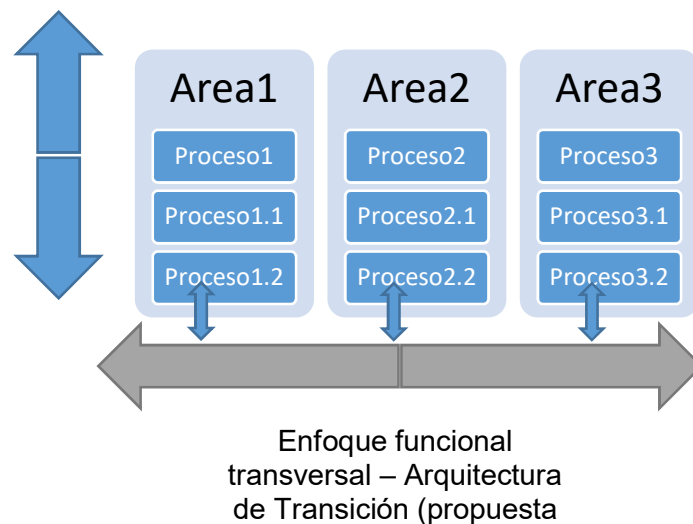
7.3.3. NECESIDADES DE INFORMACIÓN

Considerando que existen diferentes dependencias generadoras de información que hacen procesamiento, y que han venido utilizando diferentes metodologías y técnicas de desarrollo, se debe definir una única Arquitectura de Información para toda la entidad , también definir una política para gestión de información asignando responsables dependiendo de la categoría de la información. De otra parte, elaborar un Catálogo de componentes de información y definir un protocolo de gestión considerando datos (de uso internos y abiertos), flujos de información, sistemas de información y servicios de publicación. En relación con la integración con otras entidades desarrollar los diagramas y protocolos de interoperabilidad y definir un protocolo o procedimiento para la generación, actualización y control de publicación de datos abiertos y dar aplicación a la política de datos abiertos definida por el MINTIC.

7.4. SISTEMAS DE INFORMACIÓN

7.4.1. ARQUITECTURA DE SISTEMAS DE INFORMACIÓN

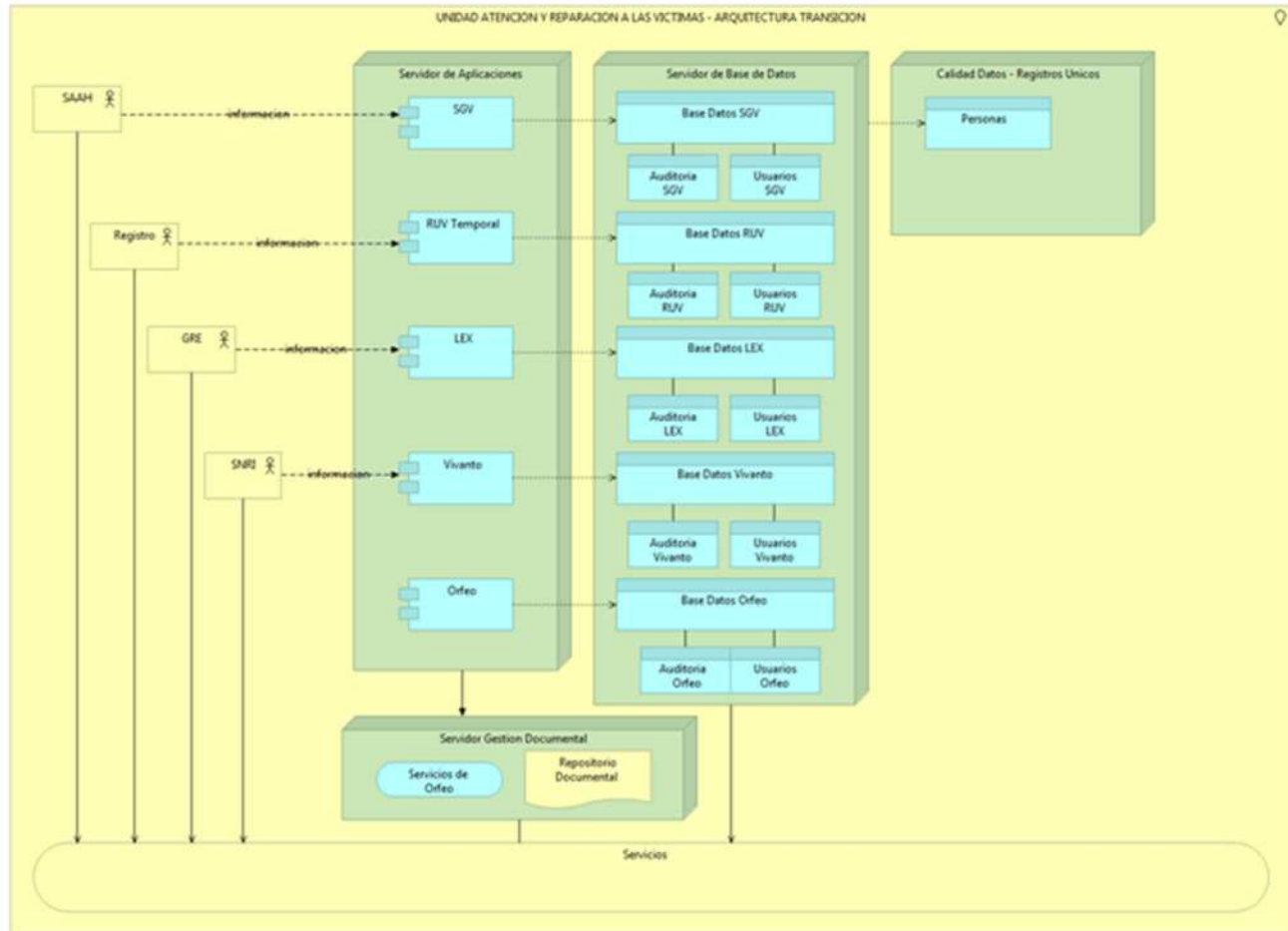
Se debe realizar un análisis de arquitectura que permita garantizar la ejecución efectiva de los objetivos estratégicos de la Unidad de Víctimas y que, de forma sinérgica y casi automática, este en constante crecimiento con el negocio, interpretando los desarrollos que en materia de Arquitectura empresarial se obtengan, la arquitectura de los sistemas de información debe reflejar la visión de empresa y de proceso en un esquema de alto nivel de cohesión e interoperabilidad y disponibilidad garantizando y/o mejorando los flujos de información, evitando la creación y mantenimiento de soluciones desacopladas o redundantes.



Gráfica 50 Enfoque Transversal Arquitectura de Información
Fuente: Grupo de Sistemas de Información - OTI

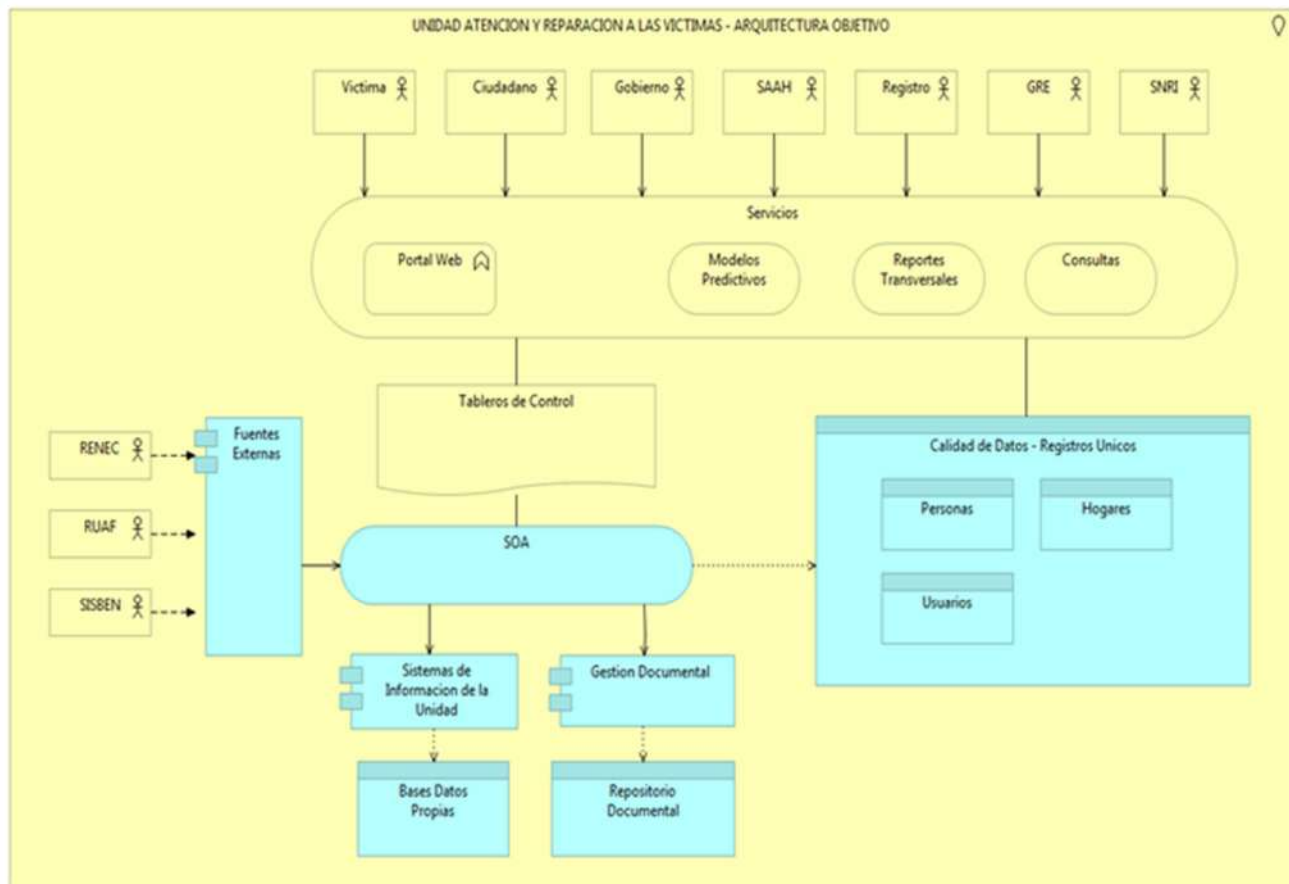
En propósito de lograr la Arquitectura Objetivo dentro del proceso de transformación o mejoramiento, es común que se presenten puntos intermedios en el camino hacia la Arquitectura Objetivo por ello se debe definir una Arquitectura de Transición, que incluye los elementos de las arquitecturas de información, sistemas de información y de servicios tecnológicos que deben ser modificados. La utilización de puntos intermedios permite la implementación de mapas de ruta por etapas, lo que disminuye riesgos y facilita su gestión.

Se presentan a continuación los esquemas de la Arquitectura de Transición y de la Arquitectura Objetivo.



Gráfica 51. Diagrama de la Arquitectura de Transición

Fuente: Arquitectura de Referencia – Grupo de Sistemas de Información OTI - UNIDAD PARA LAS VÍCTIMAS





Gráfica 52. Diagrama de la Arquitectura Objetivo
Fuente: Arquitectura de Referencia – Grupo de Sistemas de Información OTI

Son metas de la gestión de arquitectura de sistemas de información dentro del plan estratégico de sistemas las siguientes:

- Mejorar la gestión de los recursos invertidos en prestación del servicio y calidad del sector de inclusión social; con el fin de elevar los resultados en materia de acceso, calidad y eficiencia.
- Mejorar la gestión de los recursos invertidos por la unidad en la atención a las personas víctimas de la violencia en Colombia.
- Fortalecer la gestión de las unidades territoriales en cuanto al servicio de información y comunicación eficiente con la víctima.
- Mejorar la información puesta a disposición de las personas y familias víctimas.
- Aumentar la transparencia de la información del sector de inclusión, haciéndola accesible a sectores más amplios.

Así mismo, por cada uno de los segmentos de la solución de arquitectura objetivo se proponen y dentro de cada uno se identifica una meta general:

- Para el segmento de Arquitectura empresarial: Consolidar las bases para desarrollar la

 	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018	Página 103 de 127

capacidad de arquitectura empresarial a través de la propuesta del modelo de adaptación del marco de arquitectura de la Unidad, que adapta la propuesta del decreto 253 de MinTIC respecto al marco de Arquitectura TI Colombia.

- Para el segmento de Información: desarrollar un modelo de consolidación de la información, bajo una estructura general definida a través de registros únicos establecidos en el pliego de condiciones.
- Para el segmento Sistemas de Información: proponer un roadmap de implementación viable para desarrollar e implementar el estado futuro propuesto para los sistemas de información de la UNIDAD que están relacionados con los registros únicos.

7.4.2. METODOLOGÍA DE DESARROLLO


En razón a necesidad de dar al servicio soluciones de informáticas en las que se requiere controlar el ciclo de vida de desarrollo de software, y en virtud de que los tiempos de implementación son cortos, se debe mejorar el nivel de madurez en la opción de la metodología SCRUM como referente para ofrecer soluciones de manera ágil, además se debe mejorar y mantener el procedimiento de desarrollo de aplicaciones como procedimiento alineado al Sistema Integrado de Gestión de la Unidad, haciendo que el mismo sea vinculante con los lineamientos y mejores prácticas que en materia de desarrollo de software se den por parte del Estado Colombiano y los estándares de la industria, asegurando que el conocimiento y experiencia de los grupos de trabajo mejore, obteniendo beneficios en términos de tiempo y oportunidad. De otra parte, la administración del ciclo de vida de las aplicaciones y sus artefactos se debe continuar realizando con herramientas especializadas como Microsoft Team Foundation Server - TFS (archivos de código, compilados, ejecutables, documentación, scripts de base de datos, etc.), haciéndola extensiva a todos los equipos de trabajo que participan del ciclo de desarrollo de software dentro de la Unidad, para ello se debe fortalecer la capacitación en la metodología de desarrollo SCRUM y el manejo de herramientas como TFS estandarizando su aplicación para los nuevos desarrollos requeridos por la Unidad.

7.5. MODELO DE GESTIÓN DE SERVICIOS TECNOLÓGICOS

7.5.1. ARQUITECTURA DE SERVICIOS TECNOLÓGICOS

Considerando la Infraestructura del Centro de Datos actual (nube privada y eventual nube publica) y los esquemas de operación de los diferentes servicios tecnológicos como mesa de ayuda, soporte en sitio y soporte a aplicaciones, se debe diseñar e implementar una arquitectura para la infraestructura y otra para todos los servicios existentes, conformado así una vista en dos arquitecturas relacionadas (Infraestructura y Servicios).

7.5.2. INFRAESTRUCTURA Y CRITERIOS DE CALIDAD

 	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018		
	OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018
			Página 104 de 127

- **CENTRO DE DATOS**

Corresponde a la gestión de servidores, almacenamiento de información y dispositivos de backup, se cuenta con un total de 73 servidores virtuales. Se tiene como propósito reducir el número de servidores para llegar a un total de 60 optimizando su utilización y operación. Como acción de mejora se debe incluir en los Acuerdos de Niveles de Servicio con el proveedor de Centro de Datos el envío de correos electrónicos a la Unidad (Línea de Servicio Infraestructura) cuando se presenten interrupciones o caídas del sistema.

- **SISTEMAS DE ALMACENAMIENTO**

Se debe realizar depuración continua sobre la información almacenada en las bases de datos, igualmente definir y aplicar criterios de clasificación para optimizar medios de almacenamiento, esto conlleva a crear un protocolo para la gestión de los sistemas y recursos de almacenamiento.

- **RECUPERACIÓN DE DESASTRES Y CONTINUIDAD**

En los contratos celebrados con el Centro de Datos – Infraestructura no se tiene como producto un Plan de Recuperación de Desastres, por lo tanto por acción propia de la Unidad o mediante contratación a un tercero se debe implementar un plan de gestión de capacidad, continuidad, disponibilidad y seguridad de los servicios tecnológicos, que de alcance a todos los procesos y recursos de infraestructura, dotación tecnológica y sistemas de información con alcance a todos los recursos, es decir, servidores pertenecientes y no pertenecientes al Centro de Datos, equipos de escritorio, recurso humano, software en general e instalaciones. Adicionalmente se deben ejecutar fases de pruebas parciales, totales y simulacros.



7.5.3. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En relación con la Seguridad de la Información se ejecutará un Plan de Seguridad y Privacidad en donde todas las actividades definidas están fundamentadas legalmente en decretos o leyes, dichas actividades son:

- **POLÍTICAS DE SEGURIDAD DE INFORMACIÓN**

Por medio de la resolución 740 de noviembre de 2014, se adoptaron las políticas de Seguridad de la Información para todos los usuarios que accedan a servicios de información de la Unidad, utilicen equipos informáticos y de comunicaciones, interactúen con herramientas tecnológicas y/o ingresen de manera física o lógica a las instalaciones de la Unidad.

- **LEVANTAMIENTO DE INVENTARIOS DE ACTIVOS DE INFORMACIÓN**

 	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN		
	PETI – 2018		
	OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
PROCESO: GESTIÓN DE LA INFORMACIÓN			
CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018	Página 105 de 127

Durante enero de 2018 se realizó el levantamiento de los activos de información con base en el procedimiento de “Inventario de activos de información” de gestión documental, de esta forma se da cumplimiento a lo establecido en la Ley 1712 de 2014, y se logra la identificación, clasificación y valoración de criticidad de activos tipo información, software y hardware, generando y publicando los siguientes productos:

- ✓ Registro de activos
- ✓ Índice de información clasificada o reservada
- ✓ Esquema de publicación

Se tiene un Inventario de Recursos Tecnológicos de la OTI y parte de Almacén otro Inventario de Bienes de la Unidad, en el inventario de la OTI se tienen los activos de información en relación con los datos y el software de cada proceso misional, pero no se tiene aún lo relacionado con los equipos ni los recursos de centro de datos. Es necesario definir un único inventario de activos de información y fortalecer la gestión de activos de información en relación con la política, protocolo de gestión, técnicas de monitoreo y medición.

- **COMPLEMENTAR LA MATRIZ DE RIESGOS DE TI**

La Oficina de Tecnologías de la Información generó la matriz de riesgos de seguridad de la información, con un total de 11 riesgos siguiendo la Metodología de Administración Gestión de Riesgos de la Unidad. Al respecto es importante realizar un estudio sobre la pertinencia de la metodología utilizada para la Gestión de Riesgos de Seguridad dado el concepto de la Oficina de Control Interno en el sentido de no combinar en una misma matriz de riesgos de seguridad y riesgos de los otros subsistemas del Sistema Integrado de Seguridad. De otra parte, complementar dicha matriz con riesgos de TI relacionados con otros recursos y criterios de tecnología y no solo de Seguridad de la Información.

- **PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN**

En el marco de la metodología de riesgos establecida por la Oficina Asesora de Planeación de la Unidad para la Atención y Reparación Integral a las Víctimas, en el año 2017 se construyeron los planes de tratamiento respectivos.

- **PLAN DE SOCIALIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN**

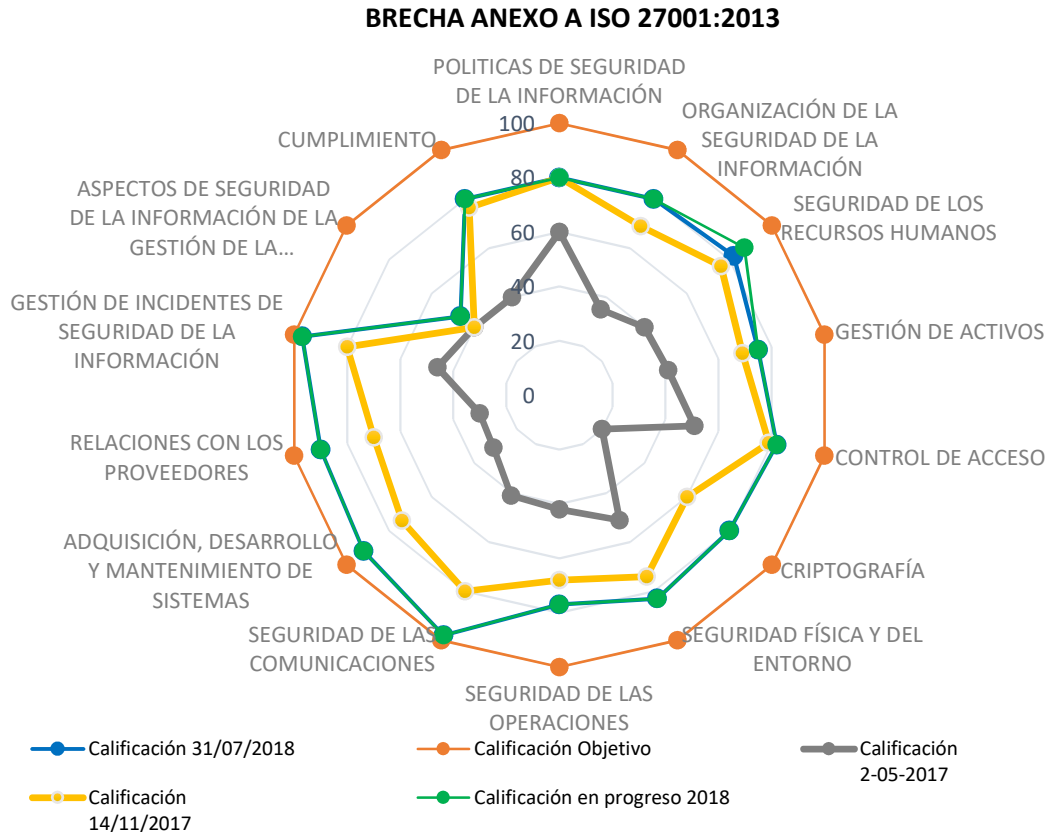
La Oficina de Tecnologías de la Información en el año 2017, estableció y ejecutó un plan de sensibilización, mediante el cual se generaron mensajes masivos en el portal web de la Unidad a través de SUMA como herramienta de publicaciones de la Oficina Asesora de Comunicaciones. Se debe considerar en el dominio de Uso y Apropiación las actividades para aplicar o articular este Plan de Socialización de tal forma que sea permanente.

- **MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

La Oficina de Tecnologías de la Información en el año 2017, realizo evaluaciones a la

implementación del Modelo de Seguridad y Privacidad de la Información del MINTIC – MSPI, obteniendo como resultado el 41 % de cumplimiento en la primera medición y el 71 % en la segunda del mes de noviembre el mismo año.

En el año 2018, se ha logrado el cumplimiento del 82% del modelo, a corte 31 de octubre de 2018:



Grafica 53. Modelo de Seguridad y Privacidad de la Información.



Fuente: Plan de Seguridad y Privacidad de la Información de la UNIDAD PARA LAS VÍCTIMAS

7.5.4. CONECTIVIDAD

- **IPV4 A IPV 6**

La conectividad a distancia está basada en una red privada de comunicaciones MPLS mediante la cual se accede desde cualquiera de las sedes de la unidad en el país, a las diferentes aplicaciones que se encuentran alojadas en los servidores del centro de datos.

Para la conectividad local cada sede o centro regional de la Unidad cuenta con un centro de cableado y una red local que conecta todos los computadores que se encuentran en operación. En cumplimiento de los requerimientos de Gobierno y para obtener una mayor eficiencia en las comunicaciones, se debe realizar la transición del protocolo de comunicaciones de IPV4 a IPV6

 	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018

para este propósito la Unidad adelanta un proyecto para realizar el análisis, diseño, desarrollo e implementación del plan de transición del protocolo IPv4 a IPv6, su puesta en funcionamiento en la red de comunicaciones, así como la operatividad de los servicios y los aplicativos de la UNIDAD DE ATENCIÓN Y REPARACIÓN A LAS VÍCTIMAS sobre el nuevo protocolo IPv6.

Se debe dar aplicación a la normatividad de Gobierno Nacional para la implementación del protocolo IPV6 definida en las siguientes disposiciones:

- ✓ Resolución 2710 de 2017 de MINTIC
- ✓ Guía de Aseguramiento del Protocolo IPv6 Seguridad y Privacidad de la Información
- ✓ Guía de Transición IPv4 a IPv6 para Colombia

Las siguientes matrices contienen la lista de los servidores del Centro de Datos y la Infraestructura Central Telefónica que serán objeto de la transición de IPV4 a IPV6

SERVIDORES DE CENTRO DE DATOS				
No. SERVIDOR	NOMBRE	O.S	MEMORIA	VCPU
1	IFX01	Windows Server 2012 R2 Standart 64 Bits	4	2
2	IFX02	Windows Server 2012 R2 Standart 64 Bits	4	2
3	TM500005	Windows Server 2008 R2 Enterprise 64 Bits SP1	60	16
4	TM00006	Windows Server 2008 R2 Enterprise 64 Bits SP1	60	16
5	TM52020007	Windows Server 2008 R2 Enterprise 64 Bits SP1	32	8
6	TN0200008	Windows Server 2008 R2 Enterprise 64 Bits	12	8
7	TM5200009	Windows Server 2008 R2 Enterprise 64 Bits SP1	32	8
8	TM200010	Windows Server 2008 R2 Enterprise 64 Bits SP1	32	8
9	TM502200150	Windows Server 2012 R2 Standart 64 Bits	12	8
10	TM0200012	Windows Server 2008 R2 Enterprise 64 Bits SP1	32	8
11	TM502200013	Windows Server 2012 R2 Standart 64 Bits SP1	12	8
12	TM512200014	Windows Server 2008 R2 Enterprise 64 Bits SP1	12	8
13	TM512200015	Windows Server 2008 R2 Enterprise 64 Bits SP1	32	8
14	TM502200021	Windows Server 2008 R2 Enterprise 64 Bits SP1	32	8
15	TM50200026	Windows Server 2008 R2 Enterprise 64 Bits SP1	12	12
16	TM50034	Windows 2003 Server Enterprise SP2	4	2
17	TM200035	Windows Server 2008 R2 Enterprise 64 Bits SP1	32	24
18	TM2200037	Windows Server 2008 R2 Enterprise 64 Bits SP1	12	12
19	TM2200038	Windows Server 2008 R2 Enterprise 64 Bits SP1	12	12
20	TM00039	Windows Server 2008 R2 Enterprise 64 Bits SP1	12	8
21	TM500011	Windows Server 2008 R2 Enterprise 64 Bits SP1	12	8
22	TM502200047	Windows Server 2012 R2 Standart 64 Bits	24	12
23	TM502200048	Windows Server 2012 R2 Standart 64 Bits	32	8
24	TM502200052	Windows Server 2008 R2 Enterprise 64 Bits SP1	32	8
25	TM502200063	Windows Server 2012 Standard	60	16
26	TM527200064	Windows Server 2012 Datacenter	12	12
27	TM502200065	Windows Server 2012 Datacenter	32	8
28	TM00066	Windows Server 2008 R2 Enterprise 64 Bits SP1	12	12
29	TM00067	Windows Server 2012 Datacenter	12	12
30	TM5200068	Windows Server 2012 Datacenter	12	12
31	TM00069	Windows Server 2008 R2 Enterprise 64 Bits SP1	12	12
32	TM500200072	Microsoft Windows Server 2012 Datacenter	8	4
33	TM502200073	Microsoft Windows Server 2012 Datacenter	12	8
34	TM7200076	Microsoft Windows Server 2008 R2 Enterprise SP1	12	2
35	TM502200077	Microsoft Windows Server 2008 R2 Enterprise SP1	12	8
36	TM501200086	Microsoft Windows Server 2012 Datacenter	12	8
37	TM501200087	Microsoft Windows Server 2012 Datacenter	12	12
38	TM520200102	Microsoft Windows Server 2012 Standard	12	12
39	TM520200103	Microsoft Windows Server 2012 Standard	12	12
40	WIN2012STD	Microsoft Windows Server 2012 Standard	12	12
41	TM5022000105	Microsoft Windows Server 2012 Standard	6.36	12
42	TM501200107	Microsoft Windows Server 2012 Standard	24	12
43	TM501200109	Microsoft Windows Server 2012 Standard	12	12
44	TM502200110	Microsoft Windows Server 2008 R2 Standard SP1	16	8
45	TM2200111	Microsoft Windows Server 2012 Standard	16	8
46	TM502200113	Microsoft Windows Server 2012 R2 Standard	12	12
47	TM501200119	Microsoft Windows Server 2012 Datacenter	12	12
48	TM501200120	Microsoft Windows Server 2012 Datacenter	12	12
49	TM501200108	Microsoft Windows Server 2012 Standard	60	16
50	TM502200128	Microsoft Windows Server 2012 Standard	16	12
51	TM502200129	Microsoft Windows Server 2012 Standard	16	12
52	TM502200130	Microsoft Windows Server 2012 Standard	16	12
53	TM000135	Microsoft Windows Server 2008 R2 Enterprise SP1	24	8
54	TM520200137	Microsoft Windows Server 2008 R2 Enterprise SP1	32	8
55	TM518200002	Microsoft Windows Server 2012 R2 Standard	3.76	8
56	TM502200151	Microsoft Windows Server 2008 R2 Standard	12	8
57	TM520200152	Microsoft Windows Server 2008 R2 Enterprise SP1	12	8
58	TM502200154	Microsoft Windows Server 2008 R2 Standard	16	12
59	TM502200173	Microsoft Windows Server 2012 Datacenter	12	8
60	TM502200195	Microsoft Windows Server 2008 R2 Enterprise SP1	32	8
61	TM502210197	Microsoft Windows Server 2008 R2 Enterprise SP1	12	8
62	TM502200198	Microsoft Windows Server 2008 R2 Enterprise SP1	32	8
63	TM502200199	Microsoft Windows Server 2008 R2 Enterprise SP1	12	12
64	TM502200200	Microsoft Windows Server 2008 R2 Enterprise SP1	60	16
65	TM520200201	Microsoft Windows Server 2008 R2 Standard SP1	12	8
66	TM502200202	Microsoft Windows Server 2008 R2 Enterprise SP1	16	8
67	TM502200203	Microsoft Windows Server 2012 R2 Standard	12	24
68	TM502200204	Microsoft Windows Server 2012 R2 Standard	12	8
69	TM502200205	Microsoft Windows Server 2012 R2 Standard	12	8
70	TM520200207	Microsoft Windows Server 2012 R2 Standard	4	8
71	TM520200208	Microsoft Windows Server 2012 R2 Standard	4	8
72	TM520200209	Microsoft Windows Server 2012 R2 Standard	4	8
73	TM520200210	Microsoft Windows Server 2012 R2 Standard	4	8

INFRAESTRUCTURA CENTRAL TELEFONIA

Localidad	Función	Sistema Operativo	Fabricante	Hardware Type	MAC Address
Bogota Avianca	OpenScape Voice Int Simplex	SLES11SP2	IBM	IBM 3550 M2	34:40:B5:A1:35:88
Bogota Avianca	OpenScape Xpressions	WIN2K8 R2 Server	IBM	IBM 3250 M4	34:40:B5:89:68:44
Bogota Avianca	OpenScape Center Extension	WIN2K8 R2 Server	IBM	IBM 3550 M3	6C:AE:8B:6B:10:CE
Bogota Avianca	OpenScape SBC	Linux	IBM	IBM 3250 M4	6C:AE:8B:15:0A:E6
Bogota Avianca	OpenScape Branch 1000	Linux	IBM	IBM 3250 M4	5C:F3:FC:F2:FA:D5
Bogota Avianca	Tarificador PCSistel	WIN2K8 R2 Server	IBM	IBM 3250 M4	34:40:B5:88:20:42
Bogota Avianca	OSO_LX (Sesap)	Linux	IBM	IBM 3250 M4	34:40:B5:88:E9:46
Bogota Cundinamarca	Gateway FXO		Media Corp	Media trix 1204	00:90:F8:08:3A:A1
Bogota Parque Santander P3	OpenScape Branch 250	Linux	Advantech	SYS-2USM02-6M01E	00:0B:AB:31:51:29
Bogota Afinsa	OpenScape Branch 250	Linux	Advantech	SYS-2USM02-6M01E	00:0B:AB:31:51:73
Bogota Parque Santander P4	OpenScape Branch 50i A84	Linux	Advantech	SYS-2USM02-6M01E	00:0B:AB:31:8E:CE
Bogota Fontibon	OpenScape Branch 250	Linux	Advantech	SYS-2USM02-6M01E	00:0B:AB:31:50:6B
Bogota Calle Real	OpenScape Branch 50i A84	Linux	Advantech	SYS-2USM02-6M01E	00:0B:AB:31:8E:32
Bogota Bavaria	OpenScape Branch 50i A84	Linux	Advantech	SYS-2USM02-6M01E	00:0B:AB:31:87:FC
Bogota Cundinamarca	OpenScape Branch 250	Linux	Advantech	SYS-2USM02-6M01E	00:0B:AB:31:52:13
Medellin	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:50:83
Cali	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:4C:4F
Bucaramanga	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:4D:E3
Pasto	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:50:A9
Pereira	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:4C:7F
Popayan	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:4B:8B
Cartagena	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:4F:87
Villavicencio	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:58:C1
Santa Marta	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:4B:F5
Barranquilla	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:4E:83
Valledupar	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:4A:85
Monteria	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:7A:12
Cucuta	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:4B:1F
Quibdo	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:85:5E
Florencia	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:4B:EF
Barrancabermeja	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:4B:E9
Sincelejo	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:4F:25
Apartado	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:7B:D8
Mocoa	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:4C:75
Manizales	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:89:4A
Ibague	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:89:98
Rioacha	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:93:88
Yopal	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:87:3E
San Jose del Guaviare	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:8E:BE
Puerto Carreño	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:89:A4
Tunja	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:93:A6
Armenia	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:7F:9E
Neiva	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:89:90
Puerto Inirida	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:86:50
Arauca	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:92:36
Mitu	OpenScape Branch 50i A84	Linux	Advantech 50i (FXO - FXS)	SYS-2USM02-6M01E	00:0B:AB:31:80:3A

7.5.5. SERVICIOS DE OPERACIÓN

Al respecto se deben definir y/o fortalecer las políticas relacionadas con la Gestión de Servicios Tecnológicos y lo siguientes aspectos:

- **INFRAESTRUCTURA**
 - GESTIÓN DE CONTINGENCIAS
 - ADMINISTRACIÓN DE BASES DE DATOS
 - GESTIÓN DE INCIDENTES
 - GESTIÓN DE MONITOREO
 - GESTIÓN DEL ALMACENAMIENTO
 - GESTIÓN DE COPIAS DE SEGURIDAD
 - GESTIÓN DE ASIGNACIÓN DE RECURSOS

- **SERVICIOS TECNOLÓGICOS**
 - GESTIÓN DE CORREO ELECTRÓNICO
 - GESTIÓN DE TELEFONÍA IP
 - GESTIÓN DE DNS
 - GESTIÓN DE DIRECTORIO ACTIVO
 - GESTIÓN DE ANTIVIRUS Y ANTISPAM
 - GESTIÓN DE SERVICIOS DE IMPRESIÓN

Las políticas para definir e implementar deben ser la base para la actualización y socialización del Catálogo o Directorio de Servicios Tecnológicos.

7.5.6. MESA DE SERVICIOS

A partir de las buenas prácticas ITIL que se aplican en la Gestión de la Mesa de Ayuda en relación con el soporte que se brinda a todos los servicios (dotación tecnológica, soporte a aplicaciones, mantenimientos preventivos, entre otros), se formulará un plan de gestión de niveles de servicios que permita fortalecer las diferentes operaciones de servicios tecnológicos y determinar la eficacia implementando métodos de monitoreo y seguimiento. Este plan comprende un diagnóstico para identificar la situación de madurez actual y de allí determinar las acciones de mejoramiento para llegar a la situación deseada de servicios con alcance a todos los recursos (procedimientos, recurso humano, software de apoyo, arboles de decisión, escalamiento, servicios de oficina, entre otros).

7.5.7. PROCEDIMIENTOS DE GESTIÓN

En relación con las operaciones de la gestión tecnológica se deben considerar los siguientes procedimientos que complementan los definidos en el Sistema Integrado de Gestión.

- Procedimiento para Gestión de Incidentes
- Procedimiento para Gestión de Cambios Tecnológicos (Infraestructura, comunicaciones)
- Procedimiento para Gestión de Continuidad

7.6. USO Y APROPIACIÓN

Aunque se han adelantado acciones de sensibilización y socialización para las soluciones con componentes tecnológicos, es necesario formular y formalizar una estrategia para Uso y Apropiación en donde se consideren aspectos como:

- Productos y servicios que se prestan
- Herramientas que se utilizan
- Recursos humanos financieros y técnicos
- Estadísticas sobre uso de tecnología al interior UV
- Indicadores cuantitativos y cualitativos
- Encuestas y cuestionarios
- Plan de Comunicaciones



De otra parte, se debe medir el impacto a partir de instrumentos que permitan valorar el nivel de aceptación de la tecnología al interior de la entidad; para ello, se formularán indicadores de uso y apropiación conforme el lineamiento LI.UA.07 Evaluación del nivel de adopción de TI.

Como parte de las actividades de adopción del Marco de Referencia de la Arquitectura de TI Colombia, se realizará un diagnóstico del estado de uso y apropiación de herramientas tecnológicas en la entidad, se hará la identificación, clasificación y priorización de los grupos de interés impactados con la implementación de las iniciativas de TI a ejecutar en el marco de la implementación del PETI, se formulará una estrategia para la gestión del cambio en proyectos de TI y se actualizarán los catálogos de componentes de información² según los actuales lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones.

De otra parte se formulará el Plan de Uso y Apropiación, el cual incluirá el Plan de entrenamiento, capacitación y sensibilización de TI, el cual, de la mano con el Plan Institucional de Capacitación, establecerá un orden y estrategia para la divulgación del conocimiento tecnológico con el objetivo de desarrollar habilidades que faciliten el cumplimiento de los objetivos misionales de la entidad. Una de las iniciativas propuestas debe ser incorporar al Plan de Capacitación Institucional, en las jornadas de inducción y reinducción, el tema de la estrategia de Gobierno Digital, con el fin de que al interior de la Entidad se alcance un alto nivel de apropiación de los temas que conforman la estrategia, de otra parte una estrategia de comunicación permanente, a través de los medios tecnológicos disponibles, intranet, SUMA, carteleras digitales, etc.

7.6.1. ESTRATEGIA PARA USO Y APROPIACIÓN

La respuesta a los nuevos retos y desafíos que enfrentamos claramente tiene un efecto directo sobre la calidad de nuestros productos y servicios; y está a su vez íntimamente ligada al buen uso de las tecnologías y a una mejor cualificación de nuestros funcionarios y contratistas, por lo cual es indispensable la incorporación y/o fortalecimiento de habilidades, competencias y conocimiento.

 GOBIERNO DE COLOMBIA  UNIDAD PARA LAS VÍCTIMAS	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018		
	OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
PROCESO: GESTIÓN DE LA INFORMACIÓN			
CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018	Página 112 de 127

Tomando como línea base la encuesta realizada, el desarrollo de la estrategia propuesta tiene los siguientes componentes:

- **FORMACIÓN**

En conjunto con el Área de Talento Humano se tiene establecido un plan de formación para optimizar las capacidades de los diferentes equipos de trabajo, de acuerdo con sus necesidades, a través de:

- ✓ Cursos presenciales
- ✓ Cursos virtuales / e-Learning
- ✓ Sensibilización
- ✓ Publicaciones
- ✓ Talleres

- **GESTIÓN DEL CAMBIO**

Estrategia para preparar a funcionarios y contratistas de la Unidad para el cambio y generar oportunidades de mejora ante el impacto de este. Para nuestro caso, hemos adoptado las siguientes etapas que van a mitigar los efectos que producen los cambios en la organización:

Etapas de preparación para el cambio: Proceso anticipación al cambio, mediante la divulgación, preparación e invitación a la participación de los usuarios y del equipo técnico.

Etapas de adopción: Se busca la apropiación del conocimiento y la puesta en práctica de las actividades desarrolladas dentro de la estrategia.

Etapas de gestión de impacto: Verifica el impacto del cambio en la mejora en el desarrollo de las actividades y procesos.



ANEXO - CARACTERIZACION DE USUARIOS

ANEXO - ESTRATEGIA GESTION DEL CAMBIO


- **MEDICIÓN**

Estrategia que nos permitirá evaluar los avances periódicos en las metas propuestas y las posibles desviaciones tempranas que nos permitan tomar acción, bien para corregirlas o bien para gestionar los cambios a que haya lugar, mediante los siguientes indicadores:

- ✓ **Apropiación de las TIC – Formación:**

 	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018

- Cantidad de funcionarios que usan e-learning / potencial de usuarios calculados
- Cantidad de funcionarios que asisten a formación presencial / usuarios convocados
- ✓ **Uso del conocimiento y habilidades en el trabajo:**
 - Número de capacitados que ha aplicado el conocimiento adquirido / población capacitada.
- ✓ **Habilidades en el uso de internet para desarrollar el trabajo diario:**
 - Cantidad de funcionarios que usaron Internet en el último mes como apoyo en el desarrollo de sus labores.
- ✓ **Cumplimiento de los programas propuestos en cuanto a Formación y Desarrollo:**
 - N° acciones de formación ejecutadas) / N°. Acciones de formación planificadas

	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018	Página 114 de 127

8. MODELO DE PLANEACIÓN

8.1. LINEAMIENTOS Y/O PRINCIPIOS QUE RIGEN EL PETI

Dando cumplimiento a la normatividad vigente, este PETI se alinea con la metodología IT4+ y el marco de referencia AE definido por el Ministerio de Tecnologías de la Información y las Comunicaciones- MINTIC. De otra parte, está enmarcado dentro del proceso de Gestión de la Información como proceso estratégico en donde se deben definir políticas y lineamientos de TI en relación con aspectos como:

- Utilizar en lo posible, estándares definidos por la industria
- Permitir en lo posible que la tecnología contribuya al buen uso de la infraestructura con crecimiento razonable (escalabilidad)
- Permitir reconfiguraciones y flexibilidad a las soluciones tecnológicas
- Dimensionar la infraestructura para soportar los requerimientos
- Procurar que la infraestructura tenga conectividad segura y oportuna
- Garantizar que la información suministrada por la Unidad a los diferentes entes e interesados sea confiable y oportuna

8.2. ESTRUCTURA DE ACTIVIDADES ESTRATÉGICAS

La Unidad de Víctimas elabora un Plan de Acción de Tecnología el cual consolida la información de los planes, programas y proyectos que el área de tecnología ejecutará en el cumplimiento de la estrategia institucional, en ese sentido se tienen las siguientes actividades estratégicas claves a ejecutar.

8.2.1. DISEÑAR E IMPLEMENTAR LA ARQUITECTURA EMPRESARIAL



Esta actividad responde a la implementación de los lineamientos y directrices del MINTIC en relación con los componentes de Arquitectura Empresarial, es decir, de un lado la arquitectura misional y la arquitectura de TI, de otro lado la implementación del modelo de gestión IT4+ definido para la Gestión de TI. Esta iniciativa debe ir avalada por la alta dirección de la Unidad y con la participación de las áreas misionales, planeación y jurídica,

8.2.2. FORMULAR E IMPLEMENTAR LA ESTRATEGIA DE USO Y APROPIACIÓN.

Hace referencia a la definición de la política de Uso y Apropiación, así como a la implementación de las diferentes técnicas y herramientas para la socialización y difusión de los diferentes componentes de tecnología, sus servicios y productos, en todas las áreas y procesos de la Unidad como a los interesados internos y externos.

8.2.3. SUMINISTRAR LOS RECURSOS PARA LAS INICIATIVAS DE GESTIÓN DOCUMENTAL DE LA UNIDAD Y EXPEDIENTE ÚNICO DIGITAL.

Dotar a la Unidad del recurso tecnológico necesario para implementar o fortalecer el Sistema de Gestión Documental de la entidad.

 	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018

8.2.4. GESTIONAR BUS DE DATOS BIZTALK.

Ampliar la cobertura del bus de datos a todas las necesidades de integración de la Unidad en relación con los servicios y sistemas de información que ofrece la OTI y la SRNI, esto, en procura de lograr fuentes únicas de información e intercambio. Y homologarlos con las directrices de la Agencia Nacional Digital.

8.2.5. APLICAR PLAN DE SEGURIDAD DE LA INFORMACIÓN.

En relación con la Seguridad de la Información ejecutar un Plan de Seguridad y Privacidad en donde todas las actividades definidas están fundamentadas legalmente en decretos o leyes, dichas actividades son:

- Políticas de seguridad de información
- Levantamiento de inventarios de activos de información
- Elaboración de matriz de riesgos de seguridad de la información
- Modelo de seguridad y privacidad de la información

De otra parte, definir procedimientos o protocolos relacionados con:

- Control de entregas de archivos planos en medios magnéticos.
- Gestión de Certificados Digitales
- Gestión de Incidentes de Seguridad
- Gestión de verificación cumplimiento de políticas.
- Borrado seguro de información
- Controles criptográficos
- Gestión de capacidad
- Gestión de ambientes de procesamiento
- Protección contra códigos maliciosos
- Aseguramiento de servicios de red
- Intercambio o transferencia de información
- Control de software
- Gestión de continuidad
- Gestión de derechos de autor
- Gestión de usuarios y contraseñas

8.2.6. INTEGRAR ESTRATEGIAS Y SERVICIOS DE INFORMACIÓN CON OTRAS ÁREAS DE LA UNIDAD

Definir e implementar procedimientos, protocolos, servicios y/o metodologías para la integración de información misional que es originada procesada y/o actualizada por las diferentes áreas de la entidad. Definir estándares de creación e interpretación de datos, definir y aplicar criterios para asegurar la calidad de la información, evitar el doble procesamiento o reprocesamiento e

información.

8.2.7. IMPLEMENTAR UN PLAN DE CONTINGENCIAS O RECUPERACIÓN DE DESASTRES.

Actualmente se cuenta con un centro de datos contratado a través de marco de Colombia Compra Eficiente que da cubrimiento a los servidores principales de la unidad, pero no incluye un plan de recuperación de desastres. Para este centro de datos y otros recursos que no hacen parte del centro de datos, se debe formular e implementar un Plan de Recuperación de Desastres que incluya todos los recursos de tecnología, inclusive lo referente a sitios alternos de operación.

8.3. ELABORAR Y EJECUTAR PLAN MAESTRO O MAPA DE RUTA

Hace referencia a las iniciativas o proyectos a ejecutar por cada uno de los dominios con las respectivas acciones o actividades por iniciativa, se encuentran en el documento adjunto PETI INICIATIVAS ACCIONES e incluyen estimación de tiempos y costos de ejecución. Este Plan Maestro contiene las iniciativas clasificadas por objetivo estratégico y dominio, es decir, Gobierno, Información, Sistemas de Información, Servicios Tecnológicos y Uso y Apropiación

8.4. DEFINIR INDICADORES DE SEGUIMIENTO AL PETI

Objetivo. Medir el cumplimiento del Plan Estratégico de Tecnología – PETI, mediante indicadores para cada uno de los seis (6) dominios de la Arquitectura, siguiendo las directrices del MINTIC como se presenta a continuación:

INDICADOR	PREGUNTA	OPCIÓN DE RESPUESTA
Porcentaje de cumplimiento en la definición de la Estrategia de TI de la entidad	Frente a la Planeación estratégica de TI	El PETI soporta el cumplimiento total de los objetivos estratégicos de la Entidad
		Contiene una hoja de ruta de iniciativas de TI
	Frente a la implementación de la estrategia de TI	La entidad realiza documentación, seguimiento y evaluación del cumplimiento del PETI
		El PETI fue comunicado y explicado a los grupos de interés de la entidad
		La entidad definió la oferta de los servicios de TI (catálogo de servicios de TI)
	% de Cumplimiento de la planeación estratégica de TI	Indique el % de cumplimiento de los objetivos del PETI
	Frente a la Arquitectura Empresarial en la entidad	La entidad cuenta con las capacidades para realizar ejercicios de AE (Personas, Procesos, Herramientas)
		Hace uso de la metodología de AE para el diseño y planeación de las iniciativas de TI
	Frente a la documentación de la Arquitectura Empresarial en la entidad	Realizó la documentación de la Arquitectura de Negocio de la entidad
		Realizó la documentación de la Arquitectura de Información de la entidad
		Realizó la documentación de la Arquitectura de Sistemas de Información de la entidad
		Realizó la documentación de la Arquitectura de Servicios tecnológicos de la entidad.



INDICADOR	PREGUNTA	OPCIÓN DE RESPUESTA
Porcentaje de cumplimiento en la implementación del Gobierno de TI en la entidad	Frente al Esquema de Gobierno TI de la entidad	Definió y usó un esquema de Gobierno de TI
	Frente a la gestión integral de proyectos de TI	Definió y uso una metodología para la Gestión integral de Proyectos de TI
	Frente a la gestión integral de proyectos de TI	Hizo uso de mecanismos para la optimización de compras públicas de TI
		Evaluó las alternativas de solución teniendo en cuenta los costos de desarrollo y mantenimiento a largo plazo de los proyectos de TI
	Frente a la Gestión de la operación de TI	Evaluó el desempeño de la gestión de TI a través de indicadores de desempeño del proceso de Gestión de TI
		Gestionó la transferencia de conocimiento por parte de los proveedores de TI
		Gestionó planes de mejora frente a los resultados de los indicadores de desempeño del proceso de Gestión TI
Porcentaje de cumplimiento en la Gestión de la Información	Frente a la Planeación y Gobierno de los Componentes de Información	Documentó los componentes de información de la Entidad
		Definió un esquema para el gobierno y la gestión de los Componentes de Inf.
		Definió las fuentes únicas de información en la Entidad
	Frente al Análisis y aprovechamiento de los Componentes de Información	Utilizó mecanismos y/o canales para el uso y aprovechamiento de los componentes de información
		Fomentó el uso y aprovechamiento de los componentes de información por parte de los grupos de interés.
	Frente a la Calidad de los Componentes de Información	Definió y utilizó un esquema de gestión de la calidad de los componentes de inf.
		Evaluó la calidad de los componentes de información de la entidad
		Implementó controles y acciones de mejora frente a la calidad de la UARIV



INDICADOR	PREGUNTA	OPCIÓN DE RESPUESTA
Porcentaje de cumplimiento en la Gestión de los Sistemas de Información	Frente a la Planeación y gestión de los Sistemas de Información	
	Frente al Soporte de los Sistemas de Información	Definió e implementó un esquema de mantenimiento y soporte a los sistemas de información incluyendo si estos son mantenidos por terceros.
	Frente al Ciclo de vida de los Sistemas de Información	Definió e implementó un esquema para el gobierno y gestión de los sistemas de información durante el ciclo de vida, que incluya planeación, diseño, desarrollo, pruebas, puesta en producción y mantenimiento.
	Frente a la Gestión de la calidad de los Sistemas de Información	Definió e implementó un plan de aseguramiento de la calidad durante el ciclo de vida de los sistemas de información que incluya criterios no funcionales y de calidad de los mismos.

Porcentaje de cumplimiento en la Gestión de los Servicios Tecnológicos	Frente a la Operación de Servicios Tecnológicos	Identificó las capacidades actuales de los Servicios Tecnológicos y proyectó las capacidades futuras requeridas para un óptimo funcionamiento
		Definió y evaluó el cumplimiento de los ANS para los servicios tecnológicos que presta la Entidad
		Implementó un plan de mantenimiento preventivo y evolutivo sobre toda la infraestructura y demás Servicios Tecnológicos de la institución
	Frente al Soporte de los Servicios Tecnológicos	Definió e implementó un procedimiento para atender los requerimientos de soporte de primer, segundo y tercer nivel, para sus servicios de TI, a través de un punto único de contacto

	Frente a la Gestión de la calidad de los Servicios Tecnológicos	La Entidad definió e implementó un plan de continuidad, capacidad y disponibilidad de los servicios tecnológicos de tal forma que este asegure el cumplimiento de los ANS establecidos
--	---	--

INDICADOR	PREGUNTA	OPCIÓN DE RESPUESTA
Porcentaje de cumplimiento en la definición de la Estrategia de Uso y Apropiación de TI en la entidad	Frente a la Estrategia para el Uso y Apropiación de TI	Definió la estrategia de uso y apropiación de TI a partir de la caracterización de grupos de interés y de la medición de indicadores de uso y apropiación de TI
	Frente a la Gestión del cambio para los proyectos de TI	Implementó estrategias de preparación para el cambio y gestión de impactos sobre los proyectos de TI

Tabla 16. Modelo de Indicadores Cumplimiento PETI
Fuente. MINTIC

 	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN		
	PETI – 2018		
	OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
PROCESO: GESTIÓN DE LA INFORMACIÓN			
CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018	Página 121 de 127

9. PLAN DE COMUNICACIONES

Para apoyar el cumplimiento del plan propuesto en este documento, es muy importante contar con una difusión integral del mismo entre la comunidad que hace parte de la Unidad para las Víctimas. Buscamos generar confianza y apropiación de los procesos propuestos para mejorar la apuesta en tecnologías de información y comunicación que adelanta la Unidad.

Método para definir el Plan de Divulgación

Al ser el PETI un instrumento dinámico, que responde permanentemente a los cambios institucionales, es importante que todos los mensajes que se definan durante su ejecución (2018 – 2021), identifiquen la fase de ejecución, las actividades particulares, a qué población está dirigida, qué se busca con dicha actividad, una honesta definición del porcentaje de avance de cada actividad y la fecha de entrega de cada actividad.

Actividades principales:

- Publicación y difusión del PETI entre la comunidad de la Unidad para las víctimas (funcionarios, contratistas y tercerizados)
- Capacitar en el uso e implementación de las herramientas y procesos desarrollados por la OTI.
- Realizar campañas pedagógicas para una adecuada implementación, uso y apropiación de las herramientas tecnológicas dispuestas en la Unidad.
- Promover la permanente retroalimentación de la comunidad de la Unidad sobre las actividades y servicios por la OTI y, a partir de ese ejercicio mejorar o reformular las herramientas y procesos propuestos.



Canales:

- Intranet
- Correo electrónico institucional.
- Boletín Virtual SUMA
- Suma TV
- Carteleras
- Activaciones presenciales en todas las sedes de la Unidad

Ejes centrales:

- Dar a conocer los procesos y procedimientos de la OTI, haciendo énfasis en su utilidad e importancia en el trabajo diario que realiza la comunidad de la Unidad para las Víctimas.
- Visibilizar las soluciones tecnológicas que funcionan actualmente y los beneficios que generan en términos de gestión y servicio al ciudadano.
- Desarrollar metodologías y herramientas que favorezcan la innovación dentro de la comunidad de la Unidad para las Víctimas. La mejor manera de hacer nuestro trabajo es escuchar a los compañeros que lo hacen día a día.

- Lograr que la capacidad tecnológica actual se integre eficazmente al modelo integrado de planeación y gestión que se implementa en la Unidad, de tal forma que se responda a los objetivos institucionales.
- Integrar eficazmente los modelos de seguridad y privacidad de la información a las prácticas cotidianas de la entidad.



 	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018
			Página 123 de 127

TABLAS

- Tabla 1. Ámbitos y Lineamientos definidos por MINTIC para estructurar el PETI
- Tabla 2. Dotación Tecnológica
- Tabla 3. Inventario de Servidores por Tipo
- Tabla 4. Inventario de Servidores de Centro de Datos
- Tabla 5. Canales de Comunicaciones
- Tabla 6. Inventario de Telefonía por Regional
- Tabla 7. Cumplimiento del Modelo de Seguridad y Privacidad de la Información del MinTIC a corte 31 de octubre de 2018
- Tabla 8. Cronograma – Plan de Seguridad y Privacidad de la Información - UARIV 2018
- Tabla 9. Lista de Cargos de la Oficina de Tecnologías de la Información
- Tabla 10. Inversión por rubro
- Tabla 11. Inversión por Tipo de Proceso en millones de pesos - fecha de corte julio 2018
- Tabla 12. Alineación de Objetivo Estratégicos DPS – UNIDAD PARA LAS VÍCTIMAS – OTI
- Tabla 13. Misión y Visión Estratégica Sectorial
- Tabla 14. Ciclo PHVA – Proceso de Gestión de la Información
- Tabla 15. Correlación de Objetivos Estratégicos UNIDAD PARA LAS VÍCTIMAS y TI
- Tabla 16. Indicadores PETI

GRAFICAS

- Grafica 1. Organigrama de la UNIDAD PARA LAS VÍCTIMAS
- Gráfica 2. Estrategias Sectoriales
- Gráfica 3. Acceso a través SUMA
- Grafica 4. Actividades de transferencia UARIV
- Grafica 5. Capacitación y Apropiación
- Grafica 6. Capacitación y Divulgación
- Grafica 7. Resultados de la encuesta pregunta 1
- Grafica 8. Resultados de la encuesta pregunta 3
- Grafica 9. Resultados de la encuesta pregunta 4
- Grafica 10. Resultados de la encuesta pregunta 5
- Grafica 11. Resultados de la encuesta pregunta 6
- Grafica 12. Resultados de la encuesta pregunta 7
- Grafica 13. Resultados de la encuesta pregunta 8
- Grafica 14. Resultados de la encuesta pregunta 9
- Grafica 15. Resultados de la encuesta Ofimática
- Grafica 16. Resultados de la encuesta Interés en Capacitación
- Grafica 17. Resultados de la encuesta Interés en Capacitación
- Grafica 18. Sistemas de Información por Tipo de Proceso
- Grafica 19. Licenciamiento ERP
- Gráfica 20. Arquitectura Actual Sistemas Información

 	PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN PETI – 2018 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI		
	PROCESO: GESTIÓN DE LA INFORMACIÓN		
	CODIGO: 130,06,07-3	Versión:01	Fecha: 28/12/2018
			Página 124 de 127

- Gráfica 21. Enfoque de la Arquitectura tradicional – Silos Organizacionales
- Gráfica 22. Diseño de Aplicaciones por Capas – Módulos Integrados
- Gráfica 23. Arquitectura Actual de los Sistemas de Información
- Gráfica 24. Arquitectura Despliegue de los Sistemas de Información
- Grafica 25 Promedio mensual solicitudes tramitadas en la Mesa de servicios
- Gráfica 26. Servicios de Computo por Demanda
- Gráfica 27. Tendencia de la capacidad de herramientas colaborativas
- Gráfica 28. Tendencia de los servicios de conectividad y telefonía
- Gráfica 29. Diagrama del Equipo de Soporte Técnico
- Gráfica 30. Inventario de Servidores de Centro de Datos
- Grafica 31. Esquema de red
- Grafica 32. Seguridad Perimetral
- Gráfica 33. Diagrama de Alto Nivel – Gestión de la Información
- Gráfica 34. Diagrama de Ruta de Información vista desde los Sistemas Fundamentales
- Gráfica 35. Comportamiento Dominio de Seguridad de la Información
- Gráfica 36. Comparativo Niveles de Riesgo
- Gráfica 37 Seguimiento mensual de recursos de inversión
- Gráfica 38. Objetivos del Sector
- Gráfica 39. Diagrama de la Estructura del Sector Inclusión
- Gráfica 40. Diagrama del Plan Estratégico Sectorial
- Grafica 41. Mapa de Procesos
- Gráfica 42. Diagrama de relación Sistemas de Información / Procesos
- Gráfica 43. Principios y valores Modelo de Gestión IT4+
- Gráfica 44. Objetivo Estratégico 1
- Gráfica 45. Objetivo Estratégico 2
- Gráfica 46. Objetivo Estratégico 3
- Gráfica 47. Análisis DOFA
- Gráfica 48. Cadena de Valor PETI
- Gráfica 49. Diagrama del Ciclo del Dato
- Gráfica 50. Enfoque Transversal Arquitectura de Información
- Gráfica 51. Diagrama de la Arquitectura de Transición
- Gráfica 52. Diagrama de la Arquitectura Objetivo
- Grafica 53. Modelo de Seguridad y Privacidad de la Información
- Grafica 33. Indicadores PETI por Dominio

GLOSARIO.

CONPES. Comité Nacional de Política Económica y Social
DPS. Departamento de Prosperidad Social
ICBF. Instituto Colombiano de Bienestar Familiar

MINTIC. Ministerio de las Tecnologías de la Información y las Comunicaciones
 MIPG. Modelo Integrado de Planeación y Gestión
 OAP. Oficina Asesora de Planeación de la UARIV
 OAC. Oficina Asesora de Comunicaciones de la UARIV
 OTI. Oficina de Tecnologías de la Información
 PETI. Plan Estratégico de Tecnologías de la Información
 PND. Plan Nacional de Desarrollo
 UARIV. Unidad para la Atención y Reparación a las Víctimas

ANEXOS

ANEXO - CATALOGO DE SISTEMAS DE INFORMACION
 ANEXO - CATALOGO DE SERVICIOS DE TI
 ANEXO - INFORME DE LICENCIAMIENTO
 ANEXO - GESTIÓN DE CAPACIDAD
 ANEXO - MATRIZ DE INICIATIVAS.
 ANEXO - POLITICAS DE TI
 ANEXO - MAPA DE RIESGOS
 ANEXO - CARACTERIZACION DE USUARIOS
 ANEXO - ESTRATEGIA PARA GESTION DEL CAMBIO

<p>Facilitadora en el proceso de construcción y elaboración: Ana Yolanda Cañón Prieto, Asesora de la Dirección General</p> <p>Preparó:</p> <p>Dirección de Registro y Gestión de la Información: Honofre Celis Hernández</p> <p>Subdirección Red Nacional de Información: Roberto Martínez Guzmán</p> <p>Oficina Asesora de Comunicaciones: Fabio Medina Ramírez</p> <p>Oficina de Tecnologías de la Información: Funcionarios y Contratistas al servicio de la OTI</p>	<p>Revisó.</p> <p>Jhon Ricardo Morales Franco – Jefe OTI Manuel Eduardo Castillo Guzmán – Jefe (e) OTI</p>
<p>Aprobó:</p> <p>Comité Institucional de Gestión y Desempeño</p>	



ANEXO 1

Catálogo de Sistemas de información

Control de cambios

Versión	Elaborada por	Revisada por	Aprobada por	Fecha	Motivo
1	Sonia Navarrete Yuri Restrepo	Ricardo Daniel	Manuel E. Castillo G.	20/11/2018	Creación revisión y aprobación



Catálogo de Sistemas de información

10/2018

OFICINA GESTIÓN DE LA INFORMACIÓN

Presentamos el catálogo de Sistemas de información alojado sobre la infraestructura de la unidad de víctimas, utilizado para soportar los diferentes procesos a cargo de la entidad.

Propósito: El catálogo tiene como propósito dar a conocer el inventario oficial de los sistemas de información de la Unidad, así como, la caracterización básica de cada uno de ellos, es un documento vivo que se mantiene actualizado permanentemente y que refleja el estado del arte de los sistemas de información de la Unidad de víctimas atendiendo los elementos mínimos contenidos en la guía para la construcción del catálogo de sistemas de información. ¹

¹ G.sis.03 Guía para la construcción del catálogo de sistemas de información. Guía técnica Versión 1.0 06 de julio de 2018

GENERALIDADES

1. CATÁLOGO SISTEMAS DE INFORMACION

El catálogo de sistemas de información tiene como fin identificar y almacenar una lista completa y actualizada de los sistemas de información de la unidad de víctimas, en este encontrará el nombre del sistema, sigla, descripción del sistema, versión, categoría, tipo de desarrollo, fabricante, proveedor de soporte, fecha de vencimiento del soporte, responsable técnico, responsable funcional, estado, fecha inactivación, licenciamiento, sistema operativo, lenguaje de programación, documentación técnica y funcional y observaciones.

Así mismo el catálogo de Sistemas de Información proporciona beneficios tales como:

- Robustecer el gobierno y gestión de los sistemas de información
- Identificar los impactos sobre los sistemas de información causados por nuevas iniciativas o proyectos en la Unidad de víctimas
- Identificar duplicidades de funcionalidades o interfaces.
- Determinar oportunidades de mejoras en los sistemas de información.
- Concentrar la información facilitando la consulta y soporte.
- Suministrar la gestión del conocimiento al interior de la entidad.
- La gestión de los sistemas de información se hace sobre la totalidad de las herramientas de la unidad conociendo sus características y el grado de interacción entre ellas.
- Permitir articular un enfoque de las múltiples iteraciones que caracterizan los sistemas de información de la unidad, así como generar alertas tempranas.
- Herramienta fundamental para la gestión y apoyo en la toma de decisiones.

2. ALCANCE

Tener un control de los activos de información asociados a los sistemas de información, facilitando la gestión, soporte y actualización de los mismos, constituyendo de esta manera un elemento fundamental de la arquitectura de sistemas de información.

3. ESTADO GENERAL

Para esta versión se tiene la siguiente estadística: versión, categoría, tipo de desarrollo, estado, sistema operativo, plataforma BD, lenguaje de programación.

ESTADO	CANT.	VERSION	CANT.	CATEGORIA	CANT.	TIPO DE DESARROLLO	CANT.	SISTEMA OPERATIVO	CANT.	LENGUAJE DE PROGRAMACION	CANT.	PLATAFORMA BD	CANT.
Activo	44	1	49	Seguimiento y control	4	Servicio asociado	1	Windows server 2012 r2	61	Acces front end	1	WEB CON BD CENTRAL	1
Inactivo	21	1,1	1	Sistema de apoyo	5	Adquirido	1			BPM	1	POSTGRES	2
		1,2	1	Estrategico	7	Interno	2			C#, ENTITY DATA MODEL	1	SQL SERVER 2012	3
		1,8	1	Misional	20	Contratacion OTI	2			ALFRESCO	1	MYSQL	4
		2	2	soporte	22	legado	9			EXCEL 2007	1	SQL SERVER 2008 R2	8
		2,03	2			Cont. Otras Dep	9			C#	2	ORACLE 11 G	42
		3	3			propio	35			NET 2005	2		
		3,2	2							C#. NET, FRAMEWORK 4.5	2		
		25,6	1							BPMESIGNA	3		
		10.5.2.4.0	1							.NET 2012	3		
		4,1,0.4	1							.JAVA	4		
		8,7,1,0	1							USSD	4		
										NET C#	7		
										PHP	9		
										.NET	21		
										HTML	1		

4. LINEAMIENTOS

La documentación del catálogo de Sistemas de Información se efectuó en cumplimiento del siguiente ámbito y lineamientos:

Ámbito	Lineamiento
Planeación y gestión de los Sistemas de Información	Catálogo de sistemas de información – LI.SIS.02
Planeación y gestión de los Sistemas de Información	Definición estratégica de los sistemas de información – li.sis.01

A continuación, encontrará la lista completa y actualizada de los sistemas de información de la unidad de víctimas.

“La definición e interpretación de cada uno de los atributos utilizados para la caracterización de los sistemas de información dentro de este inventario pueden ser consultados en la sección de Glosario.”

1. SISTEMA DE GESTIÓN PARA LAS VICTIMAS

NOMBRE DEL SISTEMA: SISTEMA DE GESTIÓN PARA LAS VICTIMAS

SIGLA: SGV

DESCRIPCIÓN DEL SISTEMA: Permite crear y escalar un caso a partir de un WS, utilizado para estrategias virtuales de atención y sistemas que ofrecen servicios complementarios de atención.

VERSIÓN: 1.0

CATEGORÍA: Misional

TIPO DE DESARROLLO: Desarrollo interno



FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: Equipo de soporte OTI

TELEFONO: N/A

CORREO: soporte.oti@unidadvictimas.gov.co

FECHA DE VENCIMIENTO DEL SOPORTE: 2018-12-31

RESPONSABLE TÉCNICO: Soporte aplicaciones OTI

RESPONSABLE FUNCIONAL: Dirección de gestión social humanitaria

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: A perpetuidad

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: C#. NET, FRAMEWORK 4.5

PLATAFORMA BD: SQL SERVER 2012

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\172.20.210.14\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Nuevos\G. Registro y Valoración A

ARQUITECTURA TECNOLÓGICA: WEB

2. PORTAL DE VIVANTO

NOMBRE DEL SISTEMA: PORTAL DE VIVANTO

SIGLA: VIVANTO

DESCRIPCIÓN DEL SISTEMA: Visor para ofrecer información consolidada sobre el registro de víctimas y facilitar el acceso a la información de ayudas, asistencia, atención y reparación, tanto de la unidad como de las distintas entidades que conforman el SNARIV. es un insumo para las entidades que atienden víctimas de conflicto armado, además ofrece facilidades para la atención al trámite de novedades en el registro único de víctimas la aplicación de encuestas de caracterización, acreditación y certificación de la condición de víctima

VERSIÓN: 1.0

CATEGORÍA: Sistema de apoyo

TIPO DE DESARROLLO: Desarrollo interno

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: Equipo de soporte subdirección RNI

TELEFONO: N/A

CORREO: soporte.oti@unidadvictimas.gov.co

FECHA DE VENCIMIENTO DEL SOPORTE: 2018-12-31

RESPONSABLE TÉCNICO: Equipo de soporte subdirección RNI

RESPONSABLE FUNCIONAL: Equipo de soporte subdirección RNI

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: A perpetuidad



SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: C#. NET, FRAMEWORK 4.5

PLATAFORMA BD: ORACLE 11G

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Nuevos\G. Respuesta Escrita\2016_17183_Buzon Jurídico

ARQUITECTURA TECNOLÓGICA: WEB

3. MODELO SUBSISTENCIA MINIMA FASE II

NOMBRE DEL SISTEMA: MODELO SUBSISTENCIA MINIMA FASE II

SIGLA: SM

DESCRIPCIÓN DEL SISTEMA: SM es un modelo que permite medir el nivel de carencias de un hogar de acuerdo a las condiciones determinadas por la encuesta PAARI y registros administrativos de la RNI que determinan factores importantes en componentes de alojamiento y alimentación. Así como la tasación de la atención humanitaria para cada componente, además realiza el proceso de colocación proyección y colocación de pagos, el registro y gestión de novedades de pago, recolocaciones y reintegros en caso de no cobro.

VERSIÓN: 1.0

CATEGORÍA: Misional

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: Mesa de Servicios

TELEFONO: Marcación abreviada 5

CORREO: soporte.oti@unidadvictimas.gov.co

FECHA DE VENCIMIENTO DEL SOPORTE: 2018-12-31

RESPONSABLE TÉCNICO: Servicios TI

RESPONSABLE FUNCIONAL: Dirección gestión social humanitaria

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: .NET C# FRAMEWORK 4.5

PLATAFORMA BD: ORACLE 11G

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\172.20.210.14\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Nuevos\G. Asistencia\2013_A_SM\2016_A_SM_FASE_2

ARQUITECTURA TECNOLÓGICA: WEB

4. ORFEO

**NOMBRE DEL SISTEMA: MODELO SUBSISTENCIA MINIMA FASE II****SIGLA:** ORFEO

DESCRIPCIÓN DEL SISTEMA: Sistema de información para el manejo de correspondencia; el DPS de donde nació la unidad de víctimas manejan Orfeo como un sistema de radicación y no como de Gestión documental perdiendo su fin como sistema, desde que nosotros migramos el sistema a nuestro data center, se ha retomado su fin como sistema de Gestión documental, con el acompañamiento del ingeniero cesar (jefe de la OTI), la doctora María del pilar (jefe administrativa y Gestión documental) y de la doctora sara Sandvik (secretaria general), en este proceso se le han tenido que cambiar la mentalidad a los usuarios sacándolo de sistema de radicación a sistema de Gestión, para poder lograr esto se le ha tenido que activar varias funcionalidades que no se utilizaban, poner filtros de seguridad y otras mejoras para que desempeñe las labores que debe cumplir.

VERSIÓN: 3.2**CATEGORÍA:** Sistema de Apoyo**TIPO DE DESARROLLO:** Legado**FABRICANTE:** S.S.P.D**PROVEEDOR DE SOPORTE:****NOMBRE:** Mesa de Servicios**TELEFONO:** Marcación abreviada 5**CORREO:** soporte.oti@unidadvictimas.gov.co**FECHA DE VENCIMIENTO DEL SOPORTE:** 2019-08-01**RESPONSABLE TÉCNICO:** Servicios TI**RESPONSABLE FUNCIONAL:** Secretaria General**ESTADO:** Activo**FECHA INACTIVACIÓN:** N/A**LICENCIAMIENTO:** N/A**SISTEMA OPERATIVO:** Windows server 2012 R2**LENGUAJE DE PROGRAMACIÓN:** PHP**PLATAFORMA BD:** ORACLE 11G**DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:**

\\172.20.210.14\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de información\Sistemas Legados\G. Documental

ARQUITECTURA TECNOLÓGICA: WEB**5. MODULO SUBSISTENCIA MINIMA FASE I****NOMBRE DEL SISTEMA: MODELO SUBSISTENCIA MINIMA FASE I****SIGLA:** SM**DESCRIPCIÓN DEL SISTEMA:** información de carencias, turnos y montos**VERSIÓN:** 3.2**CATEGORÍA:** Misional



TIPO DE DESARROLLO: Desarrollo propio
FABRICANTE: Oficina de tecnología
PROVEEDOR DE SOPORTE:
NOMBRE: Mesa de Servicios
TELEFONO: Marcación abreviada 5
CORREO: soporte.oti@unidadvictimas.gov.co
FECHA DE VENCIMIENTO DEL SOPORTE: N/A
RESPONSABLE TÉCNICO: N/A
RESPONSABLE FUNCIONAL: N/A
ESTADO: Inactivo
FECHA INACTIVACIÓN: N/A
LICENCIAMIENTO: N/A
SISTEMA OPERATIVO: Windows server 2012 R2
LENGUAJE DE PROGRAMACIÓN: NET C#
PLATAFORMA BD: ORACLE 11G
DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:
\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de información\Sistemas Nuevos\G. Asistencia\2013_A_SM
ARQUITECTURA TECNOLÓGICA: WEB

6. LEX

NOMBRE DEL SISTEMA: LEX

SIGLA: LEX

DESCRIPCIÓN DEL SISTEMA: Lex es la herramienta de gestión de acciones constitucionales de la unidad, operada por el área grupo de respuesta escrita de la subdirección general, la herramienta maneja paralelamente tres flujos tutelas, recursos y PQR, donde su estructura está basada en tareas o casos que son manejados en los perfiles alistamiento (ingreso de los datos básicos de las solicitudes), análisis (análisis de la solicitud hecha por la víctima y búsqueda de insumos para la elaboración de la respuesta), áreas misionales (encargada de generar los insumos para proyectar la respuesta), control de escalamiento (revisión de la calidad del insumo), abogado (encargado de elaborar las respuestas), firma (proceso de implantar la firma en cada respuesta), radicación (entrega de la respuesta según el flujo tutelas a juzgados, recursos a notificaciones PQR a 4/72)

VERSIÓN: 4.1.0.4

CATEGORÍA: Apoyo

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: Mesa de Servicios

TELEFONO: Marcación abreviada 5

CORREO: soporte.oti@unidadvictimas.gov.co

FECHA DE VENCIMIENTO DEL SOPORTE: 2019-08-01





RESPONSABLE TÉCNICO: Servicios TI

RESPONSABLE FUNCIONAL: Subdirección General

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: NET C#

PLATAFORMA BD: ORACLE 11G

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\172.20.210.14\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de información\Sistemas Nuevos\G. Respuesta Escrita

ARQUITECTURA TECNOLÓGICA: WEB

7. ACTOS ADMINISTRATIVOS SUBSISTENCIA MINIMA

NOMBRE DEL SISTEMA: ACTOS ADMINISTRATIVOS SUBSISTENCIA MINIMA

SIGLA: AA SM

DESCRIPCIÓN DEL SISTEMA: Generación de actos administrativos de subsistencia mínima para población víctima, para posterior notificación vía SIRAV.

VERSIÓN: 3.0

CATEGORÍA: Misional

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: Mesa de Servicios

TELÉFONO: Marcación abreviada 5

CORREO: soporte.oti@unidadvictimas.gov.co

FECHA DE VENCIMIENTO DEL SOPORTE: 2019-08-01

RESPONSABLE TÉCNICO: Servicios TI

RESPONSABLE FUNCIONAL: Subdirección General

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: NET C#

PLATAFORMA BD: ORACLE 11G

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\172.20.210.14\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de información\Sistemas Nuevos\G. Asistencia\2013_A_SM\2015_SM_AA

ARQUITECTURA TECNOLÓGICA: WEB

8. RUV TEMPORAL



NOMBRE DEL SISTEMA: RUV TEMPORAL

SIGLA: RUV

DESCRIPCIÓN DEL SISTEMA: Capturar las declaraciones de las víctimas, gestionar os procesos de valoración, glosas, distribución de formularios.

VERSIÓN: 2.0

CATEGORÍA: Misional

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Subdirección de valoración

PROVEEDOR DE SOPORTE:

NOMBRE: Subdirección de valoración

TELEFONO: N/A

CORREO: adimin.svr@unidadvictimas.gov.co

FECHA DE VENCIMIENTO DEL SOPORTE: 2019-12-31

RESPONSABLE TÉCNICO: Subdirección de Valoración y Registro

RESPONSABLE FUNCIONAL: Subdirección de Registro y valoración

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: .NET

PLATAFORMA BD: ORACLE 11G

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\172.20.210.14\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de información\Sistemas Nuevos\G. Registro y Valoración\2014_VR_VIVANTO\3. Análisis Desarrollo -

ARQUITECTURA TECNOLÓGICA: WEB

9. INDEMNIZA

NOMBRE DEL SISTEMA: INDEMNIZA

SIGLA: INDEMNIZA

DESCRIPCIÓN DEL SISTEMA: Aplicación para realizar la gestión de indemnizaciones individuales asociadas a procesos de reparación.

VERSIÓN: 3.0

CATEGORÍA: Misional

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Subdirección de reparación individual

PROVEEDOR DE SOPORTE:

NOMBRE: Julio Alejandro Diaz Pinilla

TELEFONO: 7965150 EXT 4221

CORREO: soproteh.indemniza@unidadvictimas.gov.co

FECHA DE VENCIMIENTO DEL SOPORTE: 2018-12-31





RESPONSABLE TÉCNICO: Subdirección de reparación individual
RESPONSABLE FUNCIONAL: Reparación individual _ Álvaro Tovar
ESTADO: Activo
FECHA INACTIVACIÓN: N/A
LICENCIAMIENTO: N/A
SISTEMA OPERATIVO: Windows server 2012 R2
LENGUAJE DE PROGRAMACIÓN: .NET
PLATAFORMA BD: SQL SERVER 2008 R2
DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:
\\172.20.210.14\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de información\Sistemas Nuevos\G. Reparación\INDEMNIZA
ARQUITECTURA TECNOLÓGICA: WEB

10. AHE

NOMBRE DEL SISTEMA: AHE
SIGLA: AHE
DESCRIPCIÓN DEL SISTEMA: Sistema de información que permite tramitar la atención humanitaria de emergencia para población desplazada. Es una aplicación cliente/servidor local, base de datos Oracle, clientes Access, implementado en edificio Avianca con aproximadamente 10 usuarios y en edificio Camacol aproximadamente 12 usuarios.
VERSIÓN: 3.0
CATEGORÍA: Misional
TIPO DE DESARROLLO: Legado
FABRICANTE: Oficina de tecnología
PROVEEDOR DE SOPORTE:
NOMBRE: EDWAR HEILER GIRALDO
TELÉFONO: 01-800-0911119
CORREO: EDWAR.GIRALDO@UNIDADVICTIMAS.GOV.CO
FECHA DE VENCIMIENTO DEL SOPORTE: N/A
RESPONSABLE TÉCNICO: N/A
RESPONSABLE FUNCIONAL: Subdirección de Asistencia y atención -Ana Velásquez
ESTADO: Activo
FECHA INACTIVACIÓN: N/A
LICENCIAMIENTO: N/A
SISTEMA OPERATIVO: Windows server 2012 R2
LENGUAJE DE PROGRAMACIÓN: Acces front end
PLATAFORMA BD: ORACLE 11G
DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:
\\172.20.210.14\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas



de información\Sistemas Nuevos\G. Asistencia\2013_A_AHE
ARQUITECTURA TECNOLÓGICA: WEB

11. ENTERPRISE RESOURCE PLANNING

NOMBRE DEL SISTEMA: ENTERPRISE RESOURCE PLANNING

SIGLA: ERP

DESCRIPCIÓN DEL SISTEMA: Garantizar disponibilidad y desarrollo normal de las operaciones administrativas de la unidad, con actualizaciones y nuevas versiones al software y cambios de ley. para la actual vigencia contempla:

VERSIÓN: SICOF 10.5.2.4.0 MODULO DE VIATICOS 1.7

CATEGORÍA: Soporte

TIPO DE DESARROLLO: Contratación OTI

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: Mesa de servicios

TELÉFONO: Marcación abreviada 5

CORREO: SOPORTE.OTI@UNIDADVICTIMAS.GOV.CO

FECHA DE VENCIMIENTO DEL SOPORTE: 31/12/2018

RESPONSABLE TÉCNICO: ADA SAS

RESPONSABLE FUNCIONAL: Secretaria General

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: 06/09/2019

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: Java

PLATAFORMA BD: ORACLE 11G R2

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\172.20.210.14\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\1305-2017 ERP ADA S.A

ARQUITECTURA TECNOLÓGICA: WEB

12. PAGINA WEB DE LA UNIDAD

NOMBRE DEL SISTEMA: PAGINA WEB DE LA UNIDAD

SIGLA: PAGINA WEB

DESCRIPCIÓN DEL SISTEMA: Portal de la unidad de víctimas que presenta información institucional, que integra además facilidades de registro de solicitudes con destino a la población víctima

VERSIÓN: 1.0

CATEGORÍA: Sistema de apoyo

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:



NOMBRE: Fabio Medina
TELEFONO: 7965150 EXT 3514
CORREO: FABIO.MEDINA@UNIDADVICTIMAS.GOV.CO
FECHA DE VENCIMIENTO DEL SOPORTE: 31/12/2018
RESPONSABLE TÉCNICO: Gilberto Mangones
RESPONSABLE FUNCIONAL: Comunicaciones _ Fabio Medina
ESTADO: Activo
FECHA INACTIVACIÓN: N/A
LICENCIAMIENTO: N/A
SISTEMA OPERATIVO: Windows server 2012 R2
LENGUAJE DE PROGRAMACIÓN: PHP
PLATAFORMA BD: MYSQL
DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:
\\172.20.210.14\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de información\Sistemas Legados\G. Comunicación\2013_GC_PWEB
ARQUITECTURA TECNOLÓGICA: WEB

13. SUPERACION DE LA SITUACION DE VULNERABILIDAD - CONSULTA

NOMBRE DEL SISTEMA: SUPERACION DE LA SITUACION DE VULNERABILIDAD – CONSULTA
SIGLA: SSV
DESCRIPCIÓN DEL SISTEMA:
VERSIÓN: 1.0
CATEGORÍA: Misional
TIPO DE DESARROLLO: Desarrollo propio
FABRICANTE: Oficina de tecnología
PROVEEDOR DE SOPORTE: N/A
NOMBRE: N/A
TELEFONO: N/A
CORREO: N/A
FECHA DE VENCIMIENTO DEL SOPORTE: N/A
RESPONSABLE TÉCNICO: N/A
RESPONSABLE FUNCIONAL: N/A
ESTADO: Inactivo
FECHA INACTIVACIÓN: N/A
LICENCIAMIENTO: N/A
SISTEMA OPERATIVO: Windows server 2012 R2
LENGUAJE DE PROGRAMACIÓN: .NET
PLATAFORMA BD: ORACLE 11G
DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:
\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de información\Sistemas Nuevos\G. Reparación\2015_R_SSV
ARQUITECTURA TECNOLÓGICA: WEB



14. LIQUIDADOR

NOMBRE DEL SISTEMA: LIQUIDADOR

SIGLA: LIQUIDADOR

DESCRIPCIÓN DEL SISTEMA: Esta aplicación permite la verificación de los informes de actividades de los contratistas de la unidad y genera los montos a pagar de acuerdo con las deducciones efectuadas

VERSIÓN: 1.0

CATEGORÍA: Sistema de apoyo

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: Jaime Canaval

TELEFONO: 7965150 EXT 5578

CORREO: JAIME.CANAVAL@UNIDADVICLTIMAS.GOV.CO

FECHA DE VENCIMIENTO DEL SOPORTE: 01/08/2019

RESPONSABLE TÉCNICO: Julio Bolaño

RESPONSABLE FUNCIONAL: Financiera Jennifer Carvajal

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: .NET C#

PLATAFORMA BD: SQL SERVER 2008 R2

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\172.20.210.14\Unidad_Victimas\Oficina de Tecnología\130.169

PROYECTOS\Sistemas de información\Sistemas Nuevos\G.

Financiera\2014_TH_LIQ\2016_11120_LIQIMP

ARQUITECTURA TECNOLÓGICA: WEB

15. PAARI UNIFICADO

NOMBRE DEL SISTEMA: PAARI UNIFICADO

SIGLA:

DESCRIPCIÓN DEL SISTEMA: Servicio especializado- desarrollo de requerimientos nuevos

VERSIÓN: 1.0

CATEGORÍA: Misional

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: N/A

TELEFONO: N/A

CORREO: N/A

FECHA DE VENCIMIENTO DEL SOPORTE: NA
RESPONSABLE TÉCNICO: N/A
RESPONSABLE FUNCIONAL: N/A
ESTADO: Inactivo
FECHA INACTIVACIÓN: N/A
LICENCIAMIENTO: N/A
SISTEMA OPERATIVO: Windows server 2012 R2
LENGUAJE DE PROGRAMACIÓN: BPMESIGNA
PLATAFORMA BD: ORACLE 11G
DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:
\\172.20.210.14\Unidad_Victimas\Oficina de Tecnología\130.169
PROYECTOS\Sistemas de información\Sistemas Nuevos\G.
Asistencia\2015_DGSH_PUNIFICADO\2015_9199_DGSH_PUNIFICADO
ARQUITECTURA TECNOLÓGICA: WEB

16. TURNO DE ATENCION

NOMBRE DEL SISTEMA: TURNO DE ATENCION
SIGLA:
DESCRIPCIÓN DEL SISTEMA: Portal de la unidad de víctimas que presenta información institucional, que integra además facilidades de registro de solicitudes con desino a la población víctima.
VERSIÓN: 1.0
CATEGORÍA: Estratégico
TIPO DE DESARROLLO: Contratación otras dependencias
FABRICANTE: Oficina de tecnología
PROVEEDOR DE SOPORTE:
NOMBRE: N/A
TELEFONO: N/A
CORREO: N/A
FECHA DE VENCIMIENTO DEL SOPORTE: N/A
RESPONSABLE TÉCNICO: N/A
RESPONSABLE FUNCIONAL: N/A
ESTADO: Inactivo
FECHA INACTIVACIÓN: N/A
LICENCIAMIENTO: N/A
SISTEMA OPERATIVO: Windows server 2012 R2
LENGUAJE DE PROGRAMACIÓN: Java
PLATAFORMA BD: POSTGRES
DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:
\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Nuevos\G. Financiera\2014_TH_LIQ\2016_19073_TURNO
ARQUITECTURA TECNOLÓGICA: WEB



17. VIVANTO RUV2: REGISTRO UNICO DE VICTIMAS

NOMBRE DEL SISTEMA: VIVANTO RUV: REGISTRO UNICO DE VICTIMAS

SIGLA: RUV 2

DESCRIPCIÓN DEL SISTEMA: Atender el flujo de operaciones de la Subdirección de Valoración y Registro

versión: 1.0

CATEGORÍA: Misional

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE:

TELEFONO:

CORREO:

FECHA DE VENCIMIENTO DEL SOPORTE: N/A

RESPONSABLE TÉCNICO: N/A

RESPONSABLE FUNCIONAL: N/A

ESTADO: Desarrollo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: PHP

PLATAFORMA BD: ORACLE 11G

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Nuevos\G. Registro y Valoración

ARQUITECTURA TECNOLÓGICA: WEB

18. GESTION DOCUMENTAL

NOMBRE DEL SISTEMA: GESTION DOCUMENTAL

SIGLA: GD

DESCRIPCIÓN DEL SISTEMA:

PERMITE AUTOMATIZAR LOS PROCEDIMIENTOS DOCUMENTALES, MANTENIENDO UN CONTROL SOBRE LOS DIFERENTES ESTADOS.

VERSIÓN: 1.0

CATEGORÍA: Soporte

TIPO DE DESARROLLO: Contratación OTI

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: INDENOVA

TELEFONO: N/A

CORREO: <https://jira.indenova.eu/>

FECHA DE VENCIMIENTO DEL SOPORTE: 31/07/2018



RESPONSABLE TÉCNICO: Claudia Morato

RESPONSABLE FUNCIONAL: Pedro Medina

ESTADO: Inactivo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: BPM ESIGNA

PLATAFORMA BD: ORACLE 11G

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Nuevos\G. Documental

ARQUITECTURA TECNOLÓGICA: WEB

19. MAARIV

NOMBRE DEL SISTEMA: MODELO DE ATENCION, ASISTENCIA Y REPARACION INTEGRAL A VICTIMAS

SIGLA: MAARIV

DESCRIPCIÓN DEL SISTEMA: Sistema de Información encargado de llevar el control y seguimiento de las estrategias, planes, proyectos y actividades encaminadas al cumplimiento de las medidas de reparación integral diferentes a la indemnización, en su dimensión individual y colectiva.

VERSIÓN: 25.6

CATEGORÍA: Misional

TIPO DE DESARROLLO: Legado

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE:

TELEFONO:

CORREO: maariv@unidadvictimas.gov.co

FECHA DE VENCIMIENTO DEL SOPORTE: N/A

RESPONSABLE TÉCNICO: N/A

RESPONSABLE FUNCIONAL: Reparación individual _ Herman Steven Ochoa

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: .NET

PLATAFORMA BD: SQL SERVER 2008 R2

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Nuevos\G. Reparación\2013_RI_MAARIV

ARQUITECTURA TECNOLÓGICA: WEB



20. FONDO DE REPARACION

NOMBRE DEL SISTEMA: FONDO DE REPARACION

SIGLA: FONDO DE REPARACION

DESCRIPCIÓN DEL SISTEMA: Sistema para el registro y administración de bienes recibidos para el fondo de reparación

VERSIÓN: 1.0

CATEGORÍA: Misional

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: N/A

TELEFONO: N/A

CORREO: juan.camargo@unidadvictimas.gov.co

FECHA DE VENCIMIENTO DEL SOPORTE: N/A

RESPONSABLE TÉCNICO: N/A

RESPONSABLE FUNCIONAL: N/A

ESTADO: Inactivo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: C#

PLATAFORMA BD: ORACLE

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Asociados\Fondo de Reparación\2014_GAR_FR

ARQUITECTURA TECNOLÓGICA: WEB

21. SIGO 1

NOMBRE DEL SISTEMA: SIGO 1

SIGLA: SIGO 1

DESCRIPCIÓN DEL SISTEMA: Administrar y gestionar la información suministrada a través del fud en el marco de la ley 1448 para el otorgamiento de los derechos como víctimas a las personas que declararon en el ministerio público

VERSIÓN: 1

CATEGORÍA: Misional

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: VILMA RODRIGUEZ

TELEFONO: N/A

CORREO: vilma.rodriguez@unidadvictimas.gov.co

FECHA DE VENCIMIENTO DEL SOPORTE: N/A

RESPONSABLE TÉCNICO: N/A



RESPONSABLE FUNCIONAL: N/A

ESTADO: Inactivo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: .NET

PLATAFORMA BD: SQL SERVER

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Nuevos\G. Interinstitucional\2015_GO_SIGO

ARQUITECTURA TECNOLÓGICA: WEB

22. AGENDAMIENTO

NOMBRE DEL SISTEMA:

SIGLA: Buzón

DESCRIPCIÓN DEL SISTEMA: Acreditación de la condición de víctima

VERSIÓN: 1.0

CATEGORÍA: Soporte

TIPO DE DESARROLLO: Contratación con otras dependencias

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: N/A

TELÉFONO: N/A

CORREO: N/A

FECHA DE VENCIMIENTO DEL SOPORTE: N/A

RESPONSABLE TÉCNICO: N/A

RESPONSABLE FUNCIONAL: N/A

ESTADO: Inactivo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: Java

PLATAFORMA BD: POSTGRES

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL: N/A

ARQUITECTURA TECNOLÓGICA: WEB

23. APP QUIOSCOS

NOMBRE DEL SISTEMA: APP QUIOSCOS

SIGLA: APP QUIOSCOS

DESCRIPCIÓN DEL SISTEMA: Aplicativo para automatización de los servicios de consulta y trámites disponibles en los quioscos de atención

VERSIÓN: 1.0



CATEGORÍA: Misional

TIPO DE DESARROLLO: Contratación OTI_Otras dependencias

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE: N/A

NOMBRE: N/A

TELEFONO: N/A

CORREO: N/A

FECHA DE VENCIMIENTO DEL SOPORTE: N/A

RESPONSABLE TÉCNICO: N/A

RESPONSABLE FUNCIONAL: N/A

ESTADO: Inactivo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: .NET 2005

PLATAFORMA BD: ORACLE 11G

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimias\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Nuevos\G. Atención al Ciudadano\2015_AC_CRM\3. Análisis Desarrollo - OTI\Quioscos

ARQUITECTURA TECNOLÓGICA: WEB

24. PUNTO VIRTUAL

NOMBRE DEL SISTEMA: PUNTO VIRTUAL

SIGLA:

DESCRIPCIÓN DEL SISTEMA: Primer versión de página de consultas en línea desplegadas en los kioscos de la entidad

VERSIÓN: 1.0

CATEGORÍA: Misional

TIPO DE DESARROLLO: Contratación otras dependencias

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: N/A

TELEFONO: N/A

CORREO: N/A

FECHA DE VENCIMIENTO DEL SOPORTE: N/A

RESPONSABLE TÉCNICO: N/A

RESPONSABLE FUNCIONAL: N/A

ESTADO: Inactivo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: .NET

PLATAFORMA BD: SQL SERVER 2008 R2
DOCUMENTACIÓN TÉCNICA Y FUNCIONAL: N/A
ARQUITECTURA TECNOLÓGICA: WEB

25. ASISTENCIA FUNERARIA

NOMBRE DEL SISTEMA: ASISTENCIA FUNERARIA

SIGLA: Asistencia Funeraria

DESCRIPCIÓN DEL SISTEMA: Contar con la información actualizada sobre las entregas efectivas de asistencia funeraria realizadas por las entidades territoriales a las víctimas del conflicto armado interno, generando reportes y análisis de cifras.

VERSIÓN: 1.2

CATEGORÍA: Sistema de apoyo

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: Mesa de servicios

TELÉFONO: Marcación abreviada 5

CORREO: SOPORTE.OTI@UNIDADVICTIMAS.GOV.CO

FECHA DE VENCIMIENTO DEL SOPORTE: 01/08/2019

RESPONSABLE TÉCNICO: Servicios TI

RESPONSABLE FUNCIONAL: Dirección de gestión social humanitaria – Beatriz Ochoa

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: .NET 2012

PLATAFORMA BD: ORACLE 11G

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Asociados\G. Asistencia y Reparación\2014_A_AF

ARQUITECTURA TECNOLÓGICA: WEB

26. PAARI ADOLESCENTES

NOMBRE DEL SISTEMA: PAARI ADOLESCENTES

SIGLA:

DESCRIPCIÓN DEL SISTEMA: Captura de variables de caracterización de hogares con presencia de adolescentes

VERSIÓN: 1.0

CATEGORÍA: Soporte

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: N/A

TELEFONO: N/A

CORREO: N/A

FECHA DE VENCIMIENTO DEL SOPORTE: N/A

RESPONSABLE TÉCNICO: N/A

RESPONSABLE FUNCIONAL: N/A

ESTADO: Inactivo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: BPM ESIGNA

PLATAFORMA BD: ORACLE 11G

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Nuevos\G. Reparación\2015_DGSH_PAARIAD

ARQUITECTURA TECNOLÓGICA: WEB

27. LEX TRANSFER

NOMBRE DEL SISTEMA: LEX TRANSFER

SIGLA: LEX TRANSFER

DESCRIPCIÓN DEL SISTEMA: Esta aplicación permite realizar cargues masivos de tutelas, PQR y recursos en lex desde el sistema de gestión documental

VERSIÓN: 1.0

CATEGORÍA: Soporte

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: Mesa de servicios

TELEFONO: Marcación abreviada 5

CORREO: SOPORTE.OTI@UNIDADVICTIMAS.GOV.CO

FECHA DE VENCIMIENTO DEL SOPORTE: 01/08/2019

RESPONSABLE TÉCNICO: Servicios TI

RESPONSABLE FUNCIONAL: SUBDIRECCION GENERAL - YOLANDA GUERRERO

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: C#

PLATAFORMA BD: Oracle

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Nuevos\G. Respuesta Escrita\2013_GJ_LEX

ARQUITECTURA TECNOLÓGICA: WEB

**28. LEX GENERATOR****NOMBRE DEL SISTEMA:** LEX GENERATOR**SIGLA:****DESCRIPCIÓN DEL SISTEMA:** Esta aplicación permite la radicación de documentos generados por LEX hacia el sistema de gestión documental en casos de tutelas, PQR y recursos**VERSIÓN:** 1.0**CATEGORÍA:** Soporte**TIPO DE DESARROLLO:** Desarrollo propio**FABRICANTE:** Oficina de tecnología**PROVEEDOR DE SOPORTE:****NOMBRE:** Mesa de servicios**TELEFONO:** Marcación abreviada 5**CORREO:** SOPORTE.OTI@UNIDADVICTIMAS.GOV.CO**FECHA DE VENCIMIENTO DEL SOPORTE:** 01/08/2019**RESPONSABLE TÉCNICO:** Servicios TI**RESPONSABLE FUNCIONAL:** SUBDIRECCION GENERAL - YOLANDA GUERRERO**ESTADO:** Activo**FECHA INACTIVACIÓN:** N/A**LICENCIAMIENTO:** N/A**SISTEMA OPERATIVO:** Windows server 2012 R2**LENGUAJE DE PROGRAMACIÓN:** .NET**PLATAFORMA BD:** ORACLE 11G**DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:**

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Nuevos\G. Respuesta

Escrita\2013_GJ_LEX\2016_12074_GJ_LEX_GENERATOR_PQR

ARQUITECTURA TECNOLÓGICA: WEB**29. ARANDA****NOMBRE DEL SISTEMA:** ARANDA**SIGLA:** ARANDA**DESCRIPCIÓN DEL SISTEMA:** Registrar, escalar y facilitar el trámite de los casos que ameritan soporte técnico telefónico o especializado sobre los recursos tecnológicos de la unidad a los usuarios finales**VERSIÓN:** 8.7.1.0**CATEGORÍA:** Soporte**TIPO DE DESARROLLO:** Servicio asociado**FABRICANTE:** Oficina de tecnología**PROVEEDOR DE SOPORTE:****NOMBRE:** ERT**TELEFONO:** 6919201 ó 2577116

CORREO: ajcure@aisconsultoria.com.co
FECHA DE VENCIMIENTO DEL SOPORTE: 13/12/2018
RESPONSABLE TÉCNICO: Fernando Camargo
RESPONSABLE FUNCIONAL: Fernando Camargo
ESTADO: Activo
FECHA INACTIVACIÓN: N/A
LICENCIAMIENTO: N/A
SISTEMA OPERATIVO: Windows server 2012 R2
LENGUAJE DE PROGRAMACIÓN: PHP
PLATAFORMA BD: WEB CON BD CENTRAL
DOCUMENTACIÓN TÉCNICA Y FUNCIONAL: N/A
ARQUITECTURA TECNOLÓGICA: WEB

30. ASDOC

NOMBRE DEL SISTEMA: ASDOC

SIGLA: ASDOC

DESCRIPCIÓN DEL SISTEMA: Sistema que permite gestionar y consultar los diferentes tipos documentales, desde su radicación, hasta su digitalización y consulta de imágenes en línea.

VERSIÓN: 1.0

CATEGORÍA: Soporte

TIPO DE DESARROLLO: Legado

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: Subdirección de Valoración y Registro

TELEFONO: N/A

CORREO: adimin.svr@unidadvictimas.gov.co

FECHA DE VENCIMIENTO DEL SOPORTE: 31/12/2018

RESPONSABLE TÉCNICO: Subdirección de Valoración y Registro

RESPONSABLE FUNCIONAL: SUBDIRECCION DE VALORACION Y REGISTRO - JHON PEMBERTI

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: PHP

PLATAFORMA BD: MYSQL

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Nuevos\G. Registro y Valoración\2013_VR_ASDOC

ARQUITECTURA TECNOLÓGICA: WEB



31. AHE, EMERGENCIAS Y RETORNOS

NOMBRE DEL SISTEMA: AHE, EMERGENCIAS Y RETORNOS

SIGLA:

DESCRIPCIÓN DEL SISTEMA: ES UNA APLICACIÓN DE CONSULTA DE INFORMACIÓN DE AHE Y CARACTERIZACIÓN DE HOGARES DE EMERGENCIA Y RETORNOS

VERSIÓN: 1.0

CATEGORÍA: Misional

TIPO DE DESARROLLO: Legado

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: NA

TELEFONO: NA

CORREO: NA

FECHA DE VENCIMIENTO DEL SOPORTE: NA

RESPONSABLE TÉCNICO: N/A

RESPONSABLE FUNCIONAL: N/A

ESTADO: Inactivo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: .NET C#

PLATAFORMA BD: ORACLE 11G

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Nuevos\G. Asistencia\2013_A_AHE

ARQUITECTURA TECNOLÓGICA: WEB

32. MANTIS

NOMBRE DEL SISTEMA: MANTIS

SIGLA: MANTIS

DESCRIPCIÓN DEL SISTEMA: Sistema que permite la creación, seguimiento y asignación de incidencias de un software que se presentan cuando ésta se encuentra en estado de desarrollo

VERSIÓN: 1.0

CATEGORÍA: Soporte

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE: NA

NOMBRE: NA

TELEFONO: N/A

CORREO: NA
FECHA DE VENCIMIENTO DEL SOPORTE: NA
RESPONSABLE TÉCNICO: N/A
RESPONSABLE FUNCIONAL: N/A
ESTADO: Activo
FECHA INACTIVACIÓN: N/A
LICENCIAMIENTO: N/A
SISTEMA OPERATIVO: Windows server 2012 R2
LENGUAJE DE PROGRAMACIÓN: PHP
PLATAFORMA BD: MYSQL
DOCUMENTACIÓN TÉCNICA Y FUNCIONAL: NA
ARQUITECTURA TECNOLÓGICA: WEB

33. SIRAV

NOMBRE DEL SISTEMA: SISTEMA DE INFORMACION VICTIMAS DE LA VIOLENCIA

SIGLA: Sirav

DESCRIPCIÓN DEL SISTEMA: Corresponde a una herramienta transitoria, permite la captura y administración de la información asociada a los procesos de la ley 1290:1. Registro (siniestros, víctimas, beneficiarios, documentos, oficios, pagos), 2. Administración (roles, permisos), 3. Archivo de bancos: (generación de archivo pagos, respuesta bancos), 4. Validación y registro 1290 y apalancar los procesos de notificación de la unidad y en especial de la SVR

VERSIÓN: 1.0

CATEGORÍA: Misional

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE

NOMBRE: SUBDIRECCION DE VALORACION Y REGISTRO

TELEFONO N/A

CORREO: ADIMIN.SVR@UNIDADVICTIMAS.GOV.CO

FECHA DE VENCIMIENTO DEL SOPORTE: 31/12/2018

RESPONSABLE TÉCNICO: Subdirección de Valoración y Registro

RESPONSABLE FUNCIONAL: SUBDIRECCION DE VALORACION Y REGISTRO - JHON PEMBERTI

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: .NET

PLATAFORMA BD: ORACLE 11G

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Nuevos\G. Registro y Valoración\2014_VR_SIRAVTEMP

ARQUITECTURA TECNOLÓGICA: WEB



34. SISTEMA DE INFORMACION VICTIMAS DE LA VIOLENCIA

NOMBRE DEL SISTEMA: SISTEMA DE INFORMACION VICTIMAS DE LA VIOLENCIA

SIGLA: SIV

DESCRIPCIÓN DEL SISTEMA: Sistema de información 418, base de datos en Oracle que registra la información de las víctimas con cobertura por la vigencia de la ley 418. Permite la captura y administración de la información asociada a los procesos de la ley 418: 1. Registro (siniestros, víctimas, beneficiarios, documentos, oficios, pagos) 2. Administración (roles, permisos) 3. Archivo de bancos: (generación de archivo pagos, respuesta bancos)

VERSIÓN: 1.0

CATEGORÍA: Misional

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: SUBDIRECCION DE VALORACION Y REGISTRO

TELEFONO N/A

CORREO: ADIMIN.SVR@UNIDADVICTIMAS.GOV.CO

FECHA DE VENCIMIENTO DEL SOPORTE: N/A

RESPONSABLE TÉCNICO: SUBDIRECCION DE VALORACION Y REGISTRO

RESPONSABLE FUNCIONAL: SUBDIRECCION DE VALORACION Y REGISTRO - JHON PEMBERTI

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: .NET

PLATAFORMA BD: ORACLE 11G

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Legados\G. Registro y Valoración\2012_VYR_SIV

ARQUITECTURA TECNOLÓGICA: WEB

35. SIPOD: SISTEMA DE INFORMACIÓN PARA LA POBLACIÓN DESPLAZADA

NOMBRE DEL SISTEMA: SIPOD: SISTEMA DE INFORMACIÓN PARA LA POBLACIÓN DESPLAZADA

SIGLA: SIPOD

DESCRIPCIÓN DEL SISTEMA: Sistema de información que permite la radicación, captura y estado de valoración de la declaración de desplazados

VERSIÓN: 1.0

CATEGORÍA: Misional



TIPO DE DESARROLLO: Legado
FABRICANTE: Oficina de tecnología
PROVEEDOR DE SOPORTE:
NOMBRE: SUBDIRECCION DE VALORACION Y REGISTRO
TELEFONO: N/A
CORREO: ADIMIN.SVR@UNIDADVICTIMAS.GOV.CO
FECHA DE VENCIMIENTO DEL SOPORTE: 31/12/2018
RESPONSABLE TÉCNICO: SUBDIRECCION DE VALORACION Y REGISTRO
RESPONSABLE FUNCIONAL: SUBDIRECCION DE VALORACION Y REGISTRO - JHON PEMBERTI
ESTADO: Activo
FECHA INACTIVACIÓN: N/A
LICENCIAMIENTO: N/A
SISTEMA OPERATIVO: Windows server 2012 R2
LENGUAJE DE PROGRAMACIÓN: .NET 2005
PLATAFORMA BD: ORACLE 11G
DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:
\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Legados\G. Registro y Valoración\2006_VYR_SIPOD
ARQUITECTURA TECNOLÓGICA: WEB

36. ASTREA

NOMBRE DEL SISTEMA: ASTREA
SIGLA: ASTREA
DESCRIPCIÓN DEL SISTEMA: Sistema de información para el trámite de procesos judiciales asociados a hechos victimizantes de desplazamiento
VERSIÓN: 1.0
CATEGORÍA: Soporte
TIPO DE DESARROLLO: Legado
FABRICANTE: DPS
PROVEEDOR DE SOPORTE:
NOMBRE: MESA
TELEFONO: N/A
CORREO: N/A
FECHA DE VENCIMIENTO DEL SOPORTE: N/A
RESPONSABLE TÉCNICO:
RESPONSABLE FUNCIONAL: OFICINA DE TECNOLOGIAS DE LA INFORMACION - JAIME CANAVAL
ESTADO: Activo
FECHA INACTIVACIÓN: N/A
LICENCIAMIENTO: N/A
SISTEMA OPERATIVO: Windows server 2012 R2
LENGUAJE DE PROGRAMACIÓN: .NET C#



PLATAFORMA BD: ORACLE 11G

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Nuevos\G. Respuesta Escrita\2013_GJ_LEX\ORGANIZAR\Versión 1_UARIV\2. Solicitudes y Documentos Implementación

ARQUITECTURA TECNOLÓGICA: WEB

37. SISTEMA DE INFORMACIÓN DE GESTIÓN DE OFERTA

NOMBRE DEL SISTEMA: SISTEMA DE INFORMACIÓN DE GESTIÓN DE OFERTA

SIGLA: SIGO

DESCRIPCIÓN DEL SISTEMA: Sistema de información de gestión de oferta gestiona y articula la oferta necesaria derivada de cada una de las áreas misionales de la unidad con el resto del sistema (snariv) buscando la focalización de la población víctima a atender según el objetivo de cada programa.

VERSIÓN: 2.03

CATEGORÍA: Estratégico

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: GRUPO DE OFERTA

TELÉFONO: 7965150 - 3447 / 3446

CORREO: soporte.oferta@unidadvictimas.gov.co

FECHA DE VENCIMIENTO DEL SOPORTE: 31/12/2018

RESPONSABLE TÉCNICO: Grupo de Oferta

RESPONSABLE FUNCIONAL: DIRECCIONES DE GESTIÓN INTERINSTITUCIONAL-VILMA RODRIGUEZ

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: .NET

PLATAFORMA BD: SQL SERVER

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Nuevos\G. Interinstitucional\2015_GO_SIGO

ARQUITECTURA TECNOLÓGICA: WEB

38. SEGUIMIENTO A POLÍTICA PÚBLICA

NOMBRE DEL SISTEMA: SEGUIMIENTO A POLÍTICA PÚBLICA

SIGLA: ESIGNA

DESCRIPCIÓN DEL SISTEMA: Realizar el seguimiento permanente que permita evidenciar la ejecución e implementación de la política pública para las víctimas, en



donde se evidencie el avance en el goce efectivo de los derechos y la superación del estado de vulnerabilidad de la población víctima del conflicto. Teniendo en cuenta la formulación y ejecución de los planes, programas, proyectos y acciones específicas tendientes a la atención y reparación integral que las víctimas necesitan de un esfuerzo conjunto de las entidades públicas a nivel nacional y territorial.

VERSIÓN: 1.0

CATEGORÍA: Misional

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: INDENOVA

PROVEEDOR DE SOPORTE:

NOMBRE: INDENOVA

TELEFONO:

CORREO: <https://jira.indenova.eu/>

FECHA DE VENCIMIENTO DEL SOPORTE: 31/07/2018

RESPONSABLE TÉCNICO: Claudia Morato

RESPONSABLE FUNCIONAL: SNARIV - GERARDO LOPEZ

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: BPM

PLATAFORMA BD: ORACLE 11G

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Nuevos\G. Interinstitucional\2014_CSNARIV_SPP

ARQUITECTURA TECNOLÓGICA: WEB

39. INDICE DE CONDICIONES DE RECONCILIACION NACIONAL

NOMBRE DEL SISTEMA: INDICE DE CONDICIONES DE RECONCILIACION NACIONAL

SIGLA: ICRN

DESCRIPCIÓN DEL SISTEMA: Sistema de información que permite a las entidades territoriales alimentar y visualizar indicadores cualitativos y cuantitativos que faciliten la medición del índice de reconciliación que existen entre los municipios de Colombia. El proyecto actualmente contempla un piloto de 113 municipios.

VERSIÓN: 1.1

CATEGORÍA: Estratégico

TIPO DE DESARROLLO: Contratación otras dependencias

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: N/A

TELEFONO: N/A

CORREO: N/A

FECHA DE VENCIMIENTO DEL SOPORTE: N/A



RESPONSABLE TÉCNICO: N/A

RESPONSABLE FUNCIONAL: N/A

ESTADO: Inactivo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: .NET 2012

PLATAFORMA BD: ORACLE 11G

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Legados\G. Reparación\2015_R_ICRN

ARQUITECTURA TECNOLÓGICA: WEB

40. ÍNDICE DE RIESGO DE VICTIMIZACION

NOMBRE DEL SISTEMA: ÍNDICE DE RIESGO DE VICTIMIZACION

SIGLA: IRV

DESCRIPCIÓN DEL SISTEMA: Esta aplicación permite a la persona consultar el Índice de Victimización en cualquier parte de Colombia, indicándole con una serie de colores si es bajo, medio bajo, medio, medio alto y alto.

Esta aplicación no necesita de tener usuario ni contraseña ya que cualquier persona puede entrar a la página y consultar

VERSIÓN: 1

CATEGORÍA: Estratégico

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: N/A

TELÉFONO: N/A

CORREO: N/A

FECHA DE VENCIMIENTO DEL SOPORTE: N/A

RESPONSABLE TÉCNICO: N/A

RESPONSABLE FUNCIONAL: DIRECCION DE REPARACION - ANGELICA MORENO

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: Java

PLATAFORMA BD: ORACLE

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Legados\G. Atención al Ciudadano\2011_A_IRV

ARQUITECTURA TECNOLÓGICA: WEB





41. AYUDA HUMANITARIA INMEDIATA

NOMBRE DEL SISTEMA: AHÍ

SIGLA: AHÍ

DESCRIPCIÓN DEL SISTEMA: Brindar a los enlaces territoriales una herramienta para la consulta de estado de las personas en registro y con base en ella tomar una decisión de gestionar o no la asistencia humanitaria inmediata

VERSIÓN: 1.0

CATEGORÍA: Misional

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: N/A

TELEFONO: N/A

CORREO: N/A

FECHA DE VENCIMIENTO DEL SOPORTE: N/A

RESPONSABLE TÉCNICO: N/A

RESPONSABLE FUNCIONAL: N/A

ESTADO: Inactivo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: .NET 2012

PLATAFORMA BD: ORACLE 11G

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de
Información\Sistemas Nuevos\G. Asistencia\2013_PAE_AHÍ

ARQUITECTURA TECNOLÓGICA: WEB

42. OFICINA DE CONTROL INTERNO

NOMBRE DEL SISTEMA: OFICINA DE CONTROL INTERNO

SIGLA: OCI

DESCRIPCIÓN DEL SISTEMA: Sistema para el seguimiento a planes de mejora

VERSIÓN: 2.0

CATEGORÍA: Seguimiento y control

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: Mesa de servicios

TELEFONO: Marcación abreviada 5

CORREO: SOPORTE.OTI@UNIDADVICTIMAS.GOV.CO

FECHA DE VENCIMIENTO DEL SOPORTE: 01/08/2019

RESPONSABLE TÉCNICO: Servicios TI

RESPONSABLE FUNCIONAL: OFICINA DE CONTROL INTERNO - CARLOS ARTURO ORDOÑEZ

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: C#, ENTITY DATA MODEL

PLATAFORMA BD: ORACLE 11G

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Nuevos\Oficina de Control Interno

ARQUITECTURA TECNOLÓGICA: WEB

43. SISTEMA DE INFORMACION REPARACION ADMINISTRATIVA

NOMBRE DEL SISTEMA: SISTEMA DE INFORMACION REPARACION ADMINISTRATIVA

SIGLA: SIRA

DESCRIPCIÓN DEL SISTEMA: Sistema de información de gestión de oferta gestiona y articula la oferta necesaria derivada de cada una de las áreas misionales de la unidad con el resto del sistema (snariv) buscando la focalización de la población víctima a atender según el objetivo de cada programa.

VERSIÓN: 2.03

CATEGORÍA: Sistema de Direccionamiento Estratégico

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: DPS

PROVEEDOR DE SOPORTE:

NOMBRE: GRUPO DE OFERTA

TELEFONO: 7965150 - 3447 / 3446

CORREO: soporte.oferta@unidadvictimas.gov.co

FECHA DE VENCIMIENTO DEL SOPORTE: 31/12/2018

RESPONSABLE TÉCNICO: Grupo de Oferta

RESPONSABLE FUNCIONAL: OFICINA DE TECNOLOGIAS DE LA INFORMACION - JAIME CANAVAL

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: .NET

PLATAFORMA BD: SQL SERVER

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Nuevos\G. Interinstitucional\2015_GO_SIGO

ARQUITECTURA TECNOLÓGICA: WEB



44. XLIRA

NOMBRE DEL SISTEMA: XLIRA

SIGLA: XLIRA

DESCRIPCIÓN DEL SISTEMA: Radicar de forma masiva documentos en Orfeo a partir de una planilla en Excel

VERSIÓN: 1.0

CATEGORÍA: Soporte

TIPO DE DESARROLLO: Legado

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: N/A

TELEFONO: N/A

CORREO: N/A

FECHA DE VENCIMIENTO DEL SOPORTE: N/A

RESPONSABLE TÉCNICO: N/A

RESPONSABLE FUNCIONAL: N/A

ESTADO: inactivo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: PHP

PLATAFORMA BD: EXCEL

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Legados\G. Documental\2013_GD_ORFEO\4. Manuales

ARQUITECTURA TECNOLÓGICA: WEB

45. INTERCAMBIO SEGURO DE INFORMACIÓN

NOMBRE DEL SISTEMA: INTERCAMBIO SEGURO DE INFORMACIÓN

SIGLA: INTERCAMBIO SEGURO DE INFORMACIÓN

DESCRIPCIÓN DEL SISTEMA: Proveer bandejas de intercambio de información entre usuarios registrados

VERSIÓN: 1.0

CATEGORÍA: Soporte

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE:

TELEFONO:

CORREO:

FECHA DE VENCIMIENTO DEL SOPORTE: N/A

RESPONSABLE TÉCNICO: N/A

RESPONSABLE FUNCIONAL: N/A

ESTADO: activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: ALFRESCO

PLATAFORMA BD: MYSQL

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL: \\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Legados\Red Nacional de las Información\Intercambio Seguro de Información

ARQUITECTURA TECNOLÓGICA: WEB

46. ADMINSIPOD SIPOD

NOMBRE DEL SISTEMA: ADMINSIPOD

SIGLA: ADMINSIPOD

DESCRIPCIÓN DEL SISTEMA: Aplicación que contiene las funcionalidades de administración del RUV temporal

VERSIÓN: 1

CATEGORÍA: Soporte

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: Subdirección de Valoración y Registro

TELÉFONO: N/A

CORREO: adimin.svr@unidadvictimas.gov.co

FECHA DE VENCIMIENTO DEL SOPORTE: N/A

RESPONSABLE TÉCNICO: N/A

RESPONSABLE FUNCIONAL: N/A

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: NET

PLATAFORMA BD: ORACLE 11G

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Legados\G. Registro y Valoración\VYR_ADMINRUV

ARQUITECTURA TECNOLÓGICA: WEB

47. ADMINRUV

NOMBRE DEL SISTEMA: ADMINRUV

SIGLA: ADMINRUV



DESCRIPCIÓN DEL SISTEMA: Aplicación que contiene las funcionalidades de administración del RUV temporal

VERSIÓN: 1.0

CATEGORÍA: Soporte

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: Subdirección de Valoración y Registro

TELEFONO: N/A

CORREO: adimin.svr@unidadvictimas.gov.co

FECHA DE VENCIMIENTO DEL SOPORTE: 31/12/2018

RESPONSABLE TÉCNICO: SUBDIRECCION DE VALORACION Y REGISTRO

RESPONSABLE FUNCIONAL: SUBDIRECCION DE VALORACION Y REGISTRO - JHON PEMBERTI

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: NET

PLATAFORMA BD: ORACLE 11G

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Legados\G. Registro y Valoración\VYR_ADMINRUV

ARQUITECTURA TECNOLÓGICA: WEB

48. SISTEMA DE INFORMACIÓN DE GESTIÓN DEL SUBCOMITÉ TÉCNICO DE ENFOQUE DIFERENCIAL

NOMBRE DEL SISTEMA: SISTEMA DE INFORMACIÓN DE GESTIÓN DEL SUBCOMITÉ TÉCNICO DE ENFOQUE DIFERENCIAL

SIGLA: SIGSTED

DESCRIPCIÓN DEL SISTEMA: Software de gestión de información para el control y seguimiento del plan operativo anual de este subcomité, los cuales comprenden: componentes, líneas de acción, medidas, objetivos específicos y acciones estratégicas y los resultados obtenidos en el seguimiento de los anteriores ítems.

VERSIÓN: 1

CATEGORÍA: Soporte

TIPO DE DESARROLLO: Contratación otras dependencias

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: SERGIO CANTE_CLAUDIA MORATO

TELEFONO: 7965150

CORREO: CLAUDIA.MORATO@UNIDADVICTIMAS.GOV.CO

FECHA DE VENCIMIENTO DEL SOPORTE: N/A

RESPONSABLE TÉCNICO: N/A



RESPONSABLE FUNCIONAL: N/A

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: EXCEL 2007

PLATAFORMA BD: ORACLE

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL: \\172.20.210.14\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Nuevos\G. Registro y Valoración\SISTEMA DE INFORMACIÓN DE GESTIÓN DEL SUBCOMITÉ TÉCNICO DE ENFOQUE DIFERENCIAL

ARQUITECTURA TECNOLÓGICA: WEB

49. HACKATON INMOBILIARIO PROVICTIMAS

NOMBRE DEL SISTEMA: HACKATON INMOBILIARIO PROVICTIMAS

SIGLA:

DESCRIPCIÓN DEL SISTEMA: Sistema móvil para el registro de bienes ofrecidos por el fondo de reparación

VERSIÓN: 1

CATEGORÍA: Soporte

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: N/A

TELÉFONO: N/A

CORREO: N/A

FECHA DE VENCIMIENTO DEL SOPORTE: N/A

RESPONSABLE TÉCNICO: N/A

RESPONSABLE FUNCIONAL: N/A

ESTADO: Inactivo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: USSD

PLATAFORMA BD: N/A

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL: N/A

TECNOLÓGICA: WEB

50. HACKATON VICTIMALZ

NOMBRE DEL SISTEMA: HACKATON VICTIMALZ

SIGLA:

DESCRIPCIÓN DEL SISTEMA: Sistema móvil para la difusión de la ley 1448 a través de un



juego interactivo

VERSIÓN: 1

CATEGORÍA: Soporte

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: N/A

TELEFONO: N/A

CORREO: N/A

FECHA DE VENCIMIENTO DEL SOPORTE: N/A

RESPONSABLE TÉCNICO: N/A

RESPONSABLE FUNCIONAL: N/A

ESTADO: Inactivo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: USSD

PLATAFORMA BD: N/A

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL: N/A

ARQUITECTURA TECNOLÓGICA: WEB

51. APLICACIÓN MOVIL - CONSULTA OFERTA

NOMBRE DEL SISTEMA: APLICACIÓN MOVIL - CONSULTA OFERTA

SIGLA:

DESCRIPCIÓN DEL SISTEMA: Desarrollo móvil para la presentación del mapa de oferta interactivo baja

VERSIÓN: 1

CATEGORÍA: Soporte

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: N/A

TELEFONO: N/A

CORREO: N/A

FECHA DE VENCIMIENTO DEL SOPORTE: N/A

RESPONSABLE TÉCNICO: N/A

RESPONSABLE FUNCIONAL: N/A

ESTADO: Inactivo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: USSD

PLATAFORMA BD: N/A

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL: N/A



ARQUITECTURA TECNOLÓGICA: WEB

52. HACKATON SUMATE

NOMBRE DEL SISTEMA: HACKATON SUMATE

SIGLA:

DESCRIPCIÓN DEL SISTEMA: Sistema móvil para el registro de donaciones a la unidad

VERSIÓN: 1

CATEGORÍA: Soporte

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: N/A

TELÉFONO: N/A

CORREO: N/A

FECHA DE VENCIMIENTO DEL SOPORTE: N/A

RESPONSABLE TÉCNICO: N/A

RESPONSABLE FUNCIONAL: N/A

ESTADO: Inactivo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: USSD

PLATAFORMA BD:

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

ARQUITECTURA TECNOLÓGICA: WEB

53. SISTEMA DE INFORMACIÓN DE SEGUIMIENTO Y CONTROL DE DESARROLLO

NOMBRE DEL SISTEMA: SISTEMA DE INFORMACIÓN DE SEGUIMIENTO Y CONTROL DE DESARROLLO

SIGLA: SISCOD

DESCRIPCIÓN DEL SISTEMA: Sistema de información que permite llevar el registro de todos los desarrollos hechos en la OTI y sus respectivos requerimientos y actividades ejecutadas por cada funcionario asociados a los mismos

VERSIÓN: 1.8

CATEGORÍA: Soporte

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: MARCO MONTOYA

TELÉFONO: N/A

CORREO: marco.montoya@unidadvictimas.gov.co

FECHA DE VENCIMIENTO DEL SOPORTE: 31/12/2018

RESPONSABLE TÉCNICO: Marco Montoya



RESPONSABLE FUNCIONAL: Marco Montoya

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: PHP

PLATAFORMA BD: ORACOL 11 G, R2

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de
Información\Sistemas Nuevos\G. Tecnologías de la Información\2016_SI_SISCOD

ARQUITECTURA TECNOLÓGICA: WEB

54. SISTEMA DE VOTACIÓN

NOMBRE DEL SISTEMA: SISTEMA DE VOTACIÓN

SIGLA: SISTEMA DE VOTACIÓN

DESCRIPCIÓN DEL SISTEMA: Sistema de información que permite a los usuarios de planta de la unidad realizar la elección por cada jornada electoral. Audita IP, hora y usuario de la votación.

VERSIÓN: 1.0

CATEGORÍA: Soporte

TIPO DE DESARROLLO: Desarrollo propio

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: Mesa de servicios

TELÉFONO: Marcación abreviada 5

CORREO: SOPORTE.OTI@UNIDADVICTIMAS.GOV.CO

FECHA DE VENCIMIENTO DEL SOPORTE: 01/08/2019

RESPONSABLE TÉCNICO: Servicios TI

RESPONSABLE FUNCIONAL: N/A

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: .NET

PLATAFORMA BD: SQL SERVER

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL: \\172.20.210.14\Unidad_Victimas\Oficina de
Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Nuevos\G.
Información\SISTEMA DE VOTACION

ARQUITECTURA TECNOLÓGICA: WEB

55. VISOR GEOGRÁFICO

NOMBRE DEL SISTEMA: VISOR GEOGRÁFICO

SIGLA: VISOR GEOGRÁFICO



DESCRIPCIÓN DEL SISTEMA: El visor geográfico permite la visualización de datos consolidados en bases de datos coordinados por la Red Nacional de Información, que guardan relación espacial para la generación de mapas temáticos, entre otros beneficios. Esto permite complementar el análisis de la información generada y la producción de documentos.

VERSIÓN: 1.0

CATEGORÍA: Soporte

TIPO DE DESARROLLO: CONTRATACION OTRAS DEPENDENCIAS

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: SANDRA BACCA

TELEFONO: 4261111

LÍNEA DE ATENCIÓN NACIONAL

01 8000 911 119

LÍNEA DE ATENCIÓN EN BOGOTÁ

(+57 1) 4 26 1111

CORREO: rni@unidadvictimas.gov.co

FECHA DE VENCIMIENTO DEL SOPORTE: N/A

RESPONSABLE TÉCNICO: N/A

RESPONSABLE FUNCIONAL: N/A

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: .NET

PLATAFORMA BD: ORACOL 11 G, R2

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\172.20.210.14\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Nuevos\G. Información\VISOR GEOGRAFICO

ARQUITECTURA TECNOLÓGICA: WEB

56. SIGGESTION

NOMBRE DEL SISTEMA: SIGGESTION

SIGLA: SIGGESTION

DESCRIPCIÓN DEL SISTEMA: El aplicativo SIGGESTION es una herramienta que permite formular y registrar el seguimiento a los planes de acción que registra cada dependencia, a través de validaciones que realiza la oficina asesora de planeación

VERSIÓN: 1.0

CATEGORÍA: Estratégico

TIPO DE DESARROLLO: CONTRATACION OTRAS DEPENDENCIAS

FABRICANTE: DNP

PROVEEDOR DE SOPORTE:

NOMBRE: RAFAEL BOSIGA

TELEFONO: 7965150

CORREO: Rafael.Bosiga@unidadvictimas.gov.co

FECHA DE VENCIMIENTO DEL SOPORTE: N/A

RESPONSABLE TÉCNICO: RAFAEL BOSIGA



RESPONSABLE FUNCIONAL: LILIANA GONZALEZ, EDUARDO TORRES, CARLOS PATARROYO, TATIANA FORERO

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: .NET

PLATAFORMA BD: ORACOL 11 G, R2

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\172.20.210.14\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Nuevos\Planeación

ARQUITECTURA TECNOLÓGICA: WEB

57. PAZ A LA VOZ

NOMBRE DEL SISTEMA: PAZ A LA VOZ

SIGLA:

DESCRIPCIÓN DEL SISTEMA: Multimedia que integra 4 retos y videos cortos explicativos, a través de los cuales los niños, niñas y adolescentes podrán aprender los conceptos claves del protocolo de participación. Los usuarios pueden dejar sus ideas o comentarios al final de la multimedia, los cuales pasan a ser parte de un aplicativo en Facebook, en el que pueden leer su idea y las de los demás que hayan navegado la multimedia.

VERSIÓN: 1.0

CATEGORÍA: Apoyo

TIPO DE DESARROLLO: CONTRATACION OTRAS DEPENDENCIAS

FABRICANTE: Oficina de tecnología

PROVEEDOR DE SOPORTE:

NOMBRE: FABIO MEDINA

TELEFONO: 7965150

CORREO: FABIO.MEDINA@UNIDADVICTIMAS.GOV.CO

FECHA DE VENCIMIENTO DEL SOPORTE: N/A

RESPONSABLE TÉCNICO: N/A

RESPONSABLE FUNCIONAL: N/A

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: .NET

PLATAFORMA BD: ORACOL 11 G, R2

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL: N/A

ARQUITECTURA TECNOLÓGICA: WEB

58. CENTRO DE OPERACIÓN Y MONITOREO

NOMBRE DEL SISTEMA: CENTRO DE OPERACIÓN Y MONITOREO



SIGLA: COMRS

DESCRIPCIÓN DEL SISTEMA: Captura de información referente a desplazamientos en terreno de los funcionarios de la UNIDAD durante la ejecución de sus comisiones. Monitoreo y acompañamiento de comisiones en terreno

VERSIÓN: 1.0

CATEGORÍA: Seguimiento y control

TIPO DE DESARROLLO: Adquirido sin modificación

FABRICANTE: USAID

PROVEEDOR DE SOPORTE:

NOMBRE: Mesa de servicios

TELEFONO: Marcación abreviada 5

CORREO: SOPORTE.OTI@UNIDADVICTIMAS.GOV.CO

FECHA DE VENCIMIENTO DEL SOPORTE: 01/08/2019

RESPONSABLE TÉCNICO: Servicios TI

RESPONSABLE FUNCIONAL: Luis Fernando Ortiz Montaña

ESTADO: Activo

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: .NET

PLATAFORMA BD: SQL SERVER

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\totoro\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Nuevos\Oficina de Control Interno\2016_CID_GCI

ARQUITECTURA TECNOLÓGICA: WEB

59. PIAVV

NOMBRE DEL SISTEMA: PIAVV

DESCRIPCIÓN DEL SISTEMA: Herramienta fundamental para la atención de las víctimas, debido a que desde esta se registra, ingresa, valida y se efectúan las consultas disponibles, consulta al registro único de víctimas y consulta de atención humanitaria.

VERSIÓN: 1

CATEGORÍA: ESTRATEGICO

TIPO DE DESARROLLO: PROPIO

FABRICANTE: OTI

PROVEEDOR DE SOPORTE:

NOMBRE: JAIME CANAVAL

TELEFONO: 7965150

CORREO: Jaime.canaval@unidadvictimas.gov.co

FECHA DE VENCIMIENTO DEL SOPORTE:

RESPONSABLE TÉCNICO:

RESPONSABLE FUNCIONAL: FABIOLA PERDOMO

ESTADO: Desarrollo

FECHA INACTIVACIÓN: N/A



LICENCIAMIENTO:

SISTEMA OPERATIVO: Windows server 2012 R2

LENGUAJE DE PROGRAMACIÓN: PHP

PLATAFORMA BD: SQL Server 2012

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

\\172.20.210.14\Unidad_Victimas\Oficina de Tecnología\130.169 PROYECTOS\Sistemas de Información\Sistemas Nuevos\Direcciones Territoriales

ARQUITECTURA TECNOLÓGICA: WEB

60. SISPAE – MÓVIL

NOMBRE DEL SISTEMA: SISPAE – MÓVIL

DESCRIPCIÓN DEL SISTEMA: Despliegue y disposición de la información de las cifras relacionadas la Ayuda Humanitaria de Emergencia.

VERSIÓN: 1.0

CATEGORÍA: APOYO

TIPO DE DESARROLLO: PROPIO

FABRICANTE: OTI

PROVEEDOR DE SOPORTE:

NOMBRE: ANDRES QUINTERO

TELÉFONO:

CORREO:

FECHA DE VENCIMIENTO DEL SOPORTE:

RESPONSABLE TÉCNICO:

RESPONSABLE FUNCIONAL: CONSUELO BARRERA PARRADO

ESTADO: Desarrollo

FECHA INACTIVACIÓN:

LICENCIAMIENTO:

SISTEMA OPERATIVO:

LENGUAJE DE PROGRAMACIÓN:

PLATAFORMA BD: WINDOWS SERVER 2012 R2

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

ARQUITECTURA TECNOLÓGICA: WEB

61. ENCUESTADOR MOVIL - PENDIENTE TITULARIDAD Y DOCUMENTACION TECNICA COMPLETA

NOMBRE DEL SISTEMA: ENCUESTADOR MOVIL

SIGLA:

DESCRIPCIÓN DEL SISTEMA: Aplicar la encuesta de caracterización usando dispositivos móviles

VERSIÓN: 1.0

CATEGORÍA

TIPO DE DESARROLLO: WEB

FABRICANTE:



PROVEEDOR DE SOPORTE:

NOMBRE:

TELEFONO

CORREO:

FECHA DE VENCIMIENTO DEL SOPORTE:

RESPONSABLE TÉCNICO: Andrés Fernando Quintero Quiceno

RESPONSABLE FUNCIONAL: Fredy Leonardo Estupiñán Rincón

ESTADO: Producción

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO:

SISTEMA OPERATIVO

LENGUAJE DE PROGRAMACIÓN: HTML

PLATAFORMA BD: Oracle

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

[\\totoro\Red Nacional\Repositorio Documental Herramientas SRNI\Documentacion Convenio 1169](#)

ARQUITECTURA TECNOLÓGICA: WEB

62. INVENTARIO DE FUENTES

NOMBRE DEL SISTEMA: INVENTARIO DE FUENTES

SIGLA: NO DEFINIDA

DESCRIPCIÓN DEL SISTEMA: Mantener el inventario de fuentes de información que dispone la SRNI para la aplicación de la política pública

VERSIÓN: 1

CATEGORÍA: Sistema de apoyo

TIPO DE DESARROLLO: WEB

FABRICANTE: SUBDIRECCION RED NACIONAL DE INFORMACION

PROVEEDOR DE SOPORTE:

NOMBRE: MESA DE SERVICIO SRNI

TELEFONO: 5185454 EXT 407

CORREO: SOPORTE_RNI@UNIDADVICTIMAS.GOV.CO

FECHA DE VENCIMIENTO DEL SOPORTE:

RESPONSABLE TÉCNICO: Daniel Alfredo Correa Rodriguez

RESPONSABLE FUNCIONAL: Fabian Arley Arciniegas Duarte

ESTADO: Producción

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO: WINDOWS

LENGUAJE DE PROGRAMACIÓN: .NET

PLATAFORMA BD: Oracle

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

[\\totoro\Red Nacional\Repositorio Documental Herramientas SRNI\Vivanto\Vivanto - Inventario de Fuentes](#)



ARQUITECTURA TECNOLÓGICA: WEB

63. WEB SERVICES RUV

NOMBRE DEL SISTEMA: WEB SERVICES RUV

SIGLA: NO DEFINIDA

DESCRIPCIÓN DEL SISTEMA: El web service proporciona varios métodos para realizar consulta de datos de personas incluidas en los diferentes sistemas de información de la Red Nacional de Información.

VERSIÓN: 1

CATEGORÍA: Sistema de apoyo

TIPO DE DESARROLLO: WEB

FABRICANTE: SUBDIRECCIÓN RED NACIONAL DE INFORMACION

PROVEEDOR DE SOPORTE:

NOMBRE: MESA DE SERVICIO SRNI

TELEFONO: 5185454 EXT 407

CORREO: SOPORTE_RNI@UNIDADVICTIMAS.GOV.CO

FECHA DE VENCIMIENTO DEL SOPORTE:

RESPONSABLE TÉCNICO: Daniel Alfredo Correa Rodriguez

RESPONSABLE FUNCIONAL: Edward Heiler Giraldo Carvajal

ESTADO: Producción

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO

LENGUAJE DE PROGRAMACIÓN: .NET

PLATAFORMA BD: Oracle

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

[\\totoro\Red Nacional\Repositorio Documental Herramientas SRNI\Vivanto\Vivanto - WS Dinámicos y todos sus métodos](#)

ARQUITECTURA TECNOLÓGICA: WEB

64. GESTOR DE PROYECTOS

NOMBRE DEL SISTEMA: GESTOR DE PROYECTOS

SIGLA:

DESCRIPCIÓN DEL SISTEMA: El Módulo de Atención Territorial es un servicio de Vivanto, que permite a los usuarios realizar la inscripción, aprobación y entrega de beneficios a través de proyectos generados por la Unidad de Atención y Reparación Integral a Víctimas.

VERSIÓN: 1

CATEGORÍA

TIPO DE DESARROLLO: WEB

FABRICANTE: SUBDIRECCION RED NACIONAL DE INFORMACION

PROVEEDOR DE SOPORTE:

NOMBRE: MESA DE SERVICIO SRNI



TELEFONO 5185454 EXT 407

CORREO: SOPORTE_RNI@UNIDADVICTIMAS.GOV.CO

FECHA DE VENCIMIENTO DEL SOPORTE:

RESPONSABLE TÉCNICO: Daniel Alfredo Correa Rodriguez

RESPONSABLE FUNCIONAL: Edward Heiler Giraldo Carvajal

ESTADO: Producción

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO

LENGUAJE DE PROGRAMACIÓN: .NET

PLATAFORMA BD: Oracle

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

[\\totoro\Red_Nacional\Repositorio_Documental_Herramientas_SRNI\Vivanto\Vivanto - Proyectos Territoriales](#)

ARQUITECTURA TECNOLÓGICA: WEB

65. NOMBRE DEL SISTEMA: NODO DE TIERRAS

SIGLA: NO DIFINIDA

DESCRIPCIÓN DEL SISTEMA: Implementar servicios automáticos en intercambio de información entre las entidades que hacen parte del nodo de tierras en el marco de los artículos 153 y 76 de la Ley 1448 y sus decretos reglamentarios, aplicables a la etapa administrativa, judicial y postfallo, teniendo en cuenta los lineamientos de interoperabilidad establecidos por Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC)

VERSIÓN: 1

CATEGORÍA Sistema de apoyo

TIPO DE DESARROLLO: WEB

FABRICANTE: USAID – UNIDAD DE RESTITUCION DE TIERRAS

PROVEEDOR DE SOPORTE:

NOMBRE: MESA DE SERVICIO SRNI

TELEFONO 5185454 EXT 407

CORREO: SOPORTE_RNI@UNIDADVICTIMAS.GOV.CO quien redireccionará
NODOETIERRAS.RNI@UNIDADVICTIMAS.GOV.CO

FECHA DE VENCIMIENTO DEL SOPORTE:

RESPONSABLE TÉCNICO: Jesús Edison Murcia Rodríguez

RESPONSABLE FUNCIONAL: Jaime Andrés Molina Cano

ESTADO: En pruebas

FECHA INACTIVACIÓN: N/A

LICENCIAMIENTO: N/A

SISTEMA OPERATIVO

LENGUAJE DE PROGRAMACIÓN: .NET

PLATAFORMA BD: My SQL / Oracle

DOCUMENTACIÓN TÉCNICA Y FUNCIONAL:

[\\totoro\Red_Nacional\Repositorio_Documental_Herramientas_SRNI\Nodo de Tierras](#)

ARQUITECTURA TECNOLÓGICA: WEB

GLOSARIO

Nombre del sistema: Nombre completo del sistema de información.

Sigla: Sigla o nombre corto bajo el cual se conoce el sistema de información. Si aplica.

Descripción del sistema: Descripción funcional del sistema y los servicios que presta.

Versión: Versión actual y en producción del sistema de información

Categoría: Indique la categoría del sistema, de acuerdo con la clasificación del Marco de Referencia de Arquitectura Empresarial para la Gestión de TI en el Estado:

- Sistema misional
- Sistema de apoyo
- Portales digitales.
- Sistema de direccionamiento estratégico

Tipo de desarrollo:

- Desarrollo interno
- Desarrollo externo
- Adquirido sin modificaciones
- Adquirido con modificaciones
- Software como servicio

Fabricante: Compañía que construyó el sistema de información.

Proveedor de soporte: Nombre y contacto de la empresa que brinda soporte al sistema de información (correo electrónico, teléfono).

Fecha de vencimiento del soporte: Indique la fecha hasta la cual se tiene el contrato de mantenimiento o soporte del sistema con el proveedor.

Responsable técnico: Área, proveedor o persona responsable de atender los incidentes técnicos del sistema y datos de contacto.

Responsable funcional: Área, proveedor o persona con conocimiento sobre las funcionalidades del sistema y responsable de su administración y datos de contacto. **Estado:**

- Activo (El sistema se encuentra en producción)
- Inactivo (El sistema ya no está en uso)
- En desarrollo (El sistema está siendo construido o modificado)



Licenciamiento: Indique las características o modelo del licenciamiento del software, indicando por lo menos el tipo, número y vigencia del licenciamiento asignado. **Sistema Operativo:** Sistema(s) operativos(o) sobre los cuales funciona actualmente el sistema de información.

Lenguaje de programación: Lenguajes de programación y frameworks sobre los cuales fue construido el sistema de información. Ejemplos: Java 7, C#.Net framework 4.5, php 5.3, etc.

Plataforma de Base de datos: Ejemplo: Oracle, SQL server, Postgres, MySQL, entre otros.

Documentación técnica y funcional: Indique la ubicación (URL) de la documentación detallada técnica y funcional del sistema (Arquitectura, manuales, diseños, etc..) Arquitectura tecnológica: Stand Alone, web, cliente servidor, app móvil, software as a service (nube), etc.

Arquitectura de sistemas de información: Incluye la descripción detallada de cada una de los sistemas de información y las relaciones entre ellos.

Arquitectura de referencia: está formada por un documento o un conjunto de documentos que ofrecen estructuras e integraciones recomendadas de productos y servicios de TI para formar una solución.

Arquitectura de solución: Define los activos de TI, tales como aplicaciones o componentes utilizados para soportar las funciones y procesos de la organización.

Atributo: Características o cualidades de algo.

Artefacto: Es un producto que describe una arquitectura desde un punto de vista.

Catálogo. Es una lista detallada de los sistemas de información

Instrumento. Es un medio o recurso que se puede utilizar en el desarrollo de acciones para lograr un resultado deseado.

Sistema de Información. Conjunto de componentes interrelacionados que permiten gestionar y distribuir información para apoyar la toma de decisiones y el control en una institución.

BIBLIOGRAFIA

G.SIS.03 Guía para la construcción del catálogo de sistemas de información MINTIC



Anexo 2

Catálogo de Servicios TI

09/2018

OFICINA GESTIÓN DE LA INFORMACIÓN

Presentamos el catálogo de servicios que brinda la Oficina de Gestión de la Información, donde encontrará los recursos y servicios tecnológicos dispuestos para nuestros Usuarios de tal forma que se facilite el uso de la tecnología como fuente de transformación y articulación de las estrategias de la Unidad.

Entérese cómo las herramientas tecnológicas le pueden ayudar a hacer más eficaces sus labores

Página 1/50



CONTENIDO

1. GENERALIDADES	4
¿QUIÉNES SOMOS?.....	4
¿QUÉ HACEMOS?.....	4
NUESTRA FILOSOFÍA	4
2. CATÁLOGO SERVICIOS TECNOLÓGICO	5
2.1 SOLUCIONES COLABORATIVAS	6
2.1.1 CORREO CORPORATIVO	7
2.1.2 CORREOS MASIVOS.....	9
2.1.3 SKYPE EMPRESARIAL.....	11
2.1.4 TELEFONÍA.....	12
2.1.5 VIDEOCONFERENCIA.....	14
2.1.6 TELECONFERENCIA.....	16
2.1.7 FAXSERVER.....	18
2.2 SOLUCIÓN DE ALMACENAMIENTO DE INFORMACIÓN	20
2.2.1 SOLUCIÓN DE ALMACENAMIENTO DE INFORMACIÓN	20
2.3 DOTACIÓN TECNOLÓGIA PARA SU PUESTO DE TRABAJO.....	23
2.3.1 DOTACIÓN TECNOLÓGICA PUESTOS DE TRABAJO.....	24
2.3.2 LICENCIAMIENTO ESPECIAL	26
2.4 CONECTIVIDAD.....	28
2.4.1 INTERNET DEDICADO	29
2.4.2 CONECTIVIDAD.....	31
2.4.3 INTERNET INALÁMBRICO	33



2.4.4 Mi-Fi o Modem USB	35
2.5 SISTEMAS DE INFORMACIÓN	37
2.5.1 DESARROLLO	38
2.5.2 MANTENIMIENTO Y ADECUACIÓN	40
2.5.3 ASESORÍA	42
2.6 SOPORTE A USUARIOS	45
2.6.1 MESA DE SERVICIOS.....	45
2.7 SERVICIOS ADMINISTRATIVOS	47
2.7.1 ADMINISTRACIÓN DE SERVICIOS Y RECURSOS.....	48
2.7.2 ADMINISTRACIÓN TÉCNICA	49



1. GENERALIDADES

¿QUIÉNES SOMOS?

La Oficina de Gestión de la Información está conformada por un equipo de personas amables, entusiasta, dinámicas y altamente calificadas, que aportan con su conocimiento, experiencia y compromiso al desarrollo e implementación de soluciones tecnológicas que le permitan a La Unidad brindar una respuesta integral a las víctimas, para que sean y se sientan reparadas.

¿QUÉ HACEMOS?

Nos encargamos de la ejecución de programas, acciones y proyectos relacionados con las tecnologías de la información que adopta la Unidad en coordinación con las demás dependencias, así como de la administración de líneas de servicios tecnológicos, sistemas de información, equipos, redes, herramientas tecnológicas y soporte técnico, con la finalidad de brindarle a la Unidad servicios y recursos TI que generen valor agregado a sus estrategias y se vincule a los procesos de creación de valor.

NUESTRA FILOSOFÍA

- Ofrecer soluciones a la medida.
- Racionalizar la demanda de servicios y recursos tecnológicos.
- Controlar el rendimiento de la infraestructura y recursos informáticos.
- Atender las necesidades de TI dadas por las áreas de la Unidad.
- Apoyar a la Unidad en el cumplimiento de su misión y visión, a través de soluciones tecnológicas.

INDICADOR

El indicador de desempeño definido para todos los servicios es definido con una meta mínima de 92% mensual.



2. CATÁLOGO SERVICIOS TECNOLÓGICO

Con el objetivo de que conozca, use y adopte la tecnología dispuesta para usted a través de la Oficina de Tecnologías de la Información, hemos desarrollado este catálogo tecnológico, donde encontrará las herramientas, recursos, servicios y soluciones que le permitirán aumentar la productividad y enfocarse completamente en sus labores. Mediante la implementación de nuevas estrategias soportadas en la tecnología podremos alinear nuestros esfuerzos conjuntos, generar valor y aportar al cumplimiento de la misión y visión de la Unidad.

El catálogo tecnológico se compone de 8 soluciones y/o servicios que son:



A continuación, encontrará una definición de cada servicio, los beneficios que presta y la forma de acceder a ellos.



2.1 SOLUCIONES COLABORATIVAS



Correo electrónico



Correos masivos



Lync



Telefonía

Office 365



¿Se ha preguntado si ocupa mucho tiempo desplazándose por las diferentes áreas, sedes, oficinas y direcciones territoriales de la Unidad? ¿Desarrolla proyectos con otros compañeros que hacen parte del proceso que tiene a cargo? ¿Debe comunicarse al mismo tiempo con una o más persona que se encuentran lejos? ¿Es de los que lleva siempre una USB con los documentos que maneja frecuentemente? En caso que alguna de las respuestas sea si, esta información es importante para usted. La Oficina de Tecnologías de la Información - OTI ofrece varias soluciones para sus necesidades.





La Oficina de Tecnologías de la Información brinda herramientas colaborativas que le permiten contactarse con sus compañeros de trabajo, personal externo, proveedores y otros, en cualquier lugar y a través de diferentes medios, desde su equipo de Mesa, portátil, teléfono móvil, líneas de fax o espacios de video o teleconferencia, permitiéndole acceder siempre a toda su información (correo, calendario, contactos, documentos, voz y datos), desde cualquier lugar y puede generar ambientes colaborativos, para compartir o comunicar cualquier información.

Esta forma de trabajo colaborativa le evitará realizar desplazamientos innecesarios, consigue más beneficios al compartir documentación con otros compañeros, logrando que el conocimiento en la Unidad fluya y que todos dispongamos de la información más relevante, haciéndolo más eficiente y productivo; no tiene que empezar de cero cada trabajo y nos permite desde la Oficina de Tecnologías de la Información, a través de todas las herramientas tecnológicas, racionalizar, optimizar y garantizar un mejor servicio.

¡Usted cuenta con las siguientes soluciones colaborativas, aprovéchalas!

2.1.1 CORREO CORPORATIVO

DESCRIPCIÓN

Con la cuenta de correo electrónico nombre.apellido@unidadvictimas.gov.co de Outlook puede enviar y recibir información con sus compañeros, proveedores y otros.

CARACTERÍSTICAS

- Desde el segundo semestre del 2015, se amplió la capacidad de almacenamiento de 1GB a 50GB
- La función de búsqueda le permite encontrar lo que está buscando fácilmente en su bandeja de Outlook.
- Protección frente a correo no deseado.
- Puede sincronizar su calendario y contactos con la cuenta de correo.
- Puede administrar su calendario y compartirlo con otros compañeros.
- Puede conectarse desde su móvil a la cuenta de Outlook, revisar correos, sincronizar contactos, compartir su calendario y planificar su horario.
- Revise su correo remotamente desde cualquier equipo con conexión a internet, a través de OWA.
- Block de notas directamente en su correo.
- Cuentas con un espacio de archivado ilimitado para su buzón histórico.
- Puede realizar seguimiento sobre las tareas que planifique (estado, fecha inicio, fecha fin, prioridad, indicador de privacidad y recordatorio)

Página 7/50



- Le permite el envío de invitaciones y la administración de confirmación de asistencia, para organizar fácilmente sus reuniones y eventos.
- Puede personalizar su cuenta creando una firma de correo electrónico (revise las disposiciones de firma digital de la Oficina asesora de Comunicaciones).
- El correo cuenta con herramientas para prevenir la fuga de información.

ALCANCE

El servicio de correo electrónico está enfocado a las siguientes acciones que permitan el correcto y oportuno funcionamiento del medio electrónico de comunicación de los funcionarios y/o colaboradores de la Unidad para la reparación de las víctimas.

- Gestionar y administrar el acceso a las cuentas de correo en los equipos pertenecientes a la Unidad.
- Administrar y configurar calendario
- Realizar actividades de mantenimiento y soporte en las cuentas de correo como son aplicación de buzón, permisos de buzón, recuperación de correo electrónico y cancelación de cuentas
- Administrar y realizar actividades para el bloqueo de correos electrónicos considerados como un riesgo.

COBERTURA

- La disponibilidad de este servicio es del 99,8% y se presta en un horario de 7x24x365 días.
- La cobertura de este servicio es a nivel nacional.

ACCESO

Existen varios medios a través de los cuales puedes acceder a su cuenta de correo:

- En cualquier sitio, desde el navegador, ingrese a la página Web de la Unidad, a través del icono de correo
- En su equipo ingresando a Outlook.
- Desde su teléfono móvil o Tablet, previa configuración del personal de soporte OTI.

Para mayor información puede acceder a soporte técnico a través de la mesa de servicios tecnológicos SOYtec, marcando el 5, enviando un correo a la cuenta: sopORTE.oti@unidadvictimas.gov.co, o generando un caso por el Link <http://mesadeservicios.unidadvictimas.gov.co/usdkv8/#/login/> donde encontrará personas amables y con mucho conocimiento, dispuestas a resolver sus problemas tecnológicos.



SERVICIOS OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

- La Oficina de Tecnologías de la Información brinda cuentas de correo por demanda según las solicite Talento Humano o contratos, para funcionarios y contratistas, y realiza copias de seguridad periódicas de la información contenida en las cuentas de correo.
- Monitoreo permanente del servidor de correo.
- Alojamiento, soporte y administración del correo institucional.
- Implementación de planes de mantenimiento y seguridad al servidor de correo.
- Manual de usuario

BENEFICIARIO

Los servicios se prestan a los siguientes usuarios y/o colaboradores:

- Interno (funcionarios y contratistas)

2.1.2 CORREOS MASIVOS

DESCRIPCIÓN

¿Debe enviar correos masivos como parte de una campaña o necesita transmitir información a muchas personas? La Oficina de Tecnología brinda el servicio de envío de correos masivos a diferentes dominios (Gmail, Yahoo, Hotmail u otros diferentes al de la unidad @unidadvictimas) desde su cuenta de correo Outlook, que le permitirá llegar a más de 10.000 destinatarios desde la cuenta de correo institucional.

CARACTERÍSTICAS

- Construir y mantener listas de destinatarios, para realizar envíos segmentados.
- Importar contactos desde otra cuenta de correo o de archivos locales o servicios en la nube.
- Recuerde que si desea incluir logos e imágenes que requieran diseños gráficos debe contactar a la Oficina Asesora de Comunicaciones.
- El tamaño máximo del mensaje por para grandes grupos de distribución es de 2 MB.

ALCANCE

El envío de correos masivos tiene un alcance por demanda teniendo en cuenta que es un servicio restringido por la mantención de los niveles de seguridad de la Unidad, integridad de canales de comunicación y servidores.

Una vez solicitado el servicio a la mesa de servicios, esta solicitud se enviará al área encargada quien realizará la evaluación pertinente y ofrecerá el servicio conforme a las necesidades planteadas.

DISPONIBILIDAD Y COBERTURA

- Este servicio se presta en un horario de 5x8x365.
- La cobertura de este servicio es nacional.

ACCESO

Para acceder a este servicio debe seguir las instrucciones que presentamos a continuación:

- Debe contar con una cuenta de correo institucional (@unidadvictimas)
- Debe diligenciar un archivo Excel con destinatarios.
- Elabora el cuerpo del mensaje el cual debe incluir la firma, apóyate con la Oficina Asesora de Comunicaciones.
- En caso de enviar más de un mensaje masivo se requiere establecer la programación, definiendo fechas de envío de mensajes.
- Para mayor información puede acceder a soporte técnico a través de la mesa de servicios tecnológicos SOYtec, marcando el 5, enviando un correo a la cuenta: soporte.oti@unidadvictimas.gov.co, o generando un caso por el Link <http://mesadeservicios.unidadvictimas.gov.co/usdkv8/#/login/> donde encontrará personas amables y con mucho conocimiento, dispuestas a resolver sus problemas tecnológicos.

BENEFICIARIO

Los servicios se prestan a los siguientes usuarios y/o colaboradores:

- Interno (funcionarios y contratistas)



2.1.3 SKYPE EMPRESARIAL

DESCRIPCIÓN

Skype empresarial es un servicio que le permite conectarse con otras personas a través de mensajería instantánea, video llamadas y reuniones en línea. Con esta herramienta puede integrar diferentes opciones de comunicación y colaboración en la Unidad, al incorporar video y audio conferencia, compartir aplicaciones o su escritorio, y encontrar a cualquier persona en la Unidad, evitando desplazamientos innecesarios y realizando su labor de una manera más eficiente a través de la tecnología.

CARACTERÍSTICAS

Skype le permite:

- Encontrar al contacto correcto. Skype está conectado con Outlook, así que puede ubicar a cualquier persona en la Unidad que tenga una cuenta de correo corporativo.
- Puede comunicarse con la persona elegida, ya sea por mensajería instantánea, voz, video o compartiendo su escritorio o una aplicación.
- Skype se integra con las aplicaciones de Microsoft Office. Permite una experiencia colaborativa gracias a la facilidad de compartir documentos con otra persona, llamándola directamente desde la aplicación en la que está trabajando (Word, Excel, PowerPoint, etc.), en tiempo real.
- Puede acceder a Skype desde su teléfono móvil, descargando la aplicación gratuita.
- Además, puede establecer hasta 250 conexiones simultáneas en cada sala virtual.

ALCANCE

Herramienta para realizar interacción con otras personas de la Unidad de forma remota via chat o videoconferencia.

DISPONIBILIDAD Y COBERTURA

- La disponibilidad de este servicio es del 99,8% y se presta en un horario de 7x24x365 días.
- La cobertura de este servicio es mundial.

ACCESO

- Debe contar con una cuenta de correo institucional (@unidadvictimas).

- Puede ingresar a Skype desde su equipo, portátil o smartphone, con su correo como dirección de inicio de sesión y la contraseña con la que ingresa a su equipo o correo corporativo.
- Para mayor información puede acceder a soporte técnico a través de la mesa de servicios tecnológicos SOYtec, marcando el 5, enviando un correo a la cuenta: soporte.oti@unidadvictimas.gov.co, o generando un caso por el Link <http://mesadeservicios.unidadvictimas.gov.co/usdkv8/#/login/> donde encontrará personas amables y con mucho conocimiento, dispuestas a resolver sus problemas tecnológicos.

SERVICIOS OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

La Oficina de Tecnologías de la Información le brinda esta herramienta colaborativa y además ofrece:

- Configuración de Skype en su móvil.
- Soporte técnico desde SOYtec.
- Manual de usuario.*

BENEFICIARIO

Los servicios se prestan a los siguientes usuarios y/o colaboradores:

- Interno (funcionarios y contratistas)

2.1.4 TELEFONÍA

DESCRIPCIÓN

Cuenta con una infraestructura telefónica de última tecnología que le permite comunicarse internamente con el personal de la Unidad, solo marcando su extensión, y externamente marcando el 0 y el número al cual desea comunicarte; su teléfono IP le brinda múltiples configuraciones que facilitarán sus labores.

CARACTERÍSTICAS

La Unidad cuenta con una plataforma telefónica de alta disponibilidad y un teléfono IP, es decir que se comunica a través de internet y redes de telefonía pública, servicio que puede usar y personalizar con las siguientes opciones:

- Realizar llamadas internas marcando la extensión de cuatro dígitos y confirmando con OK, y externas marcando el 0 y enseguida el número telefónico.

Página 12/50



- Ajustar tonalidad y volumen de la llamada.
- Cuenta con teclas de función programables que le permiten transferir llamadas, mantener dos llamadas independientes en el mismo instante, realizar desvío de llamadas y devolución de llamadas.
- Puede ver el registro de llamadas perdidas, marcadas o recibidas.
- Puede realizar llamadas a nivel nacional, internacional y a celular, si está entre los designados en el Artículo 14, Decreto 1737 de 1998 y Artículo 1 del Decreto 1598 de 2011.

ALCANCE

El servicio de telefonía está enfocado a las acciones que permitan el correcto y oportuno funcionamiento de los medios de comunicación de los funcionarios y/o colaboradores de la Unidad para la Reparación de las Víctimas.

- Evaluar y garantizar el medio telefónico
- El buen uso de los activos de HW y SW que intervienen en el servicio
- Identificar oportunidades de mejora de HW y SW del entorno telefónico
- Realizar actividades de mantenimiento y soporte en el entorno de comunicaciones de Unidad para la reparación de las víctimas

DISPONIBILIDAD Y COBERTURA

- Este servicio se brinda en la sede principal, demás sedes en Bogotá y fuera de Bogotá en las diferentes territoriales, sedes y oficinas.
- La disponibilidad de este servicio es del 99,6% y se presta en un horario de 7x24x365 días.

ACCESO

- Para solicitar una nueva extensión telefónica requiere ser autorizado por el Jefe de Área, mediante correo, y posteriormente realizar la solicitud a través de SOYtec, marcando la tecla 5 desde cualquier teléfono de la Unidad.
- Si está entre los designados por el Artículo 14, Decreto 1737 de 1998 y Artículo 1 del Decreto 1598 de 2011 y requiere llamadas a celular, discado nacional o internacional, debe estar autorizado por Secretaría General y posteriormente marcar la tecla 5 para informar a SOYtec, desde cualquier teléfono de la Unidad.
- La solicitud debe estar acompañada por el formato diseñado para este tipo de requerimientos

SERVICIOS OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

- Cuenta con un directorio telefónico al cual puedes acceder a través de la Intranet, para conocer las extensiones de todo el personal de la Unidad.
- Tiene soporte técnico para el servicio de telefonía, a través de SOYtec, marcando el 5, enviando correo a soporte.oti@unidadvictimas.gov.co o generando un caso por el Link <http://mesadeservicios.unidadvictimas.gov.co/usdkv8/#/login/>; si es el caso, la Oficina de Tecnologías de la Información enviará personal para resolver la falla en el sitio.
- Cuenta con un manual de usuario donde describimos cómo hacer uso de todas las características y funcionalidades de su teléfono.

BENEFICIARIO

Los servicios se prestan a los siguientes usuarios y/o colaboradores:

- Interno (funcionarios y contratistas)

2.1.5 VIDEOCONFERENCIA

DESCRIPCIÓN

¿Sabía que cuenta con un entorno colaborativo visual, que le permite reunirse con las diferentes territoriales y oficinas de la Unidad, como si tuviera a sus compañeros en la misma sala?

Ahora puede hacerlo a través de las salas de videoconferencia que se han instalado en treinta y dos (32) oficinas de la Unidad, de manera que puede programar una junta o conferencia y comunicarse en tiempo real a través de audio y video, con personal de la Unidad para las Víctimas, y así ahorrar tiempo y evitar desplazamientos innecesarios, haciendo de su reunión una provechosa experiencia de video colaboración. Es una solución sencilla, accesible y segura, con la cual la Unidad se beneficia con mejores comunicaciones, mayor colaboración y toma de decisiones más rápidas, aprovechando las oportunidades de tener una Unidad interconectada.

CARACTERÍSTICAS

En la Unidad contamos actualmente con 32 salas de videoconferencia, desde donde podemos convocar a las demás salas a nivel nacional.

Página 14/50

La solución de salas de videoconferencia te permite:

- Comunicarse con las treinta y dos (32) oficinas que disponen del equipo de video al mismo tiempo, manteniendo comunicación visual y auditiva.
- Compartir su escritorio o la aplicación que esté usando, con todos los participantes de la reunión.
- Conectarte haciendo uso de diferentes modos de presentación:
 - Modo de enfoque, donde solo se observa en la pantalla a aquella persona que se encuentre hablando por más de cinco segundos.
 - Modo de autoenfoco, donde la cámara sigue a la persona que se está dirigiendo a los demás, en caso de que decida moverse.
 - Modo integral, donde podrá observar a la totalidad de las personas que participan de la reunión y si está conectado con más de una territorial, la pantalla se dividirá en el número de oficinas participantes, observándolos a todos.
- Establecer videoconferencias de forma segura, manteniendo las políticas de seguridad corporativas.
- Definir un moderador que se encargará de conceder la palabra a los miembros de la reunión y controlarlo remotamente.
- Conferencias sencillas y accesibles, fáciles de configurar y de usar.

ALCANCE

El servicio de videoconferencias está enfocado a las acciones que permitan una adecuada y optima gestión de los medios audiovisuales por parte de los funcionarios y/o colaboradores de la unidad de reparación para las víctimas y las Dirección territorial

- Administrar el agendamiento de ocupación de los equipos audiovisuales parte de la videoconferencia.
- Administrar los equipos y medios audiovisuales pertenecientes al equipo de videoconferencias
- Dar apoyo técnico y soporte a los funcionarios.

ACCESO

Para acceder a este servicio debe:



1. Confirmar disponibilidad y separar la sala donde se moderará, haciendo la solicitud con el área administrativa.
2. Contactar a la Mesa de Servicios Tecnológicos SOYtec, marcando la tecla 5 desde su teléfono , enviando un correo a sopORTE.oti@unidadvictimas.gov.co, o generando un caso por el Link <http://mesadeservicios.unidadvictimas.gov.co/usdkv8/#/login/> ; informando específicamente:
 - Sala moderadora.
 - Salas confirmadas con las cuales se comunicará.
 - Fecha.
 - Hora de inicio y de terminación.
 - Programa o área que convoca.
 - Persona de contacto.
 - Extensión telefónica.

DISPONIBILIDAD Y COBERTURA

- Este servicio está disponible en treinta y dos (32) oficinas y sedes de la Unidad y se presta en un horario de 5x8x365.
- Apoyo y soporte técnico durante tus videoconferencias.
- Manual de usuario.

BENEFICIARIO

Los servicios se prestan a los siguientes usuarios y/o colaboradores:

- Interno (funcionarios y contratistas)

2.1.6 TELECONFERENCIA

DESCRIPCIÓN

¿Sabía que desde su teléfono IP puede establecer una teleconferencia hasta con diez (10) personas? Así es. Este servicio le permitirá comunicarse por audio con hasta 10 personas que cuenten con teléfonos de la Unidad, en cualquier sede u oficina, e invitar a otros a su conversación telefónica para entablar una reunión laboral vía teléfono IP, evitando desplazamientos y sacando el mejor provecho de todas las herramientas colaborativas, a través de la conexión a internet dispuesta en la Unidad. Página 16/50

CARACTERÍSTICAS

La Unidad cuenta con una plataforma telefónica de alta disponibilidad y usted cuenta con un teléfono que puede usar para establecer una teleconferencia, ¿cómo hacerlo? Muy simple: comuníquese con un primer invitado marcando su extensión, después de que conteste presione la tecla consulta y confirme con la tecla OK, allí el teléfono le dará tono y deberá marcar la extensión del segundo usuario. Cuando le conteste, debe presionar la tecla conferencia y confirmar con OK, y puede iniciar su conferencia; en caso de ingresar necesitar más usuarios deberá realizar el mismo procedimiento.

Este servicio permite establecer multiconferencia o comunicación por voz con más de dos usuarios.

ALCANCE

Este servicio va dirigido a los funcionarios de la Unidad y permitirá comunicarse por audio con hasta 10 personas que cuenten con teléfonos de la Unidad.

DISPONIBILIDAD Y COBERTURA

- Este servicio se brinda en la sede principal, demás sedes en Bogotá y fuera de Bogotá en las diferentes territoriales, sedes y oficinas.
- La disponibilidad de este servicio es del 99,6% y se presta en un horario de 7x24x365 días.

ACCESO

Para acceder a este servicio solo debe contar con uno de los teléfonos de la Unidad y con las extensiones de las personas con las cuales establecerá la teleconferencia. ¡Es muy simple!

- Para mayor información puede acceder a soporte técnico, a través de la Mesa de Servicios Tecnológicos SOYtec, marcando el 5, enviando un correo a la cuenta sopORTE.oti@unidadvictimas.gov.co, o generando un caso por el Link <http://mesadeservicios.unidadvictimas.gov.co/usdkv8/#/login/>; donde encontrará personas amables y con mucho conocimiento, dispuestas a resolver su problemas tecnológicos.

SERVICIOS OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

- Cuenta con un directorio telefónico al cual puede acceder a través de la Intranet, para conocer las extensiones de todo el personal de la Unidad.
- Tiene soporte técnico para el servicio de teleconferencia, a través de SOYtec, marcando el 5, enviando correo a soporte.oti@unidadvictimas.gov.co; o generando un caso por el Link <http://mesadeservicios.unidadvictimas.gov.co/usdkv8/#/login/> ;
- si es el caso, la Oficina de Tecnologías de la Información enviará personal a resolver la falla en sitio.
- Manual de usuario.

BENEFICIARIO

Los servicios se prestan a los siguientes usuarios y/o colaboradores:

- Interno (funcionarios y contratistas)

2.1.7 FAXSERVER

DESCRIPCIÓN

Cuenta con un servicio que le permite enviar, recibir fax y administrarlos, desde una página Web que sirve como interfaz de entrada y salida de documentos. Este es otro servicio tecnológico con el cual la Oficina de Tecnologías de la Información respalda sus labores y le facilita la comunicación desde y hacia el exterior.

CARACTERÍSTICAS

Este servicio permite:

- Consultar el fax que recibió, a través de una página Web de asistente de fax.
- Enviar fax a través de la página Web, los cuales llegarán al fax físico de la persona a quien lo envía.
- Manejo y administración desde la Web, a través de la página de asistente de fax.
- Tendrá un usuario y contraseña, ya sea de su área o propio, a través del cual podrá acceder a la página Web de asistente de fax.



ALCANCE

El servicio de Puestos de Trabajo está enfocado a las siguientes acciones que permitan una adecuada y óptima gestión de los equipos tecnológicos que permite recibir fax y administrarlos, desde una página Web que sirve como interfaz de entrada y salida de documentos.

DISPONIBILIDAD Y COBERTURA

- Este servicio se brinda en la sede principal, en las demás sedes en Bogotá y en las diferentes territoriales, sedes y oficinas.
- Este servicio está disponible en un horario de 7x24x365

ACCESO

Para acceder a este servicio debe:

- Contar con un teléfono de la Unidad para las Víctimas.
- Solicitar el servicio de Fax Server, a través de la Mesa de Servicios Tecnológicos SOYtec.
- La Oficina de Tecnologías de la Información le asignará un usuario y contraseña.
- Se habilitará el acceso y administración de la página de asistente de fax.

SERVICIOS OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

- Tiene soporte técnico para el servicio de Fax Server, a través de SOYtec, marcando el 5, enviando un correo a sopORTE.oti@unidadvictimas.gov.co; o generando un caso por el Link <http://mesadeservicios.unidadvictimas.gov.co/usdkv8/#/login/>;
- Si es necesario, la Oficina de Tecnologías de la Información enviará personal a resolver la falla a su sitio de trabajo.
- Cuenta con un manual de usuario donde se describe cómo hacer uso de todas las características y funcionalidades del servicio de Fax Server*

BENEFICIARIO

Los servicios se prestan a los siguientes usuarios y/o colaboradores:

- Interno (funcionarios y contratistas)



2.2 SOLUCIÓN DE ALMACENAMIENTO DE INFORMACIÓN

DESCRIPCIÓN



¿Maneja archivos con información crítica? ¿Consulta altos volúmenes de documentos, y los almacena en su equipo? ¿Comparte esta información con sus compañeros de trabajo a través de medios magnéticos y en ocasiones estos archivos están en constante actualización?

¿Sabía que la Oficina de Tecnologías de la Información pone a su disposición un servidor de archivos donde podrá almacenar y compartir sus archivos e información con otros usuarios, de manera que todos accederán a un único archivo desde su equipo de cómputo y estarás en capacidad de almacenar grandes volúmenes de información, compartiendo recursos y haciendo más eficientes sus labores? Adicionalmente, la Oficina de Tecnologías de la Información ofrece el servicio de almacenamiento virtual de hasta un 1 TB, al cual podrá acceder vía internet.

La Oficina de Tecnologías de la Información le brinda una solución de almacenamiento de información eficiente, que garantiza su alojamiento, custodia, seguridad, disponibilidad y capacidad, y le da la oportunidad de compartir la información y acceder a ella de forma centralizada y segura, conozca **sharepoint**, una herramienta de almacenamiento de información, que permita acceder a espacios de trabajo compartidos, documentos, y el alojamiento de aplicaciones compartidas.

2.2.1 SOLUCIÓN DE ALMACENAMIENTO DE INFORMACIÓN

DESCRIPCIÓN

- Información de gestión es aquella que está en continua consulta y modificación, y se encuentra disponible en línea.
- Información histórica es aquella que no está disponible en línea, a la cual se accede con previa solicitud y únicamente para consulta, no para modificarla.



CARACTERÍSTICAS

El servidor de archivos le permite:

- Almacenar y acceder a la información de su dependencia de forma centralizada.
- Alta velocidad en el acceso de datos.
- Almacenar grandes volúmenes de información.
- Ampliación de capacidad de almacenamiento, sin interrupciones de servicio.
- Compartir su información con personas autorizadas.
- Determinar a qué personas dará permisos de solo lectura o permisos de escritura de archivos.
- Almacenamiento de diferentes tipos de archivos (imágenes, documentos, PDF, Excel y videos, entre otros).
- Desde del segundo semestre del 2015, se cuenta con una capacidad de almacenamiento a virtual de 1 TB y se podrá acceder por internet.

ALCANCE

El servicio está enfocado a las siguientes acciones que permiten la administración y configuración de los sistemas de almacenamiento y respaldo de la información de manera segura, oportuna y confiable para los funcionarios y colaboradores de la Unidad de reparación de las víctimas.

- Administrar y configurar soluciones de almacenamiento, para los diferentes componentes tecnológicos de la infraestructura de TI
- Administrar, establecer acciones de seguimiento y control al correcto funcionamiento, disponibilidad, desempeño, y capacidad de la plataforma de TI.
- Verificar y realizar acciones de seguimiento y control a los sistemas de almacenamiento y respaldo de la información e identificar irregularidades en la prestación del servicio
- Realizar copia de seguridad o respaldos de información de los diferentes sistemas de información
- Definir protocolos de respaldo y recuperación del sistema operativo, del software, y de la información residente en los servidores.

DISPONIBILIDAD Y COBERTURA

- Este servicio se presta en un horario de 7x24x365.
- Su disponibilidad es del 99,8% y su cobertura es nacional.

Página 21/50



ACCESO

Para acceder a este servicio debe:

- Definir si la información es de Gestión o histórica
- La dependencia realiza la solicitud, a través de SOYtec.
- Si la información es histórica, la Oficina de Tecnologías de la Información diagnostica su estado y capacidad, y facilita los medios para extraerla; se formaliza la entrega de información a la Oficina de Tecnologías de la Información, mediante acta, luego gestiona su almacenamiento y custodia y notifica la ubicación de la información. Si requiere consultar información histórica, debe solicitar su recuperación a través de SOYtec, indicando su ubicación y el tiempo que tardará consultándola, de modo que la Oficina de Tecnologías de la Información recupera y publica la información durante el tiempo solicitado y al finalizar ese lapso la retira.
- Si la información es de Gestión, la Oficina de Tecnologías de la Información dispone de un espacio sobre el servidor de archivos y asigna los permisos necesarios al encargado de crear la estructura y alojar la información del área solicitante, para luego asignar tipos de permisos de acceso a las personas designadas, de acuerdo con la solicitud del área.

SERVICIOS OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

La Oficina de Tecnologías de la Información se encarga de:

- Gestionar el almacenamiento, que incluye: réplica de archivos, backups, asignación de permisos lectura/escritura según requerimientos; aumento de capacidad, respaldo y restauración de información.
- Custodiar y gestionar los medios magnéticos.
- Restauración de archivos de información histórica.
- Aplicar planes de mantenimiento y seguridad.
- Respaldo de la información, con una frecuencia determinada.
- Soporte técnico

BENEFICIARIO

Los servicios se prestan a los siguientes usuarios y/o colaboradores:

- Interno (funcionarios y contratistas)

2.3 DOTACIÓN TECNOLOGÍA PARA SU PUESTO DE TRABAJO

DESCRIPCIÓN



Computador



Portátil



Impresora



Escaner

¿Sabía que cuenta con puestos de trabajo que tienen todas las herramientas tecnológicas dispuestas en un ambiente adecuado, para que haga uso de ellas?

Antes de que le sea asignado un puesto de trabajo, la Oficina de Tecnologías de la Información realiza una inspección técnica, analiza las necesidades y requerimientos del sitio, desplaza a los técnicos y realiza la instalación especializada de:

- Redes de cableado estructurado de datos, eléctrica normal y regulada. Bajo el escritorio verá un tomacorriente blanco con una marquilla que dice normal (es decir red eléctrica normal), un tomacorriente naranja con una marquilla que dice UPS (es decir, red eléctrica regulada, que protege el equipo frente a cambios bruscos de voltaje o corriente) y una toma con una marquilla blanca que dice datos.

Estas redes garantizan la energía y protección de su equipo y la conexión a internet y su teléfono IP.

- El centro de cableado es desde donde la Oficina de Tecnologías de la Información administra y centraliza los servidores, la conectividad, la seguridad, los antivirus y el sistema de resguardo eléctrico -UPS.
- Adecuaciones mobiliarias y dotación de muebles necesarios para lograr el ambiente de trabajo (iluminación).
- Desarrollo de mejoras complementarias para las nuevas oficinas.

Con estas labores la Oficina de Tecnologías de la Información garantiza que se cuente con un ambiente adecuado para el desarrollo de sus labores.

Por otra parte, sabemos que para que desarrolle sus labores requiere contar con una adecuada dotación tecnológica y por eso la Oficina de Tecnologías de la Información cuenta en su catálogo con un servicio



que le brinda estos recursos y la ofimática necesaria para realizar sus labores más eficientemente, al tener la tecnología al alcance de sus manos.

2.3.1 DOTACIÓN TECNOLÓGICA PUESTOS DE TRABAJO

CARACTERÍSTICAS

La Unidad para las Víctimas brinda la siguiente dotación tecnológica:

- Portátil con cargador, mouse, pad mouse y maletín.
- Impresoras y multifuncionales.
- Escáner, servicio de escáner independiente o a través de impresora multifuncional.
- Otros suministros asociados a repuestos, elementos para videoconferencias, video beam y televisores, entre otros.
- Los equipos tecnológicos en su mayoría están en modalidad de arriendo, la cual incluye garantía y tóner en el caso de las impresoras.

ALCANCE

El servicio de Dotación tecnológica está enfocado en las siguientes acciones que permiten una adecuada y optima gestión de los equipos tecnológicos

- Administrar los computadores (de escritorio y portátiles)
- Administrar las impresoras y escáner
- Administrar los teléfonos y extensiones de los puestos de trabajo
- Administrar los puntos de red y datos del puesto de trabajo
- Soportar y realizar configuraciones ofimáticas
- Adquisición de SW, HW, servicios
- Concepto técnicos Sistemas de Información
- Concepto técnico de aplicativos y/o software
- Concepto técnico de infraestructura de TI

DISPONIBILIDAD Y COBERTURA

- La cobertura de estos recursos se brinda en sedes y oficinas, tanto a nivel regional como central de la Unidad.



- El horario de atención de solicitudes de dotación tecnológica y de entrega de soluciones se realiza durante el horario hábil de la Unidad.

ACCESO

Para realizar la solicitud de dotación tecnológica se requiere:

- El jefe de la dependencia debe enviar la solicitud al correo suporte.oti@unidadvictimas.gov.co.
- La Oficina de Tecnologías de la Información verifica la viabilidad y disponibilidad, realiza la gestión y solicita el equipo.
- Se dará respuesta a su solicitud, vía correo electrónico, con un número de ticket.
- A su sede o puesto de trabajo llegará el equipo, el cual será instalado y configurado.

En el caso de una garantía por daño del equipo o solicitud de tóner, el usuario puede realizarla directamente a través de la Mesa de Servicios Tecnológicos SOYtec.

SERVICIOS OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

La Oficina de Tecnologías de la Información se encarga de:

- Mobiliario.
- Redes.
- Adecuaciones de sedes.
- Traslado de equipos y mobiliario.
- Instalación.
- Capacitación para uso de impresoras y escáner.
- Garantía en sitio.
- Repuestos en sitio.
- Reemplazo de tóner.
- Mantenimiento preventivo y correctivo de equipos.

Para mayor información puede acceder a soporte técnico, a través de la Mesa de Servicios Tecnológicos SOYtec, marcando el 5, enviando un correo a la cuenta suporte.oti@unidadvictimas.gov.co; o generando un caso por el Link <http://mesadeservicios.unidadvictimas.gov.co/usdkv8/#/login/>; donde encontrará personas amables y con mucho conocimiento, dispuestas a resolver sus problemas tecnológicos.

BENEFICIARIO

Los servicios se prestan a los siguientes usuarios y/o colaboradores:

- Interno (funcionarios y contratistas)

2.3.2 LICENCIAMIENTO ESPECIAL

La Oficina de Tecnologías de la Información le da la posibilidad de solicitar licencias de software adicionales a las instaladas en su equipo, en caso que sus necesidades laborales lo requieran. Recuerde que sólo puede tener programas licenciados en su computador.

CARACTERÍSTICAS

Este servicio le permite:

- Solicitar la licencia de software que requiera y que no se encuentre en el software base que le fue entregado.
- Se realiza la instalación y puesta en funcionamiento del software solicitado.

ALCANCE

El servicio de licenciamiento está disponible a los usuarios que en sus necesidades laborales requieran de este servicio.

DISPONIBILIDAD Y COBERTURA

- La cobertura de estos recursos se brinda en sedes y oficinas a nivel regional y central de la Unidad para las Víctimas.
- El horario de atención de solicitudes de licenciamiento es el horario hábil de la Unidad.

ACCESO

Para realizar la solicitud:

Página 26/50



- El jefe de la dependencia debe enviar un correo con la solicitud a sopORTE.oti@unidadvictimas.gov.co.
- La Oficina de Tecnologías de la Información verifica la viabilidad y disponibilidad, realiza la gestión y solicita la licencia.
- Se informa cuando se dará respuesta a su solicitud, vía correo electrónico, con un número de ticket.
- La Oficina de Tecnologías de la Información recibe el software y los técnicos Oficina de Tecnologías de la Información realizan la configuración e instalación del mismo.

SERVICIOS OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

Cuenta con soporte técnico, a través de SOYtec, marcando el 5, enviando un correo a sopORTE.oti@unidadvictimas.gov.co; o generando un caso por el Link <http://mesadeservicios.unidadvictimas.gov.co/usdkv8/#/login/>; en caso de requerir apoyo para solicitar la licencia o frente a inconvenientes con el software.

BENEFICIARIO

Los servicios se prestan a los siguientes usuarios y/o colaboradores:

- Interno (funcionarios y contratistas)



2.4 CONECTIVIDAD

DESCRIPCIÓN



¿Requiere estar conectado con el mundo, navegar a altas velocidades para realizar consultas, establecer conexiones entre las diferentes sedes y oficinas de la Unidad, con alta calidad, confiabilidad y seguridad, a través de diferentes medios de acceso? ¿Requiere acceder a internet dentro o fuera de su oficina a través de su tableta, teléfono inteligente o portátil para el desarrollo de sus labores?

La Oficina de Tecnologías de la Información le brinda una solución tecnológica que suple sus requerimientos integrando el servicio de comunicaciones de telefonía, internet y canales dedicados e internet inalámbrico y Mi-Fi, bajo una solución robusta, homogénea y escalable.

Así es. Cada vez que la Unidad para las Víctimas abre una nueva sede, oficina o Dirección Territorial, o ingresa personal nuevo, la Oficina de Tecnologías de la Información se encarga de suministrar los equipos de telefonía, las plantas y teléfonos IP, así como de gestionar el canal dedicado, el internet, el cableado y las conexiones necesarias para su funcionamiento. También evalúa la cobertura y el tipo de acceso, dimensiona la solución, realiza la instalación, hace la configuración, las pruebas y la puesta en funcionamiento para garantizar que cuente con las comunicaciones y conectividad que requiere para desarrollar sus labores.

De igual forma, sobre la infraestructura de comunicaciones existente, la Oficina de Tecnologías de la Información realiza la gestión respecto al ancho de banda, mediante el seguimiento a los canales existentes, para lo cual verifica si su sede, oficina o Dirección Territorial requiere aumentar el ancho de banda o si es posible racionalizarlo, para que cuente siempre con un servicio adecuado según sus necesidades.



2.4.1 INTERNET DEDICADO

DESCRIPCIÓN

El servicio de internet dedicado le permite disponer de conectividad a internet permanente, con altas velocidades de carga, permitiendo conectarse con el mundo desde las diferentes oficinas, sedes y Direcciones Territoriales ubicadas en todo el país.

CARACTERÍSTICAS

- Acceso a internet para realizar consultas y compartir información de manera sencilla y rápida, con compañeros de trabajo y con el exterior.
- Red segura para transmitir el flujo de información de la Unidad para las Víctimas.
- Infraestructura robusta de conexión nacional e internacional del proveedor.
- Tiene acceso a sistemas de información y aplicaciones, a través de internet.
- La OTI cuenta con herramientas de:
 - a) Gestión y monitoreo en línea, a través de la cual realiza monitoreo y seguimiento de canales de internet y del tráfico.
 - b) Filtrado de contenido, el cual permite denegar el acceso a cierto tipo de contenido inadecuado en la red.
 - c) Modelador de tráfico, herramienta que permite distribuir el ancho de banda, dando prioridad a los aplicativos misionales de la Unidad.

ALCANCE

El servicio de Internet dedicado está enfocado en las siguientes acciones que permiten una adecuada y optima gestión del Internet:

- Administrar la conectividad de cada una de las sedes de Unidad para la relación de las Víctimas
- Monitorear el correcto funcionamiento de la infraestructura de la Red conectividad de los funcionarios.
- Tomar las medidas técnicas y administrativas para evitar ataques informáticos a las redes.
- Administrar, controlar y gestionar accesos a Internet y Páginas WEB.
- Gestionar con los proveedores ISP los requerimientos y las necesidades de conectividad
- Gestionar con los proveedores ISP las fallas y oportunidades de mejora que le compete

Página 29/50



DISPONIBILIDAD Y COBERTURA

- La cobertura de estos recursos se brinda en sedes y oficinas a nivel regional y central.
- La disponibilidad de este servicio es del 99,6% y se brinda en un horario de 7x24x365.

ACCESO

- Para realizar la solicitud de internet dedicado en las nuevas sedes, oficinas o Direcciones Territoriales, debe:
- El jefe de la dependencia debe enviar correo con la solicitud a soporte.oti@unidadvictimas.gov.co, con copia al correo del Jefe de la Oficina de Tecnologías de la Información.
- La Oficina de Tecnologías de la Información verifica la viabilidad, realiza la gestión y solicita el servicio.
- Se informa cuando se dará respuesta a su solicitud.
- La Oficina de Tecnologías de la Información coordina la implementación y se realiza el seguimiento hasta la puesta en funcionamiento.

SERVICIOS OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

La Oficina de Tecnologías de la Información se encarga de:

- Monitoreo y seguimiento del canal y tráfico.
- Gestión del ancho de banda asignado y racionalización del mismo.
- Mantenimiento preventivo.
- Mantenimiento correctivo, solicitado a través de SOYtec, marcando el 5, enviando un correo a soporte.oti@unidadvictimas.gov.co; o generando un caso por el Link <http://mesadeservicios.unidadvictimas.gov.co/usdkv8/#/login/> ;

BENEFICIARIO

Los servicios se prestan a los siguientes usuarios y/o colaboradores:

- Interno (funcionarios y contratistas)



2.4.2 CONECTIVIDAD

La conectividad le permite acceder a la red de datos de la Unidad para las Víctimas mediante canales de Fibra óptica y establecer la conexión entre las diferentes sedes, con alto desempeño, calidad y confiabilidad, mediante una red robusta; a través de este servicio puede acceder a servidores, aplicaciones y bases de datos.

CARACTERÍSTICAS

- La Unidad para las Víctimas cuenta con un esquema de alta disponibilidad, con un canal principal y uno de backup.
- Los canales dispuestos son de fibra óptica y en caso de no ser posible llegar por este medio, se presta el servicio de canal satelital.
- Dimensión de la solución de conectividad, según necesidades de la Unidad, en cuanto a velocidad y seguridad de la transmisión, anchos de banda y medios de transmisión.
- Incremento de ancho de banda asignado a cada oficina, sede o Dirección Territorial, según la demanda, los cuales son monitoreados por la Oficina de Tecnologías de la Información, para aumentar o racionalizar el recurso.
- Recursos compartidos a través de la red, como la impresión y servidor de archivos de la Unidad.

ALCANCE

El servicio de Redes y Seguridad está enfocado a las siguientes acciones que permitan la administración y configuración de la Red LAN, WAN administración de las políticas de seguridad de la información:

- Administrar, establecer acciones de seguimiento y control al correcto funcionamiento de la infraestructura de redes y comunicaciones.
- Monitorear el correcto funcionamiento de la infraestructura de la Red LAN, WAN y conectividad de los usuarios.
- Realizar configuraciones técnicas y recomendaciones en telecomunicaciones acorde a las necesidades de la Unidad para la reparación de las víctimas.
- Administrar, gestionar y monitorear la infraestructura de seguridad informática.
- Tomar las medidas técnicas y administrativas para evitar ataques informáticos a las redes.

- Realizar análisis de vulnerabilidades internas y externas generando las acciones de mitigación que correspondan.
- Velar por el cumplimiento de las políticas de seguridad informática de la Unidad.
- Administrar y gestionar accesos a Internet y Páginas WEB.
- Administrar y gestionar accesos a través de VPN para los funcionarios.

DISPONIBILIDAD Y COBERTURA

- La cobertura de estos recursos se brinda en sedes y oficinas a nivel regional y central.
- La disponibilidad de este servicio es del 99,6% y se brinda en un horario de 7x24x365.

ACCESO

- El jefe de la dependencia debe enviar un correo con la solicitud a sopORTE.oti@unidadvictimas.gov.co, con copia al correo del Jefe de la Oficina de Tecnologías de la Información.
- Para realizar la solicitud de ampliación de canal se debe enviar correo con la solicitud a sopORTE.oti@unidadvictimas.gov.co, o marcar la tecla 5 desde cualquier teléfono de la Unidad.
- La Oficina de Tecnologías de la Información valida la estadísticas de uso del canal y evalúa la viabilidad de aumento, para optimizar el recurso según el monitoreo realizado.
- Se realiza la gestión con el proveedor y se valida la ampliación, manteniendo el monitoreo y seguimiento del canal.

SERVICIOS OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

La Oficina de Tecnologías de la Información se encarga de:

- Monitoreo y seguimiento del canal y tráfico.
- Gestión del ancho de banda asignado y racionalización del mismo.
- Mantenimiento preventivo.
- Mantenimiento correctivo, solicitado a través de SOYtec, marcando el 5, enviando correo a sopORTE.oti@unidadvictimas.gov.co; o generando un caso por el Link <http://mesadeservicios.unidadvictimas.gov.co/usdkv8/#/login/>.

BENEFICIARIO

Los servicios se prestan a los siguientes usuarios y/o colaboradores:

- Interno (funcionarios y contratistas)

Página 32/50



2.4.3 INTERNET INALÁMBRICO

DESCRIPCIÓN

La red inalámbrica permite que sus dispositivos móviles o equipos portátiles puedan acceder a internet sin que haga uso de su plan de datos, navegando desde las oficinas de la Unidad, ya sea desde el puesto de trabajo o en otra ubicación dentro de la sede. A través de esta alternativa de conectividad se facilita el desarrollo de sus funciones en la oficina, cubriendo las necesidades de conectividad y movilidad, apoyando sus labores y la operación de la Unidad.

CARACTERÍSTICAS

- Esta solución le brinda movilidad al interior de las oficinas de la Unidad para las Víctimas, de manera que pueda conectarse a internet desde cualquier lugar.
- Puede conectarte a la red, a través de la tecnología Wi-Fi de su portátil, móvil o tableta, brindando acceso a su equipo.
- Al acceder a las aplicaciones e información se facilita su trabajo y la colaboración, aumentando la productividad de todos en la Unidad.
- La Oficina de Tecnologías de la Información le brinda seguridad ya que controla, gestiona y protege el acceso a la red inalámbrica.

ALCANCE

El servicio de Internet Inalámbrico está enfocado a las siguientes acciones que permitan la administración y configuración de la Red LAN, WAN administración de las políticas de seguridad basados en la conectividad inalámbrica.

- Administrar, establecer acciones de seguimiento y control al correcto funcionamiento de los dispositivos activos de red destinados a la conectividad inalámbrica.
- Realizar configuraciones técnicas y recomendaciones en telecomunicaciones acorde a las necesidades de la Unidad para la reparación de las víctimas.
- Administrar, gestionar y monitorear la infraestructura de seguridad informática.
- Tomar las medidas técnicas y administrativas para evitar ataques informáticos a las redes.
- Realizar análisis de vulnerabilidades internas y externas generando las acciones de mitigación que correspondan.
- Administrar y gestionar accesos a Internet y Páginas WEB.

DISPONIBILIDAD Y COBERTURA

- Este servicio tiene una cobertura dentro de las oficinas de la Unidad para las Víctimas, donde se encuentre. Se brinda en un horario de 7x24x365.
- Actualmente, se está ampliando la cobertura para llegar al 100% de las oficinas de la Unidad.
-

ACCESO

- La Oficina de Tecnologías de la Información está a cargo de brindar este servicio en todas las oficinas de la Unidad para las Víctimas.
- La Oficina de Tecnologías de la Información realiza la gestión, instalación y configuración remotas.
- Se realizan las pruebas de comunicación con apoyo de personal de la oficina, si ésta no se encuentra en Bogotá.
- Se informa a todo el personal de la oficina beneficiado, para que acceda a este servicio.

La información de la contraseña para acceder a la red se puede solicitar a través de la Mesa de Servicios tecnológicos SOYtec, marcando el 5, enviando un correo a sopORTE.oti@unidadvictimas.gov.co; o generando un caso por el Link <http://mesadeservicios.unidadvictimas.gov.co/usdkv8/#/login/> ;

SERVICIOS OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

La Oficina de Tecnologías de la Información se encarga de:

- Monitoreo y seguimiento de la red inalámbrica.
- Soporte tecnológico, solicitado a través de SOYtec, marcando el 5 o enviando un correo a sopORTE.oti@unidadvictimas.gov.co.
- Informar la clave de la red inalámbrica.
- Administración y configuración.

BENEFICIARIO

Los servicios se prestan a los siguientes usuarios y/o colaboradores:

- Interno (funcionarios y contratistas)



2.4.4 Mi-Fi o Modem USB

DESCRIPCIÓN

El Mi-Fi le permite acceso a internet aprovechando la tecnología 4G, navegando desde cualquier lugar que cuente con cobertura de red. A través de esta alternativa de conectividad se facilita el desarrollo de sus funciones fuera de la oficina, cubriendo sus necesidades de conectividad y movilidad, apoyando su labor y la operación de la Unidad para las Víctimas.

CARACTERÍSTICAS

- Cuenta con dos tipos de dispositivos para establecer la conexión inalámbrica: el modem USB, el cual debe conectar a su equipo o el modem MiFi, dispositivo que no requiere ser conectado al equipo, permitiéndole conectarse a internet a través de cualquier dispositivo que disponga de tecnología WiFi (portátil, Tablet, Smartphone); le permite la conexión de hasta 10 dispositivos.
- El modem actúa como punto de acceso a internet desde donde se encuentres, brindándole movilidad.
- Si usa Mi-Fi debe cargarlo para hacer uso del dispositivo.
- Navega con una velocidad de 12 Mbps.
- Capacidad de descarga de 20gb. Al agotarse, continúa navegando con velocidad de 512 Kbps.
- Comparta la conexión en reuniones y utilice el servicio en eventos.
- Este dispositivo es propiedad del operador, por lo que debe hacer buen uso del mismo.

ALCANCE

El servicio Mi-Fi o Modem USB está enfocado a las siguientes acciones que permitan la administración y configuración, préstamo del servicio Mi-Fi.

- Evaluación y análisis de las necesidades de los funcionarios de la Unidad de Víctimas y ofrecer la conectividad que cubra la solicitud
- Seguimiento sobre la solución Mi-Fi, tiempos y usuarios
- Administrar y controlar el uso del servicio Mi-Fi
- Velar por el cumplimiento de las políticas de seguridad informática de la Unidad
- Velar por el cumplimiento de las políticas de seguridad informática de la Unidad.
- Administrar y gestionar accesos a Internet y Páginas WEB.
- Gestionar con los proveedores ISP los requerimientos y las necesidades de conectividad



DISPONIBILIDAD Y COBERTURA

- La cobertura de este servicio depende del prestador de servicio de la Unidad para las Víctimas.
- Si cuenta con cobertura, el servicio se brindará en un horario de 7x24x365, teniendo en cuenta que el Mi-Fi deberá estar cargado.

ACCESO

- Para solicitar un Mi-Fi o modem inalámbrico, el jefe de área debe enviar un mensaje con la solicitud al correo soporte.oti@unidadvictimas.gov.co
- La Oficina de Tecnologías de la Información verifica la viabilidad, realiza la gestión y solicita el equipo; la entrega del modem se realiza con memorando.
- Puede empezar a usar el modem inalámbrico. Tan solo debe cargarlo, encenderlo, buscar la red desde el dispositivo (MiFi) o computador (MiFi o modem USB) y digitar el usuario y contraseña que le entregaron con el equipo.

SERVICIOS OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

- Si tiene dudas respecto al uso del modem, puede comunicarse con la Mesa de Servicios Tecnológicos SOYtec, marcando la tecla 5 desde cualquier teléfono de la Unidad o enviando un correo a soporte.oti@unidadvictimas.gov.co.

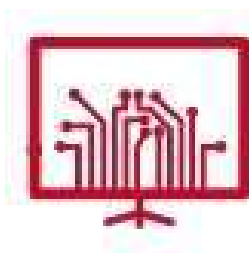
BENEFICIARIO

Los servicios se prestan a los siguientes usuarios y/o colaboradores:

- Interno (funcionarios y contratistas)

2.5 SISTEMAS DE INFORMACIÓN

DESCRIPCIÓN



¿Requiere sistematizar los procesos de su área a través de un Sistema de Información? ¿Tiene ideas para optimizar el Sistema de Información que utiliza frecuentemente? ¿El sistema de información que utiliza presenta inconvenientes o fallas? ¿Ha notado que los tiempos de respuesta de la aplicación que usa han bajado? ¿Requiere apoyo tecnológico para adquirir un software mediante un proceso de contratación? Si se le han presentado estas u otras situaciones similares, debe saber que la Oficina de Tecnologías de la Información cuenta en su catálogo con un servicio a través del cual puede solicitar el desarrollo de un nuevo sistema de información, el mantenimiento o adecuación de los sistemas de información existentes o apoyo y asesoría para la selección y aprovisionamiento de software, aplicaciones o desarrollos. Para ello, la Oficina de Tecnologías de la Información cuenta con un grupo de ingenieras e ingenieros altamente calificados, capacitados y con amplio conocimiento, quienes están dispuestos a apoyarlo, ya que queremos que cuente con nosotros como socios estratégicos que fusionan los procesos misionales con la tecnología, para obtener más cooperación y colaboración, y para entregar mayor valor, permitiéndonos innovar y obtener mejores resultados de la gestión de la Unidad en el cumplimiento de su misión. A continuación, le presentamos los servicios asociados a la solución de Sistemas de Información, cómo acceder a ellos, su cobertura, disponibilidad y los servicios Oficina de Tecnologías de la Información adicionales.



2.5.1 DESARROLLO

DESCRIPCIÓN

Este servicio realiza el análisis, diseño, desarrollo, implementación y soporte de nuevos Sistemas de Información y/o aplicaciones, bajo las mejores prácticas, para apoyar los procesos estratégicos, misionales, de apoyo y de control de la Unidad, facilitando el trabajo a través de la tecnología.

CARACTERÍSTICAS

- Realizamos el levantamiento de requerimientos, análisis, diseño, desarrollo, ejecución de pruebas, puesta en producción, estabilización y soporte técnico de las soluciones informáticas que requiere la Unidad para las Víctimas.
- Integramos la información derivada de las actividades y procesos de la Unidad que requieren automatizarse.
- Gobernamos desde la Oficina de Tecnologías de la Información todas las herramientas informáticas de la Unidad, garantizando control, seguridad, soporte y operación estable.
- Contamos con un equipo especializado de desarrolladores, documentadores, probadores y arquitectos calificados y capacitados, capaces de transformar necesidades en productos ágiles y seguros, aplicando las mejores prácticas en el tratamiento de la información y en el aprovisionamiento de soluciones.
- Contamos con el conocimiento y la sensibilidad de nuestro personal para ofrecer soluciones acordes con las necesidades de las víctimas y de los procesos de la Unidad.

ALCANCE

Desarrollar las soluciones de sistemas de información que la Oficina de Tecnologías de la Información considere que puedan ser asumidos por el equipo interno y no necesiten tercerizarse; de acuerdo con las capacidades internas. Comienza con una Solicitud de componentes tecnológicos a la Oficina de Tecnologías de la Información y termina con una solución de software en funcionamiento o con la no aprobación del desarrollo por parte de la Oficina de Tecnologías de la Información.

- Análisis de la necesidad de los funcionarios de la Unidad
- Evaluación de capacidad y posibilidad de gestión sobre las necesidades planteadas
- Desarrollo de soluciones de acuerdo a las necesidades de los funcionarios de la Unidad



DISPONIBILIDAD Y COBERTURA

- El equipo de desarrollo implementa soluciones que atienden las necesidades de la Unidad para las Víctimas para ser utilizadas en cualquier punto del territorio nacional.
- El equipo desarrolla soluciones con una metodología orientada a la obtención de resultados en el menor tiempo posible.
- Este servicio está disponible para todas las dependencias de la Unidad y para las entidades del Sistema Nacional (SNARIV) con las que se acuerden servicios a través de los procesos estratégicos, misionales, de apoyo y de control de la Unidad.

ACCESO

Para acceder a este servicio debe:

- Expresar su necesidad a la Oficina de Tecnologías de la Información.
- Posteriormente, se convoca una reunión entre la Oficina de Tecnologías de la Información y la dependencia.
- Se formalizan las necesidades y alcances de la solución a la Oficina de Tecnologías de la Información y se establece un acuerdo de servicio.
- Se asignan responsables y funciones dentro de la Oficina de Tecnologías de la Información, para garantizar la adecuada gestión del proyecto y la obtención de resultados, con el acompañamiento permanente del área.
- La Oficina de Tecnologías de la Información capacita, pone en producción y registra el desarrollo como activo de la Unidad para las Víctimas e inicia el procedimiento de mantenimiento y soporte.

SERVICIOS OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

La Oficina de Tecnologías de la Información se encarga de:

- Analizar la viabilidad del proyecto.
- Seleccionar la tecnología adecuada.
- Optimizar y alinear las soluciones para aumentar las sinergias de los procesos, a través de las herramientas que usan.
- Realizar la apropiación de nuevas tecnologías para ofrecer el mejor servicio a la Unidad y a las víctimas.
- A todo desarrollo se integran estándares de seguridad de la información.
- Se brinda soporte técnico posterior a la estabilización y puesta en producción.



- Puede acceder al soporte, a través de SOYtec, marcando el 5 o enviando un correo a soporte.oti@unidadvictimas.gov.co.

BENEFICIARIO

Los servicios se prestan a los siguientes usuarios y/o colaboradores:

- Interno (funcionarios y contratistas)

2.5.2 MANTENIMIENTO Y ADECUACIÓN

DESCRIPCIÓN

Este servicio se brinda sobre los sistemas de información que se encuentran en producción, donde se implementan correcciones o reparaciones y atención de ajustes, nuevas funcionalidades, mejora de las existentes y de procedimientos de uso, bajo las mejores prácticas, para mantener actualizadas las herramientas con que se apoya la Unidad para las Víctimas.

CARACTERÍSTICAS

- Debido a que los sistemas de información y aplicaciones deben responder y adecuarse a las necesidades de los usuarios, normas y procedimientos de la Unidad, se realizan mantenimientos correctivos a los sistemas de información después de que estos se encuentra en producción.
- En un mantenimiento correctivo de los sistemas de información se buscan, encuentran y corrigen o reparan errores; este mantenimiento se caracteriza por que se realiza después de que ha ocurrido la falla.
- A través de las adecuaciones se busca mejorar el rendimiento y el desempeño, optimizar funcionalidades, tiempos de respuesta y comunicación con otros sistemas, entre otros, con el propósito de que los sistemas y aplicaciones sean más fáciles de usar, más eficientes y más utilizados.
- Las adecuaciones pueden estar enfocadas a robustecer la funcionalidad de una aplicación, ya sea implementando o modificando requerimientos de los usuarios asociados a mejoras funcionales sobre el sistema.
- Las adecuaciones también se asocian a racionalizar la capacidad del poder de cómputo o hardware que soporta los sistemas, aumentando o disminuyendo la capacidad, lo cual se establece mediante



el monitoreo permanente que realiza la Oficina de Tecnologías de la Información a los sistemas de información.

ALCANCE

Actualizar, mantener y optimizar las soluciones de sistemas de información que la Unidad para la Reparación de las Víctimas tenga como desarrollo propio interno de la entidad

- Mantener la operatividad de los sistemas de información creados
- Administrar y controlar la integridad, accesibilidad y funcionalidad de los sistemas de información
- Optimizar y crear oportunidades de mejoramiento sobre los sistemas de información
- Atención a las necesidades y solicitudes efectuadas por los funcionarios y colaboradores de la Unidad

DISPONIBILIDAD Y COBERTURA

- La cobertura de este servicio es a nivel nacional.
- Los mantenimientos y adecuaciones se realizan en horas hábiles, salvo algunas excepciones en las que se establece en horas no hábiles para evitar la no disponibilidad de los sistemas de información, según el tipo de mantenimiento y las estimaciones de los ingenieros de la Oficina de Tecnologías de la Información.
- Este servicio está disponible para todas las dependencias de la Unidad y para entidades del Sistema nacional con las que se acuerden servicios a través de los procesos estratégicos, misionales, de apoyo y de control de la Unidad para las Víctimas.
- Los mantenimientos correctivos en aplicaciones misionales críticas se implementan de forma inmediata dada su alta prioridad.

ACCESO

Para acceder al servicio de mantenimiento correctivo debe:

- Marcar la tecla 5 o enviar un correo a soporte.oti@unidadvictimas.gov.co.
- Registrar su inconveniente con la aplicación o sistema de información, recibiendo el número de caso.
- Verificar que se realice el mantenimiento en el tiempo acordado.
- Confirmar la corrección.



SERVICIOS OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

La Oficina de Tecnologías de la Información se encarga de:

- Gestionar o ejecutar mantenimientos correctivos y adecuaciones.
- Se brinda soporte técnico posterior al mantenimiento, estabilización y puesta en producción de la aplicación o sistema de información.
- puede acceder al soporte, a través de SOYtec, marcando la tecla 5 o enviando un correo a sopORTE.oti@unidadvictimas.gov.co.

BENEFICIARIO

Los servicios se prestan a los siguientes usuarios y/o colaboradores:

- Interno (funcionarios y contratistas)

2.5.3 ASESORÍA

DESCRIPCIÓN

El servicio de asesoría ofrece recomendaciones a cualquier proceso para la incorporación de software y el acompañamiento durante el proceso de selección de tecnología de software que incluya software en calidad de servicio, adquisición o arrendamiento.

CARACTERÍSTICAS

- La Oficina de Tecnologías de la Información evalúa necesidades y recomienda las tecnologías aplicables y lo asesora en la selección de las mismas.
- La Oficina de Tecnologías de la Información brinda asesoría durante el proceso de contratación y ejecución, según corresponda, a través de las siguientes actividades:
 - a) Apoyo en la elaboración de la ficha técnica, sondeo y estudio de mercado, generación de observaciones técnicas, ajustes, modificaciones y consideraciones técnicas.
 - b) Apoyo en la elaboración del ámbito técnico del estudio previo.
 - c) Apoyo para realizar la evaluación técnica de propuestas.
 - d) Gestión de recursos sobre la plataforma tecnológica de la Unidad, para alojar y poner en producción el nuevo software.
 - e) Seguimiento durante la ejecución del proyecto.



- f) Registro del producto como activo.

ALCANCE

El servicio de Asesoría está enfocado a las siguientes acciones que permitan la toma de decisiones en la adquisición de software, servicios o soluciones informáticas de acuerdo a las necesidades de los funcionarios de la Unidad de reparación a las víctimas.

- Análisis y evaluación de las necesidades planteadas
- Investigación de soluciones que ofrece el mercado
- Determinar la solución con mejores características para el cubrimiento de la necesidad
- Acompañamiento en el proceso de adquisición
- Administración y control del licenciamiento y niveles de seguridad

DISPONIBILIDAD Y COBERTURA

- Este servicio está disponible para todas las dependencias de la Unidad para las Víctimas y se atiende en horario hábil.
- Su cobertura aplica en cualquier punto del territorio nacional en que haga presencia la Unidad.
-

ACCESO

Para acceder al servicio de asesoría tecnológica se requiere:

- Expresar su necesidad a la Oficina de Tecnologías de la Información.
- Marcar la tecla # 5 o enviar un correo a soporte.oti@unidadvictimas.gov.co, registrando su requerimiento de asesoría tecnológica.
- Analizamos, acompañamos y generamos observaciones técnicas respecto al requerimiento.
- Inicia la asesoría tecnológica.
-

SERVICIOS OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

La Oficina de Tecnologías de la Información se encarga de:

- Disponer de los recursos humanos y tecnológicos para apoyar su proceso de apropiación e incorporación de los proyectos que involucren componentes de software.
- Apoyo en la elaboración de documentos técnicos requeridos en los procesos de selección.



- Se brinda soporte técnico posterior a la estabilización y puesta en producción de la aplicación o sistema de información, marcando el 5 o enviando un correo a soporte.oti@unidadvictimas.gov.co.

BENEFICIARIO

Los servicios se prestan a los siguientes usuarios y/o colaboradores:

- Interno (funcionarios y contratistas)

2.6 SOPORTE A USUARIOS



DESCRIPCIÓN

¿Tiene inconvenientes o problemas con los recursos tecnológicos que le han asignado? ¿Requiere soporte tecnológico para continuar con sus labores? ¿Necesita apoyo para realizar video o teleconferencias o para realizar alguna presentación? ¿Requiere soporte sobre los sistemas de información y aplicaciones dispuestos por la Unidad para realizar sus labores? ¿Su correo no se actualiza, olvidó la contraseña, o tiene cualquier tipo de inconveniente tecnológico?

¿Sabía que cuenta con una Mesa de Servicios Tecnológicos, llamada SOYtec, a través de la cual se da respuesta a sus solicitudes de soporte técnico, centralizando y organizando el soporte tecnológico que se brinda a la Unidad?

SOYtec realiza el diagnóstico de su solicitud y brinda el soporte técnico de primer nivel, atendiendo remotamente las solicitudes de soporte o brindando capacitación sobre lo que debe hacer para resolver su inconveniente. De no ser así, una vez diagnosticado, se escala la solicitud de soporte a un segundo o tercer nivel, donde los ingenieros de la Oficina de Tecnologías de la Información o los proveedores solucionarán su caso.

A continuación, le presentamos los servicios de soporte dispuestos para la Unidad.

2.6.1 MESA DE SERVICIOS

DESCRIPCIÓN

La Mesa de Servicios Tecnológicos SOYtec responde a sus solicitudes de soporte técnico de forma integral, centralizada y organizada, siendo el punto único de contacto a nivel nacional dispuesto para la Unidad, donde apoyamos y atendemos las solicitudes de soporte asociadas con el catálogo de servicios tecnológicos, de forma amable, oportuna y efectiva.

CARACTERÍSTICAS

- SOYtec es el punto único de contacto para solicitar soporte tecnológico sobre cualquier producto o servicio del catálogo.



- Al recibir la solicitud, su caso se registra a través de una herramienta, asignándose un número de caso para gestionar y controlar el servicio; esto se informa vía correo electrónico.
- La mesa diagnóstica y asigna el tipo de soporte requerido según el caso.
- Al solucionar el requerimiento se informa vía correo y se le solicita confirmar si está de acuerdo con la solución aplicada.
- Recuerde evaluar la calidad del servicio, a través de la encuesta de satisfacción.
- Este servicio minimiza el tiempo de inactividad por fallas tecnológicas, permitiendo más productividad.

ALCANCE

El servicio de Mesa De Servicios Tecnológicos SOYtec recibe solicitudes de servicio, las registra en la herramienta de gestión y soluciona dentro del ANS correspondiente:

- Gestiona las solicitudes de todos los usuarios por medio de la herramienta de Gestión.
- Formar ordenadamente el proceso de gestión de las solicitudes incidentes y requerimientos que se presenten.
- Centralizar todos los casos de los usuarios, para llevar un registro cuantitativo de las solicitudes, el tiempo en respuesta y solución.
- Administrar y controlar el cumplimiento de los ANS pactados con cada línea de servicios

DISPONIBILIDAD Y COBERTURA

- La cobertura de este servicio es a nivel nacional, atendiendo a todos los usuarios de la Unidad.
- El horario de este servicio es de cinco días, de lunes a viernes, de 7:30 a.m. a 7:00 p.m.
-

ACCESO

- Para acceder a la Mesa de Servicios Tecnológicos SOYtec, solo debe marcar la tecla 5 desde cualquier teléfono de la Unidad, donde recibirá atención telefónica amable, oportuna y efectiva, de manera permanente, en el portal web o enviar un correo con su solicitud a la cuenta soporte.oti@unidadvictimas.gov.co.

SERVICIOS OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

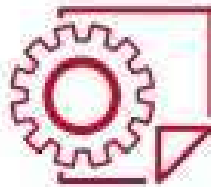
- La Mesa de Servicios Tecnológicos SOYtec diagnosticará su caso, brindándole soporte remoto o instruyéndole sobre cómo resolver su solicitud.
- En caso de diagnosticar su caso como nivel 2, se asignará personal para atender, bien sea el soporte en sitio, soporte aplicaciones, ingeniero especialista o proveedor.
- En caso de diagnosticar un soporte de nivel 3, la solicitud será atendida por los ingenieros de la Oficina de Tecnologías de la Información, el proveedor externo o por especialistas de aplicaciones.
- La Oficina de Tecnologías de la Información tiene definidos los tiempos de respuesta, según el caso, para garantizarle el menor tiempo de inactividad causada por fallas en servicios tecnológicos.
- La Oficina de Tecnologías de la Información diseña, desarrolla e implementa soluciones para mitigar problemas frecuentes, a partir del análisis de la información que recopila.

BENEFICIARIO

Los servicios se prestan a los siguientes usuarios y/o colaboradores:

- Interno (funcionarios y contratistas)

2.7 SERVICIOS ADMINISTRATIVOS



DESCRIPCIÓN

En la Oficina de Tecnologías de la Información existe un grupo profesionales encargados de administrar los diferentes recursos y servicios tecnológicos, quienes se aseguran de optimizar y racionalizar los recursos, controlar el rendimiento de la infraestructura, administrar el desempeño y capacidad de recursos TI y estimar las necesidades futuras, entre otras.

Dicho grupo está a cargo de gestionar las líneas de servicio y soluciones tecnológicas dispuestas para usted, a nivel técnico y administrativo, solicitando recursos, realizando seguimiento a los recursos nuevos y existentes, redistribuyendo recursos para optimizar su uso y realizando seguimiento al presupuesto asignado, entre otras funciones.



2.7.1 ADMINISTRACIÓN DE SERVICIOS Y RECURSOS

DESCRIPCIÓN

Este servicio consiste en realizar la gestión de la capacidad de los recursos y servicios tecnológicos, buscando racionalizar, optimizar, controlar y pronosticar su uso, oferta y demanda.

CARACTERÍSTICAS

Asociado a este servicio se realiza:

- Definición e implementación de un Plan Estratégico de Tecnologías de la Información.
- Administración de la inversión en TI.
- Administración de proyectos TI.
- Gestión de líneas de servicio y soluciones tecnológicas (infraestructura tecnológica, recursos, software, etc.)
- Definición y administración de Acuerdos de Niveles de Servicio, donde se establecen los tiempos de respuesta y atención frente a servicios y recursos, así como la disponibilidad de los servicios tecnológicos).
- Administración de servicios de terceros.
- Gestión del desempeño y capacidad.
- Gestión de continuidad.
- Administración de la Mesa de Servicios SOYtec.

ALCANCE

El servicio está enfocado a las acciones que permitan la administración de los recursos de la oficina de tecnología de la información

DISPONIBILIDAD Y COBERTURA

- La cobertura de este servicio es a nivel nacional.
- El horario en que se brinda este servicio es de 5x8x365



ACCESO

- Este servicio se ejecuta continuamente como parte de las labores diarias de la Oficina de Tecnologías de la Información.

SERVICIOS OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

La Oficina de Tecnologías de la Información cuenta con los siguientes planes, con el propósito de gestionar servicios y recursos TI:

- Plan de acción, plan de adquisición, plan de capacidad, plan de capacitación, plan de divulgación y plan de seguridad de la información.
- La gestión realizada por la Oficina de Tecnologías de la Información se asocia a la planificación, ejecución, seguimiento y monitoreo de recursos y servicios TI.

BENEFICIARIO

Los servicios se prestan a los siguientes usuarios y/o colaboradores:

- Interno (funcionarios y contratistas)

2.7.2 ADMINISTRACIÓN TÉCNICA

DESCRIPCIÓN

Este servicio consiste en realizar la gestión de la configuración, datos, ambiente físico, operaciones y cambios asociados a la administración técnica de recursos y servicios tecnológicos dispuestos para la Unidad.

CARACTERÍSTICAS

Asociado a este servicio se realiza:

- La administración de la configuración, asociada a los servicios de red que permiten conectar su equipo de cómputo con otros dispositivos y servicios de red, y del poder de cómputo que soportan los sistemas de información y las aplicaciones.
- Administración de datos, asociada a mantener disponible, íntegra y exacta la información, mediante respaldo de datos, restauración, almacenamiento, procesamiento, custodia y seguridad de la información.
- Administración de operaciones, relacionada con la definición de políticas y procedimientos de operación, protección de datos y monitoreo de infraestructura.



- Administración de cambio, respecto a la infraestructura y aplicaciones.

ALCANCE

Este servicio, está enfocado a las siguientes a que permitan el correcto y oportuno funcionamiento de la administración y configuración, asociada a los servicios de red que permiten conectar su equipo de cómputo con otros dispositivos y servicios de red

DISPONIBILIDAD Y COBERTURA

- La cobertura de este servicio es a nivel nacional.
- El horario en que se desarrolla este servicio es de 5x8x365.

ACCESO

- Este servicio se ejecuta continuamente como parte de las labores diarias de la Oficina de Tecnologías de la Información.

SERVICIOS OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

La Oficina de Tecnologías de la Información brinda los siguientes servicios frente a la administración técnica de servicios y recursos TI:

- Monitoreo, seguimiento, redistribución o asignación de la configuración técnica de servicios y recursos tecnológicos.
- Disponibilidad de información íntegra y confiable para apoyar procesos misionales.
- Políticas y lineamientos para implementar gobierno de TI.

BENEFICIARIO

Los servicios se prestan a los siguientes usuarios y/o colaboradores:

- Interno (funcionarios y contratistas)

Elaboró	Tatiana Florez Curvelo	
Revisión técnica - Elaboró:	Emma Mercedes Villamizar	
Aprobó - Jefe de la Oficina de Tecnología de la información:	Jhon Ricardo Morales Franco	
Fecha de Aprobación	27-09-2018	



Anexo 3 - Informe de Licenciamiento

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

NOVIEMBRE 2018

Tabla de contenido

GLOSARIO	2
1. CAPACIDAD DE LICENCIAS.....	3
1.1. LICENCIAS POR RESPONSABLE	3
1.2. LICENCIAS POR TIPO DE INSTALACIÓN.....	3
1.3. LICENCIAS POR TIPO DE ADQUISICIÓN	4
1.3.1. COMPRA	4
1.3.2. COMPRA Y RENOVACIÓN DE SOPORTE.....	5
1.3.3. DERECHOS DE USO	5
1.3.4. ARRIENDO.....	6
1.3.5. SUSCRIPCIÓN AL USO DE LICENCIAMIENTO.....	7
2. SOLICITUDES DE LICENCIAMIENTO ATENDIDAS EN EL PERIODO Y SERVICIOS RENOVADOS..	7

GLOSARIO

DG: Dirección General Unidad para la atención y reparación integral a víctimas.

DGI: Dirección de gestión interinstitucional.

DGSH: Dirección de gestión social y humanitaria.

DR: Dirección de reparación.

DT: Dirección territorial

FRV: Fondo de reparación de víctimas.

Licencia de software: es un contrato entre quien autoriza el uso del software y quien se beneficia de su uso, se caracteriza por definir jurídicamente los alcances y restricciones respecto al uso, por ejemplo, la instalación en un PC, o en un servidor, cantidad de usuarios que pueden acceder a la aplicación, modificación del código fuente, uso y distribución de la misma.

OAC: Oficina asesora de comunicaciones.

OAJ: Oficina asesora jurídica.

OCI: Oficina de control interno.

Producto: software de computadores o servidores.

SG: Secretaría general.

SRNI: Subdirección Red Nacional de Información.

SVR: Subdirección de valoración y registro.

GGFYC: Grupo de Gestión Financiera y Contable

Dentro de las funciones asignadas a la Oficina de Tecnologías de la Información, en lo que respecta a las diferentes herramientas utilizadas en los procesos de la Unidad, se proveen bajo diferentes modalidades de licenciamiento, aquellos productos necesarios que soporten la operación de la entidad. Entre las modalidades de licenciamiento se cuentan: compra, compra y renovación, derechos de uso, donación, servicios de arriendo y suscripción de licencias de uso.

Con el fin de mantener actualizada la estimación de necesidades de licenciamiento de la entidad, se conforma el presente informe el cual contiene una relación de la totalidad de licencias de la Unidad y la asignación por cliente.

1. CAPACIDAD DE LICENCIAS

1.1. LICENCIAS POR RESPONSABLE

La siguiente tabla presenta el número del licenciamiento identificado en la unidad, por tipo de adquisición y responsable de las mismas:

TIPO / RESPONSABLE	FRV	OTI	RNI	SRV	GGFYC	TOTAL
COMPRA	75	88	268	1	80	466
COMPRA & RENOV.SOPORTE		74				74
DERECHOS DE USO		7.859				7.859
SERVICIO_ARRIENDO		368				368
SUSCRIPCION LIC.USO		8.726	-			8.726
TOTAL	75	17.115	268	1	80	17.539

1.2. LICENCIAS POR TIPO DE INSTALACIÓN

El licenciamiento está enfocado a dos tipos de instalación por usuario final o por servidor, siendo un 97.5% del licenciamiento de tipo usuarios final (cliente):

TIPO / USUARIO	CLIENTE	SERVER	TOTAL
COMPRA	237	275	512
COMPRA & RENOV.SOPORTE		74	74
DERECHOS DE USO	7.859		7.859
SERVICIO_ARRIENDO	305	63	368
SUSCRIPCION LIC.USO	8.726		8.726
TOTAL	17.127	412	17.539

1.3. LICENCIAS POR TIPO DE ADQUISICIÓN

1.3.1. COMPRA

Bajo esta modalidad se ha clasificado aquel licenciamiento que la entidad ha adquirido a perpetuidad y no cuenta con renovación de soporte. La siguiente tabla presenta el número total de licenciamiento adquirido, sin renovación de soporte y responsable de las mismas:

Respecto al periodo anterior, no se presentaron cambios en el licenciamiento.

PRODUCTO / RESPONSABLE	FRV	OTI	RNI	SRV	GGFYC	TOTAL	ASIGNADAS
ACEDOC				1		1	1
BUSCADOR			1			1	1
CERTIFICADOS SEGUROS SSL		42				42	17
FIRMAS DIGITALES		46			80	126	30
INFORMATION BUILDER			1			1	1
MS DYNAMICS (CALL)			106			106	*
MS PROJECT SERVER (1 + 10 CALL)			11			11	*
MS SHAREPOINT (CALL)			115			115	*
PCT	75					75	-
SPSS			34			34	34
TOTAL	75	88	268	1		512	84

PRODUCTOS	CONTRATO	CANTIDAD TOTAL LICENCIAS	LICENCIAS ASIGNADAS ACTIVOS	LICENCIAS DISPONIBLES
ACEDOC	232-2010	1	1	0
BUSCADOR		1	1	0
CERTIFICADOS SEGUROS SSL	1171 2015	42	17	25
FIRMAS DIGITALES	IP-01-2018	80	30	50
INFORMATION BUILDER		1	1	0
MS DYNAMICS	OSOH-2063 de 2014 OIM	106	106	0
MS PROJECT SERVER	OSOH-2063 de 2014 OIM	11	11	0
MS SHAREPOINT	OSOH-2063 de 2014 OIM	115	67	48
PCT	075-2013	75	0	75

PRODUCTOS	CONTRATO	CANTIDAD TOTAL LICENCIAS	LICENCIAS ASIGNADAS ACTIVOS	LICENCIAS DISPONIBLES
SPSS	1506 2013	34	34	0
TOTAL, COMPRA		432	39	393

1.3.2. COMPRA Y RENOVACIÓN DE SOPORTE

En este tipo de licenciamiento se agrupan aquellos productos que fueron adquiridos a perpetuidad y cuyo soporte ha sido renovado periódicamente para garantizar la disponibilidad del servicio:

PRODUCTO	CONTRATO VIGENTE	CANTIDAD TOTAL LICENCIAS	LICENCIAS ASIGNADAS ACTIVOS	LICENCIAS DISPONIBLES
DATA QUALITY	1532 - 2018	8	8	0
ESIGNA	1533 - 2018	9	9	0
ORACLE	OC24580 – 2018; OC30021 - 2018	36	36	14
SICOF - ERP	1470-2018	1	1	0
SQL SERVER	OC28562-2018	20	18	2
BIZTALK / LIC.PROCESADOR	OC21575-2017	16	14	2
TOTAL		90	67	18

Respecto al periodo anterior, no se presentaron cambios en el licenciamiento.

1.3.3. DERECHOS DE USO

Bajo esta clasificación se encuentra el licenciamiento base asociado a los pc's y portables que la entidad utiliza en modalidad de servicio, tales como: sistema operativo, protección de antivirus y agente de la mesa de servicio:

PRODUCTO	CONTRATO	CANTIDAD TOTAL LICENCIAS	LICENCIAS ASIGNADAS ACTIVOS	LICENCIAS DISPONIBLES
DERECHOS DE USO				
ARANDA	CIE 008 – 2014	2600	2530	0
MCAFFEE	CIE 008 – 2014	2630	2629	1

WINDOWS S.O PC's	CIE 008 - 2014	2630	2629	1
TOTAL		7.860	7.808	2

1.3.4. ARRIENDO

Licenciamiento asignado en modalidad de servicio por demanda:

PRODUCTO	DESCRIPCION DETALLADA	CONTRATADAS	ASIGNADAS
ADOBE ACROBAT	ACROBAT PROFESIONAL V 11	11	9
ADOBE ACROBAT	ADOBE ACROBAT PRO DC	1	0
ADOBE AUDITION	ADOBE AUDITICION	2	2
ADOBE CREATIVE CLOUD	CREATIVE CLOUD COMPLETO	7	7
ADOBE DESIGN PREMIUM	ADOBE DESIGN PREMIUM (OPC 2 CS6) + (1 Cloud)	2	2
ADOBE DESIGN PREMIUM	ADOBE DESIGN PREMIUM CS6 Cloud Master colección	1	1
ADOBE DESIGN PREMIUM	ADOBE DESIGN PREMIUM CS6 Cloud Master colección	9	9
ADOBE ILLUSTRATOR	Adobe Illustrator CC	1	1
ADOBE INDESING	Adobe Indesing CC	1	0
ADOBE LIGHTROOM	ADOBE LIGHTROOM 6.0 MLP AOO	1	0
ADOBE PHOTOSHOP	ADOBE PHOTOSHOP CC	2	1
ADOBE PHOTOSHOP	ADOBE PHOTOSHOP CC	2	1
ADOBE PREMIER PRO	Adobe Premier Pro CC	1	1
AUTODESK	AUTOCAD 2D	2	2
AUTODESK	AUTOCAD LT2015	3	3
DREAM WEAVER	DreamWeaver CS6 12.0 MLP AOO	1	1
MICROSOFT - ACCESS	Licencia Access 2013 OLP NL	11	11
MICROSOFT - SO	Windows Professional V.10 64B	3	3
MICROSOFT - VISIO	Licencia VisioStd 2016 OLP NL	13	13
MICROSOFT- PROJECT	Licencia Project 2013 OLP	18	13
MICROSOFT -PUBLISHER	Licencia Publisher	0	0
MICROSOFT- SO	Microsoft Windows Professional 8.1 Upgrade	19	19
MICROSOFT -SPIRE DOC	Spire Doc for .NET Pro Edition	1	1
MICROSOFT - SQL SERVER	SQLSvrStd 2014	1	1
MICROSOFT - TEAMFOUNDATION CALL	Visual Studio Team Foundation SvrCal G	61	56
MICROSOFT - TEAMFOUNDATION SRV	Visual Studio Team Foundation Svr G	1	1
MICROSOFT - VISIO	Licencia VisioStd 2013 OLP NL	27	10
MICROSOFT -VISUALSTUDIO	Visual Studio Professional 2012 G	26	21
MICROSOFT -VISUALSTUDIO	Visual Studio Professional 2013 G	35	35
NITRO	NITRO PRO 9	33	33
NITRO	NITRO PRO 9	1	1
PLSQL	PL/SQL Developer 10 user license	2	2

PRODUCTO	DESCRIPCION DETALLADA	CONTRATADAS	ASIGNADAS
PLSQL	PL/SQL Developer 20 user license	1	1
PLSQL	PL/SQL Developer 20 user license	2	0,4
TELERICK	Software DevCraft Complte marca Telerick	1	1
		303	262,4

1.3.5. SUSCRIPCIÓN AL USO DE LICENCIAMIENTO

Bajo esta modalidad se han clasificado las suscripciones al uso de licenciamiento en modalidad de servicio, las cuales son adquiridas por medio de instrumentos de Colombia Compra Eficiente:

PRODCUTO/UNIDAD	CONTRATO	RENOVADAS	ASIGNADAS
ARCGIS / LIC USO	OC 30941-2018	Ilimitado	Ilimitado
AZURE / UNIDADES AZURE	OC23215-2017	2.594	1.668
	OC32040-2018	1.394	0
CRM / LIC. USO X USR	OC31263-2018	17	17
EMS / LIC. USO X USR	OC32854-2018	2.480	2.314
OFFICE 365 / LIC.USO X USR	OC29947 - 2018	2.685	2.520
TOTAL		7.456	6.519

2. SOLICITUDES DE LICENCIAMIENTO ATENDIDAS EN EL PERIODO Y SERVICIOS RENOVADOS

- ✓ Solicitud de dos (2) Licencia Power Bi desktop para la Subdirección Coordinación Nación Territorio.
- ✓ Solicitud instalación cliente Oracle por parte de Subdirección de Asistencia y Atención Humanitaria- SAAH
- ✓ De acuerdo con la Demanda del servicio en Office 365, se retiraron 25 asignaciones de licencias de uso.
- ✓ Durante el periodo se incrementó en 185 Unidades los recursos de Azure.

Elaborado por: Margarita Guillen
Oficina de Tecnologías de la Información

ANEXO 4- GESTION DE LA CAPACIDAD

Contar con un instrumento que le permita a la oficina gestionar la capacidad de los recursos tecnológicos según lo establecido en G.ST.01 Guía Del Dominio De Servicios Tecnológicos /1.2.2 Gestión De La Capacidad

OFICINA DE TECNOLOGIAS DE LA INFORMACION - NOVIEMBRE 2018



TABLA DE CONTENIDO

1. OBJETIVO	2
2. OBJETIVOS ESPECIFICOS.....	2
3. ALCANCE	2
4. MARCO CONCEPTUAL Y DE REFERENCIA	3
5. PLAN DE CAPACIDAD	4
5.1 Servicios de Dotación	4
5.2 Centro de Datos:.....	6
5.3 Conectividad	7
5.4 Telefonía	8
5.5 Herramientas Colaborativas	9
5.6 Sistemas de Información.....	10
5.7 Uso y Apropiación	12
6. MODELADO Y SIMULACIÓN DE DIFERENTES ESCENARIOS DE CAPACIDAD.....	12
7. MONITORIZACIÓN DEL USO Y RENDIMIENTO DE LA INFRAESTRUCTURA TI.....	13
7.1 Infraestructura Tecnologica	13
7.2 Licenciamiento	13
7.3 Uso y Apropiación	13
8. GESTION DE LA DEMANDA.....	14
9. CREACIÓN Y MANTENIMIENTO DE LAS BASES DE DATOS DE CAPACIDAD (CDB)	14



INTRODUCCION

La Oficina de tecnologías de la Información, brinda servicios de tecnológicos enfocados a la dotación tecnológica, centro de datos, las comunicaciones, conectividad, telefonía IP y Sistemas de Información. La Oficina de tecnologías de la información adopta e inicia la implementación de manera escalonada el modelo de Gestión de TI denominado “Modelo IT4” en el marco del Decreto 415 de 2016.

Es así como la Oficina de Tecnología de la Información ha venido implementando de manera escalonada a las estrategias sectoriales y misionales de la Unidad, formuladas en su Plan de Acción 2018 actividades estratégicas, tácticas y operativas, en consecución de fortalecer su modelo de gestión.

En la “*Guía del dominio de servicios tecnológicos*” busca que la gestión de tecnologías sea un servicio permanente que beneficie a todos los usuarios, tanto internos como externos, garantizando su disponibilidad y operación.

En el sistema integrado de gestión de Calidad la oficina de tecnologías hace parte del proceso “Gestión de la Información”, el cual cuenta con mapa de riesgos de gestión y corrupción. Entre los controles del riesgo de gestión. se encuentra “*Indisponibilidad de soporte e infraestructura tecnológica para el personal y los procesos de la Unidad*” siendo uno de los controles la gestión a la capacidad.

1. OBJETIVO

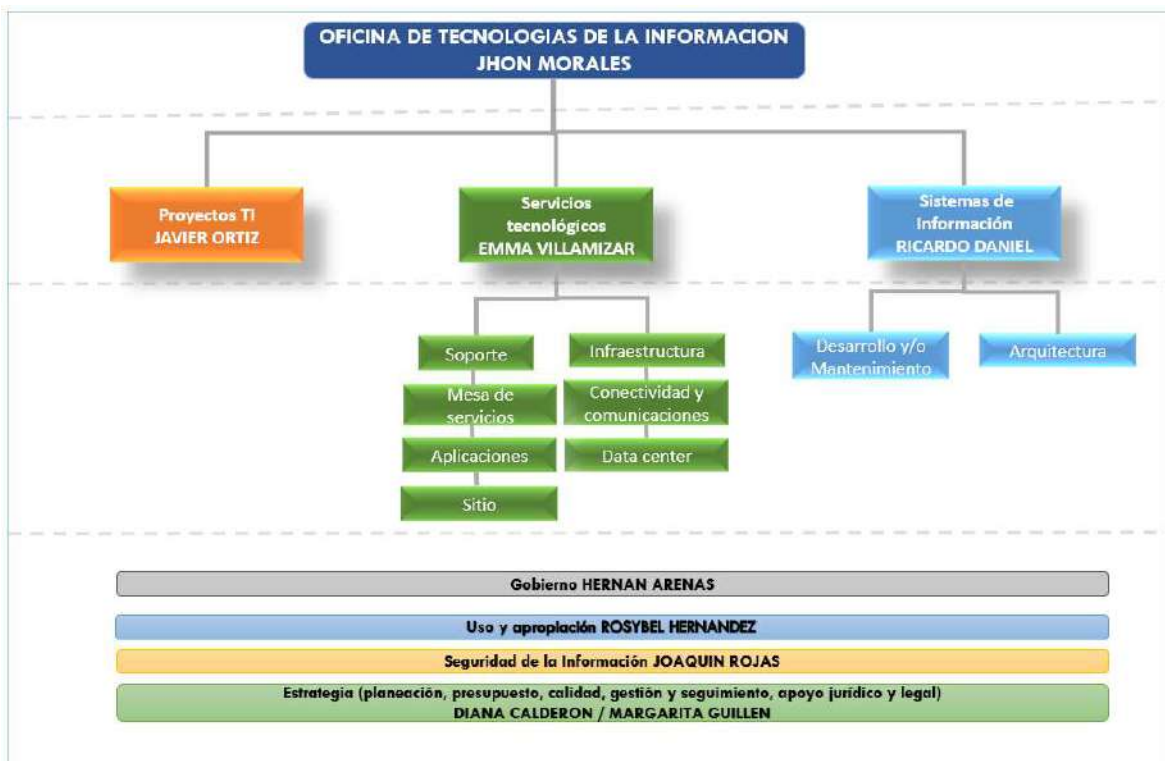
Contar con un instrumento que le permita a la oficina de tecnologías gestionar la capacidad de los recursos tecnológicos, efectuar un aprovechamiento eficiente de los mismos, y tomar acciones tendientes a mantener la oferta de los servicios tecnológicos.

2. OBJETIVOS ESPECIFICOS

- Desarrollo del plan de capacidad
- Modelado y simulación de diferentes escenarios de capacidad
- Monitorización del uso y rendimiento de la infraestructura TI
- Gestión de la Demanda
- Creación y mantenimiento de las bases de datos de Capacidad (CDB)

3. ALCANCE

La gestión de capacidad tecnológica está orientado a las líneas de servicio que la oficina de tecnologías ofrece a la unidad de víctimas tales como: *Dotación tecnológica, centro de datos, conectividad, telefonía, herramientas de colaboración y sistemas de información*. La siguiente ilustración presenta de manera gráfica la estructura organizativa interna de la oficina y sus líneas de servicio:



4. MARCO CONCEPTUAL Y DE REFERENCIA

El documento principal para la construcción de este instrumento corresponde a la *G.ST.01 Guía del dominio de Servicios Tecnológicos*¹, de igual manera, existen otros documentos consultados los cuales se referencian a continuación:

- ✓ ITIL Fundamentos de Gestión de TI
- ✓ Gestión Estratégica con TI en el Estado. IT4+
- ✓ Gobierno digital decreto 1008/2018
- ✓ Acuerdo Marco de Precios de tecnología en Colombia Compra Eficiente
- ✓ **Artículo 10 del Decreto 4802 de 2011**, la Oficina de Tecnologías de la Información de la Unidad tiene entre sus funciones:
 - i) “Administrar los sistemas de información, equipos, redes y herramientas tecnológicas y brindar el soporte técnico para su funcionamiento adecuado”.
 - ii) “Dirigir, orientar y participar en el desarrollo de los contenidos y ambientes virtuales requeridos para el cumplimiento de las funciones y objetivos de la Unidad”.

¹ G.ST.01 Guía del Dominio de Servicios Tecnológicos Versión 1.0 30 diciembre 2014

- iii) Implementar las metodologías y procedimientos que adopte la unidad para el desarrollo, instalación, administración, seguridad, y uso de la infraestructura tecnológica teniendo en cuenta los lineamientos que en la materia generan las entidades competentes.”
 - iv) “Las demás inherentes a la naturaleza y funciones de la Dependencia”
- ✓ **Plan nacional de desarrollo 2014-2018:** “Competitividad e Infraestructura Estratégicas - *Las tecnologías de la información y las comunicaciones (TIC) pasan a jugar un papel protagónico. No basta la simple provisión de infraestructura y servicios de soporte si estos no vienen acompañados de una estrategia de profundización de su uso en las empresas y en el día a día de las personas. Sin embargo, un país más competitivo no solo requiere empresas más productivas, sino también un Estado más eficiente y accesible, para lo cual las TIC se convierten en el mejor aliado para su interacción con los ciudadanos y la consecución de las metas sociales del Gobierno nacional. Las TIC permiten hacer más transparente la labor del Estado, proveerlo de información más precisa para la toma de decisiones y focalizar mejor la oferta de programas sociales. Será a través de las TIC como se llegue, a un menor costo, a la población vulnerable o a territorios apartados que históricamente no han contado con una presencia estatal fuerte*”.
- ✓ **Decreto Ley 019 de 2012:** Artículo 38-Principios de la política pública de racionalización de trámites. Contribuir a la mejora del funcionamiento interno de las entidades públicas que cumplan una función administrativa, incrementando la eficacia y la eficiencia de las mismas mediante el uso de las tecnologías de información
- ✓ **Decreto 3816 de 2003-**Comisión Intersectorial de Política y Gestión de Información en la Administración Pública-COINFO: Optimizar la inversión en tecnologías de información y de comunicaciones de la Administración Pública

5. PLAN DE CAPACIDAD

5.1 Servicios de Dotación

La oficina de tecnologías brinda en modalidad de **servicios tercerizado**, la dotación tecnológica con una cobertura a nivel nacional y centralizada compuesta por una infraestructura TI dispuesta en sitio en cada sede y/o oficina de la unidad conformada por herramientas tecnológicas, equipos de cómputo, equipos de impresión y escáner, periféricos, cableado estructurado, centros de cableado, servicio integral de video conferencia, soporte técnico, los cuales incluyen garantías y mantenimientos tanto correctivos como preventivos. Descritos así:

- i) *Brindar y Mantener el Servicio de Oficinas y Centros de Cableados*
Este servicio permite brindar un servicio de dotación tecnológica por sitio de trabajo, con una red de cableado estructurado de voz, datos, eléctrica normal y

regulada, servicio integral de video conferencia, soporte técnico y red de área local, entre otros. La siguiente tabla presenta la cobertura del servicio.

ii) *Administrar, soportar y mantener el servicio de Dotación de Equipos - Portátiles, Impresoras, Scanner, Repuestos entre otros.*

Esta actividad le permite a la oficina de tecnologías de la información brindar a la unidad tres tipos de servicios en sitio como la dotación de Pc's y Portables totalmente licenciado con su sistema operativo y antivirus, el servicio de impresión - escáner y el servicio de punto de información virtual a la víctima, bajo la modalidad de servicio por demanda durante 5 x 9 x 365 días al año.

iii) *Administrar, soportar y mantener la Mesa de Servicios Tecnológicos*, a través de esta actividad se le ofrece a la unidad un servicio centralizado de soporte de primer nivel. Este servicio inicia su implementación en las vigencias 2014 y se fortalece durante las siguientes vigencias.

Por lo anterior y con el objeto de dimensionar la **capacidad del servicio** requiere el análisis de las siguientes variables:

- ✓ Capacidad instalada al inicio de la vigencia, denominada línea base.
- ✓ Tendencia del servicio en vigencias anteriores.
- ✓ Supuesto de costeo base para asegurar la sostenibilidad del servicio.
- ✓ Incremento del 3% correspondiente al IPC.
- ✓ Traslados y/o ampliaciones de oficinas.
- ✓ Contratación Vigente y/o procesos contractuales a ser adelantados.

En consecuencia, a partir del análisis de variables previamente descritas, esta oficina asigna para los servicios de dotación tecnológica en la **vigencia 2018**, un total de recursos por valor de **(\$17.700)** Millones de pesos, con una cobertura nacional en **(41)** oficinas y/o sedes.

PRODUCTO	UNIDAD DE MEDIDA	META	ACTIVIDADES	2018
		2018		
Servicios de Dotación tecnológica	% de Cumplimiento de Servicio	96%	Brindar y Mantener el Servicio de Oficinas y Centros de Cableados	\$ 9.557.796.736
			Administrar, soportar y mantener el servicio de Dotación de Equipos - Portátiles , Impresoras, Scanner, Repuestos entre otros.	\$ 6.682.666.257
			Administrar, soportar y mantener la Mesa de Servicios Tecnológicos.	\$ 1.459.537.007
TOTAL				\$ 17.700.000.000

5.2 Centro de Datos:

Servicios **tercerizados**, los cuales se adquieren por Acuerdo Marco de Precio y otras modalidades de contratación, conformado con una infraestructura Virtualizada que permite alojar, procesar, custodiar, disponer y asegurar los sistemas de Información estratégicos, misionales y apoyo, así como bases de datos e información para el registro, atención y reparación integral a las víctimas de la Unidad, bajo un esquema de poder de cómputo por demanda.

Como parte del servicio se encuentran las siguientes categorías:

- ✓ IaaS: Infraestructura como servicios, compuesta de servidores virtuales, su unidad de medida es VM – Máquina Virtual.
- ✓ PaaS: Plataforma como servicio, compuesto por servidores virtuales de bases de datos, su unidad de medida es VM – Máquina Virtual.
- ✓ Almacenamiento: Soluciones de almacenamiento asociado a servidores virtuales dispuesto para soportar la operación. Los tipos de almacenamiento esta determinados por la velocidad de acceso a la información (Estándar – Base de datos), su unidad de medida es GB / TB, en Gigas o Terabytes.

Así mismo, la Oficina de Tecnologías de la Información debe actualizar y renovar el soporte del licenciamiento especializado requerido para servicios específicos para base de datos, información y procesos. Instalados sobre la infraestructura virtualizada del centro de datos entre ellos se encuentra:

- Software de Diagnóstico y Afinamiento de Base de datos: Permite el balanceo de las cargas de procesamiento, mejorar los tiempos de respuesta, afinar, optimizar diagnosticar y monitorear las bases de datos de motor ORACLE.
- Software manejador de procesos: Este producto modelar e implementar procesos.
- Software de procesamiento de nómina: Producto específico para liquidación de nómina, e inventarios
- Software de análisis y calidad datos: Producto específico que permite hacer minería y análisis del dato, aplicando de reglas de negocia para su transformación.
- Herramientas de Búsqueda de datos no estructurados
- Herramientas Geográficas
- Herramientas de Seguridad
- Herramientas orientadas a la integración de servicios web

Por lo anterior y con el objeto de dimensionar la **capacidad del servicio** requiere el análisis de las siguientes variables:

- ✓ Capacidad instalada al inicio de la vigencia, denominada línea base.

- ✓ Tendencia del servicio en vigencias anteriores.
- ✓ Supuesto de costeo base para asegurar la sostenibilidad del servicio.
- ✓ Incremento del 3% correspondiente al IPC.
- ✓ Entrega de información de operadores de la entidad.
- ✓ Traslados y/o ampliaciones de oficinas.
- ✓ Contratación Vigente y/o procesos contractuales a ser adelantados.

En consecuencia, a partir del análisis de variables previamente descritas, esta oficina asigna para los servicios de centro de datos en la **vigencia 2018**, un total de recursos por valor de **(\$4.377)** Millones de pesos.

PRODUCTO	UNIDAD DE MEDIDA	META	ACTIVIDADES	2018
		2018		
Servicios Cómputo por Demanda y Herramientas de Colaboración	% de Disponibilidad	99,95%	Administrar, soportar y mantener los servicios del Computo por demanda	\$ 3.425.207.778
			Actualizar y mantener licenciamiento de productos tecnologicos	\$ 951.670.224
SUBTOTAL				\$ 4.376.878.002

5.3 Conectividad

Servicios **tercerizados**, los cuales se adquieren por **Acuerdos Marco de Precios de Conectividad II** - CCE-427-1-AMP-2016 Acuerdo Marco de Precio y cobertura Nacional, conformado por Canales de Datos e Internet y servicio comunicación móvil, los cuales le permiten a la oficina de tecnologías de Información de la Unidad estar interconectada entre las oficinas y la infraestructura virtual de centro de datos y herramientas de colaboración de la entidad, así como comunicación móvil a través de MIFI.

Por lo anterior y con el objeto de dimensionar la **capacidad del servicio** requiere el análisis de las siguientes variables:

- ✓ Capacidad instalada al inicio de la vigencia, denominada línea base.
- ✓ Tendencia del servicio en vigencias anteriores.
- ✓ Supuesto de costeo base para asegurar la sostenibilidad del servicio.
- ✓ Incremento del 3% correspondiente al IPC.
- ✓ Entrega de información de operadores de la entidad.
- ✓ Proyectos y/o desarrollos de sistemas de información a disponer en producción que impacten la infraestructura virtualizada dispuesta para soportar el servicio.
- ✓ Contratación Vigente y/o procesos contractuales a ser adelantados.
- ✓ Renovación y /o adquisición de Licenciamiento.

En consecuencia, a partir del análisis de variables previamente descritas, esta oficina asigna para los servicios de conectividad en la **vigencia 2018**, un total de recursos por valor de **(\$1.182)** Millones de pesos.

PRODUCTO	UNIDAD DE MEDIDA	META	ACTIVIDADES	2018
		2018		
Servicios de conectividad y telefonía	% de Disponibilidad	99.6%	Administrar, soportar y mantener el servicio de Canales de Datos	\$ 937.315.574
			Administrar, soportar y mantener el servicio de Canales de Internet	\$ 94.995.275
			Administrar, soportar y mantener el Servicio Comunicación Movil	\$ 150.000.000
SUBTOTAL				\$ 1.182.310.849

5.4 Telefonía

El servicio de Plataforma de telefonía, le permiten a la oficina de tecnologías de la información brindar la comunicación de voz – Telefonía VoIP, internet móvil y servicios complementarios (Troncales SIP, administrador de ancho de banda entre otros) a la entidad a través de contrato interadministrativo, con una cobertura Nacional y Centralizada.

Por lo anterior y con el objeto de dimensionar la **capacidad del servicio** requiere el análisis de las siguientes variables:

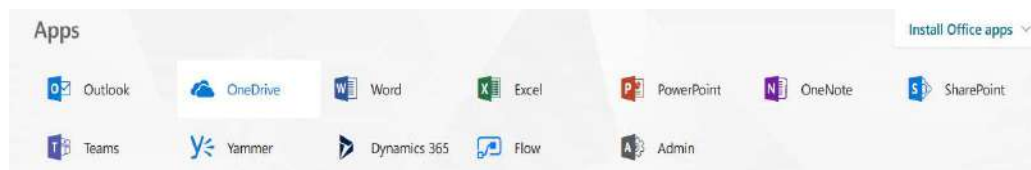
- ✓ Capacidad instalada al inicio de la vigencia, denominada línea base.
- ✓ Tendencia del servicio en vigencias anteriores.
- ✓ Supuesto de costeo base para asegurar la sostenibilidad del servicio.
- ✓ Incremento del 3% correspondiente al IPC.
- ✓ Contratación Vigente y/o procesos contractuales a ser adelantados.

En consecuencia, a partir del análisis de variables previamente descritas, esta oficina asigna para los servicios de telefonía IP en la **vigencia 2018**, un total de recursos por valor de **(\$502)** Millones de pesos.

PRODUCTO	UNIDAD DE MEDIDA	META	ACTIVIDADES	2018
		2018		
Servicios de conectividad y telefonía	% de Disponibilidad	99.6%	Administrar, soportar y mantener el servicio de Plataforma de telefonía	\$ 502.915.384

5.5 Herramientas Colaborativas

Servicio tercerizado a través de **Acuerdos Marco de Precios servicios Microsoft**, bajo plataforma unificada y acceso vía Web. Permitiendo entregar a la Unidad servicio de correo, Skype, almacenamiento por usuario, en un esquema de servicio por demanda. Las siguientes ilustraciones presentan las aplicaciones que la componen y la tendencia en la capacidad.



Por lo anterior y con el objeto de dimensionar la **capacidad del servicio** requiere el análisis de las siguientes variables:

- ✓ Capacidad instalada al inicio de la vigencia, denominada línea base.
- ✓ Tendencia del servicio en vigencias anteriores.
- ✓ Supuesto de costeo base para asegurar la sostenibilidad del servicio.
- ✓ Incremento del 3% correspondiente al IPC.
- ✓ Contratación Vigente y/o procesos contractuales a ser adelantados.

En consecuencia, a partir del análisis de variables previamente descritas, esta oficina asigna para los servicios de herramientas de colaboración en la **vigencia 2018**, un total de recursos por valor de **(\$502) Millones de pesos**.

PRODUCTO	UNIDAD DE MEDIDA	META	ACTIVIDADES	2018
		2018		
Servicios Cómputo por Demanda y Herramientas de Colaboracion	% de Disponibilidad	99.95%	Administrar, soportar y mantener el servicio de Herramientas de Colaboracion	\$ 1.881.028.363

5.6 Sistemas de Información

La oficina de tecnologías de Información de la Unidad, en procura de realizar acciones que garanticen los derechos de las víctimas y las funciones dadas por ley a la Unidad, propone actividades orientadas a la gobernabilidad de TI , soporte, actualización, construcción e integración de soluciones tecnológicas y/o Sistemas de información, que automatizan procesos y/o trámites misionales, estratégicos y de apoyo por medio de la contratación de terceros, cuya cobertura es del orden Nacional y Centralizado

A continuación, se describe cada una de las actividades que le conforman:

i) *Formular e integrar al modelo de Gobierno TI nuevos procesos Misionales y de apoyo:*

A través de esta actividad, la oficina de tecnologías de la información plantea proyectos que ofrecen soluciones tecnológicas que permitan a la entidad avanzar en la gobernabilidad, integración y atomización de sus procesos a través de diferentes productos tecnológicos, integrándolos en una arquitectura de: información, aplicaciones e infraestructura

Lo anterior se encuentra enmarcado en una adecuada Gestión de Proyectos que la Oficina de Tecnologías de la Información ha implementado por medio de mecanismos de acompañamiento en el levantamiento de requerimientos, fortaleciendo el proceso de identificación de necesidades y orientación a la implementación de estas en el marco del dominio de sistemas de Información.

En este contexto es necesario la divulgación de compromisos y cronogramas que permitan que exista entre las partes acuerdos claros y puntuales que permiten a la oficina de tecnologías de la información establecer tiempos, recursos y esfuerzos de forma tal que se pueda atender puntualmente las solicitudes de las áreas en los tiempos estimados.

Por consiguiente el desarrollo y la entrega de cada una de las soluciones se encuentran soportadas en una base sólida de un ciclo de vida de software que contempla un modelo de desarrollo ágil que permite el uso de herramientas tecnológicas y aprovechamiento de las capacidades del recurso humano, acompañado de una adecuada gestión de proyectos que aceleran y optimizan actividades que permiten el aseguramiento de un producto duradero en el tiempo con el cual se genera crecimiento y aporte de manera significativa al cumplimiento de metas de gobierno trazadas para esta vigencia.

ii) *Crear, Soportar, optimizar y/o mantener soluciones informáticas soluciones que permitan gestionar, consolidar y exponer la información.*

Bajo esta actividad la oficina de tecnologías conforma un equipo de trabajo experto en las diferentes plataformas de desarrollo tecnológicas que permiten: Crear, Soportar, optimizar y/o mantener las soluciones tecnológicas existentes, legadas o en construcción.

Entre los proyectos que impactaran la misionalidad de la Unidad se destacan la generación de lineamientos que permitan el manejo y administración de la información en tema documental, de acuerdo a la información que custodia la Unidad, encontrándose apalancado en el Proyecto de Gestión Documental liderado por la Dirección General y apoyado por la mesa técnica conformada por la Oficina de Tecnologías de la Información, Red Nacional de Información, Oficina Asesora de Planeación y el Grupo de Gestión Administrativa y Documental.

Adicional a ello la implementación de un sistema propietario, autónomo y escalable como es el Sistema de Gestión de Víctimas que le facilita a la Unidad no generar dependencias técnicas sobre los operadores y que atienda las necesidades de los procesos involucrados en la respuesta y atención a las víctimas y ciudadanos en general, proyecto que es dirigido por la Subdirección General y con apoyo técnico de la Oficina de Tecnologías permitiendo alcanzar un alto nivel de transaccionalidad desde cada uno de los procesos que intercambian información, asegurando calidad y proporcionando niveles de seguridad adecuados para el manejo sensible de este tipo de información. El Sistema de Gestión de Víctimas brindará tanto a la Unidad como a la ciudadanía en general mecanismos de comunicación más efectivo y seguros en el marco de la Ruta Integral. Por parte de la defensa jurídica de la Unidad la aplicación “LEX” en trabajo coordinado entre la Oficina de Tecnologías de la Información y el Grupo de Respuesta Escrita brinda a la Unidad el mecanismo para de atención a las solicitudes legales de víctimas y terceros, para lo cual la Oficina de tecnologías dispone de un equipo de trabajo interdisciplinar que permite crear e implementar las soluciones tecnológicas necesarias para garantizar la defensa jurídica de la entidad. Desde la Oficina de Tecnologías se incentiva y se brinda todo el apoyo necesario para la construcción de sistemas de información que permitan la operación interna y continua de sus funcionarios, para esto dispone, desarrolla e implementa soluciones tecnológicas a la medida que permitan la interacción y coordinación de las áreas misionales a fin de apoyar el cumplimiento de los objetivos estratégicos de la unidad.

Por lo anterior y con el objeto de dimensionar la **capacidad del servicio** requiere el análisis de las siguientes variables:

- ✓ Capacidad instalada al inicio de la vigencia, denominada línea base.
- ✓ Tendencia del servicio en vigencias anteriores.
- ✓ Supuesto de costeo base para asegurar la sostenibilidad del servicio.
- ✓ Incremento del 3% correspondiente al IPC.
- ✓ Contratación Vigente y/o procesos contractuales a ser adelantados.

En consecuencia, a partir del análisis de variables previamente descritas, esta oficina asigna para los servicios de herramientas de colaboración en la **vigencia 2018**, un total de recursos por valor de **(\$5.357)** Millones de pesos.

PRODUCTO	UNIDAD DE MEDIDA	META	ACTIVIDADES	2018
		2018		
Servicios de formulación, Creación e Integración de Sistemas de Información	% de Cumplimiento de avance	95%	Formular e integrar al modelo de Gobierno TI nuevos procesos Misionales y de apoyo	\$ 2.820.093.202
			Crear herramientas ó soluciones que permitan gestionar, consolidar y exponer la información	\$ 1.293.754.842
			Soportar, optimizar y mantener soluciones informáticas legadas y/o en producción	\$ 1.243.019.358
SUBTOTAL OBJ (2)				\$ 5.356.867.402

5.7 Uso y Apropiación

Según el modelo de gestión TI IT4+, define este dominio como aquel que “permite definir la estrategia y prácticas concretas que apoyan la adopción del Marco y la gestión TI que requiere la institución para implementar la Arquitectura TI”. Es así como esta oficina inicia la implantación en la vigencia 2014.

6. MODELADO Y SIMULACIÓN DE DIFERENTES ESCENARIOS DE CAPACIDAD

La oficina de tecnologías presenta ante la oficina asesora de planeación -OAP, la dirección nacional de planeación DNP y cabeza del sector, la proyección de recursos necesarios para la sostenibilidad de los servicios de la vigencia 2018, en el primer semestre de la vigencia 2017. Estas proyecciones son consignadas en el documento extendido “**Justificación Proyecto de Inversión**” cuyo código en el banco de proyectos es BPIN2014011000409, radicando dicha solicitud a través del sistema SUIFP - Sistema Unificado de Inversión y Finanzas Públicas, por medio del turno del trámite **No. 274494**. En respuesta a la aprobación de la solicitud de recursos, la entidad recibe la asignación de recursos para la vigencia 2018, por valor de **\$31.000** Millones de pesos.

Posterior a la asignación de los recursos, la oficina en el marco de sus planes acción define el plan anual de adquisiciones - PAA el cual le permite establecer la programación para la adquisición y/o renovación de los servicios tecnológicos, que esta oficina brinda a la entidad. Dicho plan es publicado en la siguiente dirección:

7. MONITORIZACIÓN DEL USO Y RENDIMIENTO DE LA INFRAESTRUCTURA TI

El seguimiento y control de la infraestructura se lleva a cabo con periodicidad mensual, el cual le permite a la oficina generar alertas tempranas y/o tomar acciones administrativas, técnicas y/o financieras para garantizar el servicio a la entidad.

7.1 Infraestructura Tecnológica

En la siguiente dirección se publica el consolidado del seguimiento de infraestructura: <https://unidadvictimas.sharepoint.com/sites/AdmonTI/Documentos%20compartidos/Forms/AllItems.aspx?viewpath=%2Fsites%2FAdmonTI%2FDocumentos%20compartidos%2FForms%2FAllItems%2Easpx&id=%2Fsites%2FAdmonTI%2FDocumentos%20compartidos%2FG%2EST%2E01%2DDominio%20Servicios%20Tecnologicos%2F02%2E2%2E2%20Gestion%20de%20Capacidad%2FInfraestructura%20TI%2FVig%202018>

7.2 Licenciamiento

La oficina a través de diferentes modalidades de contratación ha adquirido, renovado, suscrito derechos de uso y soporte al licenciamiento de los diferentes productos, herramientas que la unidad ha demandado.

El seguimiento al licenciamiento se lleva con una periodicidad mensual, el cual se registra por medio de un informe.

En la siguiente dirección se publica el consolidado del seguimiento de infraestructura: <https://unidadvictimas.sharepoint.com/sites/AdmonTI/Documentos%20compartidos/Forms/AllItems.aspx?newTargetListUrl=%2Fsites%2FAdmonTI%2FDocumentos%20compartidos&viewpath=%2Fsites%2FAdmonTI%2FDocumentos%20compartidos%2FForms%2FAllItems%2Easpx&id=%2Fsites%2FAdmonTI%2FDocumentos%20compartidos%2FG%2EST%2E01%2DDominio%20Servicios%20Tecnologicos%2F02%2E2%2E2%20Gestion%20de%20Capacidad%2FSeguimiento%20Licenciamiento>

7.3 Uso y Apropiación

La Oficina de Tecnología de la Información cuenta con un plan de divulgación cuya vigencia data de 2014, el cual ha venido implementando actividades tendientes a fortalecer las habilidades de los colaboradores a través de la difusión del conocimiento y promoción del manejo de las herramientas tecnológicas disponibles en la Unidad.

Conforme la Unidad ha venido robusteciéndose tecnológicamente, se ha venido realizando entregas funcionales, con lo cual se acompaña de actividades de expectativas,

sensibilización, divulgación, capacitaciones y apropiaciones, mediante recursos de comunicación, presenciales, sitios web para la publicación.

Durante el periodo de noviembre 2018, se llevó a cabo las siguientes sesiones:

DESCRIPCION	SESIONES	PARTICIPACION	HH	TOTAL, HH
Office365 (One Drive, Yammer, Teams)	2	4	2	4
Esigna	4		2	8
Taller de Seguridad	1		2	2
Web Cast	1		2	2
SUBTOTAL			8	16

8. GESTION DE LA DEMANDA

La demanda de los servicios es registrada en la herramienta de gestión utilizada en la mesa de servicios, la cual se denomina "ARANDA", de igual manera se cuenta herramientas complementarias de gestión para los servicios conectividad, centro de datos y sistemas de información.

Esta demanda es atendida conforme el análisis de recursos técnicos, económicos y alcance de cada uno de los contratos que esta oficina cuenta para brindar los servicios.

A continuación, se presenta conclusiones relevantes durante el periodo:

- ✓ Durante el periodo se renueva la suscripción de licencias de uso de EMS.
- ✓ Ejecución presupuestal alcanzo (95%) \$29.930 Millones y obligaciones \$23.843 Millones (78%) de la totalidad de los recursos asignados.

9. CREACIÓN Y MANTENIMIENTO DE LAS BASES DE DATOS DE CAPACIDAD (CDB)

A continuación, se presenta informaciones complementarias utilizada para el seguimiento de las capacidades, tales como:

- ✓ Consolidado de seguimiento a la inversión por periodo y vigencias:
 - ✓ <https://unidadvictimas.sharepoint.com/sites/AdmonTI/SitePages/Inicio.aspx?RootFolder=%2Fsites%2FAdmonTI%2FDocumentos%20compartidos%2FProyecto%20de%20Inversion%20%26%20PAA%2FVig%202018&FolderCTID=0x0120005907DB9>



[SEF91E84DACDAAE81F654A9EA&View=%7BC675FCB6%2DBEB0%2D4EF0%2DB933%2DD0EA7998C884%7D](https://www.unidadvictimas.gov.co/SEF91E84DACDAAE81F654A9EA&View=%7BC675FCB6%2DBEB0%2D4EF0%2DB933%2DD0EA7998C884%7D)

- ✓ Proyecto de inversión:
https://spi.dnp.gov.co/Consultas/ConsultaProyectos.aspx?id=img_Proyectos

- ✓ Plan anual de adquisiciones de la entidad:
<https://community.secop.gov.co/Public/App/AnnualPurchasingPlanManagementPublic/Index?currentLanguage=en&Page=login&Country=CO&SkinName=CCE>

- ✓ Informes de supervisión de la totalidad de servicios contratados a la fecha de corte.
- ✓ <http://portal.azure.com/>
- ✓ Módulo de administración del portal de office 365
- ✓ Portal licenciamiento Microsoft:
<https://www.microsoft.com/Licensing/servicecenter/default.aspx>
- ✓ Portal licenciamiento Adobe

Elaborado por: Margarita Guillen
Oficina de Tecnologías de la Información

SEGUIMIENTO CONSOLIDADO DE CAPACIDAD

NOVIEMBRE 2018

**OFICINA DE TECNOLOGIAS DE LA
INFORMACIÓN**



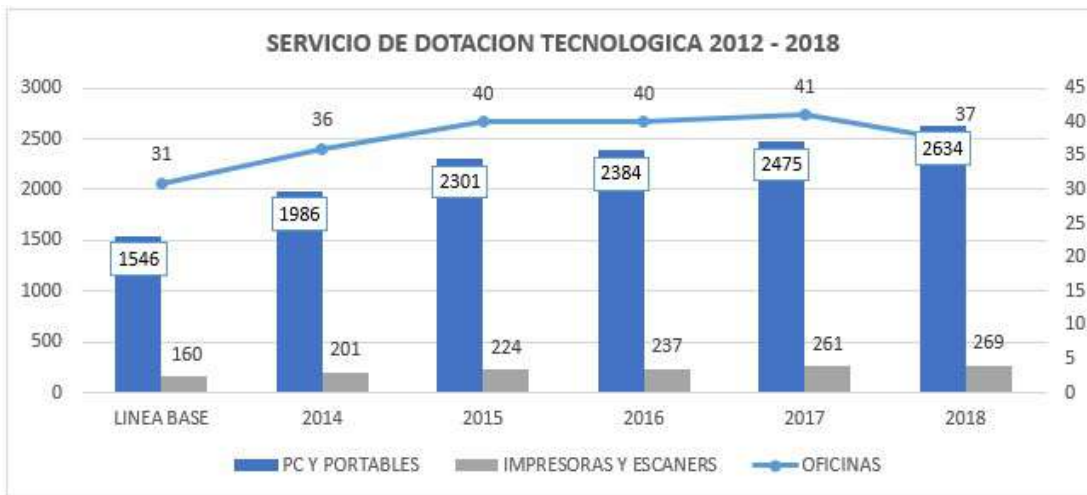
**GOBIERNO
DE COLOMBIA**



UNIDAD PARA LAS VÍCTIMAS

SEGUIMIENTO CAPACIDAD OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - DOTACIÓN TECNOLÓGICA

La oficina de tecnologías brinda en modalidad de **servicios tercerizado**, la dotación tecnológica con una cobertura a nivel nacional y centralizada compuesta por una infraestructura TI dispuesta en sitio en cada sede y/o oficina de la unidad conformada por herramientas tecnológicas, equipos de cómputo, equipos de impresión y escáner, periféricos, cableado estructurado, centros de cableado, servicio integral de video conferencia, soporte técnico, los cuales incluyen garantías y mantenimientos tanto correctivos como preventivos. Las siguientes tendencias presenta la demanda consolidada del servicio por vigencia.

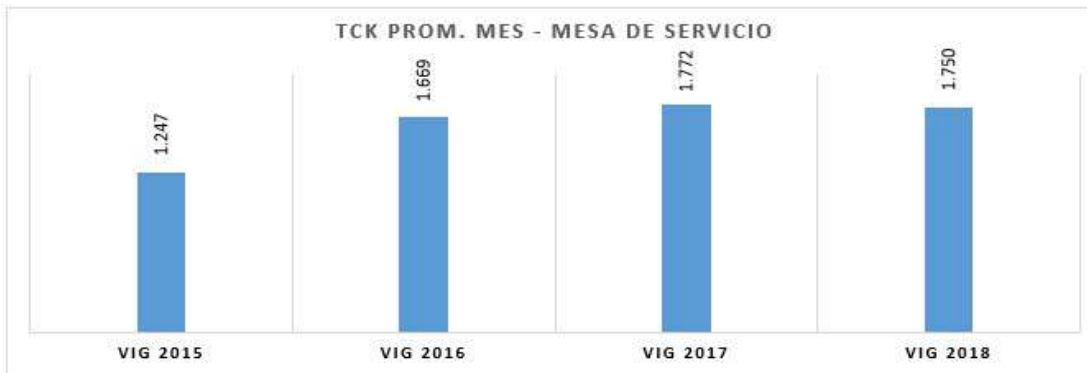


ANÁLISIS

La gráfica consolidada del servicio presenta una demanda creciente a lo largo de las vigencias en las diferentes líneas.

Esto obedece al crecimiento y cobertura de la entidad para brindar atención integral a las víctimas en cada una de las sedes de la entidad.

Del análisis de cada una de ellas, se evidencia que la línea de servicio de Pc's y portátiles presentó disminución.



ANÁLISIS

Este servicio inicia su implementación en las vigencias 2014 y se fortalece durante las siguientes vigencias.

En la vigencia 2018, Logrando atender un promedio de 1.750 solicitudes generadas por la entidad a través de los diferentes canales (telefónico, web y correo electrónico).



GOBIERNO DE COLOMBIA



UNIDAD PARA LAS VÍCTIMAS

SEGUIMIENTO DETALLADO CAPACIDAD – DOTACIÓN TECNOLÓGICA

TENDENCIA SERVICIO PC' & PORTABLES



ANALISIS EQUIPOS Y PORTABLES

La tendencia y la gráfica nos muestra un crecimiento promedio entre las vigencias 2013 - 2015 del 36%, estos crecimientos obedecen a la dinámica de la entidad y modalidad del servicio por demanda.

En la últimas vigencias 2016, 2017 la OTI orienta su esfuerzo en optimizar los recursos y obteniendo incremento de 4%, equivalente a 87 equipos promedio de incremento anual.

En el mes de noviembre de 2018 la capacidad presentó disminución del 1% frente al mes anterior.

TENDENCIA SERVICIO IMPRESION



ANALISIS IMPRESORAS Y SCANNER

La tendencia y la gráfica nos muestra un crecimiento promedio entre las vigencias 2013 - 2015 del 44%, estos crecimientos obedecen a la dinámica de la entidad y modalidad del servicio por demanda.

En la últimas vigencias 2016, 2017 la OTI orienta su esfuerzo en optimizar los recursos y obteniendo incremento de 4%, equivalente a 9 equipos promedio de incremento anual.

En el mes de noviembre de 2018 la capacidad presentó un aumento del 1% frente al mes anterior.

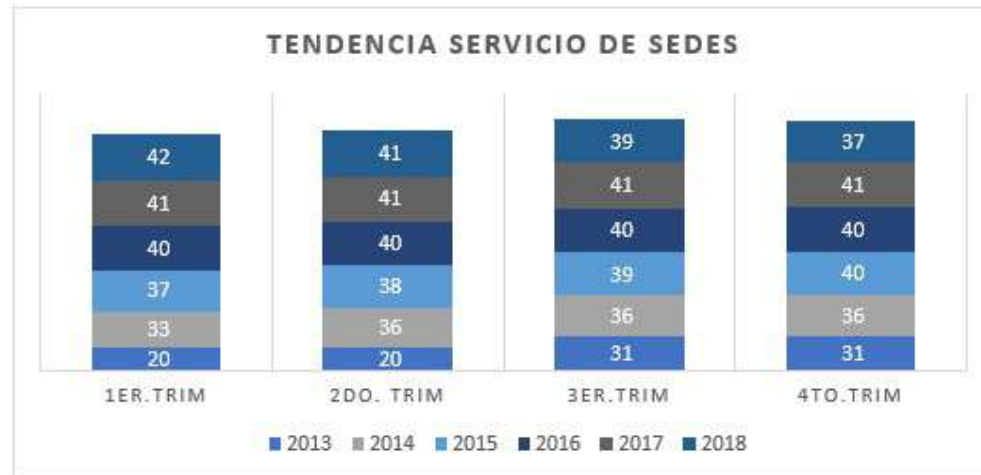
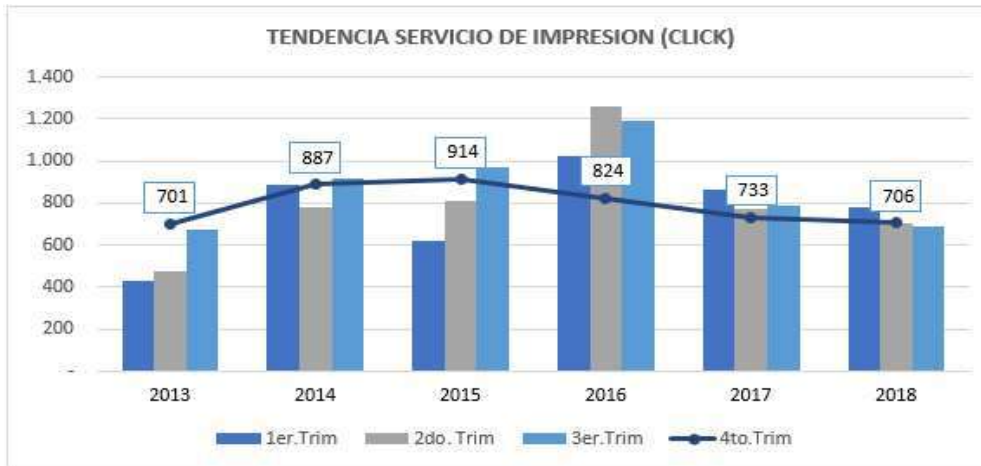


GOBIERNO DE COLOMBIA



UNIDAD PARA LAS VÍCTIMAS

SEGUIMIENTO DETALLADO CAPACIDAD - DOTACIÓN TECNOLÓGICA



ANALISIS SERVICIO DE IMPRESION

La tendencia y la gráfica nos muestra un crecimiento promedio entre las vigencias 2013 - 2015 del 44%, estos crecimientos obedecen a la dinámica de la entidad y modalidad del servicio por demanda.

En la ultimas vigencias 2016, 2017 la OTI orienta sus esfuerzo en optimizar los recursos y obteniendo disminución de 15%, equivalente a 116 clic anuales.

En el mes de noviembre de 2018 con base en la dinámica de la demanda se presentó aumento en Click de impresión.

ANALISIS SEDES

La tendencia y la gráfica nos muestra un crecimiento promedio entre las vigencias 2013 - 2015 fue 8% promedio, estos crecimientos obedecen a la dinámica de la entidad y modalidad del servicio por demanda.

En la ultimas vigencias 2017 la OTI orienta sus esfuerzo en optimizar los recursos y obteniendo disminución del 1%, equivalente a una (1) nueva sede.

En el mes de noviembre de 2018 la capacidad presentó disminución quedando en 37 sedes.



GOBIERNO DE COLOMBIA



UNIDAD PARA LAS VÍCTIMAS

SEGUIMIENTO CAPACIDAD OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - CENTRO DE DATOS NUBE PRIVADA

El Servicio Cómputo por Demanda y Herramientas de Colaboración

La oficina de tecnologías de la información de la unidad, brinda servicios de infraestructura **virtual centralizada** de cobertura nacional, en la nube bajo un esquema de cómputo por demanda, a través un servicio de Centro de datos y servicio herramientas de colaboración. Dichos servicios **servicio son tercerizado**, a través de Acuerdos Marco el cual que permite alojar, procesar, custodiar, disponer y asegurar los sistemas de Información estratégicos, misionales y apoyo, así como bases de datos e información para el registro, atención y reparación integral a las víctimas de la Unidad. A continuación se presenta los servicios consolidados por vigencia.



Esta tendencia presenta la tendencia de la infraestructura virtualizada del centro de datos principal, por cada una de las vigencias.

Dicha infraestructura esta conformada por servidores y soluciones de almacenamiento virtualizado, adicional de presentar variación en recursos de almacenamiento dado la dinámica de la entidad y respuesta y atención a los diferentes proceso que soporta.

En el mes de noviembre los servidores virtuales presentan estabilidad, a su vez se viene generando optimización de recursos mediante migración a Azure.



GOBIERNO DE COLOMBIA



UNIDAD PARA LAS VÍCTIMAS

SEGUIMIENTO DETALLADO CAPACIDAD – CENTRO DE DATOS

TENDENCIA SERVICIO IAAS



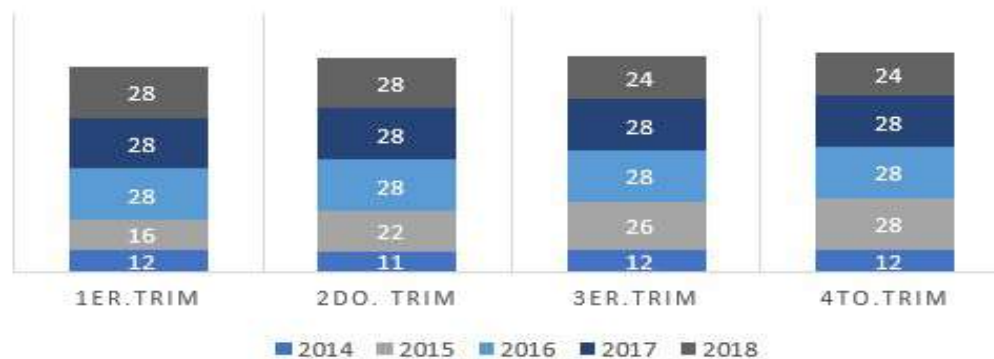
ANALISIS IAAS

La tendencias anuales de las vigencias 2013 - 2014 estuvo en el 45% promedio producto del montaje de la infraestructura para la unidad, en la vigencia 2015 se logró mantener el servicio sólo con incremento del 2%.

La OTI orienta su esfuerzo en continuar en la optimización de recursos mantener y/o mantener su capacidad, durante la vigencia 2016 – 2017 , se mantiene sin incrementar su capacidad.

En la vigencia 2018, en el mes noviembre la capacidad se mantiene.

TENDENCIA SERVICIO PAAS



ANALISIS PAAS

La tendencias anuales de las vigencias 2013 - 2014 estuvo en el 12% , en la vigencia 2015 se incremento la capacidad al 26% producto de la implementación nuevas soluciones tecnológicas, este servicio se afecta directamente, puesto que las mismas contienen un base de datos asociada.

La OTI orienta su esfuerzo en optimizar la capacidad orientado a mantenerla y/o disminuirla. Durante la vigencia 2016 se brinda el servicio sin ampliar la capacidad del mismo; En la vigencia 2017, permanece la capacidad sin incrementar.

En el periodo de noviembre la capacidad se mantiene.



GOBIERNO DE COLOMBIA



UNIDAD PARA LAS VÍCTIMAS

SEGUIMIENTO DETALLADO CAPACIDAD – CENTRO DE DATOS

TENDENCIA DE ALMACENAMIENTO OPTIMIZADO



TENDENCIA ALMACENAMIENTO ALTO RENDIMIENTO



TENDENCIA DE SERVICIO DE BACKUP



ANALISIS

La tendencias anuales de las vigencias 2013 - 2014 estuvo en el 24% promedio, en la vigencia 2015 se incremento la capacidad se incremento al 49% promedio, producto de la implementación nuevas soluciones tecnológicas, este servicio se afecta directamente.

En cumplimiento de la directriz de austeridad del gasto la OTI orientará su esfuerzo en optimizar la capacidad orientado a mantenerla y/o disminuirla, sin afectar el servicio. Durante la vigencia 2016, se optimizo el servicio en un 10% promedio.

En la vigencia 2017, se acoge al acuerdo marco de precios nube privada, en este acuerdo la clasificación del almacenamiento varia con respecto al acuerdo marco utilizado en las vigencias anteriores. Por tanto la vigencia 2017 no es comparable, sin embargo, durante la vigencia la capacidad de almacenamiento presentó un incremento en el almacenamiento de respaldo en 15%, correspondiente a 101 TB.

En el Periodo de noviembre se presentó aumento en 78 TB en almacenamiento de respaldo.



GOBIERNO DE COLOMBIA



UNIDAD PARA LAS VÍCTIMAS

SEGUIMIENTO CAPACIDAD OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - CENTRO DE DATOS NUBE PÚBLICA

La oficina de tecnologías de la información por medio de la orden de compra No. 23215 de 2017, brinda el servicio de nube pública a través de la plataforma denominada Azure con un capacidad de 2.594 Unidades equivalentes a 259.400 (USD), distribuidas en dos paquetes de 1.297 Unidades equivalentes a 129.700 (USD) cuyos códigos corresponde a CPC – 200244204 / CPC – 200244205. USD: Dólares CPC: Customer Purchase Confirmation – Confirmación de Compra del Cliente. En el mes de Noviembre de 2018 se realizó nueva orden de compra No. 32040 - 2018 de ampliación, que permitirá soportar la demanda del servicio hasta julio 2019.



Durante la vigencia 2018, de manera escalonada ha incrementado el uso de los recursos en esta nube.

La entidad a corte de septiembre utilizó el 100% de las unidades asociadas al CPC – 200244204 y se procede a activar el siguiente código CPC – 200244205 para cubrir la demanda del servicio.

La siguiente ilustración presenta la tendencia del uso de recursos del token No.2, siendo equivalente a 49 servidores virtuales, con un almacenamiento de 41 TB.

Crédito restante total: **90,644.26** usd

Buscar en elementos de filtro...

FECHA DE AMOR...	MÉTODO DE PAGO	CRÉDITO INICIAL (...)	EXPIR...	CRÉDITO RESTANTE (...)	ESTADO
14/9/2018	Clave que finaliza en TF...	129.700.00	13/10/2019	90.644.26	En uso
13/12/2017	Clave que finaliza en 6X...	129.700.00	13/12/2018	0.00	Consumido



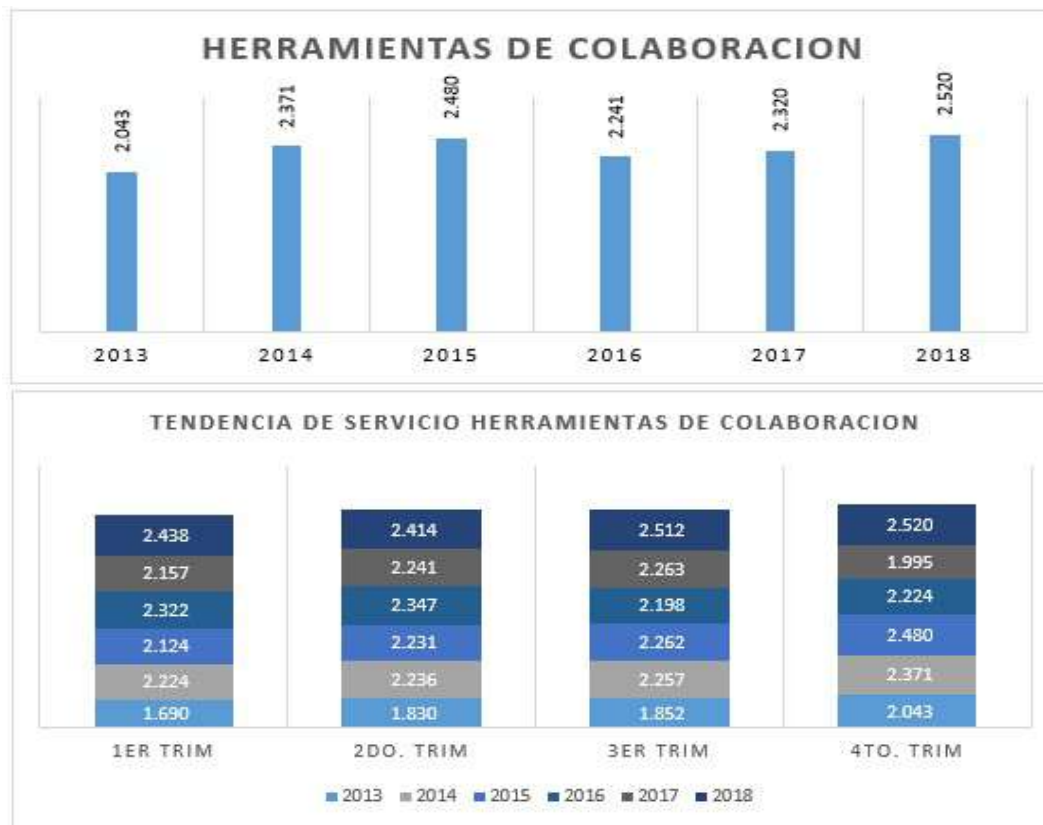
GOBIERNO DE COLOMBIA



UNIDAD PARA LAS VÍCTIMAS

SEGUIMIENTO CAPACIDAD OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - SERVICIO DE HERRAMIENTAS DE COLABORACIÓN – OFFICE 365

*Servicio herramientas de colaboración, servicio tercerizado a través de **Acuerdos Marco de Precios servicios Microsoft**, bajo plataforma unificada y acceso vía Web. Permitiendo entregar a la Unidad servicio de correo, Lync, almacenamiento por usuario, en un esquema de servicio por demanda.*



Esta tendencia presenta la tendencia del servicio de herramientas de colaboración por vigencias.

Desde la vigencia 2015, se dio inicio al uso de la plataforma OFFICE365, posterior a ella la oficina de tecnología ha optimizado el recurso sin que esto afecte la calidad del mismo hasta la fecha.

En la vigencia 2017 la oficina de tecnologías de la información por medio de la orden de compra No. 18398, brindó servicio de herramientas de colaboración con un capacidad de 2.395 licencias de uso.

Dado el incremento en la capacidad del servicio, la Oficina de Tecnologías adelantó en el primer trimestre de 2018 a través de la Orden de Compra N.º 26759 ampliación en 100 licencias de uso.

En tercer trimestre de 2018 se realizó la renovación de licencias de uso por medio de la Orden de Compra N.º 29947 con una capacidad 2.685.

En el mes de noviembre se presentó disminución del servicio en un 1% equivalente a 2.520 licencias de uso.



GOBIERNO DE COLOMBIA



UNIDAD PARA LAS VÍCTIMAS

SEGUIMIENTO CAPACIDAD OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - SERVICIO DE HERRAMIENTAS DE COLABORACIÓN – EMS

La oficina de tecnologías de la información realizó la suscripción del licenciamiento Enterprise Mobility and Security (EMS) de Microsoft para 2.160 usuarios de la Unidad por medio de la orden de compra 21573 de 2017 con el fin de implementar controles de seguridad adicionales tales como: **Análisis avanzado de amenazas - Advance Threat Analytics (ATA), Protección de la información, Gestión de identidad y acceso en dispositivos** permitiendo un mejoramiento continuo y fortalecimiento de las medidas de protección de la información manejada por los usuarios en los equipos de cómputo, dispositivos móviles o unidades de almacenamiento removibles. En el mes de noviembre de 2018 se realizó renovación de la suscripción del licenciamiento (EMS) por medio de la orden de compra 32854 – 2018 con ampliación para 2.480 usuarios de la Unidad.



El uso del licenciamiento Enterprise Mobility and Security (EMS), se genera a partir del establecimiento de políticas de seguridad y la necesidad de realizar el despliegue de funcionalidades orientadas al aseguramiento de la información. La implementación de esta herramienta de forma escalonada, inició en el último periodo de la vigencia 2017. En el mes de noviembre de 2018 se realizó renovación de suscripción y ampliación en capacidad.

La siguiente ilustración presenta la tendencia del uso de licencias a corte de noviembre de 2018.



GOBIERNO DE COLOMBIA



UNIDAD PARA LAS VÍCTIMAS

SEGUIMIENTO CAPACIDAD OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - CONECTIVIDAD & SISTEMAS DE INFORMACIÓN

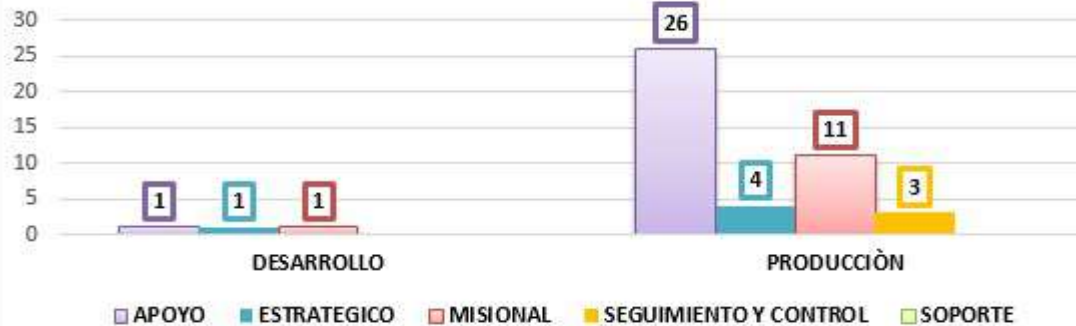
SERVICIOS DE CONECTIVIDAD Y TELEFONIA

TENDENCIA SERVICIO CONECTIVIDAD Y TELEFONIA IP



SISTEMAS DE INFORMACION

SISTEMAS DE INFORMACIÓN POR PROCESO



ANALISIS CONECTIVIDAD Y TELEFONIA

La tendencias anuales en las vigencias 2013 - 2015 el incremento de todas las líneas de servicio estuvo en el orden del 33% promedio. En la vigencia 2016, el incremento en el servicio ha sido del orden del 1% generado por la línea de comunicación móvil.

Durante la vigencia 2017 se genero una optimización del 16% en el servicio de canal de Datos. Para el periodo de Enero se presento una disminución del 38% en la línea de comunicación móvil y aumento del 2% en canales de Datos. En el mes de noviembre se mantiene la capacidad del servicio.

ANALISIS SISTEMAS DE INFORMACION

Durante la vigencia 2018, el equipo de sistema de información de la OTI brinda soporte, mantenimiento y generación de nuevas soluciones a la unidad.

Dicho equipo, conformado por 35 personas con diferentes roles.

A la fecha se encuentran dispuestos 44 soluciones en producción sobre la infraestructura centralizada del centro de datos.



GOBIERNO DE COLOMBIA



UNIDAD PARA LAS VÍCTIMAS

CONCLUSIONES

Al cierre del periodo Noviembre de 2018 se concluye:

- En el servicio de dotación Tecnológica durante el periodo del informe, tuvo el siguiente comportamiento: el componente de dotación de pc's y portables presentó disminución del 1% con respecto al periodo anterior, a su vez la capacidad en sedes presentó disminución quedando en 37 (sedes).
- En relación con impresoras y scanner presentó un aumento del 1% frente al mes anterior. Sin embargo, la tendencia en el servicio de clics es muy variable, ocasionado a la dinámica de las áreas.
- El servicio de centro de datos nube privada en el mes de noviembre presenta estabilidad en los servidores virtuales y en nube pública plataforma Azure el código CPC – 200244205 en consumo cubriendo la demanda del servicio. Además, se realizó nueva orden de compra No. 32040 - 2018 de ampliación , que permitirá soportar la demanda del servicio hasta julio 2019.
- En el servicio de conectividad y telefonía, la capacidad del servicio presenta estabilidad. Desde el mes de octubre se viene realizando mantenimiento preventivo y correctivo de los componentes incluidos en los servicios de Infraestructura telefónica en Bogotá y direcciones territoriales.
- El servicio de conectividad móvil presenta estabilidad.
- En los servicios de Herramientas de Colaboración la demanda del servicio de licenciamiento presento disminución en 1% equivalente a 25 licencias.
- En el mes de Noviembre se presentó renovación de la suscripción del licenciamiento Enterprise Mobility and Security (EMS) por medio de la orden de compra 32854 – 2018 con ampliación para 2.480 usuarios de la Unidad.
- En los servicios de Sistemas de información se presenta aumento en 44 sistemas en producción.



GOBIERNO
DE COLOMBIA



UNIDAD PARA LAS VÍCTIMAS

FUENTES DE INFORMACION

- Archivos Excel detallado con la gestión de capacidades por cada servicio:
 - ✓ Dotación Tecnológica - Equipos de Escritorio y Portátiles,
 - ✓ Dotación Tecnológica - Impresoras y Escáner,
 - ✓ Dotación Tecnológica - Servicio de Impresión Clic,
 - ✓ Centro de Datos - Servidores,
 - ✓ Centro de datos – Almacenamiento
 - ✓ Conectividad – Canales de datos e Internet
 - ✓ Conectividad – Telefonía IP
 - ✓ Conectividad – Móvil.
 - ✓ Inventario de Sistemas de Información
 - ✓ Herramientas de Colaboración-EMS
 - ✓ Consumo UND Azure
- Cierre de Servicio.

*Oficina de Tecnologías de la Información.
Elaborado por Margarita Guillen – Eleana Quintero*



GOBIERNO
DE COLOMBIA



UNIDAD PARA LAS VÍCTIMAS

¡Gracias!



GOBIERNO
DE COLOMBIA



UNIDAD PARA LAS VÍCTIMAS

SEGUIMIENTO PROYECTO DE INVERSION – PLAN ANUAL DE ADQUISICIONES

PROYECTOS DE INVERSION DE TECNOLOGIAS :

- ✓ 2014011000409;
- ✓ 2018011000425

OTROS PROYECTOS DE INVERSION:

- ✓ PREVENCIÓN Y EMERGENCIA
- ✓ CANALES DE ATENCIÓN Y
- ✓ FONDO DE REPARACIÓN

OFICINA DE TECNOLOGIAS DE LA INFORMACION
FECHA CORTE NOVIEMBRE 2018 Versión. 1.0



GOBIERNO DE COLOMBIA



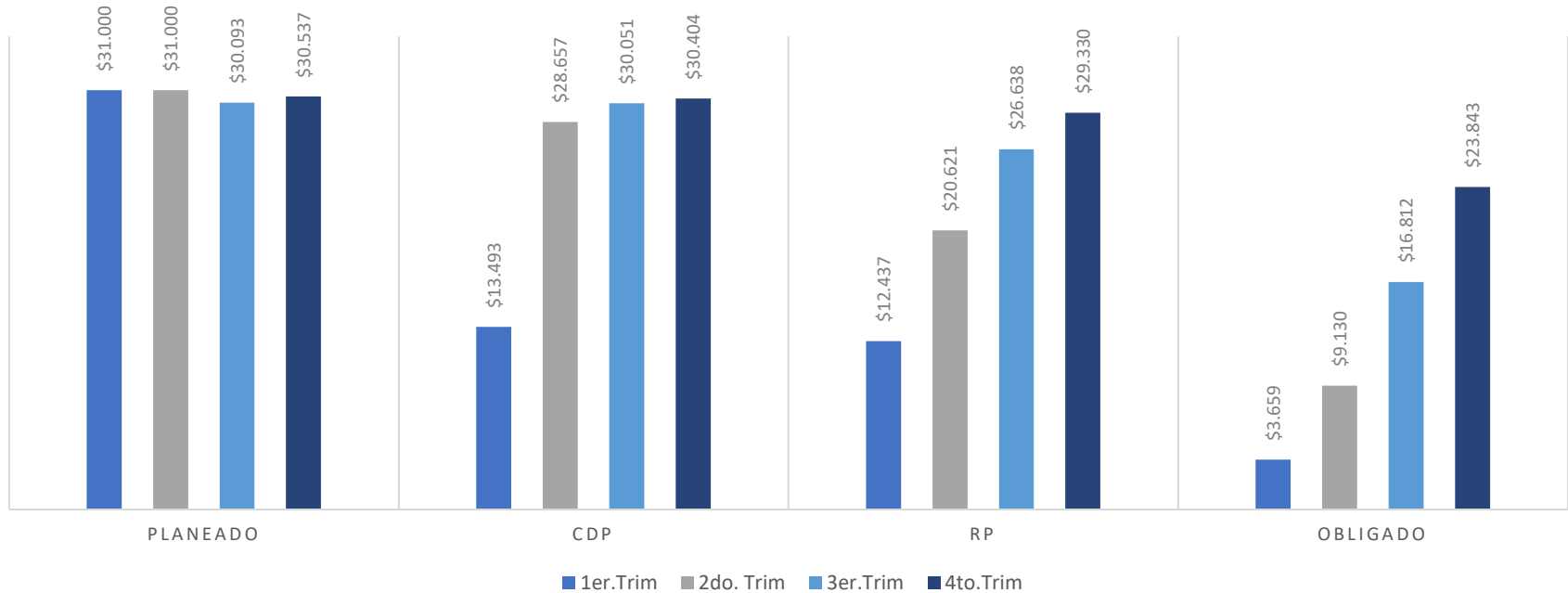
UNIDAD PARA LAS VÍCTIMAS

ASIGNACION DE RECURSOS Y SOLICITUD DE TRASLADOS VIGENCIA 2018

Para la Vigencia 2018, la oficina de tecnología ante el banco de proyectos de inversión cuenta con dos (2) proyectos, dada la reformulación del mismo. La asignación de recursos para la oficina es de un total de \$31.000 Millones de pesos.

A continuación se presenta tendencia del uso de los recursos asignados

TENDENCIA DE EJECUCION DE RECURSOS 2018 - PROYECTO DE INVERSION DE LA OFICINA DE TECNOLOGIAS EN MILLONES PESOS



98,51%

98,08%

95%

78%



GOBIERNO DE COLOMBIA

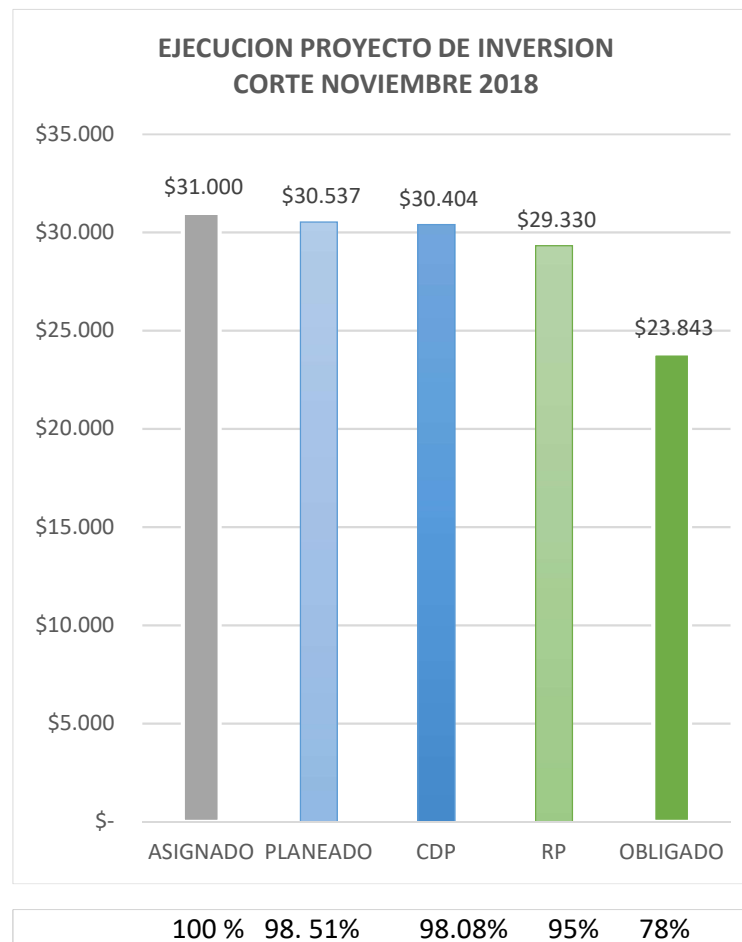


UNIDAD PARA LAS VÍCTIMAS

EJECUCION DE RECURSOS ASIGNADOS POR PROYECTO A CORTE DE NOVIEMBRE 2018 (MILLONES DE PESOS)

RUBRO	ASIGNADO	PLANEADO	CDP	RP	OBLIGADO
SERVICIOS COMPUTO POR DEMANDA - 2014011000409	\$ 6.203	\$ 6.120	\$ 6.096	\$ 6.039	\$ 5.002
SERVICIOS DE CONECTIVIDAD- 2014011000409	\$ 1.597	\$ 1.597	\$ 1.594	\$ 1.594	\$ 1.175
SERVICIOS DE DOTACION TECNOLOGICA -2014011000409	\$ 17.700	\$ 17.700	\$ 17.664	\$ 16.994	\$ 14.183
SERVICIOS DE SISTEMAS DE INFORMACION -2014011000409	\$ 4.676	\$ 4.677	\$ 4.633	\$ 4.373	\$ 3.154
SERVICIOS TECNOLOGICOS - 2018011000425	\$ 823	\$ 443	\$ 417	\$ 330	\$ 330
SUBTOTAL	\$ 31.000	\$ 30.537	\$ 30.404	\$ 29.330	\$ 23.843

TIPO DE PROCESO	ASIGNADO	PLANEADO	CDP	RP	OBLIGADO
ACUERDO MARCO PRECIOS		\$ 6.115	\$ 6.074	\$ 5.930	\$ 4.833
AGREGACION DE DEMANDA		\$ 780	\$ 780	\$ 780	\$ 780
CONTRATACION DIRECTA		\$ 20.548	\$ 20.536	\$ 19.660	\$ 16.309
RETIRADO		\$ -	\$ -	\$ -	\$ -
SELECCIÓN ABREVIADA MENOR CUANTIA	\$ 31.000	\$ 300	\$ 264	\$ 264	\$ 33
SIN PROGRAMAR		\$ -	\$ -	\$ -	\$ -
SUBASTA INVERSA ELECTRONICA		\$ 800	\$ 784	\$ 784	\$ -
TRASLADO AREA		\$ 1.864	\$ 1.864	\$ 1.864	\$ 1.864
VIATICOS & TICKETS		\$ 129	\$ 102	\$ 48	\$ 23
SUBTOTAL	\$ 31.000	\$ 30.537	\$ 30.404	\$ 29.330	\$ 23.843



Con respecto al periodo anterior 2018 , se presentó incremento en: RP's aumento en 2% correspondiente a 548M y las obligaciones aumento en 16% correspondiente a 4.941 M.



**GOBIERNO
DE COLOMBIA**

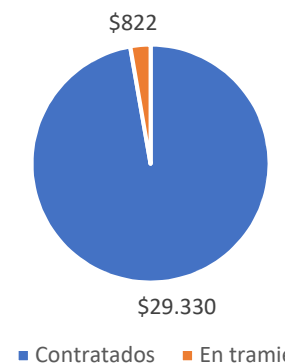


UNIDAD PARA LAS VÍCTIMAS

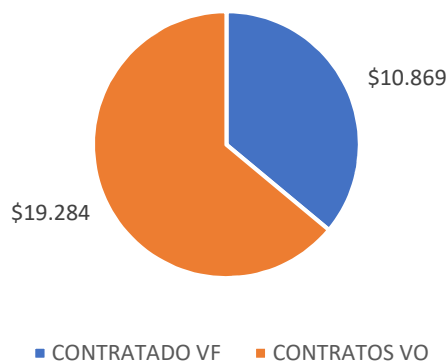
DETALLE DEL PLAN ANUAL DE ADQUISICIONES POR MODALIDAD , ESTADO Y EJECUCION FECHA DE CORTE NOVIEMBRE 2018

PROYECTO DE INVERSION TECNOLOGIA	PROCESOS CONTRATADOS		PAGOS
MODALIDAD	PROCESOS	VLR	VLR
ACUERDO MARCO	13	\$ 5.930.385.609	\$ 4.832.604.995
AGREGACION	2	\$ 780.257.772	\$ 780.257.772
CONTRATACION DIRECTA	11	\$ 19.659.745.229	\$ 16.308.535.018
SELECCIÓN ABREVIADA	1	\$ 263.608.008	\$ 33.368.128
SUBASTA	1	\$ 784.038.000	\$ -
TRASLADO - FINANCIERA	1	\$ 14.400.000	\$ 14.400.000
TRASLADO - ADMINISTRATIVA	1	\$ 1.850.000.000	\$ 1.850.000.000
TRASLADO TALENTO HUMNAO	1	\$ 47.636.028	\$ 23.430.346
SUBTOTALES POR ESTADO	31	\$29.330.070.646	\$ 23.842.596.260

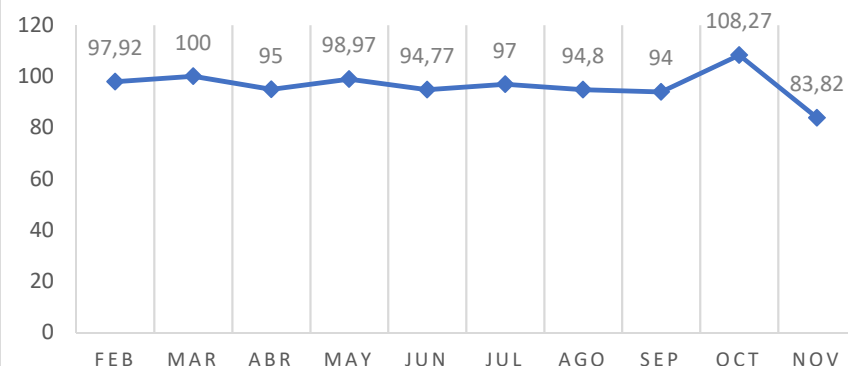
PROCESOS CONTRATADOS Y EN TRAMITE (MILLONES PESOS)



PROCESOS DE VIGENCIA FUTURA Y ORDINARIA (MILLONES PESOS)



PORCENTAJE DE USO DEL PAC SOLICITADO EN
VIG. 2018



UNIDAD PARA LAS VÍCTIMAS



DETALLE DEL PLAN ANUAL DE ADQUISICIONES POR MODALIDAD , ESTADO Y EJECUCION FECHA DE CORTE NOVIEMBRE 2018

ACUERDO MARCO PRECIOS	TIPO PROCESO / OBJETO CONTRACTUAL	CODPABS	CONTRATO	PLANEADO	CDP	RP	OBLIGADO	ESTADO
ACUERDO MARCO PRECIOS	Vigencias Futuras - Servicios de Centro de Datos	013000318	OC 12948 - 2016	\$ 1.196.364.374	\$ 1.196.364.373	\$ 1.196.364.373	\$ 1.112.237.506	CONTRATADO
ACUERDO MARCO PRECIOS	Ampliacion Servicios de Centro de Datos Modificatorio No.1	013002218	OC 12948 - 2016	\$ 729.367.459	\$ 729.213.568	\$ 729.213.568	\$ 436.033.905	CONTRATADO
ACUERDO MARCO PRECIOS	Vigencias Futuras - Servicios de Conectividad;	013000418	OC 20255 - 2017	\$ 492.485.523	\$ 492.485.523	\$ 492.485.523	\$ 489.206.278	CONTRATADO
ACUERDO MARCO PRECIOS	Ampliación Servicio de Conectividad; OTRO SI No.1 OC 20255	013003418	OC 20255 - 2017	\$ 32.130.000	\$ 32.130.000	\$ 32.130.000	\$ 27.180.000	CONTRATADO
ACUERDO MARCO PRECIOS	Ampliación Servicio de Conectividad; Modificatorio No.2 OC 20255	013001018	OC 20255 - 2017	\$ 334.393.175	\$ 331.340.845	\$ 331.340.845	\$ 230.240.819	CONTRATADO
ACUERDO MARCO PRECIOS	Apalancamiento Solicitud VF para los Servicios de Conectividad (*)	013004118		\$ 88.000.000	\$ 87.737.272		\$ -	EVENTO COTIZACION
ACUERDO MARCO PRECIOS	Servicios de Conectividad Móvil	013000718	OC 25596 - 2018	\$ 56.522.577	\$ 56.522.577	\$ 56.522.576	\$ 45.560.089	CONTRATADO
ACUERDO MARCO PRECIOS	Ampliacion Unidades Azure (*)	013004218	OC32040-2018	\$ 355.000.000	\$ 329.505.078	\$ 329.505.078	\$ 329.505.078	CONTRATADO
ACUERDO MARCO PRECIOS	Renovacion Anual de Soporte al Licenciamiento Oracle	013000618	OC 24580 - 2018	\$ 100.444.805	\$ 100.444.805	\$ 100.444.805	\$ 100.444.805	CONTRATADO
ACUERDO MARCO PRECIOS	Adquisicion Licencias Base de datos SQL Server	013002118	OC28562-2018	\$ 383.671.163	\$ 374.196.624	\$ 374.196.624	\$ 374.196.624	CONTRATADO
ACUERDO MARCO PRECIOS	Ampliación servicio Office365	013001618	OC 26759 - 2018	\$ 55.994.908	\$ 55.994.908	\$ 55.994.908	\$ 55.994.908	CONTRATADO
ACUERDO MARCO PRECIOS	Renovacion Anual Suscripcion Licencias Office 365	013002918	OC29947 - 2018	\$ 1.567.060.689	\$ 1.567.060.689	\$ 1.567.060.689	\$ 1.567.060.689	CONTRATADO
ACUERDO MARCO PRECIOS	Renovacion suscripcion Enterprise Mobility Security EMS	013002418	OC32854-2018	\$ 656.283.442	\$ 656.283.442	\$ 600.182.320		CONTRATADO
ACUERDO MARCO PRECIOS	Renovacion suscripcion Licencias CRM	013002918	OC31263-2018	\$ 67.000.000	\$ 64.944.300	\$ 64.944.299,64	\$ 64.944.300	CONTRATADO
SUB TOTAL				\$ 6.114.718.115	\$ 6.074.224.004	\$ 5.930.385.609	\$ 4.832.605.000	

MODALIDAD	TIPO PROCESO / OBJETO CONTRACTUAL			PLANEADO	CDP	RP	OBLIGADO	ESTADO
AGREGACION DE DEMANDA	Adquisicion Licencias Base de Datos ORACLE	013002518	OC30021 - 2018	\$ 423.257.772	\$ 423.257.772	\$ 423.257.772	\$ 423.257.772	CONTRATADO
AGREGACION DE DEMANDA	Renovacion Anual ELA Licencias ARGIS	013003118	OC30941-2018	\$ 357.000.000	\$ 357.000.000	\$ 357.000.000	\$ 357.000.000,00	CONTRATADO
SUB TOTAL				\$ 780.257.772	\$ 780.257.772	\$ 780.257.772	\$ 780.257.772,00	



UNIDAD PARA LAS VÍCTIMAS



**DETALLE DEL PLAN ANUAL DE ADQUISICIONES POR MODALIDAD , ESTADO Y EJECUCION
FECHA DE CORTE NOVIEMBRE2018**

MODALIDAD	TIPO PROCESO / OBJETO CONTRACTUAL			PLANEADO	CDP	RP	OBLIGADO	ESTADO
CONTRATACION DIRECTA	Vigencias Futuras - Servicios de Soporte a Telefonía IP	013000518	CIE006 - 2014	\$ 298.266.059	\$ 298.266.059	\$ 298.266.059	\$ 279.290.564	CONTRATADO
CONTRATACION DIRECTA	Ampliación Servicio de Telefonía IP; Modificadorio No.2	013003518	CIE006 - 2014 Mod.No.2	\$ 204.680.000	\$ 204.680.000	\$ 204.680.000	\$ 122.808.000	CONTRATADO
CONTRATACION DIRECTA	Vigencias Futuras - Servicios de Dotación Tecnología a la Unidad	013000218	CIE 008 - 2014	\$ 7.500.510.570	\$ 7.500.510.570	\$ 7.500.510.570	\$ 7.499.970.788	CONTRATADO
CONTRATACION DIRECTA	Ampliación Servicios de Dotación Tecnología a la Unidad; Modificadorio No.3	013002318	CIE 008 - 2014 Mod.No.3	\$ 7.730.000.000	\$ 7.730.000.000	\$ 7.730.000.000	\$ 5.449.222.941	CONTRATADO
CONTRATACION DIRECTA	Apalancamiento VF 2019 Dotación Tecnológica Adición y Prórroga No.4	013003318		\$ 734.586.226	\$ 734.586.226		\$ -	TRAMITE VF
CONTRATACION DIRECTA	Contratación de Prestación de Servicios OTI	013000118	CPS's 38	\$ 2.202.023.825	\$ 2.202.023.825	\$ 2.060.504.178	\$ 1.614.186.836	CONTRATADO
CONTRATACION DIRECTA	Renovación Anual al Soporte del Licitamiento Software Calidad de Datos	013003218	1532 - 2018	\$ 151.918.375	\$ 151.918.375	\$ 151.918.375	\$ 151.918.375	CONTRATADO
CONTRATACION DIRECTA	Vigencias Futuras - Servicios de Soporte y Mantenimiento a la plataforma ESIGNA	013000918	1121-2017	\$ 474.412.303	\$ 474.412.303	\$ 474.412.303	\$ 464.975.691	CONTRATADO
CONTRATACION DIRECTA	Renovación de Servicios de Soporte plataforma ESIGNA	013003618	1533 - 2018	\$ 854.623.672	\$ 854.623.672	\$ 854.623.672	\$ 401.751.712	CONTRATADO
CONTRATACION DIRECTA	Vigencias Futuras - Servicios Soporte a la plataforma ERP OTRO SI No.1 1305	013000818	1305 -2017	\$ 84.278.775	\$ 84.278.775	\$ 84.278.775	\$ 83.514.246	CONTRATADO
CONTRATACION DIRECTA	Ampliación Funcionalidades en la Plataforma ERP ERP OTRO SI No.2 1305	013001128	1305 -2017	\$ 53.862.375	\$ 53.862.375	\$ 53.862.375	\$ 53.862.375	CONTRATADO
CONTRATACION DIRECTA	Renvación a servicios de soporte plataforma ERP	013003018	1470 - 2018	\$ 259.089.942	\$ 259.089.942	\$ 246.688.922	\$ 187.033.490	CONTRATADO
SUB TOTAL				\$ 20.548.252.122	\$ 20.548.252.122	\$ 19.659.745.229	\$ 16.308.535.018	

MODALIDAD	TIPO PROCESO / OBJETO CONTRACTUAL			PLANEADO	CDP	RP	OBLIGADO	ESTADO
SELECCIÓN ABREVIADA MENOR CUANTIA	Mantenimientos Kits Tecnológicos Toma en Línea	013001818	1495-2018	\$ 300.000.000	\$ 300.000.000	\$ 263.608.008,00	\$ 33.368.128	CONTRATADO
SUBASTA INVERSA ELECTRONICA	Adquisición de Equipos de Seguridad de Infraestructura TIC	013003718	1535-2018	\$ 800.000.000	\$ 784.038.000	\$ 784.038.000,00		CONTRATADO
SUB TOTAL				\$ 1.100.000.000	\$ 1.084.038.000	\$ 1.047.646.008,00	\$ 33.368.128,00	

MODALIDAD	TIPO PROCESO / OBJETO CONTRACTUAL			PLANEADO	CDP	RP	OBLIGADO	ESTADO
TRASLADO AREA	Fortalecer la Infraestructura Tecnológica para soportar el proyecto expediente unico digital			\$ 1.850.000.000	\$ 1.850.000.000	\$ 1.850.000.000,00	\$ 1.850.000.000,00	CONTRATADO
TRASLADO AREA	Renovación Servicio Certificados digitales			\$ 14.400.000	\$ 14.400.000	\$ 14.400.000	\$ 14.400.000	CONTRATADO
VIATICOS & TICKETS	Garantizar los viáticos y gastos de desplazamiento de la OTI	013001918; 013002018		\$ 128.760.000	\$ 101.340.000	\$ 47.636.028	\$ 23.430.346	CONTRATADO
TOTAL				\$ 1.993.160.000	\$ 1.965.740.000	\$ 1.912.036.028	\$ 1.887.830.346	



UNIDAD PARA LAS VÍCTIMAS



**TODOS POR UN
NUEVO PAÍS**
PAZ EQUIDAD EDUCACIÓN

ESTADO PROCESO DE LIQUIDACION DE CONTRATOS

ESTADO CONTRATO	CONTRATACIÓN DIRECTA	CONTRATO DE COMPRAVENTA	CONTRATO INTER ADMINISTRATIVO	CONVENIO INTER ADMINISTRATIVO	ORDEN DE COMPRA	PRESTACIÓN DE SERVICIOS	TOTAL
VIGENTE	1	4	4	1	15	1	25
TERMINADO	2	1			4		6
INICIAR SOLICITUD DE LIQ.	3	2	1		13		16
SOLICITUD DE LIQUIDACIÓN	4		1				1
LIQUIDADO	5	11	18				30
TOTAL		2	18	24	1	32	78

- Durante el periodo se celebro sostuvo reunión con el proveedor UNE con el objeto que de finalizar la solicitud de Liquidación del contrato 005 del contrato marco 1511.
- Se genera un nuevo comunicado dirigido a CCE, solicitando actualización de usuarios aprobador para facturas remanentes.



UNIDAD PARA **LAS VÍCTIMAS**



**RECURSOS PROGRAMADOS EN EL PAA CON RECURSOS A OTROS PROYECTOS DE INVERSIÓN
FECHA CORTE DE NOVIEMBRE 2018 (MILLONES DE PESOS)**

Recursos otros proyectos de Inversión.

La oficina de tecnologías apoya a la entidad en proyectos transversales a la entidad, tal como es “Procesamiento de las imágenes digitales de los documentos misionales de la Unidad” en pro de la conformación del expediente único digital, para ello se trasladan recursos para adelantar la etapa precontractual, contractual y ejecución de los mismos.

Los recursos del proceso fue por valor de \$29.150 Millones.

TRASLADO DE AREAS A OTI 08 JUNIO 2018	VALOR	UARIV-LP-002-2018
A-3-6-3-12-31 Indemnización - Fondo	\$ 1.497.257.108	\$ 149.800.000
C-401-1500-17-0-32 Atencion Humanitaria	\$ 25.000.000.000	\$ 25.000.000.000
C-401-1500-7-0-35 Asistencia y Atencion	\$ 2.000.000.000	\$ 2.000.000.000
C-4101-1500-7-0-38 - Respuesta Escrita	\$ 2.000.000.000	\$ 2.000.000.000
SUBTOTAL	\$ 30.497.257.108	\$ 29.149.800.000

Sin embargo, mediante la resolución no. 04857 del 19 de septiembre de 2018, se declaró desierta la licitación pública UARIV-LP-002-2018 ; confirmándose por medio de las resoluciones No 07285 y 07286 de 29 de noviembre de 2018.

En consecuencia la oficina de tecnología, por medio de SIGESTION retorna los recursos asignados a los proyectos de inversión correspondientes.



**GOBIERNO
DE COLOMBIA**



UNIDAD PARA LAS VÍCTIMAS

CONCLUSIONES

- ✓ Se lleva a cabo la ejecución del PAC solicitado para el periodo de Octubre, con una **ejecución del 83,82%**. Se registra la ejecución presupuestal a cierre del periodo de Noviembre 2018, en el **Sistema SPI**.
- ✓ **Procesos Adjudicados en Noviembre:** Renovación Licencias de Uso EMS.
- ✓ **Comité Contracción:**
 - Se celebró Comité de contratación 11072018 para la solicitud de contratación de Servicios de Conectividad
 - Se realizo la apertura del evento de cotización en CCE.
 - Se celebró Comité de contratación 11132018 para la solicitud de adición y prórroga de servicios de dotación tecnológica
- ✓ Se recibe la aprobación por parte de **DPS** para la adición y prórroga de servicios de dotación tecnológica.



UNIDAD PARA **LAS VÍCTIMAS**



**TODOS POR UN
NUEVO PAÍS**
PAZ EQUIDAD EDUCACIÓN

FUENTES DE INFORMACION

- ✓ Matriz de Seguimiento al Plan anual de adquisiciones a corte de 30 de Noviembre– Oficina de Tecnologías.
- ✓ Matriz de Seguimiento Ejecución Proyecto de inversión a corte de 30 de Noviembre – Oficina de Tecnologías.
- ✓ Matriz de Seguimiento a Gestion de Capacidades – Oficina de Tecnologías.
- ✓ Matrices de Seguimiento Cadena Valor - PAA – Ejecución Contractual – Oficina de Tecnologías.
- ✓ Gestion de procesos de liquidación de contratos
- ✓ Matrices de seguimiento financiero generado por el grupo de gestión financiera y contable.
- ✓ Sistema de Información SIIF
- ✓ Sistema de Información SIGESTION
- ✓ Sistema de Información SUIFP
- ✓ Sistema de Información SPI

*Elaborado por:
Grupo de Seguimiento Financiera y Contractual – Oficina de Tecnologías de la Información*



UNIDAD PARA **LAS VÍCTIMAS**



¡Gracias!



GOBIERNO
DE COLOMBIA



UNIDAD PARA LAS VÍCTIMAS



ANEXO 5 - MATRIZ DE INICIATIVAS

Objetivo Estratégico: Acercar la Unidad a las víctimas en pro de su atención, reparación integral y ejercicio ciudadano mediante la transformación digital

Estrategia	Proyectos	Subproyectos(Temas/Actividades)	Dominio TI	Área(s) Responsable(s)	Áreas Co-Responsables y/o proveedoras de información	Facilitador Líder	Fecha Inicio	Duración
1-Ofrecer soluciones tecnológicas para facilitar a las víctimas su interacción con la Unidad optimizando la gestión y el servicio	1-1 Fortalecer la implementación del modelo de Gobierno Digital para facilitar la interacción con las víctimas	1-1-1 Definir e implementar soluciones que ofrezcan información y/o transacciones de utilidad a las víctimas sobre artefactos tecnológicos alineados a políticas de Gobierno Digital	Sistemas de Información	OTI SRNI OAC	Todas las dependencias de la Unidad que proveen servicios o información a las Víctimas	Jaime. Canaval OTI	1-dic-18	labor continua
		1-1-2 Proponer la implementación de un esquema transversal de validación en los procesos que involucren pagos a la población víctima	Información (Seguridad de la Inf.)	OTI Subdirección General	Direcciones misionales	Seguridad OTI	4-feb-19	10 meses
	1-2 Fortalecer la apertura de datos (datos abiertos)	1-2-1 Ofrecer información útil y de calidad que aporte a la atención de las víctimas, a partir de las Bases de Datos de la entidad (Cualificar BASES DE DATOS)	Información	SRNI	Todas las dependencias de la Unidad que proveen servicios o información a las Víctimas	Victor. Duran Dirección General	16-oct-18	labor continua
	1-3 Carpeta ciudadana (hoja de vida del ciudadano en el Estado Colombiano)	1-3-1 Definir contenidos a aportar por la Unidad para las Víctimas a la carpeta ciudadana	Sistemas de Información	Dirección General	Mesa de GD, Subdirección de participación ciudadana (comité ejecutivo - Mesa de Participación),	Ricardo. Daniel OTI	1-feb-19	4 meses
		1-3-2 Estructurar la entrega de contenidos establecidos por la Unidad a la carpeta ciudadana	Información	Áreas Misionales		Alexander. Holguin OTI	11-jul-19	8 meses
		1-3-3 Implementar la entrega de contenidos de la Unidad a la carpeta ciudadana	Información	SRNI	Todas las dependencias de la Unidad que proveen servicios o información de las Víctimas	Victor. Duran Dirección General	1-mar-20	labor continua
	1-4 Fortalecer el uso de herramientas de autogestión y los canales de comunicación estratégica de las víctimas en la iniciativa "Unidad en línea"	1-4-1 Fortalecer y ampliar funcionalmente los servicios informativos (de consulta)	Sistemas de Información	OTI	Todas las dependencias de la Unidad que proveen servicios o información a las Víctimas	Jaime. Canaval OTI	1-ene-19	12 meses
		1-4-2 Fortalecer y ampliar funcionalmente los servicios transaccionales	Sistemas de Información	OTI Asistencia, Reparación, OAJ		Jaime. Canaval OTI	1-ene-19	12 meses
		1-4-3 Crear la APP MÓVIL PIAV- PQRD	Sistemas de Información	OTI Asistencia, Reparación, OAJ		Jaime. Canaval OTI	10-jul-18	12 meses
		1-4-4 Fortalecer mecanismos de comunicación a las víctimas mediante redes sociales	Estrategia	SAAH (DGSH) - Atención al ciudadano OAC, OAJ, Dir Reparación	OTI y SRNI	Por definir	1-feb-19	12 meses
2-Generar sinergias con las entidades involucradas en la atención integral a la población víctima y con terceros, para contribuir a la transformación digital del Estado	2-1 Fortalecer los mecanismos de interoperabilidad para brindar información en línea a las entidades del SNARIV	2-1-1 Disposición del Modelo Integrado	Información	SRNI	OTI, Dirección General (Victor Durán)	Edward.Gira ldo SRNI	1-feb-19	48 semanas

		2-1-2 Creación de servicios tipo web para intercambio de información con las entidades del SNARIV	Información	SRNI	OTI	Edward.Giraldo SRNI	1-feb-19	48 semanas
		2-1-3 Construcción de 1 aplicación tipo APP para recopilar, disponer información y apoyar la declaración a través de dispositivos móviles.	Información	SRNI OTI		Alexander.Holguin OTI	1-mar-19	16 semanas
	2-2 Implementar iniciativas que promuevan la transformación Digital	2-2-1 Formular e implementar la reducción de trámites en lotes mediante agilidad de operaciones	Sistemas de Información	SRNI OTI		Victor.Duran Dirección General	1-feb-19	18 meses
		2-2-2 Implementar e integrar nuevas tecnologías para dar información a través de Sistemas de Información	Sistemas de Información	SRNI OTI	Todas las dependencias de la Unidad que proveen servicios o información de las Víctimas	Edward.Giraldo SRNI	1-feb-19	18 meses
		2-2-3 Promover el uso de Toma de declaración en Línea	Información	Subdirección de Registro, OTI		Alexander.Holguin OTI	2-may-19	8 meses
3-Fortalecer la seguridad y la eficiencia de la gestión interna, a partir del mejoramiento de las capacidades TI	3-1 Fortalecer el control de acceso y seguridad de los usuarios	3-1-1 Fortalecer el control de acceso físico a las instalaciones de la entidad en la sede central	Información (Seguridad de la Información)	Coordinación Administrativa y Documental		Pedro.Medina Coord. Administrativa	2-may-19	labor continua
		3-1-2 Generar una estrategia de identificación única de usuarios en las herramientas tecnológicas institucionales	Información (Seguridad de la Información)	OTI		Seguridad OTI	4-feb-19	10 meses
	3-2 Fortalecer la implementación de Gobierno digital	3-2-1 Formular e implementar la Arquitectura Empresarial de la Unidad, alineada al marco de referencia de AE del Estado Colombiano.	Estrategia	OTI Mesa de GD	Todas las dependencias	Victor.Duran Dirección General	1-sep-18	labor continua Formulación: jun2019
		3-2-2 Formular e implementar las diferentes arquitecturas de cada dominio , para conformar la Arquitectura de TI	Estrategia	OTI SRNI		Ricardo.Daniel OTI	1-feb-19	labor continua Formulación: jun2019
	3-3 Apropiar las mejores prácticas promovidas por MinTIC	3-3-1 Identificar, implementar y mantener las mejores prácticas en cada uno de los dominios de TI	Estrategia	OTI		Ricardo.Daniel OTI	15-jul-18	labor continua
	3-4 Diseñar e implementar un modelo de Continuidad de la operación de TI y gestión de incidentes	3-4-1 Definir e implementar planes que permitan garantizar la continuidad de la operación de TI, minimizando los riesgos relacionados con la seguridad de la información	Servicios Tecnológicos	OTI Mesa de Gobierno digital	Procesos misionales y de apoyo	Victor.Duran Dirección General	4-feb-19	labor continua
	3-5 Minimizar los riesgos de hurto modificación y pérdida de información	3-5-1 Implementar el plan de tratamiento de riesgos de seguridad y privacidad de la información	Información (Seguridad de la Información)	OTI Mesa de Gobierno digital	Procesos misionales y de apoyo	Seguridad OTI	1-abr-19	labor continua planes anuales



ANEXO 6

POLÍTICAS TI OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN



Contenido

INTRODUCCIÓN..... 5

POLÍTICA PARA LA ESTRATEGIA DE TI..... 6

 VISIÓN GENERAL 6

 PROPÓSITO 6

 ALCANCE 6

 POLÍTICA 6

 CUMPLIMIENTO DE LA POLÍTICA..... 7

 EXCEPCIONES..... 7

 ESTÁNDARES, POLÍTICAS Y PROCESOS RELACIONADOS 7

POLÍTICA PARA GOBIERNO DE TI 8

 VISIÓN GENERAL 8

 PROPÓSITO..... 8

 ALCANCE 8

 POLÍTICA 8

 CUMPLIMIENTO DE LA POLÍTICA..... 9

 EXCEPCIONES..... 9

 ESTÁNDARES, POLÍTICAS Y PROCESOS RELACIONADOS 9

POLÍTICA GENERAL DE USO y APROPIACION 10

 VISIÓN GENERAL 10

 PROPÓSITO 10

 POLÍTICA 10

 CUMPLIMIENTO DE LA POLÍTICA..... 11

 EXCEPCIONES..... 11

 ESTÁNDARES, POLÍTICAS Y PROCESOS RELACIONADOS 11

POLÍTICA GENERAL DE INTEROPERABILIDAD Y COLABORACIÓN..... 12

 VISIÓN GENERAL 12

 PROPÓSITO 12

 ALCANCE 12

 POLÍTICA 12

 CUMPLIMIENTO DE LA POLÍTICA..... 12

 EXCEPCIONES..... 12

 ESTÁNDARES, POLÍTICAS Y PROCESOS RELACIONADOS 12

POLÍTICA GENERAL DE GOBIERNO DEL DATO..... 13

 VISIÓN GENERAL 13

 PROPÓSITO..... 13

 ALCANCE 13

 POLÍTICA 13

 CUMPLIMIENTO DE LA POLÍTICA..... 13

 EXCEPCIONES..... 13

 ESTÁNDARES, POLÍTICAS Y PROCESOS RELACIONADOS 13





POLÍTICA GENERAL DE CALIDAD DE DATOS E INFORMACIÓN..... 14

 VISIÓN GENERAL 14

 PROPÓSITO 14

 ALCANCE 14

 POLÍTICA 14

 CUMPLIMIENTO DE LA POLÍTICA..... 14

 EXCEPCIONES 14

 NO CUMPLIMIENTO 15

 ESTÁNDARES, POLÍTICAS Y PROCESOS RELACIONADOS 15

POLÍTICA GENERAL DE DESARROLLO Y MANTENIMIENTO DE SOFTWARE..... 15

 VISIÓN GENERAL: 15

 PROPÓSITO 15

 ALCANCE: 15

 POLÍTICAS..... 15

 Generales: 15

 De Arquitectura:..... 16

 De calidad del Software: 17

 Control de Versiones:..... 17

 Seguridad de los Sistemas de Información..... 17

 Desarrollo Externo..... 17

 CUMPLIMIENTO DE LA POLÍTICA..... 18

 EXCEPCIONES 18

 NO CUMPLIMIENTO 18

 ESTÁNDARES, POLÍTICAS Y PROCESOS RELACIONADOS 18

POLÍTICA GENERAL DE CALIDAD DE SOFTWARE..... 18

 VISIÓN GENERAL: 18

 PROPÓSITO 19

 ALCANCE 19

 POLÍTICA 19

 CUMPLIMIENTO DE LA POLÍTICA..... 19

 EXCEPCIONES 19

 NO CUMPLIMIENTO 19

 ESTÁNDARES, POLÍTICAS Y PROCESOS RELACIONADOS 19

POLÍTICA PARA SERVICIOS TECNOLOGICOS 21

 VISIÓN GENERAL 21

 PROPÓSITO 21

 ALCANCE 21

 POLÍTICA 21

 CUMPLIMIENTO DE LA POLÍTICA..... 24

 EXCEPCIONES 24

 ESTÁNDARES, POLÍTICAS Y PROCESOS RELACIONADOS 24

SEGURIDAD DE LA INFORMACIÓN..... 25





VISIÓN GENERAL 25

ALCANCE 25

VIGENCIA Y ACTUALIZACIÓN DE POLÍTICAS 26

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 26

1. Organización de la seguridad de la información **¡Error! Marcador no definido.**
2. Seguridad de recursos humanos **¡Error! Marcador no definido.**
3. Gestión de activos **¡Error! Marcador no definido.**
4. Control de acceso **¡Error! Marcador no definido.**
5. Criptografía **¡Error! Marcador no definido.**
6. Seguridad física y del entorno **¡Error! Marcador no definido.**
7. Seguridad de las operaciones **¡Error! Marcador no definido.**
8. Seguridad de las comunicaciones **¡Error! Marcador no definido.**
9. Adquisición, desarrollo y mantenimiento de sistemas **¡Error! Marcador no definido.**
10. Relaciones con los proveedores **¡Error! Marcador no definido.**
11. Gestión de incidentes de seguridad en la información. **¡Error! Marcador no definido.**
12. Aspectos de la seguridad de la información de la gestión de la continuidad del negocio
¡Error! Marcador no definido.
13. Cumplimiento **¡Error! Marcador no definido.**

DEFINICIONES Y TÉRMINOS 74



INTRODUCCIÓN.

Basados en el marco de referencia las políticas de TI son directrices u orientaciones que debe generar la Oficina de Tecnologías de la Información, con el propósito de establecer pautas para lograr los objetivos propuestos en la Estrategia de TI.

En este sentido se define una política en el marco de la Estrategia Nacional de Gobierno Digital, cuyo alcance sea el grupo de ámbitos que conforman cada Dominio de la Arquitectura Empresarial, con la siguiente perspectiva.

“POLÍTICA PARA LA IMPLEMENTACIÓN DE GOBIERNO DIGITAL QUE CONTRIBUYA A LA COMUNICACIÓN DIRECTA ENTRE LA UNIDAD PARA LAS VÍCTIMAS Y LAS VÍCTIMAS, LOS DIFERENTES ACTORES SOCIALES Y LAS PARTES INTERESADAS”.

En la Figura No. 1 se observa como la política se descompone en lineamientos, los lineamientos se descomponen en estándares, los estándares se descomponen en procedimientos y los procedimientos se soportan en infraestructura, para su cumplimiento, todo contemplado en el Marco de Referencia de Arquitectura Empresarial. ¹



Por lo anterior el presente documento define las políticas de TI de la Unidad para las Víctimas, empleando marcos de referencia reconocidos como los de MINTIC, ITIL® e ISO 27001 para lograr altos niveles de eficiencia en la producción de información.

http://www.mintic.gov.co/arquitecturati/630/articles-9481_recurso_pdf.pdf

POLÍTICA PARA LA ESTRATEGIA DE TI

VISIÓN GENERAL

Alcanzar un modelo de desarrollo tecnológico altamente efectivo direccionando el diseño, implementación y evolución de una Arquitectura Empresarial alineada con las estrategias y objetivos institucionales, sectoriales y nacionales, basándose en innovación con estándares de calidad, seguridad y mejores prácticas en los servicios tecnológicos hacia los ciudadanos.

PROPÓSITO

El propósito de esta política es proporcionar las directrices para usar la tecnología como agente de transformación desde el entendimiento de la misión, las metas y los objetivos de la UARIV, con el fin de generar un significativo valor público y unos servicios de alta calidad para atender a las víctimas, este propósito se logra mediante el entendimiento claro de la situación presente de la unidad, el direccionamiento de las iniciativas, la gestión de proyectos de TI, su monitoreo y seguimiento.

ALCANCE

Tiene como cobertura el cumplimiento a toda la normatividad definida en leyes y decretos del Gobierno Nacional en relación con tecnología, y a todos los objetivos, lineamientos y directrices estratégicas definidos por el Sector de la Inclusión y la UARIV.

POLÍTICA

Objetivos:

- ✓ Servir a los ciudadanos y las instituciones de manera objetiva y transparente
- ✓ Promover el reconocimiento real de las TIC como componente integral de las estrategias institucionales de la UARIV
- ✓ Apoyar las metas estratégicas de la UARIV definiendo iniciativas direccionadas a cumplir con los objetivos estratégicos
- ✓ Mantener alineación con los objetivos estratégicos del Sector de la Inclusión y con las políticas públicas definidas por el Gobierno Nacional en materia de Tecnología



- ✓ Velar por la transformación e innovación, en búsqueda de mejorar cada día los servicios a los ciudadanos en general y a las víctimas en particular
- ✓ Procurar la Interoperabilidad e integración con las entidades usuarias de la información de la entidad
- ✓ Impulsar las comunicaciones del avance tecnológico de la entidad en relación con servicios a los ciudadanos, transformación e innovación y arquitectura empresarial.

CUMPLIMIENTO DE LA POLÍTICA

La Oficina de Tecnologías de la Información verificará el cumplimiento de esta política a través de métodos que incluyen lineamientos, estándares, métricas e indicadores a nivel interno y externo de la organización.

EXCEPCIONES

No existen excepciones para esta política.

ESTÁNDARES, POLÍTICAS Y PROCESOS RELACIONADOS

- Marco de Referencia de Arquitectura Empresarial del MINTIC
- Política de Gobierno Digital
- Decreto 1008 de Junio de 2018 mediante el cual se debe dar cumplimiento a la Política e Gobierno Digital
- Modelo de Planeación Nacional del DNP
- Objetivos Estratégicos del Sector de la Inclusión
- Objetivos Estratégicos de la UARIV
- Modelo Integrado de Planeación y Gestión de la UARIV

POLÍTICA PARA GOBIERNO DE TI

VISIÓN GENERAL

Lograr con éxito y de manera permanente el uso eficiente y controlado de los recursos financieros, humanos y técnicos utilizados en la ejecución de planes y proyectos de tecnología, para cumplir los objetivos estratégicos de la UARIV.

PROPÓSITO

Asegurar el cumplimiento de la regulación y las políticas de TI por parte de los servidores públicos de la institución, la alineación con el modelo integrado de gestión, los procesos y los esquemas de gobernabilidad, bajo los cuales pueda monitorear, evaluar y redirigir las TI, mediante la gestión, seguimiento y evaluación de proyectos.

ALCANCE

Tiene como cobertura todos los recursos humanos, financieros, tecnológicos y procedimentales disponibles en la UARIV, así como también todos los procesos organizacionales y los modelos de gestión institucionales implementados en la entidad.

POLÍTICA

Objetivos:

- ✓ Velar por que los recursos tecnológicos de información y comunicación sean utilizados en forma responsable y apropiada.
- ✓ Garantizar que el desarrollo y mantenimiento de aplicaciones se realiza acorde con un modelo integral de información institucional
- ✓ Asegurar que la adquisición de tecnología está acorde con las necesidades de la UARIV aprovechando al máximo las capacidades de los funcionarios y el presupuesto asignado para esta materia.
- ✓ Aprobar la coordinación, ejecución y supervisión de los proyectos de tecnología de información a nivel institucional.
- ✓ Asegurar que en todas en todas las Direcciones y Subdirecciones de la UARIV se cumplan las directrices y lineamientos para la ejecución y control de los proyectos con componentes de tecnología
- ✓ Promover la socialización de los documentos de políticas y normas relativos a tecnología de información, para se apliquen los principios consignados en ellos.
- ✓ Asegurar que se definan y ejecuten apropiadamente los presupuestos que se le asignen en materia de tecnología de información.
- ✓ Asegurar que los proyectos de tecnología se ejecutan bajo una metodología de proyectos definida para la UARIV



- ✓ Asegurar el cumplimiento de las metas y productos mediante el uso de indicadores

CUMPLIMIENTO DE LA POLÍTICA

La Oficina de Tecnologías de la Información verificará el cumplimiento de esta política a través de métodos que incluyen lineamientos, estándares, métricas e indicadores a nivel interno y externo de la organización.

EXCEPCIONES

No existen excepciones para esta política.

ESTÁNDARES, POLÍTICAS Y PROCESOS RELACIONADOS

- Marco de Referencia de Arquitectura Empresarial del MINTIC
- Política de Gobierno Digital
- Decreto 1008 de Junio de 2018 mediante el cual se debe dar cumplimiento a la Política e Gobierno Digital
- Modelo Integrado de Planeación y Gestión de la UARIV
- Sistema Integrado de Gestión
- Modelo de Gestión Riesgos de la UARIV
- Sistema de Gestión de Seguridad de la Información

POLÍTICA GENERAL DE USO y APROPIACION

VISIÓN GENERAL

Como parte de la Arquitectura de TI, se requieren lineamientos que faciliten a los funcionarios y partes interesadas de los servicios de la UARIV utilizar la tecnología como motor de desarrollo.

PROPÓSITO

El uso y apropiación de tecnología propende por una utilización adecuada de los servicios de TI ofrecidos por la UARIV, con el ánimo de alcanzar la mayor cantidad posible de sus partes interesadas, iniciando desde sus funcionarios y contratistas, mediante jornadas de sensibilización, capacitación, prácticas, recursos digitales, interacción con expertos y en general, con una amplia movilización hacia la transformación digital.

POLÍTICA

Con el fin de crear una cultura de buen uso y apropiación de la tecnología en los usuarios de las herramientas suministradas por la UARIV, se hace necesario establecer y adoptar las siguientes directrices:

1. Garantizar el acceso a las diferentes herramientas tecnológicas proporcionadas por la Unidad, según el rol que desempeña cada uno de los funcionarios y contratistas.
2. Diseñar y ejecutar planes de capacitación adaptados a las necesidades de cada rol dentro de la Unidad a nivel nacional.
3. Adoptar estándares internacionales de seguridad de la información en todos los sistemas que usan funcionarios y contratistas para la ejecución de sus actividades, en concordancia con las Políticas de Seguridad de la Información de la entidad.
4. Programar jornadas de sensibilización, realizar la publicación de recursos digitales, y, en general, las acciones necesarias para que la mayoría de los funcionarios y contratistas hagan parte del proceso de desarrollo de la Arquitectura TI.

Estos lineamientos y acciones estratégicas se concretan mediante la implementación de las siguientes actividades y de un sistema de evaluación periódica que permita la detección de oportunidades de mejora continua:

1. Identificación periódica de necesidades de entrenamiento, reentrenamiento y sensibilización.
2. Priorización de las necesidades por roles o grupos de trabajo.



3. Definición del proceso de entrenamiento en tecnologías.
4. Ejecución del programa de entrenamiento.
5. Verificación del cumplimiento del programa de entrenamiento establecido.
6. Publicación de recursos digitales que permitan el constante entrenamiento.

CUMPLIMIENTO DE LA POLÍTICA

La Oficina de Tecnologías de la Información verificará el cumplimiento de esta política a través de métodos que incluyen métricas e indicadores.

EXCEPCIONES

No existen excepciones para esta política.

ESTÁNDARES, POLÍTICAS Y PROCESOS RELACIONADOS

- Política de Gobierno Digital antes Gobierno en Línea – Arquitectura TI Colombia.
- Ley anti-trámites establecida mediante el Decreto 19 de 2012 en su artículo 18.
- Estrategia de Gobierno en línea 2012-2015 - Componente de transformación.



POLÍTICA GENERAL DE INTEROPERABILIDAD Y COLABORACIÓN

VISIÓN GENERAL

Los procesos de la Entidad comparten datos y posibilitan el intercambio de información entre ellos, con otras entidades y con la población Víctima.

PROPÓSITO

El propósito de esta política es mejorar la eficiencia en los procesos, lograr agilidad y calidad en los servicios, aumentar la transparencia, promover el acceso abierto a la información y proporcionar la información de valor agregado, obtenida cuando se reúnen datos procedentes de diferentes sistemas.

ALCANCE

Los Sistemas de Información Internos, el intercambio de información entre los procesos y los sistemas de información de las entidades del Sector de la Inclusión Social y la Reconciliación encabezado por el Departamento Administrativo para la Prosperidad Social (DPS) y el despliegue de servicios externos y en línea para la población Víctima.

POLÍTICA

La Unidad para las Víctimas realiza sus actividades soportándose en sistemas de información que facilitan la misión de la entidad utilizando servicios de información estandarizados y fuentes de datos únicas, para ello adopta los principios, políticas, estándares y recomendaciones establecidos por la cabeza del sector en el marco de Interoperabilidad para Gobierno en Línea.

Igualmente, el equipo humano, los responsables y líderes de interoperabilidad en cada entidad tienen el compromiso e interés para llevar a cabo las tareas que se determinen para facilitar el intercambio de información, en procura de prestar mejores servicios a la población Víctima.

CUMPLIMIENTO DE LA POLÍTICA

La Oficina de Tecnologías de la Información verificará el cumplimiento de esta política a través de métodos que incluyen lineamientos, estándares, métricas e indicadores a nivel interno y externo de la organización.

EXCEPCIONES

No existen excepciones para esta política.

ESTÁNDARES, POLÍTICAS Y PROCESOS RELACIONADOS

- Marco de interoperabilidad para Gobierno en Línea
- Estrategia de Gobierno en Línea y el Plan Vive Digital



- Ley anti-trámites establecida mediante el Decreto 19 de 2012 en su artículo 18.
- Estrategia de Gobierno en línea 2012-2015 - Componente de transformación.
- Decreto 2693 de 2012

POLÍTICA GENERAL DE GOBIERNO DEL DATO

VISIÓN GENERAL

La Oficina de Tecnologías de la Información atendiendo las directrices del ente rector promueve el desarrollo de un modelo de gobernabilidad de datos que permita permear los diferentes procesos de gobierno que se lleven a cabo en la Unidad.

PROPÓSITO

El propósito de esta política es fijar las bases del Gobierno y la Organización para orientar las estrategias, métodos y métricas estableciendo un modelo de gobierno de datos que permita alinear las políticas de TI a cada uno de los procesos de negocio de la Unidad y los que defina la Red Nacional de Información.

ALCANCE

Esta política aplica para todas las áreas de negocio de la Unidad para las Víctimas y sus respectivos procesos, ya sean estratégicos, misionales, apoyo y seguimiento y control. De igual forma contemplará la línea que defina la Red Nacional de Información para el gobierno de dato proveniente de fuentes externas.

POLÍTICA

Los datos que ofrece la Unidad para las Víctimas son el resultado del manejo adecuado en términos de administración de calidad de datos, administración de meta data, integración de datos armonizando los elementos que componen el Sistema Integrado de Gestión de Calidad.

CUMPLIMIENTO DE LA POLÍTICA

La Oficina de Tecnologías de la Información verificará el cumplimiento de esta política a través de métodos que incluyen lineamientos, estándares, métricas e indicadores a nivel interno y externo de la organización.

EXCEPCIONES

No existen excepciones para esta política.

ESTÁNDARES, POLÍTICAS Y PROCESOS RELACIONADOS

- Lineamiento de Integración de Datos.

- Lineamiento de Administración de Metadata.
- Lineamiento de acceso a los datos.
- Estándar de Integración de Datos.
- Estándar de Administración de Metadata.
- Estándar de nombramiento de objetos Base de Datos

POLÍTICA GENERAL DE CALIDAD DE DATOS E INFORMACIÓN

VISIÓN GENERAL

Los datos en la Unidad para las víctimas se consideran como un activo estratégico primordial y su valor es la base fundamental para la toma de decisiones estratégicas, tácticas y operativas. La mejora en la calidad de los datos soporta y facilita la continuidad y mejora en los procesos de prevención, atención y reparación orientados a la población Víctima, entidades del Sistema y entidades de control.

PROPÓSITO

El propósito de esta política es fijar las bases del Gobierno y la Organización para mantener datos consistentes, reales, seguros y confiables para todas las áreas de negocio dando cumplimiento a los lineamientos, normativas y procedimientos establecidos para tal fin, fomentando la transparencia, la probidad, el buen gobierno y la eficiencia administrativa.

ALCANCE

Esta política aplica para todas las áreas de negocio de la Unidad para las Víctimas que administren o manejen datos, ya sean estructurados o no estructurados.

POLÍTICA

La Unidad para las Víctimas a través de la Oficina de Tecnologías de la Información cuenta con estrategias de datos, estándares, procedimientos y métricas que permiten ofrecer información consistente, real y oportuna aplicando buenas prácticas que permiten mejorar la calidad del dato de manera permanente.

CUMPLIMIENTO DE LA POLÍTICA

La Oficina de Tecnologías de la Información verificará el cumplimiento de esta política a través de métodos que incluyen lineamientos, estándares, métricas e indicadores debidamente establecidos.

EXCEPCIONES

No existen excepciones para esta política.

NO CUMPLIMIENTO

Las herramientas asociadas a esta política que no cumplan no serán desplegadas en los ambientes productivos de la Unidad

ESTÁNDARES, POLÍTICAS Y PROCESOS RELACIONADOS

- Lineamiento de unicidad del dato.
- Lineamiento acceso de datos.
- Lineamiento de propiedad del dato.
- Lineamiento de privacidad del dato.
- Lineamiento de caracterización del dato.
- Lineamiento de administración de Meta data.

POLÍTICA GENERAL DE DESARROLLO Y MANTENIMIENTO DE SOFTWARE

VISIÓN GENERAL:

En el desarrollo de nuevos sistemas de información se deben considerar los lineamientos, estándares y buenas prácticas establecidas en de la Oficina de Tecnologías al igual que las mejoras o mantenimientos que se realicen sobre sistemas nuevos y legados aplicados por la Unidad.

PROPÓSITO:

El propósito de esta política es controlar todo el ciclo de vida del desarrollo de software garantizando la puesta en funcionamiento de los Sistemas de Información internos y externos.

ALCANCE:

Esta política aplica a todos los sistemas y servicios de información desarrollados y/o actualizados en la Unidad de Víctimas. También aplica a los funcionarios, contratistas, consultores y personal de terceros que presten el servicio a la Unidad de Víctimas.

POLITICAS.

Generales:

- Los derechos de autor de todo Proyecto de desarrollo que se construya total o parcial dentro de la Unidad de Víctimas, y su correspondiente documentación pertenecen a la Unidad de Víctimas.



- Todo Sistema de Información deberá ser registrado por el líder técnico del proyecto en el inventario de sistemas de información que la Oficina Estableció para para tal fin; el Enlace encargado del mantenimiento del inventario de sistemas deberá asegurar y verificar la veracidad de la información
- Todo Sistema de Información que se desarrolle en la Unidad de Víctimas deberá atender al Manual de Estándares para el Desarrollo de Sistemas de Información y a cualquier normatividad aplicable que sea emitida por la Oficina de tecnologías.
- Cualquier Sistema de Información deberá ser desarrollado atendiendo a los estándares para el desarrollo de sistemas, arquitecturas, políticas de seguridad y otros instrumentos normativos emita la oficina de Tecnologías de la Información.

De Arquitectura:

- Todos los sistemas de información deben estar alineados a la Arquitectura empresarial propuesta por Mintic en el manual de IT4+ y atender las necesidades de negocio de la Unidad de Atención a las víctimas.
- Los sistemas de Información contruidos dentro de la unidad de víctimas deben atender y responder a una arquitectura orientada a servicios, estos servicios deben atender a un servicio de negocio de la cadena de valor de la Entidad.
- Se debe garantizar la independencia de la plataforma en la construcción de servicios alineados a la arquitectura de sistemas de información, esto quiere decir que se debe garantizar la interoperabilidad y el intercambio de información dentro y fuera de la Entidad.
- La construcción de sistemas de información debe atender requerimientos no funcionales y atender atributos de calidad tales como Usabilidad, mantenibilidad, escalabilidad.
- Todo servicio construido deberá ser registrado por el líder técnico del proyecto en el catálogo de servicios que la Oficina Estableció para para tal fin; el Enlace encargado del mantenimiento del Catálogo de servicios deberá asegurar y verificar la veracidad de la información.

De calidad del Software:

- Elaborar y ejecutar el procedimiento de calidad para verificar que el Sistema de información y la documentación del Proyecto de desarrollo, atiendan a los acuerdos establecidos por el equipo de coordinación y a las especificaciones documentadas por el Administrador del proyecto;
- Diseñar y ejecutar las pruebas conforme al procedimiento de calidad desarrollado emitiendo las recomendaciones que considere convenientes;
- Documentar y acordar las adecuaciones que considere pertinentes con el Grupo de coordinación

Control de Versiones:

- Toda la documentación, archivos ejecutables, códigos fuente y librerías de software de los sistemas construidos, script de bases de datos, así como la documentación de paquetes de software adquiridos, debe estar bajo procedimientos de control de cambios y de versionamiento.

Seguridad de los Sistemas de Información

- Es necesario implementar controles y registros de auditoría, verificando:
 - La validación de datos de entrada.
 - El procesamiento interno.
 - La autenticación de mensajes (interfaces entre sistemas)
 - La validación de datos de salida.
- Todas las claves serán protegidas contra modificación y destrucción, y serán protegidas contra copia o divulgación no autorizada mediante almacenamiento cifrado en las bases de datos.

Desarrollo Externo.

- Para el caso que se considere la tercerización del desarrollo de software, se establecerán normas:
 - Acuerdos de licencias, propiedad de código y derechos de Propiedad Intelectual
 - Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías

- Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecido.
- Independencia del proveedor: Toda herramienta informática construida a la medida por algún proveedor o que soporte algún proceso de la Unidad de Víctimas, debe estar bajo un control total de la Oficina de Tecnologías de la Información.

CUMPLIMIENTO DE LA POLÍTICA

El cumplimiento de la Política es de obligatoriedad para los equipos que realicen tareas de desarrollo y mantenimiento de aplicaciones al interior de la Unidad o aplicaciones proveídas o desarrolladas por terceros.

EXCEPCIONES

Las excepciones a cualquier cumplimiento de la política de desarrollo de software deben ser formalmente documentadas, revisadas y aprobadas por la Oficina de Tecnologías de la Información.

NO CUMPLIMIENTO

Las soluciones que no cumplan esta política no serán desplegadas en los ambientes productivos de la Unidad.

ESTÁNDARES, POLÍTICAS Y PROCESOS RELACIONADOS

Relaciona los estándares, políticas y procesos que están relacionados con la presente política.

- Política general de seguridad de la información.
- Procedimiento de desarrollo de nuevos sistemas de información y/o funcionalidades en sistemas existentes.
- Formato de análisis, planeación y diseño de requerimiento de software.
- Estándares y reglas que se deriven de las estrategias de mejoramiento de los procesos de la Unidad.

POLÍTICA GENERAL DE CALIDAD DE SOFTWARE

VISIÓN GENERAL:

Las actividades planificadas en el Aseguramiento de la Calidad del Software son necesarias para garantizar que el software cumple con los requisitos funcionales y no funcionales que aseguran su correcto funcionamiento y verifican atributos de calidad a lo largo de todas las etapas del ciclo de vida del desarrollo de software.

PROPÓSITO:

El propósito de esta política es asegurar controles sobre las entradas al proceso de desarrollo para que sean completas, útiles en el proceso de diseño y sin ambigüedades, asegurando que el desarrollo cumple con los estándares de la Organización y el resultado cumple con los criterios y aceptación del cliente.

ALCANCE:

Esta política aplica a todos los desarrollos en la Unidad de Víctimas. También aplica a los funcionarios, contratistas, consultores y personal de terceros que presten el servicio a la Unidad de Víctimas.

POLÍTICA

La Unidad para las Víctimas adopta mecanismos de mejora continua en los procesos de desarrollo de software realizando medición, análisis y aseguramiento de la calidad de los productos entregados a fin de cumplir con las expectativas del cliente y realiza controles y pruebas en cada una de la fase del ciclo de desarrollo.

CUMPLIMIENTO DE LA POLÍTICA

El cumplimiento de la Política es de obligatoriedad para todos los desarrollos de aplicaciones al interior de la Unidad o aplicaciones proveídas o desarrolladas por terceros.

EXCEPCIONES

Las excepciones a cualquier cumplimiento de Política de desarrollo de software deben ser formalmente documentadas, revisadas y aprobadas por la Oficina de Tecnologías de la Información.

NO CUMPLIMIENTO

Las soluciones que no cumplan esta política no serán desplegadas en los ambientes productivos de la Unidad.

ESTÁNDARES, POLÍTICAS Y PROCESOS RELACIONADOS

- ISO 9001 – 2015¹: La norma ISO 9001 ayuda a las organizaciones para que puedan ofrecer productos y servicios de calidad. Así mismo, se ha convertido en una herramienta de gran utilidad para optimizar sus procesos y hacerlos más eficientes, con el principal objetivo de satisfacer a sus clientes.



La versión 2015 trae importantes cambios como el preponderante lugar que se le otorga a la gestión del riesgo y la utilización del ciclo Planificar-Hacer-Verificar-Actuar en todos los niveles de la organización. De igual manera, la norma ISO 9001:2015 está diseñada de tal manera que se puede integrar fácilmente con otros sistemas de gestión.

- ISO/IEC 25000²: proporciona una guía para el uso de las nuevas series de estándares internacionales, llamados Requisitos y Evaluación de Calidad de Productos de Software (SQuaRE). Constituyen una serie de normas basadas en la ISO 9126 y en la ISO 14598, y su objetivo principal es guiar el desarrollo de los productos de software con la especificación y evaluación de requisitos de calidad.
- ISO/IEC 12207:2008³: Establece un marco común para los procesos de ciclo de vida de software, con terminologías bien definidas. Contiene los procesos, actividades y tareas que se aplican durante la adquisición de un producto de software o servicios y el desarrollo, operación, mantenimiento.

² http://www.iso.org/iso/catalogue_detail.htm.

³ http://www.iso.org/iso/catalogue_detail.htm.

POLÍTICA PARA SERVICIOS TECNOLOGICOS

VISIÓN GENERAL

Gestionar con mayor eficacia y transparencia la infraestructura tecnológica que soporta los sistemas y servicios de información en las instituciones.

PROPÓSITO

Apoyar a la OTI en la gestión de la infraestructura tecnológica que se requiere para soportar los procesos, servicios y sistemas de información de la Unidad, así como establecer, implementar y gestionar los procesos de soporte, mantenimiento y monitoreo para lograr los niveles requeridos de seguridad y trazabilidad.

ALCANCE

Tiene como cobertura dar cubrimiento a todos los recursos, servicios y productos tecnológicos de la Unidad, utilizados en todas las dependencias a nivel nacional de la entidad.

POLÍTICA

1. DOTACION TECNOLOGICA (EQUIPOS, IMPRESORAS, ESCANER Y OTROS ELEMNTOS TECNOLOGICOS)

RESPONSABILIDADES DE LA OFICINA DE TECNOLOGIA

- La OTI debe velar y llevar inventario de la infraestructura tecnológica que la oficina provee a la UNIDAD, acorde con las necesidades existentes de la misma.
- La OTI debe determinar la vida útil de los equipos tecnológicos, con el fin de brindar un servicio óptimo a los funcionarios y contratistas de la UNIDAD.
- La OTI debe participar en los contratos de adquisición de bienes y/o servicios, donde se incluyan equipos o componentes tecnológicos.
- La OTI debe Emitir avales técnicos en los contratos que adquiera la UNIDAD, de bienes y servicios contengan componentes de TI.
- La OTI debe confirmar que los elementos tecnológicos adquiridos por diferentes áreas de la UNIDAD cumplen con las especificaciones técnicas, de lo contrario solicitar la devolución de estos.
- La OTI debe realizar mantenimiento preventivo y correctivo de los equipos tecnológicos.
- La OTI debe verificar que los elementos tecnológicos cuenten con disponibilidad de puntos eléctricos, datos y el área física adecuada para la instalación.
- La OTI debe ser la única responsable del traslado y/o movimiento de los elementos tecnológicos dentro de las áreas y entre las diferentes sedes de la UNIDAD.

- La OTI debe solicitar al grupo de Grupo de Gestión Administrativa y Documental la infraestructura y disponibilidad eléctrica de las sedes, previamente a la instalación de los elementos tecnológicos.
- La OTI debe llevar inventario de los programas informáticos instalados en los equipos.
- La OTI debe avalar la instalación de los programas informáticos solicitados para instalación.
- La OTI debe informar a los usuarios sobre el uso y manejo adecuado de los equipos y programas informáticos instalados.
- La OTI debe autorizar el acceso a la red de dominio.

RESPONSABILIDADES DE LOS FUNCIONARIOS Y CONTRATISTAS

- El USUARIO debe utilizar los equipos asignados solo para las tareas o actividades relacionadas con la UNIDAD.
- El USUARIO no debe efectuar solicitudes de reparación de equipos personales a la oficina de tecnología.
- El USUARIO debe solicitar los elementos tecnológicos a las oficinas de tecnologías, según las funciones asignadas.
- El USUARIO debe cumplir con el procedimiento de gestión de solicitudes de la oficina de tecnologías.
- El USUARIO debe informar a la oficina de tecnologías los ingresos, retiros y traslados del personal para realizar la asignación de elementos tecnológicos y cuentas de usuario.

2. SOFTWARE Y HERRAMIENTAS COLABORATIVAS

➤ RESPONSABILIDADES DE LA OFICINA DE TECNOLOGIA

- La OTI debe llevar inventario de los aplicativos instalados en las diferentes áreas de la UNIDAD.
- La OTI debe velar la legalidad del licenciamiento de todos los aplicativos instalados en la UNIDAD.
- La OTI debe tener la custodia de los aplicativos de la UNIDAD.
- La OTI debe proveer software de informática y de almacenamiento en la nube a los funcionarios y contratista de la UNIDAD, para asegurar el correcto almacenamiento de la información.
- La OTI debe instalar agentes de monitoreo y antivirus, para proteger los equipos de amenazas.
- La OTI debe restringir el acceso a sitios web no autorizados por la UNIDAD.
- La OTI debe velar por el respaldo de la información.
- La OTI debe proveer guías de uso de las herramientas colaborativas.

➤ RESPONSABILIDADES DE LOS FUNCIONARIOS Y CONTRATISTAS

- El USUARIO debe almacenar la información en los espacios proveídos por la oficina de tecnologías (servidores de archivo. OneDrive).
- El USUARIO debe asegurar la información crítica y sensible de la UNIDAD en los espacios de almacenamiento.
- El USUARIO no debe desinstalar el antivirus y los agentes de monitoreo de equipos, ya que es de alto riesgo para la seguridad ante el peligro de los virus.
- El USUARIO debe informar a la oficina de tecnologías en caso de presentarse cualquier problema de amenazas en su equipo.

3. SOPORTE TECNICO A LA INFRAESTRUCTURA TECNOLOGICA

➤ RESPONSABILIDADES DE LA OFICINA DE TECNOLOGIA

- Todas las solicitudes de Soporte Técnico deberán ser recibidos a la mesa de servicio por vía telefónica al #5, correo electrónico soporte.oti@unidadvictimas.gov.co o al portal web <http://mesadeservicios.unidadvictimas.gov.co/usdkv8/#/login/>, quien le dará las instrucciones necesarias a los niveles que corresponda el servicio.
- La mesa de servicios debe realizar el diagnostico de primer nivel y escalar según la criticidad del caso.
- La OTI debe definir los tiempos de respuesta a cada uno de los servicios y notificar a los usuarios cuando realicen una solicitud.
- La OTI debe asegurar la satisfacción del usuario a través de la encuesta de satisfacción.
- La OTI debe recibir e instalar los equipos tecnológicos solicitados por las diferentes áreas de la UNIDAD, así mismo debe formalizar a través de acta la instalación y entrega de los elementos tecnológicos.
- La OTI debe dar soporte técnico únicamente a los elementos tecnológicos de la UNIDAD.
- La OTI debe velar por el estado de los equipos, para asegurar el óptimo funcionamiento de estos.

➤ RESPONSABILIDADES DE LOS FUNCIONARIOS Y CONTRATISTAS

- El USUARIO debe realizar las solicitudes de soporte técnico a través de vía telefónica al #5, correo electrónico soporte.oti@unidadvictimas.gov.co o al portal web <http://mesadeservicios.unidadvictimas.gov.co/usdkv8/#/login/>.
- El USUARIO debe tener disponibilidad de tiempo para atender al técnico que dará solución a su solicitud.

- El USUARIO debe responder la encuesta de satisfacción recibida por correo electrónico con la solución del caso. Con el fin de medir y mejorar la calidad del servicio.
- El USUARIO no deben manipular, ni cambiar y/o extraer partes de los elementos tecnológicos.

4. CENTROS DE CABLEADO

➤ RESPONSABILIDADES DE LA OFICINA DE TECNOLOGIA

- La OTI debe restringir el acceso a personal no autorizado a los centros de cableado.
- La OTI debe Mantener en condiciones físicas adecuadas para el funcionamiento de los equipos.

➤ RESPONSABILIDADES DE LOS FUNCIONARIOS Y CONTRATISTAS

- El USUARIO debe reportar el mal estado de los equipos tecnológicos.
- El USUARIO No debe ingresar a los centros de cableado sin autorización de la Oficina de tecnología.
- El USUARIO No debe ingresar elementos que no sean de componente tecnológico a los centros de cableado.

CUMPLIMIENTO DE LA POLÍTICA

La Oficina de Tecnologías de la Información verificará el cumplimiento de esta política a través de métodos que incluyen lineamientos, estándares, métricas e indicadores a nivel interno y externo de la organización.

EXCEPCIONES

No existen excepciones para esta política.

ESTÁNDARES, POLÍTICAS Y PROCESOS RELACIONADOS

- Marco de Referencia de Arquitectura Empresarial del MINTIC
- Acuerdo Marco de Precios
- Decreto 1008 de Junio de 2018 mediante el cual se debe dar cumplimiento a la Política e Gobierno Digital
- Modelo de Planeación Nacional del DNP
- Objetivos Estratégicos del Sector de la Inclusión
- Objetivos Estratégicos de la UARIV
- Modelo Integrado de Planeación y Gestión de la UARIV

SEGURIDAD DE LA INFORMACIÓN

VISIÓN GENERAL

Las políticas de seguridad de la información establecidas e incluidas en este documento son un componente fundamental para la gestión en seguridad de la información de la UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS y se convierten en la base para la implantación de los controles, los procedimientos y los estándares de seguridad.

Las políticas de seguridad de la información deberán ser conocidas y cumplidas por todos los funcionarios, contratistas y partes interesadas de la UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS. El incumplimiento de las mismas se considerará un incidente de seguridad, que de acuerdo con el caso podrá dar lugar a un proceso disciplinario para los funcionarios y se convertirá en una causa válida de terminación del contrato con los contratistas, sin perjuicio de la iniciación de otro tipo de acciones a las que haya lugar. Para reportar un evento sospechoso o un incidente de seguridad, por favor póngase en contacto con el delegado de la Dirección General para tal fin, en los canales de comunicación que se destine para tal fin.

ALCANCE

Este documento define las Políticas de Seguridad de la Información que deben ser cumplidos por funcionarios, contratistas y terceros, que:

- Accedan a información de la UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS o de las Víctimas.
- Usen equipos informáticos y de telecomunicaciones conectados a la infraestructura de la Entidad.
- Diseñen, construyan, prueben y/o usen herramientas tecnológicas y/o servicios informáticos de la Entidad.
- Ingresen de manera física o lógica a las instalaciones de la Entidad.

VIGENCIA Y ACTUALIZACIÓN DE POLÍTICAS

Estas Políticas se encuentran vigentes a partir de la fecha en la que se publica la primera versión de este documento y se entiende incorporado a las obligaciones de los funcionarios y a los contratos que la UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS celebre con contratistas.

La Política de Seguridad de la Información seguirá un proceso de actualización permanente, de acuerdo con los cambios organizacionales (culturales, estructurales, operativos), del entorno, tecnológicos y las normas que se expidan al respecto.

La definición, actualización y mantenimiento de esta Política, es responsabilidad de la Oficina de Tecnologías de la Información en el marco del Subsistema de Gestión de Seguridad de la Información del Sistema Integrado de Gestión.

Este documento se actualizará cuando se presenten cambios importantes en la Entidad. En las revisiones se tendrán en cuenta factores como: incidentes de seguridad, nuevas vulnerabilidades detectadas, cambios dentro de la infraestructura organizacional o tecnológica, cambios en los procesos, en los objetivos de la Entidad, entre otros.

La Oficina de Tecnología de la Información es la dependencia que gestiona y brinda apoyo técnico en materia de Seguridad Informática y de Telecomunicaciones a las dependencias de la entidad.

Cualquier excepción a lo establecido en esta política, deberá contar con la aprobación formal del Comité Institucional de Gestión y Desempeño.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

- 1. Organización de la seguridad de la información**
- 1.1. Organización interna**
- 1.1.1. Contacto con autoridades y grupos de interés especial**

La Oficina de Tecnologías de la Información en Articulación con la Oficina Asesora de Comunicación tiene las siguientes responsabilidades relacionadas al contacto con autoridades:

- Generar y mantener actualizado el listado de contactos, autoridades y grupos de interés de seguridad de la información, para poder gestionar eficientemente las diferentes actividades de

seguridad de la información. Dentro de los contactos actualizados se deben tener mínimo COLCERT (Grupo de respuesta a Emergencias cibernéticas en Colombia), CCP (Centro Cibernético Policial), MinTIC (Ministerio de Tecnologías de la Información y las Comunicaciones) y el DPS

- Documentar los contactos con autoridades y grupos de interés para atender casos que afecten la disponibilidad, confidencialidad e integridad de los activos de información de interés nacional o sectorial, dicho listado debe ser administrado por la Oficina de Tecnologías de la Información.

1.1.2. Seguridad de la información en la gestión de proyectos

Identificar riesgos que impacten la información en los proyectos que involucren cualquier tipo de manejo de la información de la población Víctima, los cuales deben ser evaluados por la Oficina de Tecnologías de la Información.

Definir y tomar las acciones para mitigar los riesgos que impacten la información en los proyectos que involucren cualquier tipo de manejo de la información de la población Víctima, los cuales deben ser evaluados por la Oficina de Tecnologías de la Información.

Lineamientos:

- a) Identificar y valorar riesgos de los estudios previos de contratación.
- b) Identificar controles de seguridad de la información durante la construcción de estudios previos para contratación, orientados a la definición de la propiedad de la información y el aseguramiento en términos de confidencialidad, integridad y disponibilidad.
- c) Los sistemas de información y servicios adquiridos a través de terceras partes deben cumplir con las políticas y lineamientos definidos para el desarrollo de software por la Oficina de Tecnologías de la Información.
- d) Establecer durante el contrato con terceros un acuerdo de confidencialidad para asegurar la confidencialidad, integridad y disponibilidad de la información el cual tiene una vigencia desde su firma con una extensión posterior a la finalización de dicho contrato.

- e) Identificar los requerimientos no funcionales relacionados con el aseguramiento de la información, para proyectos de desarrollo o adquisición de software.
- f) Identificar los proyectos tecnológicos que involucren información confidencial para incorporar controles de seguridad en las diferentes fases del proyecto.

1.2. Dispositivos Móviles y Teletrabajo

Es responsabilidad de los usuarios usar las herramientas dispuestas por la Oficina de Tecnologías de la Información para el manejo de información fuera de las instalaciones de la Entidad, las cuales cuentan con controles que se establecen en el Sistema de Gestión de Seguridad de la Información para la protección de los datos de la Entidad almacenados o consultados en dispositivos móviles o equipos de cómputo personales.

Divulgar las recomendaciones sobre el uso de servicios informáticos en lugares públicos o ubicaciones diferentes a las instalaciones de la Entidad, dicha actividad está a cargo de La Oficina de Tecnologías de la Información en articulación con la oficina Asesora de comunicación.

Lineamientos:

- a) Los usuarios deben reportar pérdida o divulgación de información de la Entidad a la Mesa de Servicios Tecnológicos de la Unidad, por medio de los siguientes canales autorizados:
 - Correo: soporte.oti@unidadVictimas.gov.co
 - Marcando el 5 desde las instalaciones de la Entidad
 - Celular: 321 496 7149 (Mesa de servicios tecnológicos)
 - Teléfono fijo: 437 9487 (Mesa de servicios tecnológicos)
- b) Los usuarios autorizados para manejar información sensible de la Entidad fuera de las instalaciones deben gestionar el cifrado de la data con el grupo de seguridad de la información de la Oficina de Tecnologías de la Información.
- c) Es obligatorio el cumplimiento de los siguientes controles por parte de los usuarios que manejan información de la Entidad en dispositivos móviles o que se hacen parte de la estrategia de Teletrabajo o trabajo remoto:
 - Participar en jornadas de sensibilización en seguridad de la información
 - Configurar credenciales de acceso en los equipos de cómputo o dispositivos de los usuarios (Usuario y contraseñas que cumplan con los requisitos de seguridad).

- Evitar desatender el equipo de cómputo o dispositivo móvil.
 - Evitar conectarse a redes públicas.
 - Actualizar periódicamente las contraseñas.
 - Conocer y aplicar los procedimientos de seguridad de la información.
 - Usar software licenciado.
 - En caso de que los equipos sean provistos por los operadores, este debe garantizar la instalación del antivirus, de acuerdo con las especificaciones técnicas definidas por la Unidad para la Atención y Reparación Integral a las Víctimas. Para los equipos provistos por el usuario, este debe garantizar la instalación y actualización del antivirus.
 - Los usuarios deben usar guaya, para los computadores portátiles.
 - Los usuarios deben realizar copia de respaldo de la información sensible para la Entidad almacenada en los equipos de cómputo, en los mecanismos dispuestos por la Oficina de Tecnologías de la Información, mediante solicitud a la mesa de servicios tecnológicos.
- d) Los usuarios deben usar las herramientas dispuestas por la Oficina de Tecnologías de la Información para el manejo de la información sensible de la Entidad.
- e) Los usuarios deben firmar el acuerdo de confidencialidad de la información, para el acceso y uso de la información clasificada o reservada de la Entidad. Quién administra la información clasificada o reservada, a la cual se requiere acceso, debe validar la firma del acuerdo de confidencialidad por parte del usuario.

2. Seguridad de recursos humanos

La Entidad debe contratar personal idóneo y se debe asegurar que entiendan sus responsabilidades en relación con las políticas y lineamientos de seguridad de la información y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o de los equipos empleados para su tratamiento.

Lineamientos

- a) El grupo de Gestión de Talento Humano debe documentar la verificación de antecedentes, referencias laborales y soportes de experiencia del personal en el proceso de selección para vacantes de planta.
- b) La dependencia responsable del proceso de contratación del personal en el esquema de prestación de servicios debe documentar la verificación de antecedentes, referencias laborales y soportes de experiencia relacionada.



- c) Todos los funcionarios, contratistas y terceros de la Entidad deben reportar por medio de los canales apropiados, cualquier caso de fuga, modificación no autorizada o pérdida de información sensible almacenada en el equipo de cómputo o dispositivo personal. Así como el eventual incumplimiento identificado de políticas, lineamientos y procedimientos de seguridad de la información establecidos.
- d) El funcionario, contratista o colaborador, es responsable de la información que produzca u obtenga, así como de los recursos tecnológicos y de software asignados por la Entidad.
- e) Los funcionarios, contratistas y terceros con relación contractual deben conocer y aplicar las políticas, lineamientos, procedimientos y recomendaciones de seguridad de la información de la Entidad.
- f) Se prohíbe a los usuarios realizar copia no autorizada de información o software (código fuente o archivos compilados) de la Entidad.
- g) No está permitido para ningún usuario realizar actividades tales como borrar, alterar o eliminar información de la Entidad de manera no controlada o sin autorización, de tal forma que se afecte la operación de la Unidad.
- h) Los funcionarios, contratistas y terceros de la Unidad, deben usar los activos de la Entidad, únicamente para el cumplimiento de sus funciones, en el marco de la misión de la Unidad.
- i) Los funcionarios, contratistas y terceros de la Unidad, deben evitar el uso de dispositivos tales como CD, DVD, USB o discos duros portables, para el almacenamiento o transporte de información clasificada o reservada de la Entidad, sin la utilización de controles que eviten la divulgación de información.
- j) Los funcionarios, contratistas y terceros de la Unidad no deben divulgar información considerada como clasificada o reservada en lugares públicos o privados, mediante conversaciones o situaciones que puedan comprometer la seguridad o el buen nombre de la Entidad. Esta restricción se extiende inclusive con posterioridad a la terminación de los contratos.
- k) Los funcionarios, contratistas y terceros de la Unidad deben asistir a los escenarios de sensibilización en seguridad de la información, cuando sea invitado.
- l) Los funcionarios, contratistas y terceros de la Unidad, deben evitar desatender el equipo de cómputo o dispositivo móvil. Adicionalmente deben actualizar periódicamente las contraseñas, usar software licenciado y autorizado por la Oficina de Tecnologías de la Información.



- m) La Oficina de Tecnologías de la Información puede verificar el software instalado en los equipos de cómputo asignados a usuarios de la Entidad. Adicionalmente, esta Oficina puede desinstalar el software no autorizado de los equipos de cómputo asignados a los usuarios.
- n) Es responsabilidad de los usuarios realizar copia de respaldo de la información sensible para la Entidad almacenada en equipos de cómputo o dispositivos móviles, teniendo en cuenta los mecanismos dispuestos por la Oficina de Tecnologías de la Información.
- o) Los funcionarios, contratistas y terceros, durante el proceso de vinculación a la Unidad, deben recibir el manual del sistema de gestión de seguridad de la información.
- p) La Oficina de Tecnologías de la información en articulación con la Oficina asesora de comunicaciones debe realizar la difusión masiva de las políticas y lineamientos y sus correspondientes actualizaciones, así como de las recomendaciones para la protección de la información de la Entidad, con base en el plan de socialización que se genere para tal fin.
- q) La Oficina de Tecnologías de la información puede realizar evaluaciones a los funcionarios y contratistas para medir la apropiación de las políticas, lineamientos y recomendaciones de seguridad de la información.
- r) Los funcionarios, contratistas y terceros de la Unidad, no deben utilizar sus cuentas de correo personal para manejar información de la Entidad.
- s) Los funcionarios, contratistas y terceros de la Unidad, no deben extraer discos duros o cualquier otro componente interno de los equipos de cómputo asignados o de cualquier dispositivo tecnológico dispuesto por la Entidad. Solamente el personal de soporte técnico calificado y autorizado por la Oficina de Tecnologías de la Información puede realizar estos procedimientos.
- t) Dentro de las Instalaciones de la Unidad, se debe portar en un lugar visible el carnet de la Entidad, asignado a cada funcionario, contratista o colaborador.
- u) Todo funcionario, contratista o colaborador debe registrar el ingreso y salida de elementos tecnológicos (solicitados por el personal de seguridad) en las instalaciones de la Entidad.
- v) Para el uso de información de la Unidad en dispositivos personales, por ejemplo, computadores, asistentes digitales (Tablet y Smartphone), el usuario debe aplicar adicionalmente los siguientes controles de seguridad:



- Configurar credenciales de acceso en los equipos de cómputo o dispositivos de los usuarios (Usuario y contraseña).
- Evitar conectarse a redes públicas alámbricas e inalámbricas.
- Instalar antivirus y actualizarlo.
- Usar guaya de seguridad para computadores portátiles.

2.1. Desvinculación o cambio de rol

El jefe directo para el caso de funcionarios o el supervisor del contrato para contratistas o terceros de la Unidad, deben gestionar el proceso de inactivación de los privilegios de acceso sobre los sistemas de información y/o herramientas de la Unidad, toda vez que el personal haya finalizado el vínculo laboral con la Entidad o que cambia de rol no debe continuar con acceso a la información no autorizada.

Lineamientos:

- a) Todo funcionario, contratista o colaborador que se retire de la Unidad o cambie de dependencia debe hacer acta de entrega del cargo la cual debe entregar al jefe de la dependencia o supervisor del contrato, de cualquier activo de información mantenido, usado o producido durante el desarrollo de sus funciones.
- b) Tras la finalización de la vinculación laboral, el jefe del funcionario o el supervisor del contratista o colaborador que se desvincula debe ejecutar el procedimiento desactivación de usuarios de sistemas de información, a través del Formato “Solicitud de inactivación recursos tecnológicos con código 130,13,15-2”. Adicionalmente se debe remover cualquier documentación que lo identifique como un miembro activo de la Entidad.
- c) El jefe del funcionario o el supervisor del contratista o colaborador debe remover todos los derechos de acceso que no fueron aprobados para el traslado, comprendiendo: accesos lógicos y/o físicos, llaves, tarjetas de identificación, suscripciones y demás elementos no requeridos en su nuevo rol.
- d) Cuando el funcionario, contratista o colaborador está en proceso de desvinculación y tiene conocimiento de contraseñas para cuentas de usuario que deban permanecer activas temporalmente, éstas deben ser cambiadas tras la finalización de su vinculación laboral o traslado de dependencia.
- e) Para los cargos que administren información confidencial o con un alto nivel de susceptibilidad a divulgación o modificación no autorizada, el jefe del funcionario o el supervisor del contratista o colaborador debe levantar un acta de entrega del cargo o de las actividades realizadas por el funcionario, contratista o colaborador, donde quede registrado

el estado y ubicación de los activos de información que le fueron asignados para el desarrollo de sus funciones o actividades. El acta debe almacenarse en el expediente del funcionario, contratista o colaborador.

- f) El jefe del funcionario o el supervisor del contratista o colaborador del proceso debe identificar y documentar las credenciales de acceso asignadas a cada uno de los usuarios que cambian de rol o se desvinculan de la Entidad.

3. Gestión de activos

Los procesos de la Entidad deben mantener el inventario de activos actualizado anualmente, donde se identifique el responsable de su generación, administración y/o custodia a nivel de proceso. Este inventario adicionalmente debe clasificar los activos en relación con la confidencialidad y debe permitir evidenciar la criticidad de la información en términos de confidencialidad, integridad y disponibilidad.

Lineamientos

- a) Todos los procesos deben identificar, elaborar y mantener un inventario de activos, en el “Formato de Registro de Activos de información 710,14,15-15”, en el marco del procedimiento de generación del inventario de activos de información.
- b) La información, física, digital, los sistemas de información, los servicios y los equipos, son de propiedad de la Entidad.
- c) Los activos deben ser utilizados de forma ética por los usuarios y en cumplimiento de las leyes y reglamentos vigentes, con el fin de evitar daños o pérdidas sobre la operación o la imagen de la Entidad. Los recursos de la Unidad son proporcionados con el único fin de ejecutar la operación de la Unidad para la Atención y Reparación Integral para las Víctimas. A continuación, se listan los lineamientos detallados para el uso de internet, mensajería interna y correo:
- I. No se permite el acceso a páginas relacionadas con pornografía, drogas, alcohol, música, concursos en la web, juegos y entre otras que no tengan relación con el desempeño de las funciones o actividades de la Entidad.
 - II. No se permite la descarga, uso, intercambio y/o instalación de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables, herramientas de hacking, software malicioso, o que generen un riesgo para la Información de la Entidad.
 - III. La Unidad puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación de cada usuario, desde cualquier puerto y/o protocolo utilizado, como parte de las funciones de administración de la plataforma tecnológica.



- IV. Cada uno de los usuarios será responsable de realizar un uso adecuado del internet y mensajería interna, y en ningún momento podrá ser usado para realizar prácticas ilícitas que atenten contra la Entidad, terceros, legislación vigente, políticas o lineamientos de seguridad de la información.
- V. Los funcionarios, contratistas y terceros, no podrán asumir en nombre de la Unidad posiciones frente a encuestas de opinión, foros u otros medios similares.
- VI. Los funcionarios, contratistas o terceros que hagan parte de redes sociales virtuales como Facebook, Twitter, LinkedIn, Instagram u otros que permitan cualquier tipo de opinión no deberán publicar datos relacionados con la Unidad, que no sean avalados y publicados por la Oficina Asesora de Comunicaciones.
- VII. La mensajería instantánea y el correo electrónico de uso interno o externo debe ser usado exclusivamente para el desempeño de las funciones en el marco de la operación de la Unidad. La información, los mensajes y correos electrónicos son propiedad de la Entidad, quién tendrá la potestad de inspeccionar, registrar y evaluar la información intercambiada por estos medios, como parte de las funciones de administración de la plataforma tecnológica.
- VIII. Solo se permite el uso de Skype Empresarial para mensajería instantánea interna y externa relacionada con actividades propias de la Entidad.
- IX. Se acepta el uso eventual de cuentas de correo externas (Hotmail, Gmail, Yahoo, entre otras), con previa autorización de la dependencia encargada de la implementación del Sistema de Gestión de Seguridad de la Información, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva, y que no interfiera y/o divulgue información de las actividades de la Entidad
- X. Los mensajes y la información contenida en los buzones de correo corporativo y equipos de cómputo son propiedad de Unidad.
- XI. No se podrán enviar o reenviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.
- XII. Toda información confidencial de la Unidad que requiera ser enviada fuera de la Entidad, deberá enviarse de acuerdo con los procedimientos “Articulación Interinstitucional y dinamizadora de la información 520.06.08-27” establecidos para tal fin.
- XIII. Ningún funcionario o contratista, con excepción de los requerimientos de ley y administración de la plataforma tecnológica, está autorizado para revisar los correos electrónicos Institucionales de los usuarios o sus correspondientes registros de auditoría.
- XIV. Los usuarios deben evitar de enviar información clasificada o reservada a terceros o personal interno mediante el correo electrónico. Se deben agotar las opciones de consulta de sistemas de información existentes para cubrir este tipo de requerimientos. Cuando sea estrictamente necesario el envío de información por correo electrónico, deben aplicarse controles orientados a evitar la fuga de información.



- XV. Los funcionarios son responsables de la información que es enviada desde su correo electrónico.
- d) Todos los funcionarios, contratistas y terceros para terminar su relación laboral con la Unidad, deben devolver todos los activos de la organización que se encuentren a su cargo.
 - e) La información debe ser clasificada por los usuarios, contratistas y terceros en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada. Se debe seleccionar uno de los siguientes tres (3) niveles en términos de confidencialidad: información pública, reservada o clasificada.
 - f) Todos los funcionarios, contratistas y terceros deben etiquetar la información física o digital que genere la Entidad (información pública, reservada o clasificada). Para los correos electrónicos, si su contenido es de categoría clasificada o reservada, de uso interno o público, debe marcarse el correo electrónico para que pueda ser identificado.
 - g) Todos los funcionarios, contratistas y terceros deben proteger la información almacenada en dispositivos removibles en cuanto a su acceso, uso, transporte, almacenamiento y eliminación, acorde con su nivel de clasificación, teniendo en cuenta los lineamientos de seguridad de la información que la Entidad establece.
 - h) Los dispositivos removibles asignados a los funcionarios y contratistas de la Entidad deben ser devueltos en los términos y condiciones definidas al momento de la asignación.
 - i) El funcionario o contratista de la Entidad que recibe dispositivos removibles, suministrados por la Entidad, es responsable de su buen uso y cuidado.
 - j) Los siguientes lineamientos que deben cumplir los funcionarios, contratistas y terceros, para la protección de la información clasificada o reservada durante el transporte de equipos que la contengan son:
 - I. El funcionario o contratista, debe validar la utilización de un transporte confiable y adecuado para los activos de información.
 - II. El transporte de información en medios (electrónica o impresa) debe contemplar mecanismos que no permitan su uso no autorizado, preservando así la confidencialidad, integridad y disponibilidad de la misma.
 - III. Se deben establecer controles para el transporte de información, que contemplen el uso de servicios de mensajería certificada, a través de contratos formales, donde se establezcan acuerdos de niveles de servicio, que contemplen los mecanismos de seguridad que deben ser proporcionado por el contratista.



- IV. Entre los acuerdos de niveles de servicio se debe contemplar la garantía de uso de recipientes cerrados, entrega certificada, embalaje con sellos de seguridad a prueba de apertura no autorizada, el uso de rutas diferentes para las entregas, entre otros.
- V. La empresa que provee el servicio de transporte de información en equipos provistos por la Unidad debe garantizar procesos adecuados de embalaje para la protección de estos medios de almacenamiento de factores ambientales y deben ser estipulados a nivel contractual.
- VI. El funcionario o responsable del transporte, debe llevar un registro que identifique el contenido de los medios, la protección aplicada, al igual que el tiempo de transporte, y el recibo en su destino.

4. Control de acceso

El acceso a los activos de información de la Unidad para la Atención y Reparación Integral a las Víctimas debe estar permitido únicamente a personal autorizado, ya sea con vinculación laboral vigente en caso de usuarios internos, o con acuerdo de intercambio de información entre Entidades en caso de usuarios externos y/o proveedores.

Los Lineamientos listados a continuación son responsabilidad los usuarios:

- a) El personal con privilegios de acceso a sistemas de información debe contar con vinculación laboral vigente con la Unidad o con terceros que tengan contrato vigente con la entidad y autorización de acceso al activo, teniendo en cuenta los requisitos documentados en el procedimiento "Creación de usuarios en sistemas de información de la Entidad 130.06.08-3".
En el caso de entidades públicas o privadas se debe establecer un acuerdo de intercambio de información para el acceso a la información de la entidad.
- b) Para el acceso a sistemas de información por parte de usuarios contratados a través de terceros, se debe documentar la correspondiente autorización, por parte de la persona delegada para tal fin por el supervisor del contrato.
- c) Los usuarios de entidades externas deben contar con la autorización del colaborador designado, en el marco del acuerdo de intercambio de información, y la autorización del proceso propietario del activo.
- d) Se deben ejecutar los procedimientos, para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información. Los privilegios de acceso deben estar documentados.
- e) Los usuarios deben proteger la información confidencial de la Entidad contra el acceso no autorizado, uso indebido o modificación no autorizada o controlada.



- f) El custodio de la información debe establecer controles, teniendo en cuenta su criticidad.
- g) La información confidencial de la Entidad que sea necesaria transportar en medios magnéticos removibles debe estar cifrada, para protegerla contra el acceso no autorizado o uso indebido durante el transporte.
- h) En caso de cambio de dependencia se deben remover todos los derechos de acceso que no requiere el usuario en su nuevo rol, el jefe inmediato y/o el supervisor del contrato son los responsables de reportar a la Oficina de Tecnologías de la Información dicho cambio.
- i) En caso de finalización de vinculación laboral con la Entidad, se deben remover todos los derechos de acceso previo a la liquidación del contrato en caso de contratistas o paz y salvo en caso de funcionarios.
- j) Los funcionarios, contratistas y terceros deben proteger sus credenciales de acceso a Sistemas de Información y a servicios de red, y por ningún motivo se deben compartir o divulgar contraseñas.
- k) Las credenciales de acceso a sistemas de información de la Entidad deben ser individuales y es responsabilidad de los usuarios no compartirlas.
- l) Las contraseñas de los usuarios deben cumplir con los siguientes parámetros:
- Debe tener una longitud mínima de 8 caracteres alfanuméricos.
 - No contendrá nombres o números telefónicos, ni tampoco números o letras consecutivas o repetidas.
 - Debe contener al menos un número, una letra minúscula y una mayúscula.
 - Las contraseñas son de uso personal y por ningún motivo se debe divulgar a otros usuarios.
- m) Las contraseñas no deben ser reveladas por vía telefónica, correo electrónico o por ningún otro medio. En caso de creación de usuarios en Sistemas de Información o directorio activo, se entregará una contraseña temporal al usuario por medio de correo electrónico o llamada telefónica. Es responsabilidad del usuario cambiarla en su primer uso.
- n) Los usuarios no deben habilitar la opción “recordar clave en este equipo”, en el navegador de internet.
- o) Se debe reportar cualquier caso donde se evidencie el uso compartido de credenciales de acceso a herramientas tecnológicas.
- p) Se debe modificar la contraseña cada 2 meses o antes si el usuario lo considera necesario.



- q) Los usuarios no deben usar las credenciales de acceso de otros usuarios ni intentar apoderarse de sus claves, ni probar una gran cantidad de combinaciones posibles para identificar contraseñas de usuarios legítimos, para acceder a un Sistema de Información o equipo de cómputo de la Entidad.
- r) Se debe reportar cualquier sospecha de hurto de contraseñas.
- s) Se debe controlar el acceso a los registros de auditoría para que solamente el personal autorizado pueda acceder a ellos, en el marco de la administración de la plataforma tecnológica.
- t) Se deben generar registros de auditoría, respecto al ingreso a los Sistema de Información.
- u) Los sistemas de información de la Unidad para la Atención y Reparación Integral a las Víctimas deben contar con mecanismos de identificación individual de los usuarios y con procedimientos para el control de acceso a los mismos.
- v) Queda prohibida la reproducción total o parcial de la información física o digital de la Entidad, por cualquier medio o procedimiento, por tanto, se debe tener autorización previa del responsable en caso de ser requerido.
- w) Los usuarios no deben alterar o divulgar información que la Entidad considere clasificada o reservada. Puesto que pueden ser causales de procesos de responsabilidad de acuerdo con la normatividad vigente.
- x) En caso de pérdida, robo, daño, alteración, divulgación no autorizada y/o fuga de información física como consecuencia del descuido o actuación riesgosa por parte de un funcionario, contratista o colaborador de la Entidad, el responsable del incidente debe asumir las sanciones correspondientes y asumir los daños y perjuicios que se ocasionen.
- y) Los usuarios no deben acceder a la información de la Entidad sin previa firma del acuerdo o compromiso de confidencialidad.

5. Criptografía

El responsable del almacenamiento y/o transporte de información crítica confidencial, cuando se considere necesario, debe usar controles criptográficos, definidos en el marco del sistema de gestión de seguridad de la información.

Lineamientos:



- a) La Oficina de Tecnologías de la Información es la dependencia encargada de gestionar las llaves públicas y privadas que se generan en el esquema de intercambio seguro de información.
- b) Las llaves públicas generadas en la implementación del esquema de intercambio seguro de información deben ser almacenadas por los usuarios en el repositorio de llaves de la herramienta <http://intercambio.unidadVictimas.gov.co/share/page>
- c) La custodia de las llaves privadas generadas para los usuarios, en el marco del esquema de intercambio seguro de información, es de responsabilidad de cada usuario, y se prohíbe su divulgación o uso por parte de un tercer usuario.
- d) Todos los usuarios deben considerar las reglamentaciones o normas nacionales e internacionales, relacionadas a cifrado o protección de información.
- e) La Oficina de Tecnologías de la Información es la dependencia encargada de la administración de la plataforma para la generación de certificados digitales para implementación del protocolo SSL en sitios o herramientas Web de la Entidad.

6. Seguridad física y del entorno

El proceso de gestión administrativa debe implementar controles de acceso físico a las instalaciones de la Entidad para prevenir el acceso no autorizado, daño o interceptación de la información almacenada o consultada en la Entidad.

Lineamientos:

- a) No se autoriza el acceso a las instalaciones de la Entidad a los visitantes o personal no vinculado laboralmente, a menos que un funcionario o contratista activo de la Entidad lo apruebe. Dicho funcionario será responsable por el visitante durante su permanencia en las instalaciones de la Entidad. Es responsabilidad de todos los funcionarios, contratistas y terceros informar el incumplimiento de este ítem.
- b) Se exige a todos los visitantes, sin excepción, el porte de la ficha o escarapela en un lugar visible, en las sedes que cuenten con este mecanismo. Así mismo, todos los funcionarios, contratistas y terceros deben portar su carné en un lugar visible mientras permanezcan dentro de las instalaciones de la Entidad. Los funcionarios, contratistas y terceros que no cuenten con el carné, deben realizar la gestión necesaria para contar con el mismo y en caso de pérdida o robo, deben realizar la denuncia e informar de inmediato al área encargada. Las sensibilizaciones sobre el uso del carnet o la escarapela de identificación se harán en articulación con la Oficina Asesora de comunicaciones.



- c) Todos los funcionarios, contratista y terceros que autoricen la entrada a visitantes a las instalaciones de la Entidad deben acompañarlos durante el tiempo de permanencia.
- d) Todas las puertas que utilizan el sistema de control de acceso deben permanecer cerradas y es responsabilidad de todos los funcionarios, contratistas y terceros evitar que las puertas permanezcan abiertas.
- e) Las reuniones de funcionarios y contratistas de la Entidad que deban ser desarrolladas con personas externas o visitantes, se realizarán en las salas previstas para este fin. Es responsabilidad de todos los funcionarios, contratistas y terceros informar el incumplimiento de este ítem.
- f) Es responsabilidad de todos los funcionarios, contratistas y terceros de la Entidad borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo. Igualmente, no se deben dejar documentos o notas escritas sobre las mesas al finalizar las reuniones.
- g) Los visitantes que requieran asistir a las oficinas de la Entidad por periodos superiores a 2 días consecutivos deben ser presentados al personal cercano del proceso donde permanecerán, informando el motivo de la visita y periodo de inicio y finalización de la visita. Los visitantes deben ser registrados en las bitácoras de acceso o salida de las instalaciones, por parte del personal de vigilancia.
- h) Los equipos portátiles deben permanecer asegurados con guaya de seguridad o guardados bajo llave durante la noche y en horarios en los cuales el funcionario responsable no se encuentre en su sitio de trabajo.
- i) El acceso a las instalaciones de la Entidad está permitido únicamente al personal autorizado y controlado mediante distintos mecanismos de control de acceso físico (áreas de recepción con personal, vigilancia física y/o sistemas biométricos). Es responsabilidad de todos los funcionarios, contratistas y terceros informar el incumplimiento de este ítem.
- j) Los centros de cableado ubicados en las instalaciones de la Entidad se definen como áreas seguras identificados visualmente, por tal razón deben contar como mínimo con los siguientes mecanismos de protección física y control de acceso, que permita el ingreso exclusivamente al personal autorizado por la Oficina de Tecnologías de Información.

I. Acceso mediante sistemas de seguridad (llave o tarjeta de acceso o control biométrico)

II. Detección de incendios

III. Cámaras conectadas al circuito cerrado de televisión

IV. Aire acondicionado

V. Energía regulada y sistema de UPS.

Es responsabilidad de todos los funcionarios, contratistas y terceros informar el incumplimiento de este ítem. Los centros de cableado deben ser utilizados únicamente para los fines autorizados por la Oficina de Tecnología de la Información. Por lo que se prohíbe su uso como bodegas de almacenamiento. Es responsabilidad de todos los funcionarios, contratistas y terceros informar el incumplimiento de este ítem.

- k) Las áreas de oficinas contarán con los siguientes mecanismos de protección física:
 - I. Acceso mediante sistema biométrico y/o personal de vigilancia.
 - II. Detección de incendios
 - III. Cámaras conectadas al circuito cerrado de televisión
 - IV. Fuente de energía regulada

- l) Sólo se permitirá el acceso de terceros a las áreas seguras, con propósitos específicos y deben efectuarse el registro de ingreso (fecha y horario de ingreso y salida) en la bitácora destinada para este fin. Los terceros deben ser acompañados por parte del personal responsable del centro de datos.

6.1. Equipo

Se debe implementar controles orientados al aseguramiento de equipos, servicios de apoyo y cableado eléctrico y de datos, para prevenir la pérdida, daño, robo o no disponibilidad de activos.

Lineamientos:

- a) El Grupo de Gestión Administrativa debe implementar controles para minimizar la posibilidad de presentarse casos de robo, incendio, explosivos, humo, agua o falla en el suministro de agua, polvo, vibración, efectos químicos, interferencia en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y/o vandalismo).
- b) La Oficina de Tecnologías de la Información, debe definir y divulgar las recomendaciones relacionadas con evitar comer, consumir líquidos o fumar cerca de las instalaciones de procesamiento de información o centros de cableado.
- c) El Grupo de Gestión Administrativa y la Oficina de Tecnologías de la Información deben hacer seguimiento de las condiciones requeridas de suministro eléctrico, así como las condiciones ambientales tales como temperatura y humedad, para determinar los escenarios que puedan afectar negativamente la operación de las instalaciones de procesamiento de información.



- d) El cableado de energía eléctrica y datos debe estar debidamente protegido para evitar la interceptación, interferencia o daño, por medio de canaletas definidas para tal fin, es responsabilidad de todos los funcionarios, contratistas y terceros informar el incumplimiento de este ítem.
- e) Las estaciones de trabajo ya sean equipos portátiles o equipos de escritorio asignados por la Entidad, no deben ser usados personas externas a la Entidad, es responsabilidad de todos los funcionarios, contratistas y terceros informar el incumplimiento de este ítem.
- f) Los equipos tales como máquinas de copiado o multifuncionales deben estar ubicados en zonas de acceso restringido a terceros. La configuración de estos equipos está permitida únicamente a personal técnico autorizado por la Oficina de Tecnologías de la Información. Es responsabilidad de todos los funcionarios, contratistas y terceros informar el incumplimiento de este ítem.
- g) El Grupo de Gestión administrativa debe autorizar la salida de equipos y expedientes físicos de la Entidad siempre y cuando tenga la aprobación del grupo de seguridad de la Información.
- h) Los equipos portátiles son responsabilidad del usuario, a quien se autoriza el transporte y uso del equipo, por tal razón se debe evitar descuidarlos o desatenderlos. En casos de viaje siempre se deberán llevar como equipaje de mano.
- i) La Oficina de Tecnologías de la Información debe realizar el borrado seguro de la información almacenada en discos duros (portables o de equipos de cómputo) que se entreguen al proveedor de servicios o que se reasignen a otro usuario para su uso.
- j) Los usuarios deberán bloquear su equipo o estación de trabajo cada vez que se retiren de su sitio de trabajo y solo se podrán desbloquear con la contraseña del usuario. Al finalizar sus actividades diarias, deberán salir de todas las aplicaciones y apagar la estación de trabajo. En caso de que requiera mantener el equipo encendido, este debe estar bloqueado y con la pantalla apagada.
- k) En horas no hábiles o cuando los sitios de trabajo se encuentren desatendidos, los usuarios deben dejar la información confidencial o privada protegida bajo llave. Esto incluye: documentos impresos, CDs y dispositivos de almacenamiento.
- l) Los usuarios deben retirar de forma inmediata todos los documentos confidenciales que envíen a las impresoras. Así mismo, no se debe reutilizar papel que contenga información confidencial o privada.

- m) Todos los funcionarios, contratistas y terceros deberán usar en sus estaciones de trabajo el fondo de pantalla y el protector de pantalla corporativo, el cual se activará automáticamente después de máximo cinco (5) minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

6.1.1. Mantenimiento de los equipos

Se debe planificar e implementar un plan de mantenimiento preventivo que contenga los lineamientos que a continuación se describen.

Lineamientos

Responsabilidades de los funcionarios, contratistas y terceros:

- a) Mantener los equipos de acuerdo con las especificaciones de los fabricantes.
- b) Registrar las fallas, mantenimientos correctivos y preventivos, como evidencia de la gestión.
- c) Contar con un inventario detallado del Hardware y del Software presente en los equipos de cómputo.
- d) Verificar que el mantenimiento preventivo o correctivo es realizado por personal calificado y autorizado por la Oficina de Tecnologías de la Información.
- e) Tener en cuenta las políticas de las aseguradoras para la realización de los mantenimientos.
- f) Inspeccionar la integridad de los equipos antes de ponerlos de nuevo en operación, después de un mantenimiento.

La oficina de Tecnologías de la información programa dos actividades de mantenimientos al año en los equipos que se encuentren en modalidad de arrendamiento, los directores son responsables de las siguientes actividades:

- a) Atender el cronograma de actividades de mantenimiento y socializar con los funcionarios de cada dirección territorial.
- b) Identificar la lista de técnicos que se envía previamente el correspondiente a la sede y validar su identificación.
- c) Tener en cuenta las fechas definidas para el desarrollo de las actividades y la cantidad de días que estarán los técnicos en cada sitio.

- d) Informar a cada funcionario en las sedes para que permita el trabajo de los técnicos en las fechas establecidas en el cronograma.
- e) Hacer extensivo el cronograma a las personas que tengan asignados equipos portátiles, de tal forma que estos se encuentren en la sede el día de la actividad, para poder realizar el procedimiento.
- f) Los usuarios deben colaborar y facilitar la realización de mantenimientos preventivos liderados por la Oficina de Tecnologías de la Información.
- g) El técnico encargado realiza una visita por equipo, si en la primera oportunidad no se logra ejecutar el servicio, se reprogramará la visita por segunda vez, si esta es fallida, se levantará un acta donde consta que el usuario no permitió realizar el mantenimiento.
- h) El usuario es responsable de la información que custodia, por lo tanto, debe entregar el equipo apagado cuando el técnico haga el mantenimiento.
- i) El usuario debe asegurar sus objetos personales y dispositivos electrónicos (celulares, memorias USB, otros dispositivos), evitando la pérdida de objetos.
- j) Terminado el mantenimiento el usuario debe validar el correcto funcionamiento de los equipos. Si se encuentra el equipo en óptimas condiciones los usuarios deben firmar el reporte que entrega el técnico.
- k) Si presenta inconformidad o daño de los elementos o el servicio, el usuario debe notificar a la Oficina de Tecnologías de la Información o a la mesa de servicios tecnológicos (#5) o por correo electrónico a la cuenta sopORTE.oti@unidadVictimas.gov.co o mantenimientopreventivo@unidadvictimas.gov.co.

7. Seguridad de las operaciones

7.1. Procedimientos operacionales y responsabilidades

7.1.1. Gestión del cambio

Se debe realizar el control de cambios, para los procesos, la infraestructura y los sistemas de información de manera segura, garantizando la confidencialidad, disponibilidad e integridad de los activos, la Oficina de Tecnologías de la información es la encargada de liderar dichos controles.

Se deben especificar aspectos como identificación y registro de cambios significativos, planificación y pruebas previas y posteriores de los cambios a realizar, valoración de impactos, tiempos de no disponibilidad del servicio, comunicación a los procesos pertinentes.

Lineamientos

- a) Los usuarios no deben realizar cambios en los equipos de cómputo de trabajo, tanto a nivel hardware y/o software relacionado con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, fondo de pantalla y/o protector de pantalla corporativo. Estos cambios podrán ser realizados únicamente por la Oficina de Tecnologías de la Información de la Unidad para la Atención y Reparación Integral a las Víctimas.
- b) El inventario de activos se actualizará como mínimo una vez al año o cada vez que se presenten cambios representativos en la operación o en la infraestructura que soporta los procesos de la Entidad, dicho inventario es responsabilidad de todos los procesos de la Entidad.
- c) La Unidad establecerá el comité de control de cambios para aprobar los cambios a nivel tecnológico que se presenten y así realizar el proceso de evaluación.

7.1.2. Gestión de la capacidad

Se deben asegurar los recursos como dotación tecnológica, infraestructura y sistemas de información necesarios, para la operación.

Lineamientos

- a) Proveer la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información.
- b) Identificar el comportamiento de los servicios informáticos y evitar cuellos de botella potenciales y dependencia del personal clave, que podrían presentar una amenaza para la seguridad o servicios del sistema, y planificar la acción apropiada.

7.1.3. Separación de los entornos de desarrollo, pruebas y producción

Se deben Implementar controles para reducir los riesgos de accesos o cambios no autorizados en los ambientes donde se soportan y desarrollan los sistemas de información de la Unidad para la Atención Integral a las Víctimas y terceros con relación contractual.

Lineamientos

- a) Definir y documentar los lineamientos, para paso en producción, así como para la administración de los ambientes.

- b) Garantizar que los ambientes tienen las mismas características técnicas o similares para validar el funcionamiento de las aplicaciones.
- c) Antes de colocar los cambios en ambientes de producción, deben instalarse en ambiente de pruebas y realizar el proceso de verificación definido para aceptación.
- d) Las herramientas de desarrollo, editores o compiladores no deben tener acceso hacia los ambientes de producción.
- e) Realizar algún tratamiento para los datos sensibles o evitar copiarlos en ambiente de producción.

7.2. Protección contra códigos maliciosos

Todos los sistemas de información deben ser protegidos teniendo en cuenta un enfoque con controles humanos, físicos, técnicos y administrativos.

Lineamientos

- a) Los equipos que manejan información de la Unidad para las víctimas deben estar protegidos con antivirus que cuente con actualización automática.
- b) Los equipos de cómputo realizarán periódicamente análisis de virus por medio de política habilitada en la consola.
- c) La Oficina de Tecnologías de la Información podrá hacer seguimiento al tráfico de la red cuando se tenga evidencias de actividad inusual o degradación en el desempeño.
- d) La Oficina de Tecnologías de la Información debe mantener documentados los presuntos incidentes de seguridad de la información reportados por funcionarios, contratistas y terceros de la Unidad para la Atención y Reparación Integral a las Víctimas y hacer seguimiento de los eventos inusuales que se presentan y que afecten la seguridad de la información o tengan un impacto considerable en el desempeño de los sistemas informáticos.
- e) Se prohíbe el uso de software no autorizado por la Oficina de Tecnologías de la Información.
- f) Llevar a cabo revisiones regulares del software y del contenido de datos de los sistemas que apoyan los procesos críticos de la operación.
- g) Se deben definir las responsabilidades relacionadas con la protección de software malicioso en los sistemas de información.



- h) Se debe realizar un reporte y recuperación de ataques de software malicioso.

7.3. Copia de respaldo

Los líderes de cada uno de los procesos son los responsables de gestionar el respaldo de toda la información de su respectivo grupo de trabajo mínimo una vez al año, almacenándola en la nube por medio de la herramienta OneDrive, con el fin de mantener disponibles los datos que por de valor para la Entidad. En el caso de los procesos que tienen apoyo de operadores, el respaldo de la información debe hacerse antes de la terminación del contrato garantizando la disponibilidad, integridad y confidencialidad de la información.

Lineamientos:

La UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS define los siguientes lineamientos para la realización de copias de respaldo.

- a) La Oficina de Tecnologías de la Información debe establecer e implementar un plan de copias de respaldo (Servidores).
- b) La Oficina de Tecnologías de la Información debe determinar el procedimiento o protocolo para la restauración de información (Servidores).
- c) Los líderes de cada uno de los procesos son los responsables de identificar los activos críticos, los cuales deben tener copia de respaldo.
- d) Los líderes de los procesos son los responsables de identificar los activos de información a los cuales se les debe realizar copia, con el fin de establecer periodicidad, prioridad, medio de respaldo y método de generación de copia de seguridad.
- e) El grupo de infraestructura tecnológica de la Oficina de tecnologías de la Información debe proporcionar o gestionar el espacio físico y digital para el almacenamiento de las copias de seguridad.
- f) El grupo de infraestructura tecnológica de la Oficina de tecnologías de la Información debe establecer el ambiente de restauración de las copias de seguridad para certificación de la calidad del mismo.
- g) El grupo de Infraestructura Tecnológica de la Oficina de tecnologías de la Información debe definir roles y responsables de realizar las actividades de copias de respaldo.
- h) Gestión documental es el responsable de definir tiempos de retención de copias de seguridad e históricos según las tablas de retención de documental definidas por la UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS.

- i) La Oficina de Control interno realiza el control y seguimiento al proceso de copia de respaldo de la información y restauración.

7.4. Registro y monitoreo

Se deben registrar los eventos inusuales y dejar la evidencia de la gestión que se realiza.

Lineamientos

- a) El grupo de infraestructura tecnológica y el grupo de desarrollo de la Oficina de Tecnologías de la Información, en el marco de sus competencias, deben asegurar la identidad del dispositivo o ubicación, si es posible, e identificador del sistema.
- b) El grupo de infraestructura tecnológica y el grupo de desarrollo de la Oficina de Tecnologías de la Información deben registrar los intentos de acceso al sistema exitosos, rechazados y registros de datos exitosos y rechazados y otros intentos de acceso a recursos.
- c) El grupo de infraestructura tecnológica de la Oficina de Tecnologías de la Información es la responsable de los cambios a la configuración del sistema y uso de privilegios.
- d) La Oficina de Tecnologías de la Información es la responsable de realizar el monitoreo de las aplicaciones y utilitarios del sistema, así como archivos a los que se tuvo acceso, y el tipo de acceso.
- e) El grupo de infraestructura tecnológica de la Oficina de Tecnologías de la Información debe tener un inventario de direccionamiento y protocolos de red.
- f) El grupo de infraestructura tecnológica, el grupo de desarrollo de la Oficina de Tecnologías de la Información debe asegurarse que la información de registros o logs se protejan contra alteración y acceso no autorizado.

7.5. Control del software operacional

Se debe establecer un protocolo y control formal, para el control de la instalación de software o sistemas de información en ambientes de producción

Lineamientos

- a) El grupo de sistemas de información es el responsable de verificar que todo software puesto en producción debió haber sido verificado en ambiente de pruebas y validado con el usuario final.

- b) El grupo de sistemas de información es el responsable de verificar debe utilizar un sistema para el control de las versiones de los componentes e ítems de configuración.

7.5.1. Instalación de software en sistemas de producción

Se debe gestionar todo lo necesario para el despliegue a producción incluyendo el código fuente y de bases de datos. Se debe revisar la asignación de actividades y tiempos para la entrega de las soluciones.

Lineamientos sobre la adquisición, desarrollo y mantenimiento de sistemas de información:

- a) La Oficina de Tecnologías de la Información debe implementar el procedimiento y/o protocolo para la gestión de cambios de sistemas de información en ambiente productivo y/o configuración de los ambientes.
- b) La Oficina de Tecnologías de la Información debe solicitar la autorización del propietario de la Información y/o unidad funcional, en caso de tratarse de cambios a sistemas de procesamiento de la misma.
- c) La Oficina de Tecnologías de la Información debe verificar que la documentación relacionada con la instalación o despliegue de software en ambiente productivo se encuentre completa.

7.6. Gestión de vulnerabilidades técnica

Se debe tener el inventario de activos de información actualizado, identificando el tipo de activo. se deben tener fuentes de información técnica que notifiquen sobre las vulnerabilidades descritas. Así mismo, disponer de fuentes de información técnica que informen sobre las vulnerabilidades descubiertas

Lineamientos

- a) Tener actualizado el inventario de activos de información y tener definidos los roles y responsabilidades relacionados con las vulnerabilidades técnicas.
- b) Identificarlos riesgos asociados a las vulnerabilidades técnicas.
- c) Valorar los riesgos antes de realizar una actualización.
- d) Probar y evaluar los parches antes de su instalación, asegurándose de la eficiencia de estos.
- e) La gestión de vulnerabilidades debe estar alineada con la gestión de riesgos y la gestión de incidentes de seguridad de la información.

- f) Se deben identificar y corregir fallas de software o configuraciones después de ser detectadas.
- g) Verificar que los correctivos no afecten la funcionalidad la funcionalidad y/o rendimiento en los sistemas de información.
- h) Identificar falencias que no pueden ser corregidas y ofrecer alternativas, para minimizar el riesgo.
- i) Dejar evidencia de la gestión.

7.7. Consideraciones en la auditoría de sistemas de información

Se deben planificar y acordar los requisitos y actividades de la auditoría con el fin de minimizar la interrupción de la operación en entidad.

Se deben planificar y acordar los controles de auditoría en los sistemas de información

Lineamientos

- a) Realizar la planeación general de los trabajos de auditoría para determinar su alcance, metas anuales y metodología a seguir, bajo los parámetros establecidos.
- b) Supervisar la ejecución de los planes detallados de trabajo y el desarrollo de las auditorías internas.
- c) Coordinar y analizar los resultados de las auditorías realizadas con base en marcos de referencia de común aceptación.
- d) Proponer nuevos enfoques de auditoría, identificación de riesgos, recomendación de nuevos controles, y diseño e implementación de controles.
- e) Actualizar los instrumentos de acuerdo con los cambios en las normas, leyes y regulaciones, en la innovación tecnológica y en la innovación en los procesos.
- f) Las pruebas deben realizarse en ambientes controlados a los cuales se les debe limitar el acceso al software y los datos deben ser únicamente en modo lectura.
- g) Las pruebas de auditoría que requieran un uso alto de recursos computacionales deben realizarse fuera de horas laborales para evitar fallas de rendimiento en la prestación del servicio.



- h) Se debe hacer seguimiento de todos los accesos y regístralos, para producir un rastro de referencia.

8. Seguridad de las comunicaciones

8.1. Gestión de seguridad de las redes

Se deben establecer controles, para asegurar las redes y/o servicios relacionados.

Lineamientos

- a) Se deberían establecer las responsabilidades y procedimientos para la gestión de equipos de redes.
- b) La responsabilidad operacional por las redes se debe separar de las operaciones de computo, en donde sea apropiado.
- c) Las actividades de gestión se deben coordinar para optimizar el servicio de la organización, así mismo, se debe asegurar que los controles se apliquen en forma coherente a través de la infraestructura de procesamiento de información sin afectar el servicio.
- d) Restricción de conexión de dispositivos a través del puerto USB, Bluetooth o cualquier otra tecnología inalámbrica.
- e) Para el caso de computadores portátiles, se deben proteger mediante el uso de guayas de seguridad.
- f) Restricción de privilegios de administrador a nivel de sistema operativo. (Para equipos asignados por la Unidad o por cualquier operador).
- g) Uso de software licenciado e instalado por la Oficina de Tecnología de la Información, para equipos asignados por la Unidad para las Víctimas. La Unidad podrá revisar periódicamente los equipos proveídos por el operador o por la Entidad para garantizar el uso de software licenciado.
- h) Realización de copias de seguridad periódicas de la información sensible en el marco de la Ley 1581 de 2012.

Adicionalmente los usuarios deben:

- a) No desatender el equipo o dispositivo sin realizar el bloqueo correspondiente.
- b) No conectarse a redes inalámbricas públicas o sin protección.

- c) Actualizar periódicamente las contraseñas que se manejen dentro de los sistemas de información.
- d) Reportar máximo a las siguientes 24 horas cualquier evento de fuga, modificación no autorizada o pérdida de información sensible almacenada en el dispositivo.
- e) No divulgar la información sensible almacenada en dispositivos.
- f) Aplicar los controles de seguridad de la información de acuerdo con la tecnología establecida e indicada por el Equipo de seguridad y riesgo Informático de la Oficina de Tecnologías de la Información.

8.2. Transferencia de información

Los funcionarios, contratistas y terceros deben Implementar políticas, procedimientos y controles de transferencia de información establecidos por la Oficina de Tecnologías de la Información, para proteger la transferencia de información, sabiendo que se deben:

- Implementar acuerdos la transferencia segura de información del negocio entre la organización y las partes externas.
- Proteger adecuadamente la información incluida en la mensajería electrónica.
- Identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.

Lineamientos:

- a) La Oficina de tecnologías de la información debe revisar las medidas de detección y protección contra el código malicioso que pudiere ser transmitido a través de las comunicaciones electrónicas.
- b) Gestión de talento humano, gestión contractual y los proveedores que contraten personal en misión, para el desarrollo de las funciones de la Unidad deben Incluir las responsabilidades de empleados, contratistas y cualquier otro usuario de no comprometer la Organización.
- c) La Oficina de tecnologías de la información debe Implementar técnicas criptográficas.
- d) Todos los funcionarios, contratistas y terceros deben considerar el uso respecto a la información sensible enviada a dispositivos de impresión (impresoras, fotocopiadoras y faxes).



- e) La Oficina de tecnologías de la información debe validar el uso de comunicaciones inalámbrica.
- f) La Oficina de tecnologías de la información debe revisar las medidas de restricciones y controles asociadas el reenvío de información sobre medios de comunicación (por ejemplo, el reenvío automático del correo electrónico hacia direcciones externas.
- g) La Oficina de Tecnologías de la Información debe realizar capacitación al personal respecto de las medidas preventivas que deben adoptar cuando intercambien información sensible a través de diferentes medios de comunicación.
- h) Todos los funcionarios, contratistas y terceros son responsables del control y la notificación de transmisiones, envío y recepción de información.
- i) En los procesos de transferencia de información se deben identificar controles para notificación sobre emisión, transmisión, envío y recepción.
- j) Los dispositivos de red deben asegurar la trazabilidad sobre el uso de medios de comunicación y el no repudio.
- k) La Oficina de tecnologías de la información debe definir estándares técnicos mínimos para el empaquetado y la transmisión.
- l) La Oficina de tecnologías de la información es la encargada de definir los requisitos de seguridad en la plataforma de correo, para transferencia de información.
- m) Todos los funcionarios, contratistas y terceros deben reportar los incidentes de seguridad de la información, que se encuentren en las categorías descritas en el presente documento en el numeral 3.15 GESTIÓN DE INCIDENTES DE SEGURIDAD EN LA INFORMACIÓN. (ISO 27001:2013/ A.16.).
- n) El proceso de Gestión Documental debe establecer rotulado para la información sensible o crítica, garantizando que los significados de los rótulos sean inmediatamente comprendidos y que la información sea adecuadamente protegida.
- o) Todos los funcionarios, contratistas y terceros deben aplicar protección de los medios de almacenamiento cuando se realice tránsito de los datos.
- p) Todos los funcionarios, contratistas y terceros deben formular apropiadamente los acuerdos sobre medios tradicionales documentales y/o medios electrónicos.

- q) La Oficina de tecnologías de la información debe establecer la propiedad y responsabilidad para la protección de datos, derechos de copia, conformidad de las licencias de software y consideradas similares.
- r) La Oficina de tecnologías de la información y el supervisor del contrato con el proveedor deben socializar, sensibilizar y divulgar las campañas para el buen uso de los sistemas de mensajería electrónica con el Operador.
- s) Considerar los siguientes aspectos para el diseño de los acuerdos de confidencialidad con funcionarios, contratistas y terceros:
- i. Establecer y definir la información que será objeto de protección (información confidencial).
 - ii. Establecer la duración esperada para el acuerdo y las acciones requeridas antes, durante y después de finalizada la obra y/o labor a realizar.
 - iii. Establecer la propiedad de la información, los secretos comerciales y la propiedad intelectual, y cómo esto se relaciona con la protección de información confidencial.
 - iv. Definir los privilegios de uso permitido de información confidencial y los derechos del firmante para usar la información.
 - v. Validar el derecho a actividades de auditoría y de seguimiento que involucran información confidencial.
 - vi. Validar el proceso de notificación y reporte de divulgación no autorizada o fuga de información confidencial.
 - vii. La UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS realizará la identificación, revisión, documentación y actualización periódica de los requisitos para los acuerdos o compromisos de confidencialidad que cumplan con los requerimientos de protección de información de la Entidad.
 - viii. Todos los usuarios de bienes y servicios informáticos de la Entidad deben comportarse de acuerdo con lo establecido en la cláusula, acuerdo y/o compromiso de confidencialidad y uso adecuado de los recursos informáticos.
 - ix. Este requerimiento también se aplicará para los casos de contratación de personal temporal o cuando se permita el acceso a la información y/o a los recursos de la Entidad a personas o entidades externas.
 - x. El acuerdo o compromiso de confidencialidad será vigente mientras el funcionario, contratista, colaborador o persona externa a la Entidad, cuente con el acceso a la información.

9. Adquisición, desarrollo y mantenimiento de sistemas

9.1. Requisitos de seguridad de los sistemas de información

Esta política de requisitos de seguridad de los Sistemas de Información tiene como alcance los siguientes temas, que aplican para la Unidad para la Atención y reparación Integral a las Víctimas, los operadores y terceros:

- a) Análisis y especificación de requisitos de seguridad de la información
- b) Seguridad de servicios de las aplicaciones en redes públicas
- c) Protección de las transacciones de los servicios de aplicaciones

Definir los requisitos de los sistemas de información con los parámetros establecidos en la construcción y se debe hacer mantenimiento correctivo y evolutivo del software.

Lineamientos

- a) La Oficina de tecnologías de la información y los procesos funcionales relacionados deben analizar el alcance y las especificaciones de las soluciones tecnológicas determinando el impacto que tiene sobre el sistema de información y sus funcionalidades.
- b) La Oficina de tecnologías de la información y los procesos funcionales relacionados deben establecer el plan de trabajo con actividades, responsables, tiempos y fechas de ejecución.
- c) La Oficina de tecnologías de la información debe identificar cambios en el alcance revisando las especificaciones, recursos asignados y costos asociados a la solución.
- d) La Oficina de tecnologías de la información y los procesos funcionales relacionados deben realizar el levantamiento de las especificaciones funcionales y de diseño con mínimo (historia de usuarios y criterios de aceptación).
- e) La Oficina de tecnologías de la información debe documentar los prototipos, arquitectura física y lógica en los sistemas de información que hacen parte de la Entidad.
- f) La Oficina de tecnologías de la información y los procesos funcionales relacionados deben elaborar escenarios de pruebas, para garantizar que la solución tecnológica cumple con los requisitos y necesidades establecidas dentro del marco de seguridad y a nivel funcional.
- g) La Oficina de tecnologías de la información y los procesos funcionales relacionados deben realizar el desarrollo o ajuste en el sistema y verificar a través de pruebas que se cumplan con lo diseñado evitando errores.
- h) La Oficina de tecnologías de la información y los procesos funcionales relacionados deben ejecutar pruebas unitarias e integrales de la funcionalidad creada o modificada.

- i) La Oficina de Tecnologías de la Información debe incorporar los requerimientos de seguridad de la información en la documentación para nuevos desarrollos o nuevas funcionalidades de los sistemas de información.
- j) La Oficina de Tecnologías de la información deben realizar el análisis, identificación y el correspondiente tratamiento de riesgos, para los documentos y arquitectura generada en la fase de diseño, con el fin definir los controles adecuados a implementar, teniendo en cuenta que estos deben ser proporcionales en costo y esfuerzo respecto al valor del activo de información que se quiera proteger.
- k) La Oficina de Tecnologías de la Información debe realizar pruebas correspondientes sobre el código fuente de la aplicación.
- l) La Oficina de Tecnologías de la Información debe gestionar el Hacking ético sobre las herramientas en producción en ambientes controlados de manera periódica o cuando se realice alguna actualización tecnológica.

9.2. Seguridad en los procesos de desarrollo y soporte

Durante el análisis y diseño de las aplicaciones, se deben identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se deberán diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos.

La Unidad para la Atención y Reparación Integral a las Víctimas debe asegurar que se realice el análisis e implementación de los requerimientos de seguridad en el software y/o sistemas de información que se desarrollen o se adquieran, debe incluir controles de autenticación y auditoría de usuarios, verificación de los datos de entrada y salida, y que se implementen buenas prácticas para un desarrollo seguro.

Lineamientos

- Para las fases de requerimientos, análisis, diseño, implementación, codificación, fase de pruebas, control de acceso a los códigos fuentes, Protocolo de Control de Cambios en el Desarrollo,
- Revisión Técnica de los Cambios en Sistema Operativo, Restricciones del Cambio de Paquetes de software, Desarrollo Externo de Software se deben cumplir con los siguientes lineamientos:

Fase de Requerimientos:

- Control de autenticación: Se deben implementar controles de autenticación que garanticen que el funcionario es quien dice ser y de esa forma solo las personas autorizadas puedan acceder a los sistemas. Estos mecanismos de autenticación pueden ser basados en:
 - Algo conocido: Ejemplo, un password (Unix) o passphrase (PGP)
 - Algo poseído: Ejemplo, una tarjeta de identidad, una tarjeta inteligente (smartcard), dispositivo usb tipo epass token, tarjeta de coordenadas, smartcard o dongle criptográfico.
 - Una característica física del usuario o un acto involuntario del mismo: Ejemplo, verificación de voz, de escritura, de huellas, de patrones oculares
- Control de roles y privilegios: Se deben implementar controles para establecer la granularidad de la información que pueda manejar los funcionarios y los accesos a las aplicaciones.

Fase de Análisis y Diseño:

- Administración de Contraseñas: Todas las contraseñas deben ser protegidas contra modificación, destrucción, copia o divulgación no autorizada mediante almacenamiento cifrado en las bases de datos.
- Acceso a componentes y administración de sistemas: Se deben implementar controles que determinen el nivel de accesos a la información, menús, parametrización del sistema y demás componentes para administrar el sistema.
- Pistas de auditoría: Se debe generar un log detallado de todas las actividades que se hacen en el sistema. Este log deberá permitir almacenar las actividades habituales del sistema que involucren modificación de la información o inicios de sesión y deberá permitir la opción de generar un log más detallado de todas las actividades realizadas por los usuarios o grupo de usuarios para temas de trazabilidad, investigación y seguimiento a problemas.
- Gestión de Sesiones: Se deben implementar mecanismos que permitan que los usuarios autenticados tengan una asociación con sus sesiones robusta y criptográficamente segura, que se hagan cumplir los controles de autorización y de esta forma se prevengan los típicos ataques web, tales como la reutilización, falsificación e interceptación de sesiones.
- Datos históricos: Se deben almacenar los datos históricos de la información para disponer de ella en diferentes momentos de la historia.
- Manejo apropiado de errores: Se deben implementar controles que permitan administrar las fallas intencionales o no intencionales en nuestro sistema generando excepciones tan pronto aparece un error.

- Separación de Funciones (Segregación): Se debe evitar que una misma persona tenga acceso a dos o más responsabilidades dentro del sistema, de tal forma que pueda realizar acciones o transacciones que lleven a la consumación de un fraude.
- Revisión Técnica de los Cambios en Sistema Operativo: Se deben implementar controles para asegurar que no se produzca un impacto en su funcionamiento o seguridad cuando se realicen cambios a nivel de sistemas operativos.

Fase de Implementación y Codificación:

- Validación de Datos de Entrada: Se deben realizar validaciones que aseguren la validez de los datos ingresados.
- Validación y codificación de Datos de Salida: Se deben implementar mecanismos de cifrado y control de acceso a la información de modo que los puedan ver las personas autorizadas.
- Se debe dejar un documento de evidencia con el resultado de las pruebas de desarrollo que se realicen.
- Aseguramiento del Ambiente en producción y de Desarrollo: Se deben definir protocolos seguros (SSL), de cifrado y de control de fuga de información.
- Certificados de Sitio Seguro y Persona Jurídica: Se deben adquirir certificados de sitio seguro para ambientes de producción expuestos en la red pública para asegurar la transmisión de información. Así mismo, se deben firmar digitalmente los documentos por medio de un PJEE para asegurar la integridad de los mismos.
- Seguridad en las comunicaciones: Se deben asegurar los canales de comunicación para minimizar el riesgo de fuga de información.
- Manejo de errores y logs: Se debe contar con una trazabilidad de información para llegar a la solución de problemas o a la identificación de incidentes
- Elaboración de documentación técnica: Se debe contar con un registro de las configuraciones y funcionalidades del sistema el cual sirva de consulta para revisiones de errores del sistema, capacitaciones y transferencias de conocimiento sobre el mismo.

- Codificación Segura: Se deben tener en cuenta para minimizar el riesgo de problemas en los desarrollos de la Entidad:
 - No rechazo (Non-repudiation): Se deben usar técnicas para verificar la identidad del emisor y/o el receptor de un mensaje.
 - Soporte criptográfico: si se usa criptografía ¿Qué operaciones la usan? ¿qué algoritmos y tamaños de Protección de datos de usuario se usan?:
 - Protección de datos de usuario: Se debe especificar una política para la gestión de datos de usuario (control de acceso y reglas de flujo de información).
 - Identificación y autenticación: Se deben usar técnicas de validación de identidad.
 - Gestión de seguridad: Se deben definir roles y perfiles de usuario para establecer los niveles de acceso asociados.
 - Manejo adecuado de memoria: se deben implementar controles en los códigos fuentes que permitan prevenir desbordamiento de memoria.
 - Estandarización: Se deben estandarizar las funciones y mecanismos de seguridad para establecer un nivel adecuado para la seguridad de la información.
 - Control de acceso: El sistema debe soportar la limitación del número y tipo de sesiones, el nivel de concurrencia y que proporcionen información sobre sesiones anteriores al usuario para ayudar a la detección de intrusos.

Fase de pruebas:

- Protección de los Datos de Prueba del Sistema: Para las pruebas de los sistemas, se utilizarán datos extraídos del ambiente operativo y en lo posible realizar procesos de ofuscación de información para proteger los datos de prueba, así mismo se debe establecer normas que contemplan lo siguiente:
 - Solicitar autorización formal para realizar una copia de la base operativa como base de prueba, llevando registro de tal autorización.
 - Eliminar inmediatamente completadas las pruebas, la información operativa utilizada.
 - Los datos del ambiente operativo no deben permanecer más de un mes en pruebas. Una vez cumplido este periodo deben ser borrados.

- Seguridad en paso a producción: Se debe disponer de los elementos de hardware y software necesarios para poner en producción el desarrollo minimizando los tiempos de no disponibilidad del sistema.

Control de Acceso a los Códigos Fuente

Para reducir la probabilidad de alteración de programas fuentes, se deben aplicar las siguientes pautas:

- Inspección de código por fases
- Comprobación de gestión de configuraciones
- Proveer al Área de Desarrollo los programas fuente solicitados para su modificación, manteniendo en todo momento la correlación programa fuente /ejecutable.
- Llevar un registro actualizado de todos los programas fuente en uso, indicando nombre del programa, versión, fecha de última modificación y fecha / hora de compilación y estado (en modificación, en producción).
- Administrar las distintas versiones de una aplicación.
- Establecer que todo programa objeto o ejecutable en producción tenga un único programa fuente asociado que garantice su origen.
- Prohibir el acceso a todo operador y/o usuario de aplicaciones a los ambientes y a las herramientas que permitan la generación y/o manipulación de los programas fuente.
- Realizar las copias de seguridad y pruebas de restauración de los programas fuente cumpliendo los requisitos de seguridad establecidos por la Unidad en los procedimientos que surgen de la presente política.
- Enviar a custodia externa las copias de seguridad de los programas fuentes cifradas y rotuladas de acuerdo con los procedimientos de la Unidad.

A fin de minimizar los riesgos de alteración de los sistemas de información, Oficina de Tecnologías de la Información debe implementar controles estrictos durante la realización de cambios. Para ello se deben contemplar los siguientes controles:

Verificar que los cambios sean propuestos por usuarios autorizados y presentados al comité de gestión de cambios de la Oficina de Tecnologías de la Información para su correspondiente aprobación.

- Solicitar la autorización del propietario de la Información y/o unidad funcional, en caso de tratarse de cambios a sistemas de procesamiento de la misma.
- Revisar los controles y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios.
- Solicitar la revisión del Oficial de Seguridad de la Información para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.
- Mantener un control de versiones para todas las actualizaciones de software, con el propósito de restablecer a la configuración anterior.
- Establecer los riesgos de realizar los cambios y los riesgos de no realizarlo.
- Restricciones del Cambio de Paquetes de software: previa autorización del responsable del activo de información y el líder de Gestión de Tecnologías de Información

Revisión Técnica de los Cambios en Sistema Operativo:

Cada vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas deben ser revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad. Para ello, se debe contemplar:

- Revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio.
- Garantizar que los cambios en el sistema operativo sean informados con antelación a la implementación.

Restricciones del Cambio de Paquetes de software:

En caso de considerarlo necesario la modificación de paquetes de software suministrados por proveedores, y previa autorización del responsable de la información se debe:

- Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.

- Evaluar el impacto que se produce si la Unidad de Víctimas se hace cargo del mantenimiento.
- Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

Desarrollo Externo de Software:

Para el caso que se considere la tercerización del desarrollo de software, se establecen las siguientes pautas:

- Acuerdos de licencias, propiedad de código y derechos de Propiedad Intelectual.
- Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.
- Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos.

9.3. Datos de prueba

Proteger los datos de prueba que se entregan a los desarrolladores, asegurando que no revelen información confidencial de los ambientes de producción.

Lineamientos:

- a) La Oficina de Tecnologías de la Información debe verificar que la información que es entregada a los desarrolladores para sus pruebas no revelará información confidencial de los ambientes de producción.
- b) La Oficina de Tecnologías de la Información debe eliminar la información de los ambientes de pruebas, una vez concluyan.

10. Relaciones con los proveedores

10.1. Seguridad de la información en las relaciones con el proveedor

Los integrantes del Comité Institucional de Gestión y Desempeño son los únicos que pueden aprobar los acuerdos con los proveedores los requisitos necesarios para mitigar los riesgos de

seguridad de la información asociados con la cadena de suministro que impacten la continuidad de la operación o los servicios de tecnologías y comunicación.

Lineamientos

El Equipo de Seguridad y Riesgo Informático de la Oficina de Tecnologías de la Información de la Unidad para las Víctimas incluirá dentro de los acuerdos con los proveedores los requisitos necesarios para mitigar los riesgos de seguridad de la información asociados con la cadena de suministro que impacten la continuidad de la operación o los servicios de tecnologías y comunicación.

10.2. Gestión de entrega del servicio del proveedor Seguridad de la información en las relaciones con el proveedor

Se deben monitorear los servicios tecnológicos a intervalos periódicos entre proveedores y supervisores del contrato.

Lineamientos:

- c) Llevar a cabo auditorías de los proveedores, junto con la revisión de reportes de auditores independientes, si están disponibles, y seguimiento a los hallazgos identificados.
- d) Suministrar información acerca de incidentes de seguridad de la información y revisar esta información según se exija en los acuerdos y en cualquier directriz y procedimiento de soporte.
- e) Revisar los rastros de auditoría del proveedor, y los registros de eventos de seguridad de la información, problemas operacionales, fallas, rastreo de fallas e interrupciones relacionadas con el servicio entregado.
- f) Resolver y gestionar cualquier problema identificado.
- g) Revisar los aspectos de seguridad de la información de las relaciones de los proveedores con sus propios proveedores.
- h) Asegurar que el proveedor mantenga una capacidad de servicio suficiente, junto con planes ejecutables destinados a asegurar que se mantienen los niveles de continuidad del servicio acordados, después de fallas considerables en el servicio, o después de un desastre.
- i) Establecer acuerdos de niveles de servicio con los proveedores y entregar informes de seguimiento al cumplimiento del servicio.

- j) Los proveedores deben reportar a los supervisores el listado de personal que se ha desvinculado de su compañía con el propósito de retirar los accesos a los servicios y/o información propia de la Entidad.

11. Gestión de incidentes de seguridad en la información.

11.1. Gestión de incidentes de seguridad de la información y mejoras Seguridad de la información en las relaciones con el proveedor

Es deber de todo funcionario, contratista o colaborador informar el incumplimiento de los lineamientos descritos en el presente documento.

Cualquier incumplimiento identificado debe remitirse al Equipo de Seguridad y Riesgo Informático de la Oficina de Tecnologías de la Información a través de la mesa de servicios tecnológicos, quien determinará si el evento se considera como incidente de seguridad de la información, teniendo en cuenta las categorías y criterios de clasificación. Posteriormente reportará el evento a la secretaría técnica de dicho comité, para los fines pertinentes orientados al tratamiento de caso.

Lineamientos:

- **Categorías de incidentes de seguridad de la información**

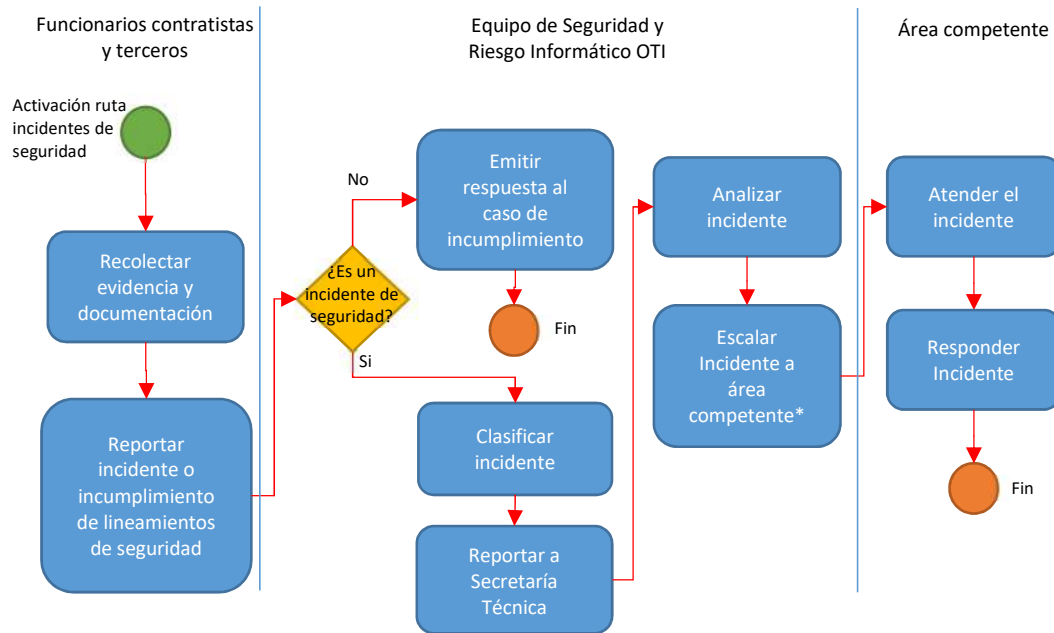
Si el incumplimiento es sujeto de clasificación teniendo en cuenta las siguientes categorías, se debe considerar como incidente de seguridad de la información.

Categoría	Criterios de clasificación Se asigna la categoría si:
Fuga de información	-Se evidencia divulgación no autorizada de información de la Unidad
Acceso no autorizado	- Se evidencia que una persona ingresa a un sistema de información sin credenciales de acceso - Se evidencia que una persona (interna o externa) tiene credenciales de acceso asignadas a otro usuario - Personal no autorizado ingresa a las instalaciones de la Unidad
Ataque	- Se evidencia intención de afectar un recurso específico - Se modifica la imagen institucional en aplicaciones de la Unidad - No se cuenta con la disponibilidad de un sistema de información por ataques de denegación de servicio (Clasificación asociada al ítem 3 Denegación de servicio)

Categoría	Criterios de clasificación Se asigna la categoría si:
	- Se evidencia caso de suplantación ya sea en correo electrónico o en páginas web
Código dañino	- El daño (modificación o indisponibilidad de la información) se manifiesta en memorias USB que alteran la información - El daño (modificación o indisponibilidad de la información) se manifiesta en un equipo y el vector de propagación fue por medio de USB contaminada o correo malicioso
Denegación de servicio	- El sistema de información no responde por alta cantidad de peticiones - El sistema de información se encuentra con latencia o degradación del servicio
Robo o pérdida	- Se presenta robo o pérdida de equipos portátiles, cargadores, periféricos de entrada y salida - Se presenta robo o pérdida de elementos personales en las instalaciones de la Unidad.
Alarmas de sistemas de monitoreo	Estos incidentes son reportados por dispositivos de seguridad según las reglas implementadas
Usos inadecuados	- Si se ingresa texto copiado de internet en documentación oficial de la Unidad, sin registrar la fuente - Si se publica comunicados en nombre de la Entidad sin revisión y aprobación del proceso de comunicación estratégica.

- Proceso general del registro y la atención a incidentes de seguridad

A continuación, proceso general con las partes involucradas:



* En esta etapa del proceso se debe informar a los miembros del comité de seguridad de la información.

12. Aspectos de la seguridad de la información de la gestión de la continuidad del negocio

12.1. CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN Seguridad de la información en las relaciones con el proveedor

La Administración de Continuidad del Negocio debe ser parte integral de la administración del riesgo de la Unidad para la Atención Integral a las Víctimas.

Lineamientos

- En la Unidad para la Atención y Reparación Integral a las Víctimas se deben tener recursos identificados, para tener una respuesta efectiva por parte de los funcionarios contratistas y terceros en caso de contingencia o eventos catastróficos que se presenten y que afecten la continuidad de la operación de la entidad.
- Se debe tener una comunicación adecuada con los funcionarios, contratistas, terceros, proveedores y terceras partes interesadas.

12.2. Redundancias y alta disponibilidad de la información Seguridad de la información en las relaciones con el proveedor

Se debe asegurar la alta disponibilidad de la información a través de redundancias de conectividad, dispositivos de comunicación y centros de datos.

Lineamientos

- a) La Oficina de Tecnologías de la Información debe analizar y establecer los requerimientos de redundancia y alta disponibilidad para los sistemas de información críticos e los diferentes sistemas de información de la entidad.
- b) Se debe definir el mecanismo de alta disponibilidad ya sea Cluster Activo (Balanceo de Carga) o Activo Pasivo (File Over) según los criterios del sistema de información a asegurar.
- c) La Oficina de Tecnologías de la Información debe evaluar y probar soluciones de redundancia tecnológica y seleccionar la solución que mejor cumple los requerimientos.
- d) Administrar soluciones de redundancia tecnológica y realizar pruebas periódicas sobre dichas soluciones, para asegurar el cumplimiento de los requerimientos de disponibilidad de la entidad.

13. Cumplimiento

13.1. Cumplimiento de los requisitos legales y contractuales

Se deben identificar y documentar los requisitos legales y contractuales manteniéndolos actualizados, para cada sistema de información y para toda la Entidad. Así mismos se debe tener documentado el procedimiento que asegura el cumplimiento de la legislación.

Se debe proteger los registros contra pérdida, destrucción, falsificación acceso no autorizado y liberación no autorizada de acuerdo con los requisitos legales y contractuales.

Se debe asegurar el cumplimiento de la política de privacidad y protección de la información de datos personales como se exige la Ley 489 de 1998, la Ley 1448 de 2011, Ley 1581 de 2015, y los Decretos 4802 de 2011 y 1083 de 2015, 1074 de 2015 y demás normas concordantes, establece las políticas de privacidad y protección de datos personales.

Por último, se debe usar controles criptográficos en cumplimiento de la legislación cuando sea aplicable.

13.2. Derechos de propiedad intelectual

La Unidad para la Atención y Reparación Integral a las Víctimas debe velar por el cumplimiento de la legislación relacionada con la seguridad de la información, entre ella la referente a derechos de autor y propiedad intelectual, razón por la cual todo software usado en la Unidad debe cumplir con los requerimientos legales y de licenciamiento aplicables. El incumplimiento de las normas de propiedad intelectual puede derivar en sanciones penales, fiscales y disciplinarias.

La Oficina de Tecnologías de la Información será responsable de mantener el control de todas las licencias de software, hardware y aplicaciones utilizadas por la UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS. Se prohíbe el uso de software ilegal o no licenciado. Los usuarios no deben instalar y utilizar software no autorizado en sus estaciones de trabajo. La Oficina de Tecnologías de la Información debe realizar revisiones periódicas a los sistemas de información y estaciones de trabajo, a fin de verificar el cumplimiento del lineamiento.

13.2.1. Lineamientos generales

- a) Los funcionarios no deben utilizar software no autorizado, software no licenciado, hacer distribución o modificación cuando no esté autorizado por el propietario, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.
- b) Los usuarios únicamente deben utilizar software autorizado la Oficina de Tecnologías de la información de la Entidad.
- c) Cuando el personal de la Oficina de Tecnologías de la información de la Entidad encuentre programas instalados en los equipos de cómputo asignados a los usuarios, sin el respectivo licenciamiento o autorización, deben proceder a desinstalarlos y deben informar inmediatamente al grupo de seguridad de la información.
- d) Se debe definir en los términos de contratación con los operadores, para que los equipos de cómputo tengan software instalado con las respectivas licencias de uso, instaladores y fuentes, manuales de usuario entre otros.
- e) Los funcionarios, contratistas y terceros siempre deben dar crédito al autor cuando la información no es producida por ellos mismos, citando la frase o párrafo directamente del original y acreditar la autoridad.

13.2.2. Lineamientos para la propiedad intelectual de la información de la entidad

- a) Todo software, páginas web, documentos, material de contenido gráfico, logos, signos distintivos, programas de televisión, programas de radio, objetos que contengan la imagen o nombre de la entidad, entre otros; será de propiedad de La Unidad para la Atención y Reparación Integral a las Víctimas así sean creados o desarrollados por los funcionarios, contratistas y terceros, dentro de los horarios laborales, o en cumplimiento de las actividades propias del contrato sujeto a las formalidades contenidas en el artículo 183 de la Ley 23 de 1982.
- b) Debe tener previa autorización de la Oficina Asesora de Comunicaciones el uso de las imágenes institucionales. Si alguna persona usa los logos de la Unidad para las Víctimas sin la autorización correspondiente, podrá tener sanciones penales, fiscales y disciplinarias.
- c) Es responsabilidad de la dirección, subdirección o proceso gestionar la licencia Creative Commons, para garantizar los derechos de propiedad intelectual y derechos de autor a nombre de La Unidad para la Atención y Reparación Integral a las Víctimas. Adicionalmente es necesario informar al Grupo de Seguridad de la Información y el proceso de gestión jurídica, dejando un registro como evidencia.

13.2.3. Lineamientos para software

13.2.3.1. Lineamientos para software libre

Se autoriza el uso de software libre que esté aprobado por la Oficina de Tecnologías de la Información. En caso de requerir un software libre que no se haya instalado anteriormente, se debe realizar la solicitud a través jefe, director o subdirector de la dependencia, con la debida justificación dirigido a la Oficina de Tecnologías de la Información, quien es la dependencia responsable de llevar un inventario del software de la Entidad.

13.2.3.2. Lineamientos para software de propietario

- a) Cuando La Unidad para la Atención y Reparación Integral a las Víctimas adquiere un software de propietario es obligatorio revisar las condiciones contractuales, para saber el alcance, (entrega del sistema de información, entrega del servicio, derechos patrimoniales y autorización a modificaciones futuras). Los sistemas de información adquiridos o desarrollados por terceros tienen que contar con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual del mismo.

- b) En el caso de requerir nuevo software la Entidad evaluará las necesidades de la dependencia u proceso que va a ser uso del mismo.
- c) Se debe verificar con el proveedor los requerimientos mínimos a nivel de hardware y software donde será instalado el aplicativo. Sólo se adquirirán las últimas versiones liberadas de los productos de software comerciales seleccionados, salvo situaciones específicas.
- d) Para los softwares por suscripción o como servicio se debe contar con la autorización del propietario del software o el contrato que avale el uso del mismo.
- e) Para el caso de los sistemas operativos que se utilicen en la Unidad para la Atención y Reparación Integral a las Víctimas, solo se podrán utilizar los que estén aprobados por la Oficina de Tecnologías de la Información.

13.2.4. Lineamientos para las aplicaciones

13.2.4.1. Lineamientos para las aplicaciones desarrolladas por proveedores y/o terceros

Cuando La Unidad para la Atención y Reparación Integral a las Víctimas adquiere un software con un subcontratista es obligatorio revisar las condiciones contractuales, para saber el alcance, entrega de documentación de arquitectura del sistema de información, entrega del servicio (mantenimiento y soporte), derechos patrimoniales y autorización a modificaciones futuras. Los sistemas de información adquiridos o desarrollados por terceros tienen que contar con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual del mismo.

13.2.4.2. Lineamientos para las aplicaciones propias

13.2.4.2.1. Lineamientos para las aplicaciones heredadas y/o donadas

Cualquier software heredado debe tener la licencia o soporte de transferencia del licenciamiento a La Unidad para la Atención y Reparación Integral a las Víctimas. En dicha licencia se debe indicar si es objeto de modificaciones el código transferido a la Entidad.

13.2.4.2.2. Lineamientos para las aplicaciones desarrolladas por la Entidad

- a) En caso de desarrollos propios de la Entidad se debe verificar la documentación entregada, se cuenten con artefactos de software y las versiones correspondientes para preservarlas en varios medios y se guarde copia de respaldo externa, así mismo deben estar registrados en la Dirección General de Derechos de Autor.

- b) La dirección, subdirección o proceso serán responsables de gestionar el registro en la entidad competente de la aplicación desarrollada para garantizar los derechos de propiedad intelectual y derechos de autor a nombre de La Unidad para la Atención y Reparación Integral a las Víctimas. Adicionalmente es necesario informar al Grupo de Seguridad de la Información y al proceso de gestión jurídica, dejando un registro como evidencia.
- c) Establecer en la contratación de desarrollo de software o aplicativo a la medida de las necesidades de la entidad, por lo cual el proveedor debe entregar el código fuente y documentación de todos los módulos, que permita a los funcionarios, contratistas y terceros realizar los ajustes en forma autónoma. Durante el periodo de garantía del software la Entidad no debe realizar modificaciones, contractualmente, ya que corresponden a las responsabilidades del proveedor.

13.2.5. Los sitios Web oficiales de La Unidad para la Atención y Reparación Integral a las Víctimas

Los funcionarios, contratistas y terceros responsables de la publicación de la información en los sitios WEB oficiales de la entidad, deben atender el cumplimiento de las normas en materia de propiedad intelectual.

La entidad se reserva el derecho de efectuar revisiones esporádicas al cumplimiento de las normas en materia de propiedad intelectual.

13.3. Protección de registros

13.4. Privacidad y protección de los datos personales

- La Unidad para la Atención y Reparación Integral a las Víctimas, en ejercicio de las facultades legales, en especial las conferidas por la Ley 489 de 1998, la Ley 1448 de 2011, Ley 1581 de 2015, y los Decretos 4802 de 2011 y 1083 de 2015, 1074 de 2015 y demás normas concordantes, establece las políticas de privacidad y protección de datos personales, con el propósito de determinar las directrices del tratamiento de los datos personales asociados a su responsable, procedimiento y finalidad, en el marco de las funciones de la Entidad, considerando:
- Que la Constitución Política de Colombia contempla en su artículo 20 el derecho fundamental de acceso a la información; y en su artículo 15, los derechos y garantías a quienes ostentan la titularidad de dicha información, como, la protección a la intimidad personal y familiar, al buen nombre, y a conocer, actualizar y rectificar la información que sobre ellas se haya recolectado,



almacenado, o haya sido objeto de uso, circulación o supresión de las bases de datos y archivos de entidades públicas y privadas.

- Que en desarrollo del artículo 15 de la Constitución Política se expidió la Ley 1581 de 2012 por medio de la cual se establece los principios y disposiciones aplicables al tratamiento de datos personales que se encuentren registrados en cualquier base de datos de entidades tanto de carácter público como privado; la cual fue reglamentada por el Decreto 1074 de 2015.
- Que en el literal f) del artículo 18 de la mencionada normativa se establece como deber de los responsables y encargados del tratamiento de datos, adoptar el manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley, y en especial para la atención de consultas y reclamos por parte de los titulares de los datos personales.
- Que para el tratamiento de los datos personales suministrados por el titular de la información debe contarse con la autorización o consentimiento expreso del titular de conformidad con lo establecido por el artículo 3 de la Ley 1581 de 2012 y el principio de libertad consagrado en la misma disposición. No obstante, dicha autorización no es necesaria para el tratamiento de los datos cuando se trate Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial, datos de naturaleza pública, casos de urgencia médica o sanitaria, tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos y datos relacionados con el Registro Civil de las Personas.
- Que la Ley 1712 de 2014 de transparencia y regulación del derecho de acceso a la información pública nacional, contempla nuevos principios, conceptos y procedimientos para el ejercicio y garantía del referido derecho.
-
- Que el artículo 30 de la Ley 489 de 1998, determina que la función administrativa se desarrolla conforme a los principios constitucionales en particular los atinentes a la buena fe, igualdad, moralidad, celeridad, economía, imparcialidad, eficacia, eficiencia, participación, publicidad, responsabilidad y transparencia.
- Que mediante el artículo 166 de la Ley 1448 de 2011 se crea la Unidad de Atención y Reparación Integral a las Víctimas como una Unidad Administrativa Especial con personería jurídica y autonomía administrativa y patrimonial, y el Decreto 1084 de 2011 la adscribe al Departamento para la Prosperidad Social, y tiene como propósito establecer las medidas judiciales, administrativas, sociales y económicas, individuales y colectivas, para garantizar la reparación integral de las víctimas y hacer posible el goce efectivo de sus derechos.
- Que para dar aplicación a la Ley 1581 de 2012 y su Decreto Reglamentario 1074 de 2015, “Por la cual se dictan disposiciones generales para la protección de datos personales.”, expedidos



por el Gobierno Nacional, La Unidad para la Atención y Reparación Integral a las Víctimas, viene implementado el Sistema de Integrado de Gestión para dar cumplimiento a lo estipulado en dicha normativa.

- Que mediante la Resolución 0893 del 2 de septiembre de 2013, se adoptó el “Sistema Integrado de Gestión en la Unidad para la Atención y Reparación Integral a las Víctimas” la cual involucra los requerimientos del Sistema de Gestión de Calidad bajo la norma NTCGP 1000:2009 y cualquier otro modelo de excelencia que asuma la Entidad, por lo que se hace necesario adoptar la Política de tratamiento de datos personales de la Unidad para las Víctimas.
- Que la Unidad para la Atención y Reparación Integral a las Víctimas como entidad de naturaleza pública, encargada de la ejecución e implementación de la política pública para víctimas y garante de la protección de derechos fundamentales de Habeas Data, a la intimidad y el acceso a la información, es la responsable del tratamiento de los datos personales que en el ejercicio de su actividad deban ser recolectados, almacenados, o para uso, transferencia, circulación y supresión, razón por la cual, en cumplimiento de la normativa vigente se adopta las políticas para el tratamiento de datos personales.

Lineamientos:

- a) Ley 1581 de 2012 y el Decreto 1377 de 2013.
- b) Ley 489 de 1998, la Ley 1448 de 2011.
- c) los Decretos No. 4802 de 2011 y 1083 de 2015, 1074 de 2015 y demás normas concordantes,

13.5. Revisiones de seguridad de la información

Las revisiones del cumplimiento de los requisitos de seguridad de la información se realizan a través de las auditorías internas del sistema integrado de gestión de La Unidad para la Atención y Reparación Integral a las Víctimas o evaluaciones de la Oficina de Control Interno.

DEFINICIONES Y TÉRMINOS

Atributo: Es la descripción de una característica que un sistema de información o componente de software debe tener durante su despliegue, uso o evolución. Dicha descripción debe ser lo suficientemente precisa para poder establecer de manera no ambigua si realmente un sistema de información o componente de software la cumple.

Análisis: Se determinan los elementos que intervienen en el sistema a desarrollar, su estructura, relaciones, evolución temporal, funcionalidades y qué comportamiento tendrá.

Arquitectura de sistemas de información: Incluye la descripción detallada de cada una de los sistemas de información y las relaciones entre ellos. Cada sistema de información debe contar con una ficha técnica que los describa.

Calidad del software: Es el grado con el que un sistema, componente o proceso cumple los requerimientos especificados y las necesidades o expectativas del cliente o usuario.

Capacidad de Prueba: Es la medida de la facilidad con la que el software, al ser sometido a una serie de pruebas, puede demostrar sus fallas.

Ciclo de vida del software: Un modelo de ciclo de vida software es cualquier caracterización descriptiva de la evolución del software. Es sencillo articular un modelo de ciclo de vida que indique cómo deben ser desarrollados los sistemas software.

Compleitud: Se refiere a datos que de acuerdo con un conjunto particular se han dejado vacíos o con valores predeterminados.

Conformidad: Valores de datos de un tipo similar que han sido introducidos de forma confusa o inutilizables.

Consistencia: Aparición de tipos dispares de registros de datos en un conjunto de datos creado para un solo tipo de datos.

Dato: Representación simbólica (numérica, alfabética, algorítmica) de un atributo o variable cuantitativa.

Desempeño: Nivel en el cual un sistema o componente cumple con su funcionalidad dentro de ciertas restricciones dadas como velocidad, exactitud, uso de memoria y capacidad de respuesta.

Duplicidad: Se refiere a los datos que se encuentran de manera repetitiva en un conjunto de datos con información significativa en común.

Exactitud: Precisión de los datos en un conjunto determinado, esto puede hacer referencia a una fecha o fuente de referencia.

Información: La información se compone de un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente; esta a su vez permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.

Integridad: Corresponde a las características comunes de datos y su estado de corrección y completitud de estos.

Metadato: Datos altamente estructurados que describen información, contenido, calidad, condición y otras características de los datos.

Pruebas funcionales: Aquellas evaluaciones que se realizan sobre la ejecución de funcionalidades del sistema, verificando la existencia de errores, defectos o fallas en la solución software comparándola frente a los requerimientos funcionales.

Pruebas no funcionales: Aquellas evaluaciones que se realizan sobre los elementos que están presentes en los resultados de la ejecución de funcionalidades del sistema.

Plataforma de Interoperabilidad: Es el conjunto de herramientas necesarias para que los sistemas de información del Estado conversen entre sí. Integra los diferentes servicios y trámites prestados por el Estado. Se compone de: 1) Lenguaje común para el intercambio de información entre aplicaciones, y, 2) tramitador en Línea que procesa la información al controlar y regular la interoperabilidad.

Marco de Interoperabilidad: Conjunto de elementos que orientan el intercambio de información a nivel público y está constituido por: principios, políticas, un modelo de administración, un modelo de madurez, un modelo de medición, un conjunto de recomendaciones, protocolos, estándares y guías metodológicas.

Métricas: Medida efectuada sobre programas, documentación que permite comparar con unos valores de referencia obtener conclusiones para tomar decisiones sobre un tema en concreto.

Servicio de intercambio de información: Mecanismo para intercambiar información a través de un medio de transmisión electrónico, magnético o telemático.

Sistema: Conjunto de partes o elementos organizados y relacionados que interactúan entre sí con el fin de lograr un objetivo. Estos consisten en una entrada y una salida.



Verificación de software: Técnica y actividad ligada al control de calidad del software se trata de comprobar si los productos construidos en una fase de ciclo de vida satisfacen los requisitos establecidos en una fase anterior y/o si el software construido satisface los requisitos del usuario.

Acuerdos de Niveles de servicio: El modelo de Acuerdo de Nivel de Servicios consiste en un contrato en el que se estipulan los niveles de un servicio en función de una serie de parámetros objetivos, establecidos de mutuo acuerdo entre ambas partes, así, refleja contractualmente el nivel operativo de funcionamiento, penalizaciones por caída de servicio, limitación de responsabilidad por no servicio, etc. En esta parte del contrato se describe y obliga a un nivel específico de calidad en el suministro. Los puntos que debe cubrir un acuerdo de niveles de servicio son: servicio, soporte a clientes y asistencia, provisiones para seguridad y datos, Garantías del sistema y tiempos de respuesta, disponibilidad entre otros.

Activo: En seguridad de la información se refiere a la información que tenga valor para la organización y a los elementos relacionados con la misma, como por ejemplo sistemas, elementos de hardware, personas e instalaciones.

Análisis de vulnerabilidad: Es la medida o grado de debilidad de ser afectado por amenazas o riesgo según la frecuencia y severidad de los mismos. La vulnerabilidad depende de varios factores, entre otros: La posibilidad de ocurrencia del evento, la frecuencia de ocurrencia de este, los planes y programas preventivos existentes, la posibilidad de programación anual entre otros.

Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Casos de prueba: Son los escenarios o condiciones con las cuales se evidencia y revisa si un requisito de un sistema de información o aplicación está implementado satisfactoriamente.

Cifrado: Es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

Confiabilidad de la Información: Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Confidencialidad: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Contrato: Acuerdo, generalmente escrito, por el que dos o más partes se comprometen recíprocamente a respetar y cumplir una serie de condiciones.

Criptografía: El objetivo de la criptografía es diseñar, implementar, implantar, y hacer uso de sistemas criptográficos para dotar de alguna forma de seguridad.

Hacking - Hackear: Es el ingreso ilegal a computadores, páginas y redes sociales con el objetivo de robar información, suplantar la identidad del dueño, beneficiarse económicamente o protestar.¹

Hacking Ético: Es en sí una auditoría efectuada por profesionales de seguridad de la información, quienes reciben el nombre de “pentester”. A la actividad que realizan se le conoce como “hacking ético” o “pruebas de penetración”.²

Información pública. “Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal”. (Ley 1712 de 2014)

Información pública clasificada. “Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley”. (Ley 1712 de 2014)

Información pública reservada. “Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley”. (Ley 1712 de 2014)

Derecho a la intimidad: “El derecho a la intimidad implica la facultad de exigir de los demás el respeto de un ámbito exclusivo que incumbe solamente al individuo, que es resguardo de sus posesiones privadas, de sus propios gustos y de aquellas conductas o actitudes personalísimas que no está dispuesto a exhibir, y en el que no caben legítimamente las intromisiones externas. Algunos tratadistas han definido este derecho como el ‘control sobre la información que nos concierne’” (Sentencia C-913/10 - Sala Plena de la Corte Constitucional)

Desarrollo de software: Proceso continuo, ordenado en fases y ejecutado en el tiempo, que permite la publicación de sistemas de información en ambiente de producción.

Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

¹ <http://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html>

² <https://revista.seguridad.unam.mx/numero-12/hacking-%C3%A9tico-mitos-y-realidades>

Dispositivos cifrados: Medio de almacenamiento removable con un mecanismo de seguridad el cual permite cifrar la información almacenada, de la tal forma que, en caso de interceptación o robo, se mitigue el riesgo de divulgación no autorizada de información ya que la información no es legible sin la correspondiente clave o llave de acceso.

Dispositivos removibles: son unidades de almacenamiento independientes del computador y que pueden ser transportados libremente. Los dispositivos de almacenamiento que se contemplan en este procedimiento son: memorias USB, discos duros extraíbles y discos cifrados.

Ejemplo de Riesgo de Seguridad de la Información : Fuga, revelación o divulgación de información sensible y/o confidencial de la Entidad, debido al acceso a sistemas de información por parte de usuarios no autorizados por uso inadecuado de credenciales de acceso y/o equipo de cómputo de usuarios legítimos del sistema de información.

Evaluación de Riesgos: Evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operación de la entidad.

Incidente de Seguridad: Es un evento adverso en el sistema o la red que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas y en cualquier medio, ya sea digital, en papel, en pantallas de computadoras u otro.

Integridad: Salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Impacto: Acción directa de una amenaza o riesgo en un grupo de personas.

Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el sistema de información.

Mitigación: Acciones desarrolladas antes, durante y después de un siniestro, tendientes a contrarrestar sus efectos críticos y asegurar la supervivencia del sistema, hasta tanto se efectúe la recuperación.

No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.



Ofuscación: En [computación](#), la ofuscación se refiere al acto deliberado de realizar un cambio no destructivo, ya sea en el [código fuente](#) de un [programa informático](#) o [código máquina](#) cuando el programa está en forma [compilada](#) o binaria, con el fin de que no sea fácil de entender o leer.³

PJEE: Un conjunto de reglas a seguir relacionadas a seguridad, que usa la encriptación de datos para realizar conexiones seguras entre el usuario a través de su navegador de internet y el servidor de Cibercolegios.com, de modo que la transmisión de datos entre uno y el otro se produzca con la seguridad y privacidad necesaria.⁴

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de Gobierno en línea versión 2012 la correlativa obligación de proteger dicha información en observancia del marco legal vigente.⁵

Propietario de Información: unidad organizacional o proceso donde se crean los activos de información.

Protección a la duplicación: consiste en asegurar que una transacción es única, a menos que se especifique lo contrario.

Requerimiento: Es una característica que el sistema debe tener o es una restricción que el sistema debe cumplir para satisfacer las necesidades del solicitante.

Responsable por el activo de Información: es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

Resguardo: Medio por el cual se protege la información, para garantizar la confidencialidad, integridad y disponibilidad de la información y los activos.

Responsable de Seguridad de la Información: Es la persona con la función de supervisar el cumplimiento de la presente Política.

³ <https://es.wikipedia.org/wiki/Ofuscaci%C3%B3n>

⁴ <http://www.cibercolegios.co/certificados-de-seguridad/>

⁵ Fuente de definiciones, Modelo de seguridad y privacidad de la información MINTIC.



Responsable de la administración del activo: funcionario asignado por el proceso de almacén e inventarios, para la custodia y administración de dispositivos removibles, quien está autorizado para su asignación o préstamo a funcionarios y contratistas de la Entidad.

Riesgo de Seguridad de la Información: Es el potencial de que una amenaza pueda explotar una vulnerabilidad de un activo de información afectando la operación o imagen de la Entidad.

Para reconocer los riesgos sobre los activos de información de la Unidad para la Atención y Reparación Integral a las Víctimas, se deben determinar las vulnerabilidades y amenazas que pueden afectar la integridad, confidencialidad y disponibilidad de cada activo de información; las amenazas son generadoras de eventos que ocurren, y las vulnerabilidades son las debilidades inherentes al activo.

Seguridad de la Información: Son todas aquellas medidas preventivas de los sistemas de información que permitan resguardar y proteger la información.

SNARIV: Es el Sistema Nacional de Atención y Reparación Integral a las Víctimas, está constituido por el conjunto de entidades públicas del nivel gubernamental y estatal en los órdenes nacional y territoriales y demás organizaciones públicas o privadas, encargadas de formular o ejecutar los planes, programas, proyectos y acciones específicas, que tiendan a la atención y reparación integral de las víctimas.⁶

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

Validación: Se realiza al comparar si el resultado de las pruebas de usuario es correcto.

Verificación: Se realiza al comparar si el resultado de las pruebas internas es correcto, frente a la solicitud inicial.

⁶ <http://www.unidadvictimas.gov.co/es/gestion-interinstitucional/sistema-nacional-de-atencion-y-reparacion-integral-las-victimas/77>



ANEXO 7

Mapa de Riesgos

Proceso Gestión de la Información

OBJETIVO DEL PROCESO: Gestionar los servicios, gobierno y capacidad tecnológica que soporta la operación y las necesidades de la Unidad frente a las tecnologías de la información y articular a las entidades que conforman la red nacional de información para facilitar el flujo eficiente de información que permita realizar el seguimiento a la implementación

No	Proceso	Riesgo	IDENTIFICACION				RIESGO INHERENTE			CONTROLES		
			Causas	Consecuencias	Tipo de Riesgo	Probabilidad	Impacto	Nivel riesgo	Zona de Riesgo	Descripción	Correctivo- Impacto Preventivo- Probab.	Calificación De 0 a 50 = 0 De 51 a 75=1 De 76 a 100 = 2
1	GESTION DE LA INFORMACION	Indisponibilidad de soporte e infraestructura tecnológica para el personal y los procesos de la Unidad	Retrasos en la entrega de soluciones, recursos y/o servicios por parte de terceros, asociados a dotación tecnológica, conectividad y centro de datos	Operativa	Gestión/operativo	5	5	25	Extrema	El personal que apoya el seguimiento a los servicios y recursos tecnológicos que brinda la OTI, realiza un seguimiento mensual a la capacidad de las diferentes líneas de servicio al cierre del mes, tomando acciones preventivas o correctivas para controlar la infraestructura tecnológica, lo cual se evidencia en los instrumentos de seguimiento por línea, en las alertas tempranas a la dirección y acciones establecidas si aplica.	Preventivo	70
			Falta de unificación en controles y protocolos de acceso en la administración de los edificios que limitan los horarios de ingreso, permisos, logística, para la entrega de la dotación tecnológica y de soporte técnico	Afectación en la credibilidad o imagen						La supervisión de los servicios de Tecnología a través de proveedores TI, realiza un seguimiento mensual a los acuerdos de niveles de servicio (ANS) establecidos en los contratos al cierre del periodo, validando que el servicio recibido se encuentra dentro de los ANS establecidos; en caso de estar fuera de los rangos se aplican descuentos al valor facturado, lo que se evidencia en los pagos.	Correctivo	90
			Fallas en la prestación de servicios y recursos tecnológicos brindados por terceros que no están bajo el control de la OTI en los puntos de atención a víctimas.	Legal						El enlace de plan de acción y el equipo de soporte tecnológico, realiza un seguimiento mensual, la semana siguiente al cierre del mes, donde se establece el porcentaje de cierre de soportes tecnológico oportunos frente a las diferentes líneas de servicio, el cual debe ser igual o superior al 92%, y en caso de que la tendencia sea a disminuir ese porcentaje se envían alertas a los responsables previo al cierre del mes, cuya evidencia esta asociada a la matriz de seguimiento mensual y a los correos con alertas si aplica	Preventivo	90
			Superar el límite de recursos establecidos según las proyecciones OTI							Los líderes de las líneas de servicio de infraestructura y soporte tecnológico han establecido procedimientos independientes, los cuales son actualizados según se establece en el marco de la implementación del Sistema Integrado de Gestión o cuando se considera pertinente, lo cual brinda mayor claridad al usuario solicitante para que acceda a los diferentes recursos y servicios de TI, dejando como evidencia los registros identificados en cada uno de los procedimientos.	Preventivo	85
			Deficiencias en cuanto a los constantes cambios y ajustes en el plan anual de adquisiciones, que presentan reprocesos en la gestión de recursos financieros							La líder de soporte tecnológico gestiona la ejecución de un mantenimiento preventivo anual a los equipos de computo de la Unidad, el cual se ejecuta en los meses de junio a julio, lo que permite prevenir fallas en los equipos, de manera que se desplaza un técnico de soporte y realiza el mantenimiento en sitio de cada equipo, dejando como evidencia la firma de un acta por persona.	Preventivo	70
			Recortes presupuestales no contemplados durante la ejecución de la vigencia							El enlace SIG de la OTI apoyado por @s líderes de las líneas de servicio de infraestructura y soporte tecnológico, realiza la identificación, recolección de evidencia, descripción según la norma, cargue y levantamiento de no conformidades a los procesos que hacen uso inadecuado de los recursos y servicios tecnológicos, con una frecuencia variable dependiendo de que se presente dicha situación, con el fin de concientizar a los procesos frente al correcto uso del recurso o servicio TI y evitar que se presente de nuevo, dejando como evidencia los soportes para el levantamiento y el cargue de la no conformidad en la herramienta y su aprobación por parte del enlace de la OAP.	Correctivo	85
			Incumplimiento e inoportunidad en la ejecución de procedimientos transversales tales como viáticos, contratación, contratación de personal para la vigencia, pagos, entre otros.									
			Ajustes no contemplados inicialmente, solicitados por cambios a nivel directivo y/o de gobierno que impactan la planificación presupuestal inicial.									
			Retrasos o reprocesos en las actividades planificadas generadas por los cambios de gobierno									
			Incertidumbre por cambios de gobierno en cuanto a modificaciones en los objetivos o fines perseguidos por la Unidad, ajustes en los equipos de trabajo y sus líderes (CIO), planes, programas y proyectos.									
Inconvenientes en el entorno (fallas energía, terremotos, incendios, bloqueos, etc.)												
Retraso por encolamiento para atender solicitudes de soporte tecnológico												
Retraso en la disponibilidad de recursos financieros debido a procesos administrativos												
Inadecuada percepción frente a la atención al cliente de la mesa de servicios tecnológicos												
Falla en la comunicación de la toma de decisiones de nivel estratégico que no fluye hacia el nivel táctico y no se divulga oportunamente, que implica modificaciones y/o ajustes en proyectos/contratos												
Debilidades frente a la sensibilización y conocimiento de TI a nivel nacional y territorial.												
Desconocimiento y debilidades de los procesos que realizan contrataciones TI sin asesoramiento de la Oficina de Tecnologías de la Información												
Las contrataciones de necesidades tecnológicas no cubiertas aún en los acuerdos marco de precios (AMP), que generan otros tipos de selección de contratación, que implican un esfuerzo administrativo y técnico (análisis técnico, análisis del sector, análisis financiero) del personal que apoya estos procesos												

2	GESTION DE LA INFORMACION	Incumplimiento en la entrega de desarrollo y/o soporte de sistemas de información	Incumplimiento e inoportunidad en la ejecución de procedimientos transversales tales como contratación, contratación de personal para la vigencia, pagos, entre otros.	Operativa	Gestión/operativo	5	5	25	Extrema	El personal que realiza el desarrollo y soporte de sistemas de información que brinda la OTI, realiza el reporte de actividades en las herramientas establecidas mensualmente, tomando acciones puntuales en caso de desviaciones para dar cumplimiento a los procedimientos, lo cual se evidencia en las matrices de seguimiento de soporte y de desarrollo y soportes de las acciones establecidas si aplica.	Correctivo	90
			Fallas en la asignación a la OTI de tareas y actividades que no son de su competencia por la falta de claridad de los líderes de los procesos frente a los límites establecidos en las funciones asignadas a su cargo según el decreto 4802	Afectación en la credi						Preventivo	85	
			Falta de congruencia de los procesos de la Unidad frente a los límites establecidos en las funciones asignadas a su cargo según el decreto 4802, en el establecimiento de la interacción real entre procesos y la ejecución de sus procedimientos.	Legal						Preventivo	90	
			Falta de claridad de los requerimientos funcionales frente a las solicitudes.							Correctivo	85	
			Debilidades en cuanto a la segmentación de equipos de desarrollo distribuidos en las diferentes áreas dificultando tareas de alineación, control e integración de información y funcionalidades							Preventivo	75	
			Falta de formalización o actualización en el SGC de algunos procesos o procedimientos que al requerir su automatización provocan una alta cantidad de cambios a voluntad del usuario solicitante respecto al requerimiento inicial que impacta el alcance, tiempo y recursos en el desarrollo									
			Deficiencias en cuanto a los constantes cambios y ajustes en el plan anual de adquisiciones, que presentan reprocesos en la gestión de recursos financieros.									
			Incertidumbre por cambios de gobierno en cuanto a modificaciones en los objetivos o fines perseguidos por la Unidad, ajustes en los equipos de trabajo y sus líderes (CIO), planes, programas y proyectos.									
			Inadecuada ejecución del procedimiento de desarrollo y/o de soporte que genera sobrecarga de soporte de aplicativos o generación de nuevos desarrollos y/o funcionalidades									
			Insuficiente recurso humano para el desarrollo o Rotación de personal a cargo de desarrollo o soporte									
			Infraestructura de hardware y software insuficiente									
			Incumplimiento de terceros en caso de que exista un proceso contractual frente al sistema de información									
			Retrasos en la ejecución del procedimiento de soporte									
			Debilidad en el desarrollo e implementación de políticas para gestión y gobernabilidad de TI.									
			Fallas en las contrataciones TI asociadas a sistemas de información donde los procesos no solicitan asesoramiento a la Oficina de Tecnologías de la Información									
Falla en la comunicación de la toma de decisiones de nivel estratégico que no fluye hacia el nivel táctico y no se divulga oportunamente, que implica modificaciones y/o ajustes en proyectos/contratos asociados a sistemas de información												
Fallas en la prestación de servicios y recursos tecnológicos brindados por terceros que no están bajo el control de la OTI en los puntos de atención a víctimas.												
Dependencia de sistemas de información no desarrollados por OTI y/o de la calidad de información de los datos necesarios para que el sistema entre en operación												

3	GESTION DE LA INFORMACION	Dificultad para generar los insumos que den respuesta a las solicitudes de información remitidas por los clientes internos y/o externos	Ausencia de intercambio de información con las entidades de las cuales se requiere información	Operativa	Gestión/operativo	4	16	Extrema	Los líderes de los grupos de trabajo internos de la SRNI, por demanda realiza la identificación de necesidades de Información, teniendo como base solicitudes de información internas o externas o basados en el historico, la evidencia de este control puede ser correo electronico con la identificación de la necesidad o acta o lista de asistencia de reunión.	Preventivo	85
			Las fuentes de información dispuestas en la RNI, no cubren las necesidades y requerimientos que permitan generar los insumos solicitados.	Legal					El profesional de alistamiento, cada vez que se reciba una fuente, realiza una validación de la misma, en particular para las mediciones de Subsistencia Mínima, Superación de Situación de Vulnerabilidad e Indicadores de Goce Efectivo de Derechos, de acuerdo a los mínimos requeridos. El soporte de este control es la aprobación del metadato en el inventario de fuentes.	Correctivo	85
			Falta de infraestructura tecnológica adecuada y disponible, y exceso en los tiempos y/o requisitos para la formalización de los acuerdos y/o convenios	Afectación en la credi					El grupo Articulación y fortalecimiento, 2 veces en el año, realiza una mesa de trabajo con las entidades del SNARIV en el marco del Subcomité de Sistemas de Información, para identificar fuentes que puedan ser útiles, en particular para mediciones de Indicador de Goce Efectivo de Derecho - IGED en cumplimiento de lo ordenado en los autos, el soporte de este control es el acta y lista de asistencia de esta mesa	Preventivo	70
			Falta de intercambio de información en tiempo real con algunas entidades con las que se tiene acuerdo o convenio, por lo que la información se desactualiza rápidamente y falta de disposición de la información acordada entre la Unidad y las entidades						El procedimiento de Articulación y fortalecimiento, mensualmente verifica de manera aleatoria el cumplimiento de lo establecido en los acuerdos y/o convenios entre la Unidad y las Entidades. En caso de incumplimiento, se notifica a la entidad respectiva y queda evidencia de lo anterior el envío del correo electrónico.	Preventivo	70
			Desconocimiento de la información respecto a la asistencia, atención y reparación que han recibido las víctimas por parte de las entidades que conforman el SNARIV.						El colaborador encargado de la creación de usuarios, tres veces en el año, realizará socialización acerca de la creación de usuarios, uso y manejo de la herramienta vivanto, al equipo de la SRNI de Articulación y fortalecimiento territorial y nacional, la evidencia queda soportada mediante acta y lista de asistencia	Correctivo	85
4	GESTION DE LA INFORMACION	Entregar información inexacta o inconsistente o incompleta al cliente interno y/o externo	Fallas en la recolección de la información por parte de la fuente	Operativa	Gestión/operativo	4	12	Alta	El grupo de Articulación y fortalecimiento, cada vez que se oficializa el acuerdo de intercambio de información, genera un anexo técnico al anterior documento donde se encuentran las reglas que rigen el intercambio, acompañado del diccionario de datos, que es el insumo para el entendimiento de la fuente, para las entidades que no aplican documento técnico esta información queda en un oficio. El soporte de este control es el documento técnico anexo al acuerdo o el oficio.	Preventivo	85
			Cambios no autorizados de la información en el origen	Legal					El grupo alistamiento de la información, cada vez que recibe una fuente, la dispone en un esquema de base de datos sobre ORACLE, conservando la estructura y el dato original, así mismo se realiza el registro en la herramienta inventarios con el fin de conocer la fecha en que se hizo el cargue de la misma. el soporte de este control es el registro en la herramienta inventarios	Preventivo	90
			Perdida o deterioro de la información que imposibilita su acceso	Afectación en la credi							0
			Acceso abusivo a la información antes de ser procesada								0
			La información de los sistemas de información internos tienen deficiencias en la calidad de los datos que se generan y que se utiliza como insumo para la gestión								0

5	GESTION DE LA INFORMACION	Pérdida parcial o total de la Confidencialidad, integridad y/o Disponibilidad de los sistemas de información y/o la información registrada en documento físico o digital como consecuencia de: - Acciones involuntarias y/o deliberadas de usuario y/o - Vandalismo o hurto Debido a: (Ver columna Causas)	Almacenamiento de información sin protección	Operativa	Seguridad de la información	4	4	16	Extrema	El equipo de soporte técnico de la Oficina de Tecnologías de la Información, cuenta con el servicio de mesa de servicios tecnológicos, donde los usuarios pueden solicitar y/o enviar su caso y el equipo de soporte técnico de la mesa de servicio según sea el caso, realiza la gestión sobre él o lo escala, teniendo en cuenta la clasificación y ANS, La evidencia que se genera son los indicadores mensuales en mesa de servicio.	Correctivo	90
			Ausencia de mecanismos de monitoreo a la actividad de los empleados y/o terceros.	Legal						El equipo de soporte técnico de la Oficina de Tecnologías de la Información, realiza la instalación del software según sea el caso teniendo en cuenta el licenciamiento autorizado por esta oficina. La evidencia que se genera son los tickets en mesa de servicio.	Preventivo	85
			Ausencia de mecanismos de monitoreo a la actividad de los empleados y/o terceros.	Disciplinaria						El equipo de infraestructura realiza el monitoreo frecuente de la capacidad disponible de almacenamiento en servidores de aplicación, bases de datos y File Servers, así como de los canales de conectividad, a través de las herramientas establecidas para tal fin. En caso de identificar la necesidad de mejorar la capacidad del recurso tecnológico, se realiza la correspondiente solicitud al proveedor. La evidencia es la operación de la herramienta para el monitoreo en tiempo real de los servidores.	Preventivo	70
			Falla, daño o degradación de equipos.	Afectación en la credi						El equipo de soporte técnico de la Oficina de Tecnologías de la Información, gestiona junto con el proveedor de la dotación tecnológica, el mantenimiento preventivo de equipos de cómputo, mínimo una vez al año. La evidencia que se genera son las actas del mantenimiento.	Preventivo	70
			Ubicación geográfica de las instalaciones en una zona de alto impacto por eventos externos (desastres naturales, orden público, entre otros).							El equipo de soporte técnico de la Oficina de Tecnologías de la Información, cada vez que asigna un equipo de cómputo al usuario final, realiza la instalación de antivirus en cada máquina. La evidencia es el agente de antivirus instalado en cada máquina de usuario y/o informe de la herramienta EPO de McAfee.	Preventivo	90
			Acceso no controlado a información sensible / confidencial.							La Oficina de Tecnologías de la Información, cuenta de manera permanente con el servicio de centro de datos tercerizado que permite el almacenamiento de sistemas de información (aplicaciones y bases de datos). La evidencia corresponde a los informes de supervisión del contrato de centro de datos que se genera mensualmente	Preventivo	75
			Personal inconforme o molesto.							El equipo de infraestructura de la Oficina de Tecnologías de la Información, conforme a las políticas, implementa reglas de filtrado web para controlar el acceso a sitios Web indebidos con una frecuencia por demanda. La evidencia consiste en la configuración de las reglas en la herramienta tecnológica.	Preventivo	75
			Ausencia o insuficiencia de políticas, procedimientos y directrices de seguridad.							El equipo de seguridad y riesgo informático de la Oficina de Tecnologías de la Información, realiza el monitoreo de amenazas mensualmente, por medio de un análisis avanzado sobre los casos atípicos que se presenten con la cuenta de dominio asignada por la entidad a los usuarios. La evidencia consiste en la matriz con los tickets de la mesa de servicios tecnológicos creados por parte del equipo de seguridad en función del resultado del análisis.	Preventivo	75
			Ausencia de registros de auditoría.							El colaborador de soporte RNI, cada vez que reportan el retiro de un funcionario de la Unidad o colaborador designado de una entidad, realiza la inactivación de las credenciales de acceso a los sistemas de información administrados por la SRNI, como evidencia queda el estado del usuario en el sistema como inactivo.	Preventivo	75
			Ausencia o insuficiencia de documentación de uso y/o administración.							El profesional de instrumentalización de la información, de acuerdo a la demanda, corre una consulta en la base de datos de las herramientas administradas por la SRNI, para verificar posibles fugas de información o pérdida de confidencialidad de la misma, como evidencia queda el reporte de consulta generado	Correctivo	75
			Ausencia o insuficiencia de procedimientos de Monitoreo de los recursos de procesamiento de información.									
			Arquitectura insegura de la red.									
			Puertos o servicios activos no requeridos.									
Documentación insuficiente o desactualizada.												

Pérdida de		Pérdida de		Pérdida de		Pérdida de		Pérdida de		Pérdida de		
6	GESTION DE LA INFORMACION	Confidencialidad y/o Disponibilidad e Integridad por hurto o daño de equipos y/o Unidades de almacenamiento extraíbles en los que se almacene información sensible en texto claro, es decir no cifrado, fuera de las instalaciones de la Entidad por	Ausencia o insuficiencia de procedimientos para el manejo información clasificada, fuera de las instalaciones	Operativa	Seguridad de la información	3	2	6	Moderada	El equipo de seguridad y Riesgo Informático de la Oficina de Tecnologías de la Información, dispone la solución de discos duros portables cifrados y su procedimiento, con una frecuencia que depende de la demanda de los usuarios, cómo evidencia se generan los registros del procedimiento.	Preventivo	90
			Ausencia o insuficiencia en el control de los activos que se encuentran fuera de las instalaciones	Legal						El equipo de Seguridad y Riesgo informático, dispone del servicio de cifrado de la información, gestionado por medio de la instalación de la herramienta Gpg4Win que sirve para generar la llaves públicas y privadas que permiten realizar el proceso de cifrado del emisor y del receptor en el proceso de transferencia de la información, con una periodicidad que depende de la demanda del servicio por parte de los usuarios. Cómo evidencia se cuenta con tickets de mesa de servicio con la que se gestiona la instalación del software.	Preventivo	75
			Almacenamiento de información sin protección, en medios de almacenamiento Extraíbles	Disciplinaria								
			Ausencia de mecanismos de monitoreo de los activos manejados por los empleados y/o terceros, fuera de las instalaciones de la Entidad	Afectación en la Integ								
		Hurto, fraude o sabotaje de equipos, medios, información o documentos.	Afectación en la credi									
7	GESTION DE LA INFORMACION	Pérdida de confidencialidad, integridad o disponibilidad ocasionada por la infiltración en el servidor, en el dispositivo de red y/o el sistema de información debido al acceso no autorizado como consecuencia de captura de credenciales transferidas en texto claro, durante el ingreso vía web. Activos: Servidores.	Transferencia y/o almacenamiento de información en texto claro.	Operativa	Seguridad de la información	3	3	9	Alta	El equipo de infraestructura de la Oficina de Tecnologías de la Información, implementa el control de acceso a servidores teniendo en cuenta las IPs autorizadas, según solicitud por demanda, que aplica únicamente a la necesidad del equipo de Sistemas de Información. Cómo evidencia se generan los registros del procedimiento establecido.	Preventivo	90
			Espionaje (intercepción, ingeniería social)	Afectación en la credi						El equipo de infraestructura de la Oficina de Tecnologías de la Información, por medio del firewall perimetral restringe el acceso a servidores, teniendo en cuenta los permisos autorizados, según solicitud por demanda, de acuerdo a la necesidad del equipo de Sistemas de Información e infraestructura. La evidencia es la solicitud que se diligencia al proveedor y su envío al Centro de datos.	Preventivo	75
				Disciplinaria								
				Legal								
8	GESTION DE LA INFORMACION	Pérdida de disponibilidad y/o integridad en ambiente productivo en el sistema al presentarse errores durante la ejecución de modificaciones debido a la falta definición, aplicación u omisión de alguna de las actividades del procedimiento de gestión de cambios.	Ausencia o insuficiencia de un proceso de análisis y tratamiento de riesgos.	Operativa	Seguridad de la información	3	3	9	Alta	El equipo de Sistemas de Información de la Oficina de Tecnologías de la Información, realiza el soporte a sistemas de información custodiados por esta oficina, cada vez que es requerido. Cómo evidencia se generan los registros del procedimiento establecido.	Preventivo	90
			Ausencia o insuficiencia de políticas, procedimientos y directrices de seguridad.	Legal						El equipo de Sistemas de Información de la Oficina de Tecnologías de la Información, cuenta con una herramienta para el versionamiento del código fuente de sistemas de información administrados por esta oficina. El versionamiento es de manera permanente y la evidencia de este procedimiento se encuentra en la correspondiente herramienta.	Preventivo	90
			Testeo inadecuado o insuficiente.	Afectación en la credi								
			Falta o ausencia del protocolo o procedimiento para la gestión de cambios									

9	GESTION DE LA INFORMACION	<p>Pérdida de disponibilidad, integridad y/o confidencialidad en el sistema de información debido a ausencia o insuficiencia de copias de respaldo; o debido a vulnerabilidades no corregidas explotadas y/o falta de protección por código malicioso.</p>	Ausencia o insuficiencia de copias de respaldo.	Operativa	Seguridad de la información	3	3	9	Alta	El equipo de Infraestructura de la Oficina de Tecnologías de la Información, genera las copias de respaldo de servidores de aplicación y bases de datos, de manera diaria, con retención de 5 días. Este procedimiento se evidencia en los logs que se generan al realizar el respaldo de la información	Preventivo	70
			Ausencia o insuficiencia de mantenimiento.							El equipo de soporte técnico de la Oficina de Tecnologías de la Información, cada vez que asigna un equipo de cómputo al usuario final, realiza la instalación de antivirus en cada máquina. La evidencia es el agente de antivirus instalado en cada máquina de usuario y/o informe de la herramienta EPO de McAfee.	Preventivo	90
			Ausencia o insuficiencia de actualizaciones.							El equipo de infraestructura de la Oficina de Tecnologías de la Información, conforme a las políticas, implementa reglas de filtrado web para controlar el acceso a sitios Web indebidos. La evidencia consiste en las reglas configuradas en la herramienta tecnológica.	Preventivo	75
			Falta de protección contra virus y/o código malicioso.									
			Ausencia o insuficiencia de documentación de uso y/o administración.									
10	GESTION DE LA INFORMACION	<p>Pérdida de la confidencialidad de información física o digital debido a actividades de ingeniería social de un intruso que aproveche el desconocimiento de políticas, procedimientos y directrices de seguridad por parte de un colaborador, proveedor y/o terceras partes. *Información</p>	Ausencia o insuficiencia de políticas, procedimientos y directrices de seguridad.	Operativa	Seguridad de la información	3	3	9	Alta	El equipo de seguridad y Riesgo informático de la Oficina de Tecnologías de la Información, dispone la solución de discos duros portables cifrados, los cuales se pueden solicitar en cualquier momento a través de la mesa de servicios tecnológicos. El ticket que se genera en la mesa es la evidencia de la prestación del servicio.	Preventivo	85
			Insuficiente entrenamiento, capacitación o sensibilización.	Disciplinaria						El equipo de soporte técnico de la Oficina de Tecnologías de la Información, cuenta con el servicio de mesa de servicios tecnológicos, donde los usuarios pueden solicitar y/o enviar su caso y el equipo de soporte técnico de la mesa de servicio según sea el caso, realiza la gestión sobre él o lo escala, teniendo en cuenta la clasificación y ANS, La evidencia que se genera son los indicadores mensuales en mesa de servicio.	Correctivo	90
			Ausencia de control de los activos que se encuentran fuera de las instalaciones.	Operativa						El equipo de seguridad y Riesgo Informático, genera anualmente el plan de socialización de políticas, lineamientos y mejores prácticas relacionadas con seguridad de la información, orientado a funcionarios y contratistas de la Entidad	Preventivo	55
			Acceso no controlado a información sensible / confidencial.	Operativa								

OBJETIVO DEL PROCESO: Gestionar los servicios, gobierno y capacidad tecnológica que soporta la operación y las necesidades de la Unidad frente a las tecnologías de la información y articular a las entidades que conforman la red nacional de información para facilitar el flujo eficiente de información que permita realizar el seguimiento a la implementación de la política pública para apoyar el c

No	Proceso	Riesgo	IDENTIFICACION				RIESGO				CONTROLES				RIESGO RESIDUAL			
			Causas	Consecuencias	Tipo de riesgo		Probabilidad	Impacto	Nivel Riesgo	Zona de Riesgo	Descripción	Correctivo o Preventivo	Calificación	Probabilidad	Impacto	Nivel Riesgo	Zona de Riesgo	
1	GESTION DE LA INFORMACION	Modificación o extracción de la Información alojada en los servidores o bases de datos asociada a las víctimas, para obtener un beneficio personal o para un tercero	Sistemas de información vulnerables de manipulación o adulteración	Afectación en la credibilidad	Riesgos de corrupción	2	20	40	ALTA	El equipo de sistemas de información implementan el control de acceso a aplicativos, mediante el uso de usuario y password en las aplicaciones de la Unidad cada vez que los usuarios ingresan a los aplicativos para los sistemas de información cuyo desarrollo esta a cargo de este equipo. La frecuencia de implementación es por demanda y su evidencia es la funcionalidad implementada en el sistema de información.	preventiva	60	1	5	5	BAJA		
			Falta de controles de acceso en los sistemas de información	Legal						El equipo de infraestructura implementa reglas de acceso a los servidores de aplicación y de bases de datos, mediante la configuración de firewall, cuya frecuencia depende de la configuración de un nuevo servidor para aplicación o base de datos.	preventiva	70						
			Carencia de validaciones y verificaciones de los procedimientos efectuados con la información	Disciplinaria						Cada administrador funcional de los sistemas de información es el responsable de la creación, modificación o inactivación de credenciales de acceso de usuarios del aplicativo a su cargo o en su defecto el autorizado delegado por parte de la Dirección General, con base en las solicitudes que reciba por parte de los líderes del proceso según lo establecido en el procedimiento de creación de usuarios. La frecuencia depende de la demanda de solicitudes, y como evidencia se cuenta con los registros de solicitudes de creación de usuario.	preventiva	90						
			Acceso no autorizado a servidores, servicios o aplicaciones y bases de datos							Implementación del procedimiento de acceso remoto a servidores y bases de datos, a cargo del equipo de infraestructura de la OTI, con una frecuencia que depende de la demanda de solicitudes, como evidencia se cuenta con los registros generados de su implementación.	preventiva	90						
			Selección y vinculación inadecuado del personal de la entidad							Establecimiento del procedimiento de gestión de incidentes de seguridad de la información, a cargo del equipo de seguridad de la información de la OTI, con el cual se atienden los casos presentados por la Unidad frente a los incidentes de seguridad de la información, tomando acciones preventivas o correctivas según el caso si aplica, este procedimiento se implementa con una frecuencia por demanda si se generan casos, dejando como evidencia los registros identificados en cada uno de los procedimientos.	correctiva	90						
			Inadecuada selección de roles a los usuarios por parte de los administradores funcionales de los sistemas de información															
			Compartir al personal ajeno a la entidad la clave y el usuario asignado a personal de la Unidad para el acceso a sistemas de información															
			Falta de implementación del procedimiento de administración del talento humano para el retiro de funcionarios o contratistas por parte del jefe o supervisor, frente a la desactivación de usuarios en sistemas de información una vez el usuario se desvincula de la entidad.															
			Inadecuada autorización por parte de supervisores para el uso de equipos de cómputo a terceros con acceso a información confidencial y a sistemas de información															
			Manejo inadecuado de la información por parte de usuarios legítimos (autorizados formalmente)															
Validaciones y controles periódicos y/o intermedios insuficientes por parte de los procesos misionales después de la firma de acuerdos de confidencialidad																		
Debilidades en cuanto al control de acceso a las instalaciones de la entidad.																		
Fallas en cuanto al acceso a copias no controladas de bases de datos y/o ambientes de pruebas por parte del personal con acceso a las mismas.																		
2	GESTION DE LA INFORMACION	Usar indebidamente la información dispuesta por la SRNI para obtener beneficios diferentes a lo establecido en la ley, protocolos y procedimientos, favoreciendo a terceros.	Falta de control en la salida de información desde la SRNI	Operativa	Riesgos de corrupción	3	5	15	MODERADA	El grupo de articulación, cada vez que se actualice el protocolo de solicitud de información a la SRNI en el marco del SIG, realiza la socialización sobre el mismo a los articuladores territoriales, como evidencia del control queda correo electrónico o acta o lista de asistencia.	preventiva	85	1	5	5	BAJA		
			Debilidad de controles para el acceso a los datos	Afectación en la credibilidad						La SRNI, cada vez que se presente, remite alertas sobre los eventos de uso o acceso indebido de la información al área correspondiente por medio de correo electrónico, quedando como evidencia el envío del mismo.	correctiva	70						
			Falta de implementación de certificados de seguridad al acceso a las herramientas	Legal						La SRNI, cada vez que un usuario requiere la creación de credenciales de acceso para la herramienta Vivanto o Caracterización, solicita el diligenciamiento y remisión del formato de aceptación de acuerdo de confidencialidad junto con el documento de identidad, en caso de no cumplir con estos documento no se tramita la solicitud. Como evidencia del control queda cargado el acuerdo de confidencialidad diligenciado y firmado, así como el documento de identidad en el aplicativo vivanto	preventiva	90						
			Suplantación de usuarios para el acceso a las herramientas															
3					Riesgos de corrupción						0					0		
										0								
										0								
										0								
4					Riesgos de corrupción						0					0		
										0								
										0								
										0								
5					Riesgos de corrupción						0					0		
										0								
										0								
										0								



CONTROL DE CAMBIOS					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	Luz Marina Galindo R.	Rosybel Hernández D.	Manuel E. Castillo G.	31-10-2018	Creación, revisión y aprobación

Anexo 8

Caracterización de usuarios

Caracterización de grupos de valor - LI.UA.02 Matriz de Interesados



Introducción

Aspectos generales

- Alcance
- Objetivos
- Metodología

Resultados

1. Usuarios Internos - Variables
 - Perfil profesional
 - Tipo de contratación
 - Herramientas y/o servicios utilizados
2. Usuarios Externos
 - 2.1. Población Víctima - Variables
 - Edad
 - Discapacidad
 - Etnia
 - Género
 - Región Geográfica
 - 2.2. Entidades Externas- Variables
 - Tipo de entidad: Snariv, No Snariv
 - Cobertura Geográfica: Nacional, Territorial
 - Sector: Pública, Privada, Mixta
 - Tamaño (Dispersión)
 - Sector del que depende
3. Estrategia
4. Bibliografía



Introducción

El ejercicio de caracterización de los grupos de valor surge de la necesidad de diseñar e implementar de manera más eficiente, la acción integral de la Unidad hacia sus usuarios. Para ello se hace indispensable identificar las características, necesidades, intereses, expectativas y preferencias de éstos.

Al identificar y profundizar en los anteriores aspectos, es posible hacer los ajustes necesarios a la oferta de productos y servicios de la Unidad, fortalecer la estrategia de comunicación entre la Unidad y los diferentes actores de acuerdo con sus particularidades y de esta manera, por un lado, lograr la optimización de las acciones hacia la calidad del servicio, responder y retroalimentar satisfactoriamente los requerimientos de la población objetivo y finalmente, lograr una participación enriquecedora de los grupos de valor frente a los objetivos de la Unidad.

En razón a que consideramos que es indispensable en primer lugar fortalecer el desempeño hacia el interior de la Unidad para así mejorar la oferta de productos y servicios hacia los grupos de usuarios externos, hemos decidido realizar la caracterización tanto de nuestros usuarios internos como de la población víctima que es nuestra razón de ser como Entidad, así como de las entidades del Sistema Nacional de Atención y Reparación Integral a las Víctimas-SNARIV, con la finalidad de mejorar de optimizar las herramientas y la calidad del servicio, para el logro de los objetivos de la Unidad y la satisfacción de la población usuaria.



Alcance

Usuarios internos a nivel nacional, Población Víctima a nivel nacional y entidades que componen el Sistema Nacional de Atención y Reparación Integral a las Víctimas (SNARIV).

Objetivos

Generales

Identificar las características, intereses, necesidades y clasificar en grupos con características afines la población víctima, las entidades que tanto SNARIV como no SNARIV que interactúan con la Unidad, y los usuarios internos con el fin de optimizar las estrategias de uso y apropiación de las herramientas que tienen a disposición.

Específicos

1. Segmentar los grupos de valor a partir de las variables identificadas.
2. Identificar las herramientas a las que tiene acceso cada grupo.
3. Gestionar acciones que permitan optimizar el conocimiento y uso de las herramientas que requiere cada grupo.
4. Proponer estrategias de comunicación para que los diferentes grupos conozcan y usen las herramientas que se pongan a su disposición.

Metodología

Se estableció una primera segmentación basada en los perfiles de los diferentes usuarios de los servicios y productos proporcionados por la Unidad, así:

1. **Internos a la Unidad:** grupos de valor y/o usuarios a quienes se les provee la infraestructura tecnológica (hardware y Software) para el correcto desempeño de sus funciones dentro de la Unidad.
2. **De Entidades Externas:** corresponde a los grupos de valor y/o usuarios que interactúan con la Unidad y que requieren de servicios y/o productos que provee la Unidad en el cumplimiento de sus funciones como entidad del estado.



INTERNO	EXTERNO
POBLACIÓN OBJETIVO	POBLACIÓN OBJETIVO
Estratégico Táctico Operativo	Entidades SNARIV Víctimas
HERRAMIENTAS	HERRAMIENTAS
Software Recurso Humano Infraestructura Procesos	Servicios Información





Resultados

1. Usuarios internos

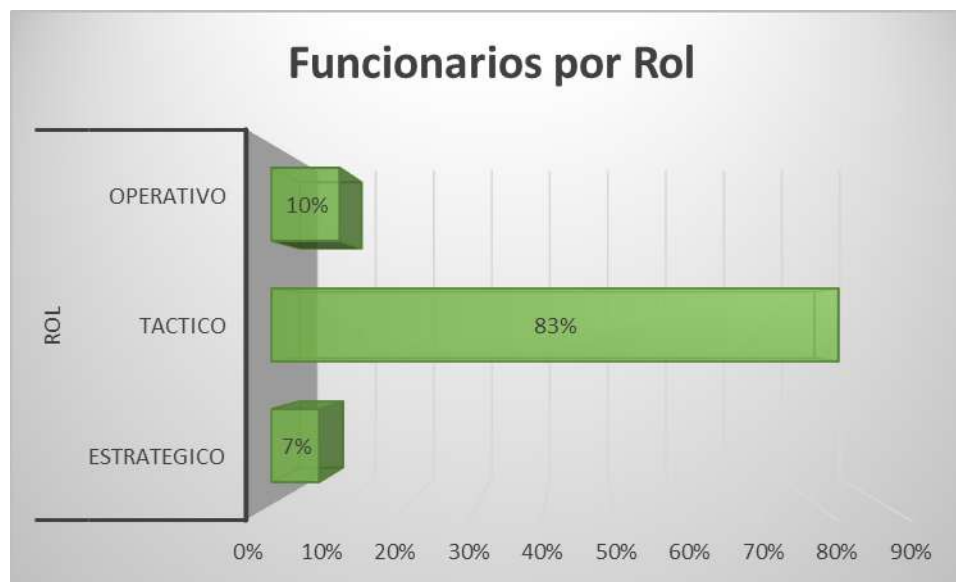
A partir de la matriz anterior, y tomando en cuenta la Resolución No. 04224 del 29 de agosto de 2018, por la cual se establece la estructura de la Unidad para las Víctimas y se distribuyen los cargos de la planta global, se establecieron los siguientes perfiles, teniendo en cuenta el nivel profesional, las funciones que desempeñan al servicio de la Unidad y las competencias requeridas para el desempeño de esas funciones.

1.1. Tipo de Usuario

1.1.1. Funcionario de Planta

- 1.1.1.1. **Estratégicos:** (57) directores y subdirectores, profesionales con maestría con muy buen conocimiento del entorno, capacidad de planeación a largo y mediano plazo, liderazgo, toma de decisiones y habilidades de gestión presupuestal. Aplica el conocimiento profesional en la resolución de problemas, articula potencialidades y necesidades individuales con las de la Unidad para optimizar la calidad de las contribuciones de los equipos de trabajo y de las personas en el cumplimiento de las metas y objetivos de la Unidad.
- 1.1.1.2. **Tácticos:** (714) Nivel profesional y profesional especializado, se caracteriza porque adquiere y desarrolla permanentemente conocimientos, conoce e interpreta la organización, establece y mantiene relaciones recíprocas con redes internas y externas, de forma participativa, integrando esfuerzos facilitando la consecución de los objetivos de la Unidad. Asume el rol de orientador y guía de un equipo, promoviendo la efectividad en la consecución de metas y objetivos institucionales. Considera varias alternativas de solución a los problemas y toma acciones concretas consecuentes con la opción escogida.
- 1.1.1.3. **Operativos:** (86) Nivel asistencial que presenta ideas y métodos novedosos y concretas actividades para la consecución de los objetivos institucionales, coopera con otros. Recoge únicamente la información necesaria para cumplir con sus tareas y la maneja con respecto. Cumple con los compromisos adquiridos y facilita la labor con sus superiores y compañeros. Transmite información oportuna y objetiva.

Distribución de perfiles-Funcionarios de Planta



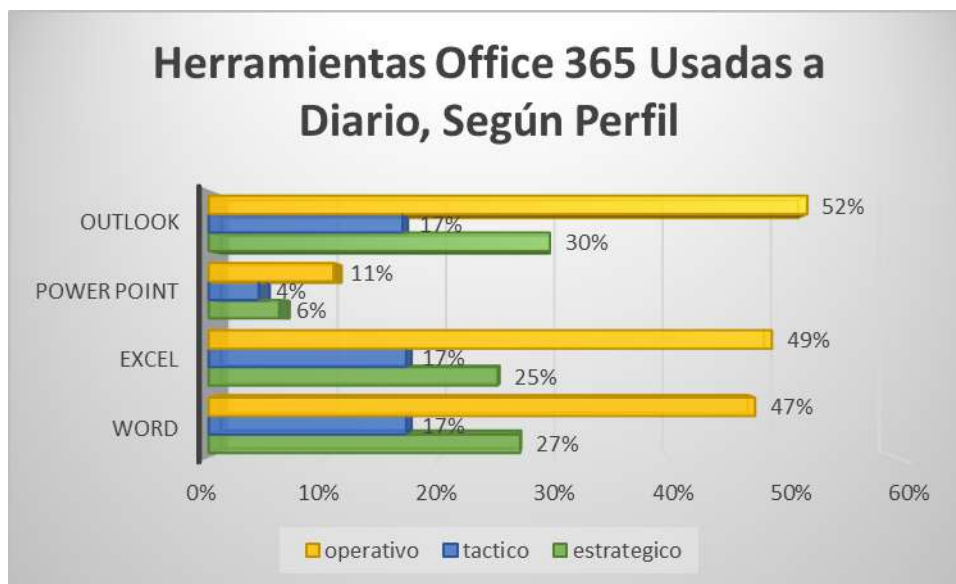
1.1.2. Contratista y Operador

- 1.1.2.1. **Contratista Táctico:** Nivel profesional y profesional especializado, se caracteriza porque adquiere y desarrolla permanentemente conocimientos, mantiene relaciones recíprocas con redes internas y externas, de forma participativa, integrando esfuerzos facilitando la consecución de los objetivos de la Unidad. Promueve la efectividad en la consecución de metas y objetivos institucionales. Considera varias alternativas de solución a los problemas y toma acciones concretas consecuentes con la opción escogida.
- 1.1.2.2. **Contratista y Operador Operativo:** Nivel asistencial que concretas actividades para la consecución de los objetivos institucionales, coopera con otros. Recoge únicamente la información necesaria para cumplir con sus tareas y la maneja con respeto. Cumple con los compromisos adquiridos y facilita la labor con sus superiores y compañeros. Transmite información oportuna y objetiva.

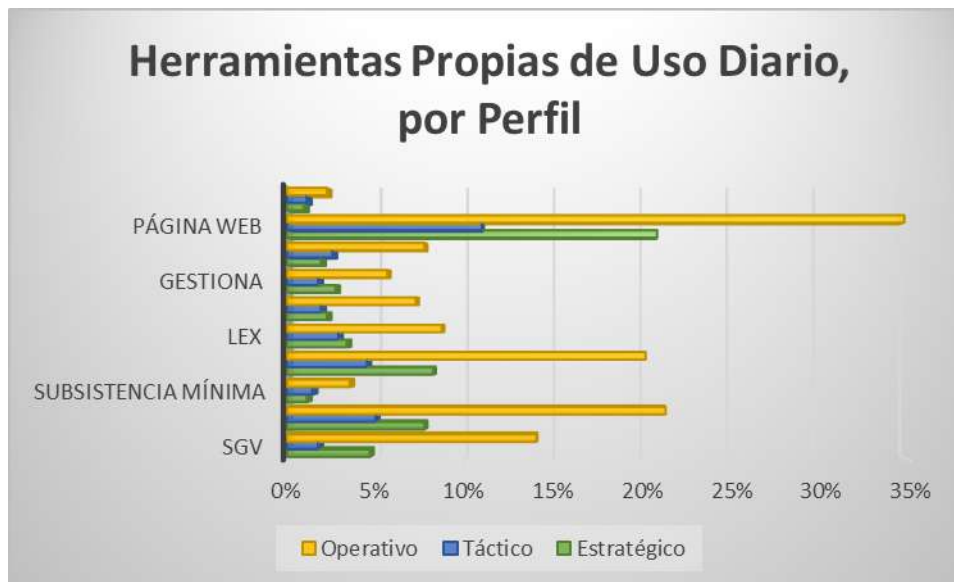
Distribución de Perfiles – Contratistas y Operadores



Herramientas y /o servicios utilizados Office 365



Desarrollos Propios



2. Usuarios Externos

2.1. Población Víctima

En el marco de la implementación de la política pública para las víctimas, se entiende enfoque diferencial como un principio que se establece en los términos del artículo 13 de la Ley 1448 de 2011 para la implementación de las medidas de prevención, protección, atención, asistencia y reparación a las víctimas.

El enfoque diferencial es un principio rector de la política pública para la prevención, atención, asistencia y reparación integral a las víctimas desde su dimensión individual y colectiva, que permite focalizar nuestra mirada y reconocer que hay poblaciones con características particulares en razón a su edad, género, orientación sexual y discapacidad; (Artículo 13 de Ley 1448 de 2011) y en razón a su pertenencia étnica (Decretos Ley 4633, 4634 y 4635 de 2011).

El enfoque étnico es también, un conjunto de medidas y acciones diferenciadas, dirigidas a garantizar la igualdad material de estas poblaciones, las cuales permiten: enfrentar la situación de vulnerabilidad acentuada en el marco del conflicto, contribuir a la superación de esquemas de discriminación, barreras sociales, exclusión, injusticias históricas, territoriales, entre otras; y la satisfacción de bienes servicios y oportunidades.



Con base en lo anterior, consideramos que el enfoque diferencial “es un método de análisis, de actuación y de evaluación de la población, basado en la protección de los derechos fundamentales de las poblaciones desde una perspectiva de equidad y diversidad.

Para el desarrollo de la caracterización de la población Víctima, que es el objetivo por el cual existe la Unidad para las Víctimas, adoptamos la metodología del enfoque diferencial y analizamos las siguientes variables:

Edad: Reconoce características particulares en razón a la edad de las personas. Incluye niños, niñas, adolescentes, jóvenes y persona mayor.

Discapacidad: Incluye el reconocimiento de diversos tipos de discapacidad; Física, auditiva, visual, cognitiva, mental, múltiple y las vulnerabilidades que otras afectaciones como el conflicto armado acentúan en la discapacidad.

Etnia: Reconoce características particulares en razón a la identidad cultural de las personas y comunidades. Incluye el reconocimiento de las comunidades y pueblos indígenas, comunidades negras, afrocolombianas, raizales, palenqueras y del pueblo Rom o gitano.

Género/diversidad sexual: Reconoce características particulares debidas a las identidades de género y las orientaciones sexuales diversas.

Adicionalmente se evaluaron otras variables como:

Región: Reconoce las diferencias históricas, políticas, geográficas, climáticas, culturales, lingüísticas de la población.



Distribución de la Población Víctima por Edad



Distribución de la Población Víctima por Género



Distribución de la Población Víctima por Etnia



Población Víctima con/sin Discapacidad



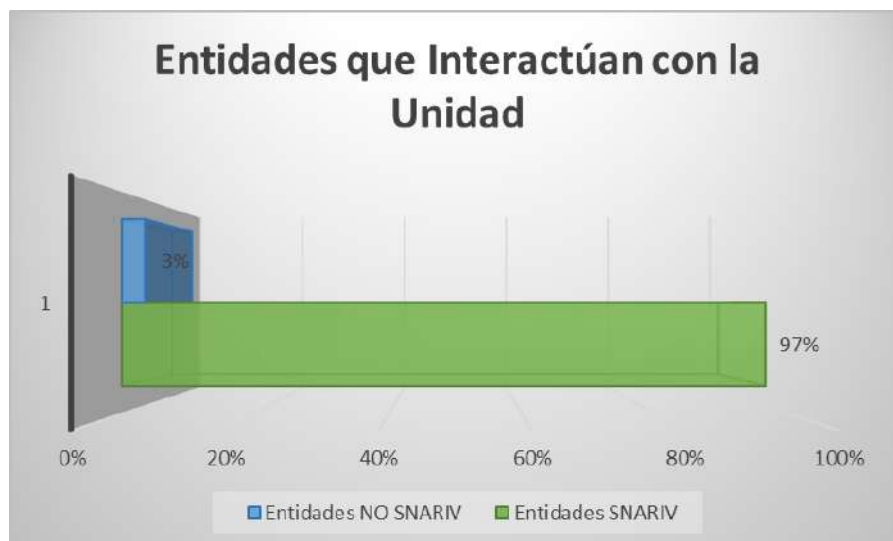
Distribución de la Población Víctima por Región



2.2. Entidades Externas

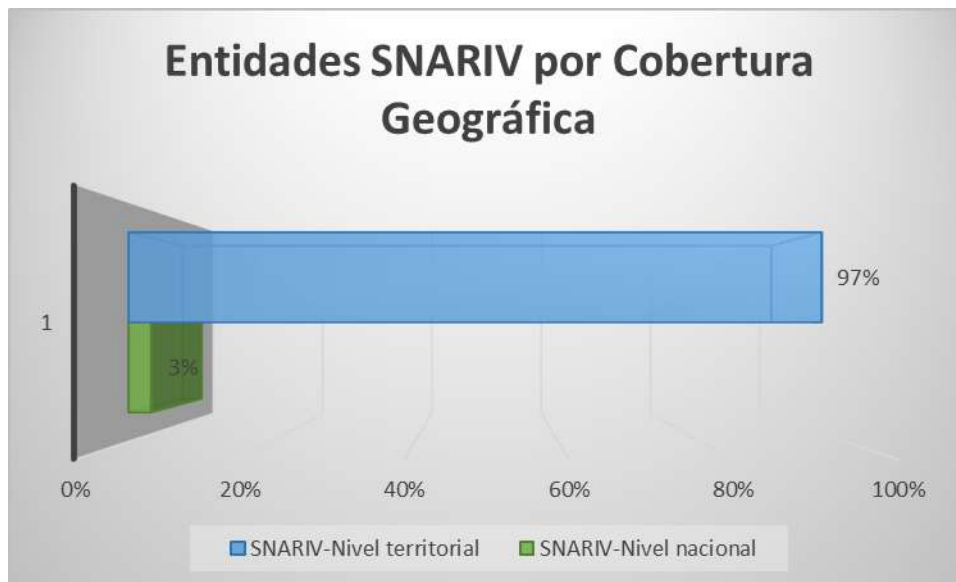
De acuerdo con las solicitudes gestionadas ante la Red Nacional de Información (RNI), las entidades con las cuales se realiza cruce de información son:

Distribución por tipo de entidad

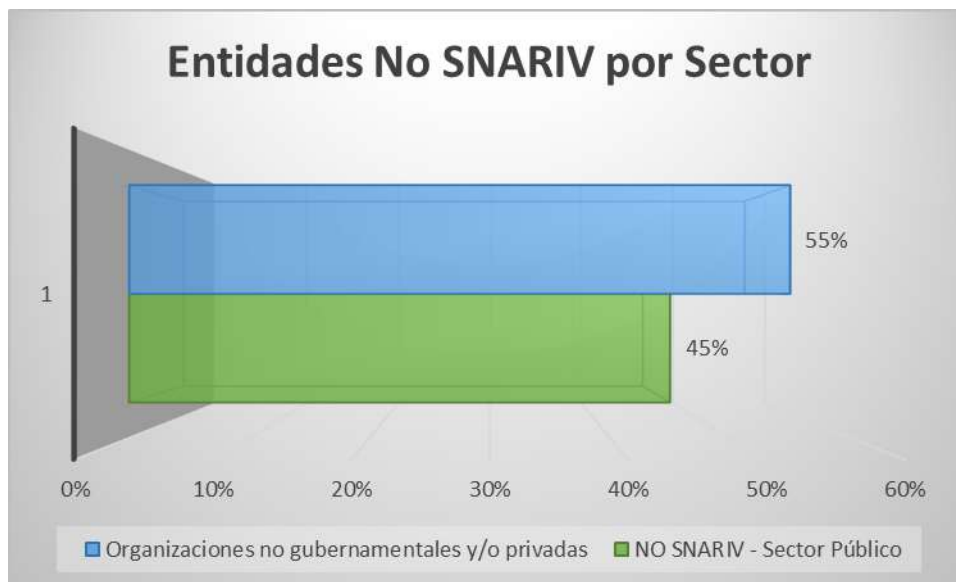




Entidades SNARIV por Cobertura Geográfica

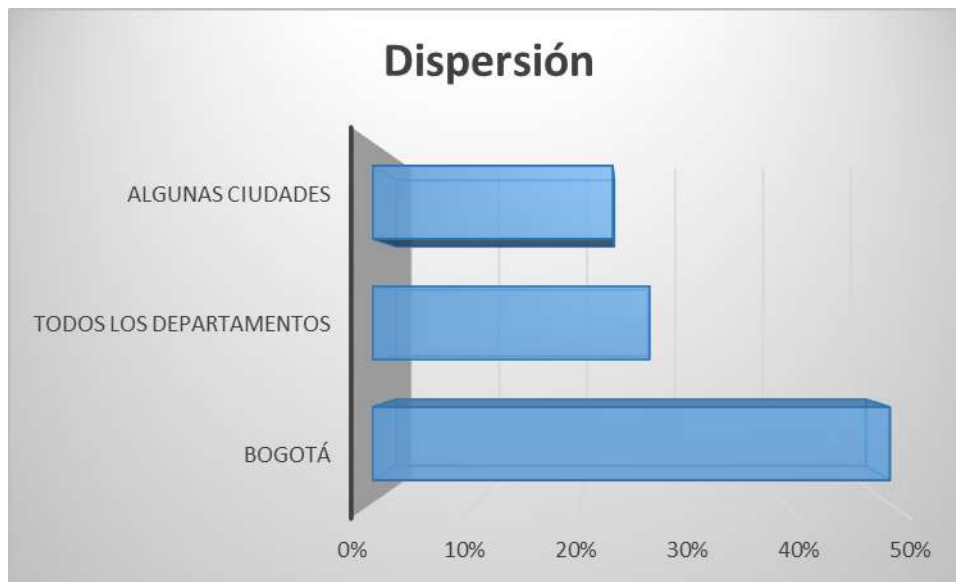


Entidades No SNARIV por Sector

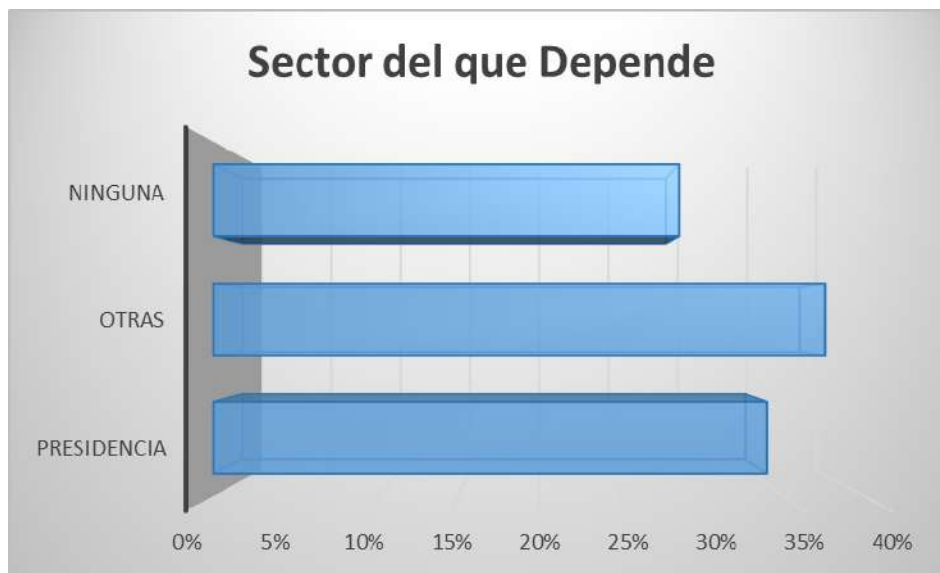




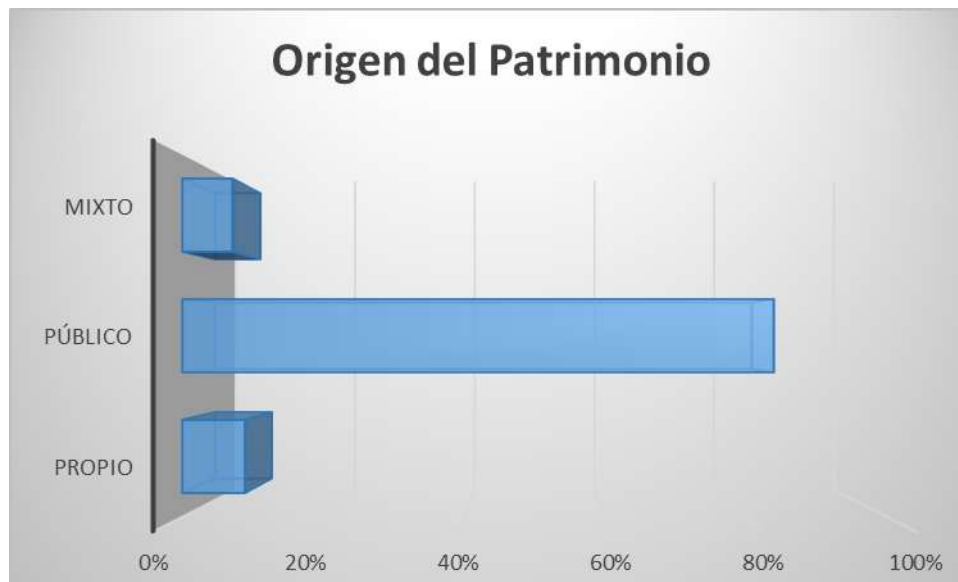
Entidades SNARIV por Tamaño



Entidades SNARIV por Sector de Dependencia



Entidades SNARIV por Origen del Patrimonio



3. Estrategia

Como parte de este primer ejercicio, se recopiló información que administra la Subdirección Red Nacional de Información – SRNI sobre las entidades SNARIV y no SNARIV que interactúan con la Unidad, la Dirección General sobre diferentes actores sociales que fueron convocados a la Audiencia Pública de Rendición de Cuentas, sobre funcionarios y Contratistas por parte de áreas como Gestión de Contratación, la Dirección de Registro y Gestión de la Información, Talento Humano, Dirección de Gestión Social y Humanitaria, entre otras.

Para la caracterización de los usuarios internos:

VARIABLES USUARIOS INTERNOS		ECONOMICA	MEDIBLE	ASOCIATIVA	CONSISTENTE	PUNTAJE
TIPOLOGIA	TIPO DE CONTRATO	1	1	1	1	4
	PERFIL PROFESIONAL	1	1	1	1	4
	USO DE HERRAMIENTAS	1	1	1	1	4



Para la caracterización de la población víctima:

VARIABLES	POBLACION VICTIMA	ECONOMICA	MEDIBLE	ASOCIATIVA	CONSISTENTE	PUNTAJE
DEMOGRAFICAS	EDAD	1	1	1	1	4
	GENERO	1	1	1	1	4
	ETNIA	1	1	1	1	4
	DISCAPACIDAD	1	1	1	1	4
	LENGUAS	1	1	1	1	4
GEOGRAFICAS	UBICACIÓN	1	1	1	1	4

Para la caracterización de funcionarios y contratistas, se determinaron las siguientes variables:

VARIABLES ENTIDADES EXTERNAS		ECONOMICA	MEDIBLE	ASOCIATIVA	CONSISTENTE	PUNTAJE
GEOGRAFICAS	COBERTURA GEOGRAFICA	1	1	1	1	4
	DISPERSIÓN	1	1	1	1	4
	UBICACIÓN PRINCIPAL	1	0	1	1	3
TIPOLOGIA	FUENTE DE RECURSOS	1	1	1	1	4
	CANALES DE ATENCION DIS	1	1	1	1	4
	SECTOR DEL CUAL DEPENDE	1	1	1	1	4

4. Bibliografía

http://www.secretariatransparencia.gov.co/prensa/2016/Documents/guia-de-caracterizacion-de-ciudadanos-usuarios-e-interesados_web.pdf

<http://www.unidadvictimas.gov.co/es/direccion-de-registro-y-gestion-de-la-informacion/red-nacional-de-informacion-rni/37825>

<http://www.unidadvictimas.gov.co/es/oferta-institucional/294>



CONTROL DE CAMBIOS					
Versión	Hecha por	Revisada por	Aprobada por	Fecha	Motivo
1.0	Seguridad de la Info, Gobierno OTI	Rosybel Hernández D.	Manuel E. Castillo G.	27-11-2018	Creación, Revisión y Aprobación

Anexo 9

Estrategia de Gestión del Cambio

Referencia: Lineamiento LI.UA.06 – Preparación para el cambio

Unidad para la Atención y Reparación Integral a las Víctimas

Página 1 de 19

Línea de atención nacional: 01 8000 91 11 19 - Bogotá: 426 11 11

Sede administrativa: Calle 16 No. 6 - 66 Edificio Avianca - Piso 19 - Bogotá, D.C.

Ventanilla única de radicación: Calle 16 No. 9 - 64 local Mezanine 101

Horario: 8:00 a.m. a 4:00 p.m. Correo electrónico: notificacionesjuridicauariv@unidadvictimas.gov.co

www.unidadvictimas.gov.co

Síguenos en:





Tabla de contenido

Contenido

1. Introducción.....	3
2. Aspectos Generales	
2.1. Contexto.....	4
2.2. Alcance.....	4
2.3. Objetivos.....	4
3. Marco Legal y de Referencia.....	5
4. Marco Conceptual	6
5. Herramientas de Gestión del Cambio.....	7
6. Preparación para el cambio: Uso y Apropiación	7
7. Gestionando el cambio en Proyectos de TI	12
8. Documentos Asociados.....	19
9. Bibliografía.....	19

Unidad para la Atención y Reparación Integral a las Víctimas

Página 2 de 19

Línea de atención nacional: 01 8000 91 11 19 - Bogotá: 426 11 11

Sede administrativa: Calle 16 No. 6 - 66 Edificio Avianca - Piso 19 - Bogotá, D.C.

Ventanilla única de radicación: Calle 16 No. 9 - 64 local Mezanine 101

Horario: 8:00 a.m. a 4:00 p.m. Correo electrónico: notificacionesjuridicaivariv@unidadvictimas.gov.co

www.unidadvictimas.gov.co

Síguenos en:





1. Introducción

Nada es Permanente, Excepto el Cambio – Heráclito.

Las organizaciones deben cambiar constantemente porque el entorno cambiante así lo exige y la capacidad de adaptación al cambio es fundamental para que los proyectos de tecnología sean exitosos y generen valor. Hoy las empresas que hacen Gestión de Cambio eficaz terminan exitosamente el 69% de los proyectos, frente al 41% de éxito de las empresas que no tienen implementada una política de Gestión del Cambio¹.

No es suficiente con gerenciar proyectos que entreguen el producto esperado, a tiempo y dentro de los costos; sino, además, es necesario que los usuarios del producto entiendan los cambios introducidos y utilicen correctamente los productos. Necesitamos anticiparnos al impacto del cambio y comprometer a las partes interesadas, de esta manera se garantiza no sólo el éxito del proyecto sino su sostenibilidad a través del tiempo y se crea una cultura de mejora continua.

Con el fin de minimizar el impacto y fortalecer la interacción entre los diferentes grupos de interés de la Unidad, frente a los cambios que se producen como resultado de la implementación de nuevos proyectos de tecnología, se hace necesario definir planes que faciliten y estandaricen la gestión del cambio, de tal suerte que se garantice que los proyectos entreguen no solo productos sino valor, y a su vez se genere el ciclo de mejora continua en la prestación de los servicios de tecnología y su uso y apropiación.





2. Aspectos Generales

2.1. Contexto

En desarrollo del objetivo de la política de Gobierno Digital: “Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital”, las entidades del estado nos enfrentamos a desafíos más complejos en los proyectos de TI, como por ejemplo el desafío de lograr que las personas se comprometan con el éxito de los mismos, y que conozcan y se apropien de los productos entregados.

La Gestión de Cambio eficaz proporciona seguridad en las personas, lo cual se traduce en la reducción del impacto negativo y la minimización de antagonismos. Amplía la resiliencia y prepara a la organización para una mejor aceptación de los cambios.

La Oficina de Tecnologías de la Información asume el liderazgo y la responsabilidad como agente de cambio en los proyectos de TI, diseña e implanta el presente plan de gestión del cambio, en el cual incluye el conjunto de prácticas, recursos y herramientas que considera necesarias para lograr el objetivo propuesto.

2.2. Alcance

Todas las áreas de impacto, identificadas dentro de cada uno de los proyectos de TI que se implementen dentro de la Unidad.

2.3. Objetivos

2.3.1. General

Definir e implementar el plan de gestión del cambio asociado a los proyectos de TI que sean emprendidos en la Unidad.

2.3.2. Específicos

1. Definir las mejores prácticas para gestionar el cambio en los proyectos de TI.
2. Definir las etapas para gestionar el cambio en los proyectos.
3. Definir las actividades para desarrollar dentro de cada etapa del proceso de gestión del cambio.





3. Marco Legal y de Referencia

La Arquitectura TI le permite al Estado ser más eficiente al unir los esfuerzos de sus entidades. Se basa en el Marco de Referencia que alinea la gestión TI con la estrategia del Estado. Incluye las arquitecturas sectoriales y territoriales y un modelo de uso y apropiación.

El marco de referencia es el principal instrumento para implementar la Arquitectura TI de Colombia y habilitar la Estrategia de Gobierno Digital (antes Gobierno en línea). Con él se busca habilitar las estrategias de TIC para servicios, TIC para la gestión, TIC para el gobierno abierto y para la Seguridad y la privacidad.

Para los efectos, el gobierno nacional define el marco legal que apoya la adopción de los lineamientos y estrategias, mediante la siguiente normativa:

Ley 1341 de 2009, definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC.

Conpes 3670 de 2010, Lineamientos de Política para la continuidad de los programas de acceso y servicio universal a las Tecnologías de la Información y las Comunicaciones.

Decreto 2618 de 2012, se modifica la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones y se dictan otras disposiciones.

Decreto 2693 de 2012, se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009, 1450 de 2011.

Decreto 1008 de 2018, Política de Gobierno Digital antes Gobierno en Línea.

Según el lineamiento LI.UA.06, Arquitectura TI Colombia, establece que en la Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces, está la responsabilidad de elaborar un plan de gestión del cambio para facilitar el Uso y Apropiación de los proyectos de TI.

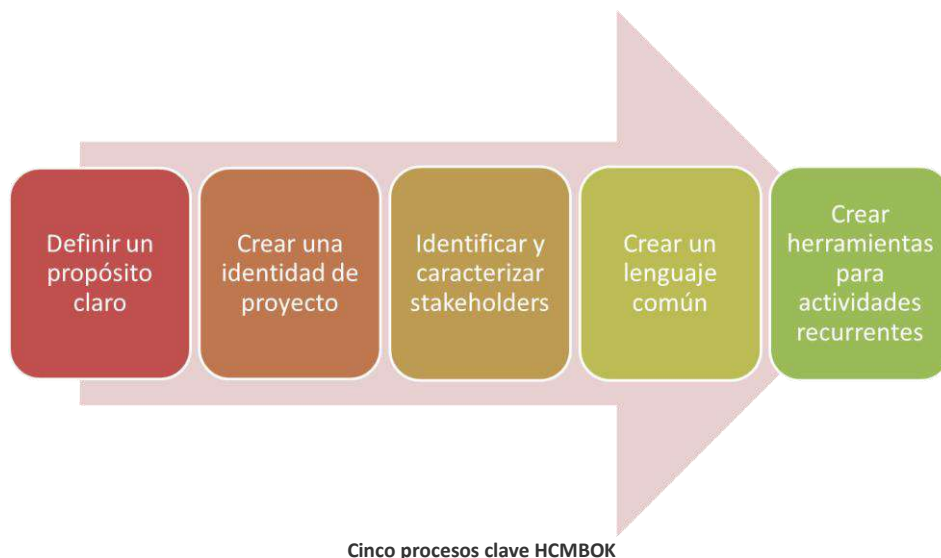


4. Marco Conceptual

“La gestión de cambios es una capacidad organizativa esencial que repercute por toda la cartera, los programas y la gestión de proyectos de la empresa. Todos los cambios estratégicos de las organizaciones se logran a través de programas y proyectos, y las organizaciones exitosas impulsan el cambio mediante la gestión eficaz de sus proyectos y programas”².

Planificar una iniciativa estratégica de gestión del cambio, no es otra cosa que desarrollar un plan cuyo objetivo principal es comprometer con el cambio a las personas de todas las jerarquías de la organización. Generar compromiso implica conquistar y se conquista estableciendo sistemas de reconocimiento que refuercen las conductas positivas que promuevan el cambio.

El Instituto para la Gestión Humana del Cambio (**Human Change Management Institute**) - HUCMI – ha desarrollado toda una disciplina alrededor de la Gestión del Cambio y ha creado el Cuerpo de Conocimiento de la Gestión Humana del Cambio– HCMBOK, por sus siglas en inglés, en cuyos principios nos basaremos para desarrollar la presente Estrategia de Gestión del Cambio, para ello tomaremos inicialmente sus 5 procesos clave, cuyo flujo es el siguiente:



² Pulso de la Profesión, cómo hacer posible el cambio organizativo mediante iniciativas estratégicas. Informe Detallado del PMI- Tricia S. Cabrey, Amy Haughey.





5. Mejores Prácticas y Herramientas de Gestión de Cambio

Acogiendo el cuerpo de conocimiento desarrollado mediante los procesos clave abordados por el HCMBOK, nos proponemos establecer como herramientas de gestión del cambio en los proyectos de TI, las siguientes:

- 4.1. Liderar la idea: Debemos crear la necesidad del cambio, asegurarnos de que sea comprendida de tal forma que se generen emociones positivas. La Entidad debe creer en ella.
- 4.2. Crear equipos de cambio: La idea, una vez ha generado el compromiso de la gente, debe ser desarrollada por un equipo dispuesto a empujar para que la idea sea llevada a la práctica.
- 4.3. Comunicar e involucrar: La información y los indicadores que informan sobre su avance deben asegurar que transmiten lo que requerimos en cada momento, no se debe dejar perder el foco ni la motivación.
- 4.4. Fijarse en los procesos y en las tareas: todo cambio supone modificar procedimientos y es necesario hacer seguimiento detallado de los cambios.
- 4.5. Desarrollo organizativo: Cultura, los cambios profundos, a menudo requieren que el comportamiento de las personas cambie. Frente a nuevas ideas es frecuente encontrar reacciones negativas, que se oponen al cambio y que pueden llevar al fracaso los proyectos. Una buena comprensión y gestión de estos parámetros culturales puede revertir ese impacto y optimizar la probabilidad de éxito. Para evitar el antagonismo, es indispensable conocer cultura, comprenderla y gestionarla.
- 4.6. Movilizadores de personas: Debemos conocer las motivaciones y emociones de las personas, y alinearlas con el proyecto: crear programas de retribución, reconocimiento, formación, gestión del conocimiento, competencias. Utilizar todas las herramientas necesarias para mantener la motivación de las personas.
- 4.7. El desarrollo de personas: Cambiar la cultura y el saber de las organizaciones, requiere a menudo cambiar el saber, fortalecer competencias y desarrollar nuevas.

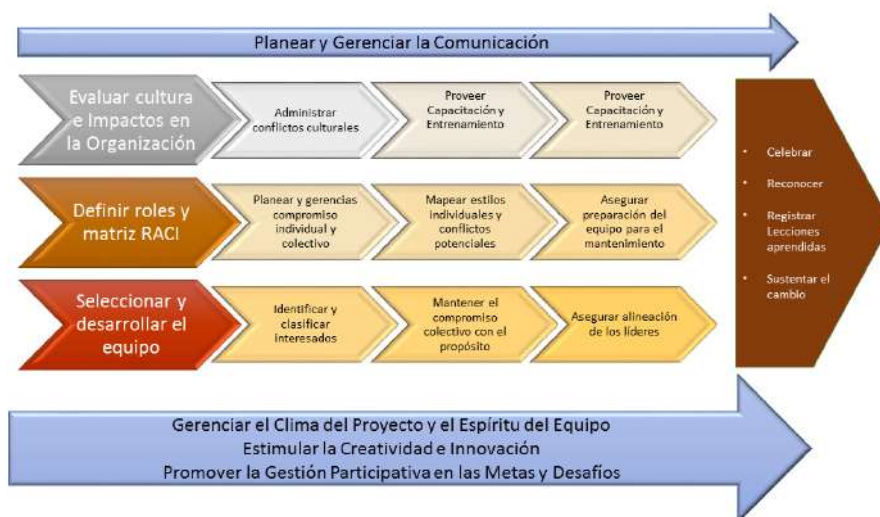
6. Preparación para el Cambio: Uso y Apropiación

La respuesta a los nuevos retos y desafíos que enfrentamos claramente tiene un efecto directo no sólo sobre la calidad de nuestros productos y servicios, sino que tiene un efecto positivo o negativo en nuestra cultura organizacional y por ende la productividad de nuestro talento humano.

La velocidad con que se dan los cambios en nuestro entorno nos obliga a evolucionar, a cambiar constantemente y a gestionar el cambio dentro de la Entidad, no como una actividad más, sino

Unidad para la Atención y Reparación Integral a las Víctimas

como una estrategia, como una buena práctica para imprimir en nuestra cultura organizacional. Para ello, se plantea adoptar las etapas propuestas por el HCMBOK, de acuerdo con la siguiente imagen:



Etapas para la Gestión del Cambio – HCMBOK

Para los efectos, se crea la necesidad de diseñar e integrar la gestión del cambio como una estrategia transversal a todos los proyectos de tecnología que se emprendan dentro de la Unidad, y se plantean las siguientes etapas, que no necesariamente son aplicables a todo tipo de proyectos, se elegirán y desarrollarán aquellas que apliquen de acuerdo con la naturaleza y tamaño de cada uno de éstos.

- 6.1. Identificación, clasificación y gestión de la matriz de interesados del proyecto: identificar y caracterizar a todas las personas que serán impactadas de cualquier forma por el proyecto es importante para determinar las demás etapas. Las actividades para desarrollar son:
 - 6.1.1. Identificar al patrocinador, la persona responsable de alcanzar el propósito del cambio, sus actividades pueden ser especialmente la comunicación, la resolución de conflictos y la promoción del compromiso en todos los interesados.
 - 6.1.2. Preparar al patrocinador para la promoción del proyecto, en cuanto al objetivo, el propósito, el tiempo de duración del proyecto, las áreas de impacto identificadas.



- 6.1.3. Identificar a toda la audiencia que va a ser impactada directa o indirectamente, dentro o fuera de la Entidad.
- 6.1.4. Diligenciar la matriz de interesados, debe ser reevaluada y actualizada constantemente, se sugiere diligenciar la matriz RACI.
- 6.2. Definición de los objetivos, propósitos, metas e identidad del proyecto: El objetivo de un cambio es su principal motivación, es la forma como se va a cautivar a la audiencia y generar el compromiso que se requiere para el éxito del proyecto. Se deben desarrollar las siguientes actividades:
 - 6.2.1. Crear el propósito del cambio: Todo cambio debe tener un propósito capaz de mover el alma y el cuerpo de las personas hacia el cambio. El propósito es la oportunidad para maximizar el compromiso por parte de todos los interesados, por lo tanto, debe ser enfocado en el factor humano.
 - 6.2.2. Definir las metas en tiempo, costo y recursos, deben ser negociadas con el equipo del proyecto y con el patrocinador. Deben ser alcanzables y medibles.
 - 6.2.3. Definir el logotipo (si aplica) y nombre del proyecto, con los cuales va a ser comunicado y promovido dentro de la Entidad.
- 6.3. Preparar el diagnóstico organizacional: evaluar las características de la cultura y determinar la predisposición del clima para los impactos y los riesgos del cambio: La evaluación de las características de la cultura organizacional proporciona información sobre los potenciales impactos y riesgos del cambio. Las actividades que se deben desarrollar:
 - 6.3.1. Realizar entrevistas para mapear los trazos culturales más evidentes
 - 6.3.2. Mapear misión, visión, prácticas en la gestión de personas.
 - 6.3.3. Evaluar los riesgos potenciales para el cambio de la cultura y evaluar las oportunidades de cambio de la cultura.
 - 6.3.4. Elaborar el diagnóstico
 - 6.3.5. Trazar el plan de gestión
- 6.4. Definir los roles y responsabilidades de la gestión del cambio del proyecto: La comprensión clara del rol de cada persona en el proyecto es clave para lograr el compromiso. Las actividades que se deben desarrollar:
 - 6.4.1. Definir la estructura de gestión del proyecto, debe ser acordada con los interesados y el patrocinador.
 - 6.4.2. Comunicar la estructura de gestión del proyecto.



- 6.5. Preparar el ambiente físico para el proyecto: Un ambiente físico adecuado puede ser factor de inspiración y motivación, promueve la integración de equipo, facilita la comunicación y estimula la creatividad. Es responsabilidad del gestor de cambios, aunque no siempre es posible contar con un espacio exclusivo, por lo tanto, está sujeto a la aprobación por parte de la Alta Dirección.
- 6.6. Definir la asignación y el desarrollo del equipo del proyecto: Designar o invitar a las personas que harán parte del equipo del proyecto. Las actividades que se deben desarrollar son:
 - 6.6.1. Definir los perfiles técnicos y comportamentales requeridos para el proyecto.
 - 6.6.2. Negociar la asignación del equipo
 - 6.6.3. Establecer el compromiso de que las personas que participan tendrán espacio en la Entidad al terminar el proyecto.
 - 6.6.4. Invitar o designar a cada participante.
- 6.7. Definir y ejecutar los entrenamientos preliminares del equipo: Desarrollar nuevas habilidades en los miembros del equipo, de ser requerido. Las actividades que se deben desarrollar:
 - 6.7.1. Identificar las habilidades nuevas que se deban desarrollar en el equipo.
 - 6.7.2. Comunicar y ejecutar el plan de entrenamiento.
 - 6.7.3. Establecer y ejecutar el plan de acción de gestión del cambio.
- 6.8. Planear y Gerenciar la Comunicación: La comunicación eficaz puede ser un factor clave en el éxito de los proyectos, si nos aseguramos de que los mensajes llegan y son correctamente entendidos por todas las audiencias, se tiene alta probabilidad de que obtengamos el compromiso de ellas. Las actividades que se deben desarrollar son:
 - 6.8.1. Planear la comunicación del propósito del proyecto
 - 6.8.2. Planear la rutina de comunicaciones tanto internas como externas al proyecto
 - 6.8.3. Definir el canal y forma de las comunicaciones ordinarias
 - 6.8.4. Monitorear la necesidad de comunicaciones no planeadas
 - 6.8.5. Verificar que los mensajes hayan sido entendidos
- 6.9. Gestionar el clima, conflicto, motivación, estrés, comportamientos: El clima del equipo del proyecto debe ser evaluado continuamente con el fin de mantener la motivación de los miembros del equipo y controlados los comportamientos que afecten el buen desempeño. Las actividades que se deben desarrollar son:
 - 6.9.1. Evaluar las potenciales situaciones de conflicto y monitorearlas
 - 6.9.2. Clasificar los conflictos de acuerdo con su naturaleza: lógica y psicológica



- 6.9.3. Aplicar intervenciones: con mentorías y/o entrenamiento.
 - 6.9.4. Definir el perfil motivacional del equipo
 - 6.9.5. Asegurar que el ambiente físico tenga lo necesario para la motivación del equipo
 - 6.9.6. Identificar, reconocer y celebrar pequeñas victorias.
 - 6.9.7. Monitorear continuamente el clima: Ausentismo, exceso de conflictos y comportamientos hostiles
- 6.10. Medir los resultados de la gestión del cambio: Todas las metas y objetivos propuestos dentro de la planeación del proyecto deben ser medibles con el fin de que podamos identificar tempranamente los potenciales problemas y tomar los correctivos necesarios para retomar el rumbo. Las actividades que se deben desarrollar son:
- 6.10.1. Definir indicadores apropiados para el proyecto
 - 6.10.2. Monitorear los resultados y efectuar los ajustes necesarios

6.11. Matriz RACI

RACI proviene de las siglas en inglés:

- Responsable (responsible): Quien ejecuta una tarea. Su función es “HACER”.
- Accountable (aprobador): Quien vela porque la tarea se cumpla, aún sin tener que ejecutarla en persona. Su función es “HACER que se HAGA”.
- Consulted (consultado): Persona o área que debe ser consultada respecto de la realización de una tarea.
- Informed (informado): Persona o área que debe ser informada respecto de la realización de una tarea.

Función de la Matriz RACI:

1. Identificar las actividades de un proceso.
2. Identificar / definir los principales roles funcionales asociados al proceso
3. Asignar los códigos “RACI” a cada tarea
4. Identificar ambigüedades o problemas (solapamientos, vacíos, dudas, etc.) y trabajar para solucionarlos.
5. Distribuir la matriz e incorporar la retroalimentación
6. Comunicarla de modo efectivo a todos los involucrados en el proceso.
7. Una matriz está viva y debemos asegurar que se haga actualice periódicamente.
8. Un mismo rol puede ser compartido por más de una persona o viceversa.





Ejemplo de matriz RACI:

TAREA/PERSONA	PERSONA 1	PERSONA 2	PERSONA 3	PERSONA 4
TAREA 1	R	I	C	A
TAREA 2	C	C	R	
TAREA 3	I	A		I
TAREA 4	C		A	A
TAREA 5		R	I	R
TAREA 6	C	I		C

7. Gestionando el Cambio en Proyectos de TI

Los cambios a nivel de tecnología de la información serán aprobados por el Comité de Cambios Interno OTI.

Se deben controlar los cambios organizacionales de impacto TI realizados por la Entidad y los diferentes operadores, valorando los riesgos asociados a:

- Dotación tecnológica.
- Centros de datos.
- Cambios y mejoras en las redes.
- El uso de nuevas tecnologías.
- Cambios en las ubicaciones físicas de las instalaciones de servicio.
- Cambios en la infraestructura tecnológica
- Contratación externa de otros proveedores.
- Los controles nuevos o modificados para resolver incidentes de seguridad de la información y mejorar la seguridad.
- La adopción de nuevos productos o versiones/ediciones más recientes.
- Nuevas herramientas y ambientes de producción.

Las actividades anteriormente mencionadas se controlan por medio del contrato con los terceros con los que se tiene relación contractual, desarrollos propios y las actas en las que se revisan detalladamente aspectos relacionados con seguridad de la información.

Los cambios urgentes, tal como cambios de configuración generados a raíz de un incidente o una vulnerabilidad detectada que afecta la operación de la Entidad, no requiere autorización del Comité de Cambios Interno OTI, pero se debe informar el resultado a través del Formato de





Gestión de Cambios Tecnológicos.

Se deben identificar los activos relacionados con los cambios (información, bases de datos, Software, hardware y personal), en el formato de gestión de cambios tecnológicos.

El proponente del cambio debe presentar el formato de gestión de cambios tecnológicos al Comité de Cambios Interno OTI. Si los cambios son necesarios, pero el plan de implementación no es aprobado, quien presenta el cambio es el responsable de modificar el formato con el nuevo plan.

La Unidad debe planificar, implementar y controlar los cambios relacionados con seguridad de la información, las instalaciones, aplicaciones, herramientas y los sistemas de información, los cuales pueden afectar la operación, a través del Comité de Cambios Interno OTI.

Los cambios organizacionales, culturales, estructurales, operativos, asociados al entorno tecnológico deben ser revisados por los dueños de los procesos asociados y por el Comité de Cambios Interno OTI.

La Oficina de Tecnologías de la Información de la UNIDAD PARA LA ATENCIÓN Y REPARACIÓN INTEGRAL A LAS VÍCTIMAS es la única que puede realizar cambios en los equipos de cómputo de trabajo, tanto a nivel hardware y/o software relacionado con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina. El fondo de pantalla y/o protector de pantalla corporativo es administrado únicamente por la Oficina Asesora de Comunicaciones.

Los cambios que afecten o puedan afectar la seguridad de la información en la organización, cambios en los procesos que interfieren en la operación de la entidad, instalaciones y sistemas de procesamiento de información deben tener aprobación por el Comité de Cambios Interno OTI institucional antes de iniciar con la fase de implementación.

Se debe evaluar el estado actual de los procesos, sistemas de información o proveedores actuales, en comparación con los elementos propuestos, para identificar los impactos en la operación. A tales efectos, el líder funcional o dueño del proceso respectivo, realizará las gestiones pertinentes para oficializar los cambios en la documentación del Sistema Integrado de Gestión de la entidad.

Todos los cambios de la Oficina de Tecnologías de la Información deben quedar documentados, con el fin de tener trazabilidad de estos.

En caso de ser necesario se divulgan los cambios que afecten la operación, infraestructura, por los diferentes canales de información con el apoyo de la Oficina Asesora de Comunicaciones y la

Unidad para la Atención y Reparación Integral a las Víctimas

Oficina Asesora jurídica.

7.1. Definiciones

Cambio³: Todo evento que afecte una plataforma informática y de telecomunicaciones, procesos, procedimientos, cultura, sistema, servicio, configuraciones o procesos que impliquen instalación, modificación, adición, retiro, en elementos como hardware, software o cualquier componente de los servicios de la Oficina de Tecnologías de la Información.

Cambios urgentes: Los cambios no contemplados que subsanan un incidente. Estos ajustes se deben realizar lo antes posible, ya que afectan ampliamente la prestación de un servicio de producción y son generados a partir de una emergencia.

Cambio estándar: Es todo cambio definido, planeado, aprobado y completamente documentado.

Comité de Cambios Interno OTI: Grupo de personas de la Oficina de Tecnologías de la Información responsables y/o relacionadas con la gestión de cambios. Este Comité está compuesto por:

- El Jefe de Oficina de Tecnologías de la Información o quien delegue.
- Un representante de cada línea de servicios tecnológicos
- Personal de la Entidad relacionado con el cambio (En caso de requerirse).

Gestión⁴: Actividades coordinadas para dirigir y controlar una organización.

Gestión del cambio (GC)⁵: Es la planificación y evaluación del proceso de cambio en la Unidad, para asegurar que, si éste se lleva a cabo, se haga de la forma eficiente, teniendo en cuenta las posibles consecuencias y forma de mitigarlas, siguiendo los procedimientos establecidos y asegurando en todo momento la calidad y continuidad del servicio.

Impacto⁶: Medida de la criticidad derivada por un cambio o incidente.

Marcha atrás (Roll Back): Corresponde a las actividades definidas por el responsable del cambio y aprobado por el Comité de Cambios Interno OTI, por el cual se permite revertir el cambio, sin afectación de la operación.

³ <https://www.mintic.gov.co/arquitecturati/630/w3-article-9262.html>

⁴ <http://iso9001calidad.com/definicion-de-terminos-586.html>

⁵ <https://www.unidadvictimas.gov.co/sites/default/files/documentosbiblioteca/procedimientogestiondelcambiov2versionfinal1.doc.pdf>

⁶ <https://www.mintic.gov.co/arquitecturati/630/articles-9262-recurso.pdf.pdf>



7.2. Actividades

N° PC	Descripción	Entradas/ Insumos	Responsable/área o grupo de trabajo	Salidas, productos, registros	CI/CE
1.	Recibir solicitud de cambio y asignar según la línea de servicio competente.	Correo electrónico o entrada desde procedimientos de tecnología (ej:desarrollo)	Oficina de Tecnologías de la Información	Ticket de la mesa de servicios	CI
2.	Evaluar la solicitud del cambio, con la revisión de la viabilidad y su alcance. ¿El cambio es necesario? Si: continúa con la actividad 3 No: continúa con la actividad 6 para cierre de ticket.	Ticket de la mesa de servicios tecnológicos	Líder de la línea de servicios competente	Ticket de la mesa de servicios tecnológicos y/o Formato de gestión de cambios tecnológicos y/o solicitud de cambio urgente	CI
3.	Gestionar la revisión de la solicitud de cambio por el Comité de Cambios Interno OTI.	Ticket de la mesa de servicios tecnológicos y/o Formato de gestión de cambios tecnológicos y/o solicitud de cambio urgente	Líder de la línea de servicios competente	Formato de gestión de cambios tecnológicos y/o correos electrónicos con aprobaciones o rechazo del cambio	CI
4.	Implementar cambio	Formato de gestión de cambios tecnológicos y/o correos electrónicos con aprobaciones	Líder de la línea de servicios competente	Formato de gestión de cambios tecnológicos	CI
5.	Informar el resultado de la implementación a los miembros de Comité de Cambios Interno OTI de cambios interno OTI.	Formato de gestión de cambios tecnológicos	Líder de la línea de servicios competente	Correo electrónico con Formato de gestión de cambios tecnológicos	CI
6.	Cerrar Ticket.	Formato de gestión de cambios tecnológicos	Líder de la línea de servicios competente	Ticket de la mesa de servicios tecnológicos cerrado	CI



7.3. Formato de Gestión de Cambios Tecnológicos

FORMATO GESTIÓN DE CAMBIOS TECNOLÓGICOS			
No. de Ticket de mesa de servicios tecnológicos		Fecha Solicitud:	
IDENTIFICACIÓN DEL SOLICITANTE DEL CAMBIO			
Nombre	Cargo	Teléfono/Ext	Correo Electrónico
EQUIPO DE TRABAJO (PERSONAS NECESARIAS PARA REALIZAR EL CAMBIO)			
Nombre	Cargo	Teléfono/Ext	Correo Electrónico
Antecedentes del Cambio (¿Por qué se requiere?):			
Descripción del Cambio (¿qué se requiere?):			
Alcance del Cambio:		Prioridad del cambio:	
		Urgente ()	
		Alto ()	
		Medio ()	
		Bajo ()	

Unidad para la Atención y Reparación Integral a las Víctimas

www.unidadvictimas.gov.co

Síguenos en:





Estrategia (¿cómo se realizará el cambio?)					
Análisis de Impacto					
Riesgos y consecuencias de no realizar el cambio					
¿Qué procesos o activo se afecta por el cambio?					
¿Qué beneficios del cambio trae el cambio?					
<i>Riesgos identificados</i>					
Recursos que se afectan por el cambio (activos, aplicaciones, personas, servicios o procesos)					
<i>Calificación de los riesgos identificados</i>					
<i>Opciones de manejo del riesgo</i>					
PLAN DE IMPLEMENTACIÓN DEL CAMBIO					
Plan Actividades Previas del Cambio					
TAREA	FECHA/HORA INICIO	FECHA/HORA FINALIZACIÓN	RESPONSABLE	ENTREGABLE	NUMERO CELULAR
Plan de ejecución					
TAREA	FECHA/HORA INICIO	FECHA/HORA FINALIZACIÓN	RESPONSABLE	ENTREGABLE	NUMERO CELULAR





Plan de Pruebas (SI APLICA)					
TAREA	FECHA/HORA INICIO	FECHA/HORA FINALIZACIÓN	RESPONSABLE	ENTREGABLE	NUMERO CELULAR
Marcha atrás (Roll Back):					
observaciones (si existen)					
FASE DE APROBACION					
<i>¿Se requiere realizar ajustes? Si _____ No _____</i>					
Cambios requeridos (si se requieren)					
Solicita		Aprueba:			
NOMBRE					
FIRMA		No. Acta de comité:			
Fecha Aprobación:		Observaciones:			
Día	Mes	Año			
SEGUIMIENTO					
<i>¿El cambio fue eficaz? Si _____ No _____</i>					
Descripción del seguimiento					





8. Documentos Asociados

Plan Estratégico de Tecnologías de la Información – PETI. Unidad para la Atención y Reparación Integral a las Víctimas – UARIV.

9. Bibliografía

G.UA.01 Guía del Dominio Uso y Apropiación. Guía técnica V.1.0. 2014

Guía Práctica para la Gestión del Cambio en las Organizaciones. PMI.

HCMBOK. <https://www.hucmi.com/es/hcmbok/>

<https://www.estrategiaynegocios.net/lasclavesdeldia/936658-330/7-herramientas-para-gestionar-el-cambio-que-hacen-posible-la-innovaci%C3%B3n>