El futuro es de todos

Unidad para la atención y reparación integral a las víctimas

Plan de Seguridad y Privacidad de la Información

Vigencia 2019 - 2021

TABLA DE CONTENIDO

1. INTRODUCCIÓN

En Colombia, en el año 2011 se estableció la Ley 1448, mediante la cual se crea la institucionalidad para la atención, asistencia y reparación integral de la población víctima del conflicto armado, generando la inherente necesidad del manejo de información de carácter personal de los ciudadanos.

En este contexto, la Unidad para la Atención y Reparación Integral a las Víctimas obtiene y genera información sensible que requiere protección en términos de la confidencialidad, integridad y disponibilidad en el marco del cumplimiento normativo colombiano.

En consecuencia, la Unidad ha avanzado en la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI del MinTIC, el cual establece controles técnicos y administrativos con base en la Norma ISO 27001:2013.

Teniendo en cuenta lo anterior, a través de este documento, se ilustran las mediciones de avance en la implementación del MSPI (años 2017 y 2018) y se define el plan de seguridad y privacidad de la información para la Entidad para las vigencias 2019 al 2021, planteando un ajuste en el indicador de madurez del modelo incorporando un factor de cobertura proporcional en términos de procesos, servicios, aplicaciones o servidores, de acuerdo a la naturaleza del control que se evalúe.

Es importante mencionar que, la definición del plan de seguridad y privacidad de la información se realiza con base en las directrices del MinTIC y las líneas de operación relacionadas con seguridad de la información en la Entidad, que permiten generar la capacidad requerida para la ejecución de las actividades definidas en este documento.

Es de relevancia indicar que el plan de seguridad y privacidad de la información se diseña con dos (2) líneas de trabajo:

- Plan de trabajo seguridad – Enlaces SIG y MIPG
- Plan de control operacional

Los cuales se relacionan entre si, con actividades comunes o complementarias orientadas a la implementación del Modelo de Seguridad y Privacidad de la Información, con el apoyo de los diferentes procesos de la Entidad en un escenario de responsabilidad compartida para el aseguramiento de la información de la población víctima del conflicto armado en Colombia.

www.unidadvictimas.gov.co
Síguenos en:
Línea de atención nacional:
01 8000 91 11 19 - Bogotá: **426 11 11**
Sede administrativa:
Carrera 85D No. 46A-65
Complejo Logístico San Cayetano - Bogotá, D.C.

2. DEFINICIONES:

Confidencialidad: Propiedad que impide la divulgación de información a personas o sistemas no autorizados.

Disponibilidad: Característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

Integridad: garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento.

Seguridad: Protección de los activos de información, contra amenazas que garanticen la continuidad del negocio, minimizando el riesgo y maximizando las oportunidades de la unidad.

3. JUSTIFICACIÓN:

El Estado colombiano cuenta con normatividad vigente que obliga el adecuado tratamiento de la información manejada por la Entidad en términos de confidencialidad, integridad y disponibilidad. Entre otras se citan:

- Ley 1448 de 2011, Artículo 29: "…Las autoridades garantizarán la confidencialidad de la información suministrada por las víctimas…"

"Brindar información veraz y completa a las autoridades encargadas de hacer el registro y el seguimiento de su situación o la de su hogar, por lo menos una vez al año, salvo que existan razones justificadas que impidan suministrar esta información. Las autoridades garantizarán la confidencialidad de la información suministrada por las víctimas y de manera excepcional podrá ser conocida por las distintas entidades que conforman el Sistema Nacional de Atención y Reparación de las Víctimas para lo cual suscribirán un acuerdo de confidencialidad respecto del uso y manejo de la información.

Hacer uso de los mecanismos de atención y reparación de acuerdo con los objetivos para los cuales fueron otorgados."

- Ley 1437 de 2011, Capítulo IV, "utilización de medios electrónicos en el procedimiento administrativo".

"Los procedimientos y trámites administrativos podrán realizarse a través de medios electrónicos. Para garantizar la igualdad de acceso a la administración, la autoridad deberá asegurar mecanismos suficientes y adecuados de acceso gratuito a los medios electrónicos, o permitir el uso alternativo de otros procedimientos."

• Ley 1581 de 2012, g) Principio de seguridad:
"La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento."

• Ley 1581 de 2012, Artículo 17, ítem d: "Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento"

• Ley 1712 de 2014, "principio de transparencia":
"Principio conforme al cual toda la información en poder de los sujetos obligados definidos en esta ley se presume pública, en consecuencia, de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en esta ley."

• Ley 1712 de 2014, artículo 7: "Disponibilidad de la información"
"En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente ley, a través de medios físicos, remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten."

• Ley 1712 de 2014 -Título III "Excepciones acceso a la información"
"Información exceptuada por daño de derechos a personas naturales o jurídicas. Es toda aquella información pública clasificada, cuyo acceso podrá ser rechazado o denegado de manera motivada y por escrito."

• Decreto 1413 de 2017, artículo 2.2.17.6.6, "Seguridad de la información."
"Los actores que traten información, en el marco del presente título, deberán adoptar medidas apropiadas, efectivas y verificables de seguridad que le permitan demostrar el correcto cumplimiento de las buenas prácticas consignadas en el modelo de seguridad y privacidad de la información emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones, o un sistema de gestión de seguridad de la información certificable. Esto con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información."

• Decreto 1413 de 2007, artículo 2.2.17.6.1, "Responsable y encargado del tratamiento":
"Los operadores de servicios ciudadanos digitales serán responsables del tratamiento de los datos personales que los ciudadanos le suministren directamente y encargados del

tratamiento respecto de los datos que otras entidades le proporcionen.”

• Artículo 2.2.17.6.3, “Responsabilidad demostrada”:
“Los operadores de servicios ciudadanos digitales deberán adoptar medidas apropiadas, efectivas y verificables que le permitan demostrar el correcto cumplimiento de las normas sobre tratamiento de datos personales. Para el efecto, deben crear e implementar un Programa Integral de Gestión de Datos (PIGD), como mecanismo operativo para garantizar el debido tratamiento de los datos personales.”

• Decreto 1413 de 2007, artículo 2.2.17.6.5, “Privacidad por diseño y por defecto”:
“Los operadores de servicios ciudadanos digitales deberán atender las buenas prácticas y principios desarrollados en el ámbito internacional en relación con la protección y tratamiento de datos personales que son adicionales a la Accountability, y que se refieren al Privacy by design (PbD) y Privacy Impact Assessment (PIA), cuyo objetivo se dirige a que la protección de la privacidad y de los datos no puede ser asegurada únicamente a través del cumplimiento de la normativa, sino que debe ser un 'modo de operar de las organizaciones, y aplicarlo a los sistemas de información, modelos, prácticas de negocio, diseño físico, infraestructura e interoperabilidad, que permita garantizar la privacidad al ciudadano y a las empresas en relación con la recolección, uso, almacenamiento, divulgación y disposición de los mensajes de datos para los servicios ciudadanos digitales gestionados por el operador”

• Decreto 1413 de 2017, artículo 2.2.17.5.10, “Derechos de los usuarios de los servicios ciudadanos digitales”:
“
1. Registrarse de manera gratuita eligiendo al operador de servicios ciudadanos digitales de su preferencia entre aquellos que estén vinculados por el articulador.
2. Aceptar, actualizar y revocarlas autorizaciones para recibir información, comunicaciones y notificaciones electrónicas desde las entidades públicas a su elección a través de los servicios ciudadanos digitales.
3. Hacer uso responsable de los servicios ciudadanos digitales a los cuáles se registre.
4. Interponer peticiones, quejas, reclamos y solicitudes de información en relación con la prestación a los servicios ciudadanos digitales.
5. Elegir y cambiar libremente el operador de servicios ciudadanos digitales
6. Solicitar en cualquier momento, y a través de cualquiera de los medios de atención al usuario, su retiro de la plataforma de servicios en· cuyo caso podrá descargar su información a un medio de almacenamiento propio.
”

• Decreto 1413 de 2017, artículo 2.2.17.2.1.1 “Descripción de los servicios ciudadanos digitales, 1.5 servicio de interoperabilidad:
Cualquier desarrollo en el marco de los servicios ciudadanos digitales especiales deberá hacer uso de o estar soportado en los servicios ciudadanos digitales básicos cuando lo requieran.”

• Decreto 612 de 2018, artículo 1. “Integración de planes institucionales y estratégico. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web.”

• Conpes 3854 de 2016, objetivo general “Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país”.

Por lo anterior, la Unidad para la Atención y Reparación Integral a las Víctimas debe emprender acciones orientadas a la protección de la información que gestiona, realizando la identificación y tratamiento de riesgos de la información de los activos críticos que la soportan, de manera que se establecen y realiza el seguimiento a dichas acciones en el marco del plan de acción y del Sistema Integrado de Gestión.

4. ANTECEDENTES:

La Unidad para la Atención y Reparación Integral a las Víctimas implementa el modelo de seguridad y privacidad de la información del MinTIC – MSPI, en el marco del subsistema de Gestión de Seguridad de la Información.

4.1. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En el año 2017 la Oficina de Tecnologías de la Información realizó dos (2) mediciones de la evaluación de la implementación del Modelo de Seguridad y Privacidad de la Información del MinTIC – MSPI. En el 2018, realiza una medición bajo el mismo modelo como se aprecia a continuación:

www.unidadvictimas.gov.co
Síguenos en:
Línea de atención nacional:
01 8000 91 11 19 - Bogotá: 426 11 11
Sede administrativa:
Carrera 85D No. 46A-65
Complejo Logístico San Cayetano - Bogotá, D.C.

Figura 1: Mediciones del MSPI 2017-2018

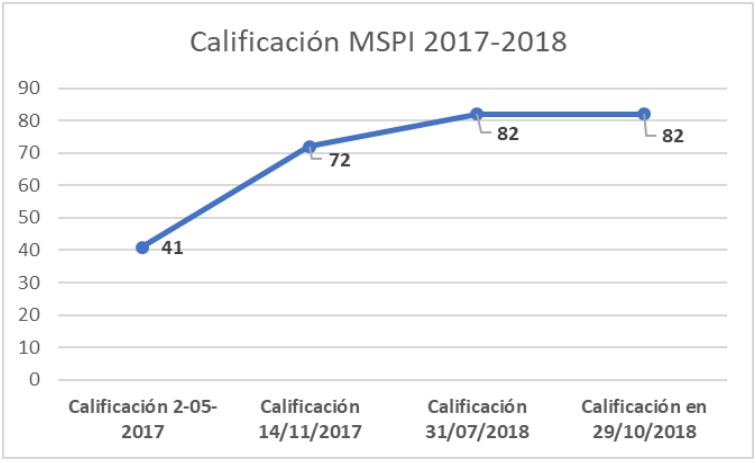

Figura 2: Incremento en la medición del MSPI 2017-2018

En el mes de mayo de 2017 se obtuvo un promedio total de 41% en la evaluación de los controles; en el mes de noviembre del mismo año, se reevaluó el modelo mostrando un avance de 72% en el promedio total de evaluación de los controles, lo cual permitió evidenciar la gestión del grupo de seguridad de la información. Posteriormente, en julio

de 2018 se realizó una tercera medición que registró el cumplimiento del modelo en un 82%.

5. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN:

La Oficina de Tecnologías de la Información de la Unidad, con base en los antecedentes registrados, formula el plan de seguridad y privacidad de la información, teniendo en cuenta las directrices del Ministerio de las Tecnologías de la Información y las Comunicaciones – MinTIC, con base en la necesidad del aseguramiento de la información de la Población Víctima del Conflicto Armado en Colombia.

5.1. OBJETIVO:

Fortalecer el aseguramiento de la información que genera y/o interopera la Unidad para la Atención y Reparación Integral a las Víctimas, a través de la implementación ordenada y sistemática de políticas y controles, en el marco del Modelo de Seguridad y Privacidad de la Información del MinTIC, para preservar la confidencialidad, integridad y disponibilidad de la información relacionada con la población Víctima en el marco de la Ley 1448 de 2011.

5.2. OBJETIVOS ESPECÍFICOS (OE):

a. Gestionar la implementación de políticas, lineamientos, buenas prácticas y recomendaciones de Seguridad de la Información en la Entidad y/o con las partes interesadas.

b. Gestionar la implementar controles de seguridad que permitan fortalecer el aseguramiento de la información de la población víctima, en el marco del Modelo de Seguridad y Privacidad de la Información del MinTIC.

c. Realizar seguimiento a la implementación del Modelo de Seguridad y privacidad de la Información, mediante la actualización de la herramienta proporcionada por el MinTIC para tal fin, teniendo en cuenta el indicador de cobertura o despliegue de los controles.

d. Fomentar en los procesos de la Entidad, la gestión de riesgos de seguridad de la información, con base en los activos críticos identificados y las acciones para el correspondiente tratamiento.

5.3. ALCANCE:

La Oficina de Tecnologías de la Información proyecta el plan de trabajo en el marco del Plan de Acción – Modelo Integrado de planeación y Gestión y Plan de implementación del Sistema Integrado de Gestión, teniendo en cuenta el siguiente esquema de procesos y tecnología de la Unidad para la Atención y Reparación Integral a las Víctimas, en el cual se involucran las partes interesadas, una muestra de las aplicaciones que apoyan los procesos misionales de la Entidad y la infraestructura que las soporta. Adicionalmente el plan de trabajo se proyecta teniendo en cuenta la normatividad relacionada, con los componentes del esquema:

Esquema de procesos y tecnología de la Unidad para la Atención y Reparación Integral a las Víctimas – abril 2019

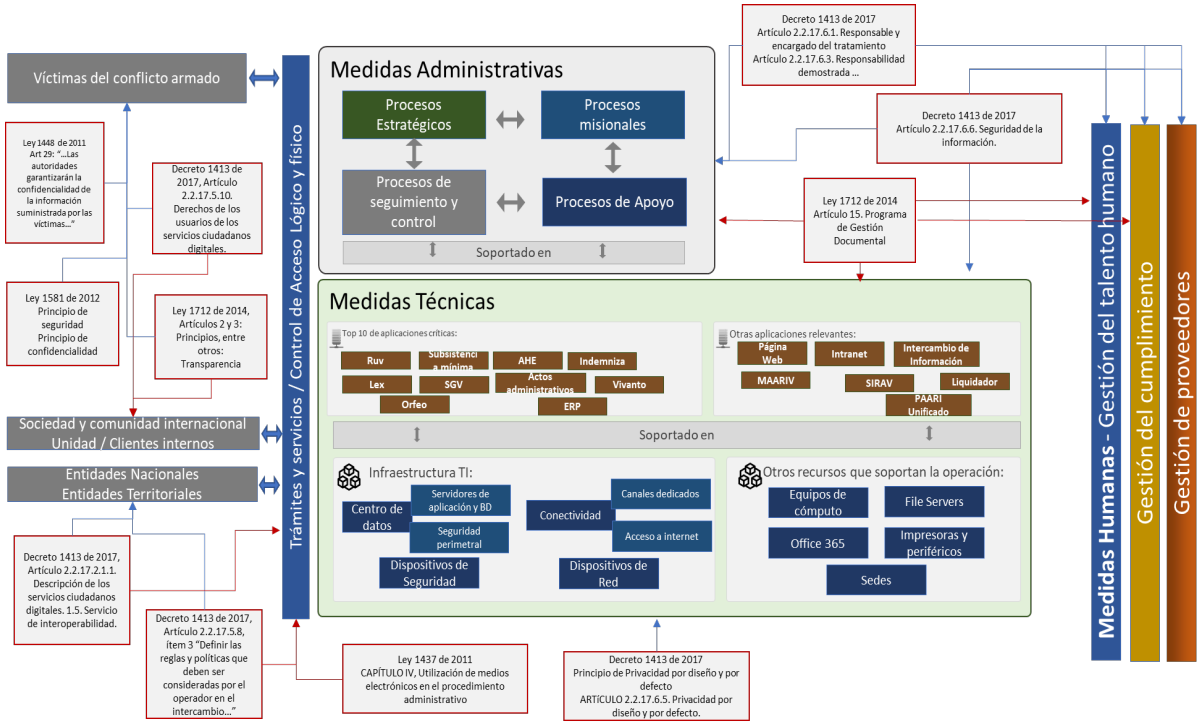

Figura 3: Esquema de procesos y tecnología de la Entidad

La seguridad y privacidad de la información es un elemento transversal a los componentes incluidos en el anterior esquema, razón por la cual, las medidas de aseguramiento a nivel técnico, humano y administrativo aplican para la totalidad de procesos de la entidad, partes interesadas, proveedores y operadores logísticos que

gestionen o manejen activos críticos de la entidad en términos de confidencialidad, integridad y disponibilidad.

5.4. DISEÑO:

El plan de seguridad y privacidad de la información se construye en el marco del Subsistema de Gestión de Seguridad de la Información de la Entidad, teniendo como referencia el ciclo PHVA[1], el cual según el Modelo de Seguridad y Privacidad de la Información del MinTIC se define como planificación, implementación, evaluación de desempeño y mejora continua.

A continuación, se listan los resultados más relevantes requeridos para cada fase, tomando como referencia el Modelo de Seguridad y Privacidad de la Información del MinTIC:

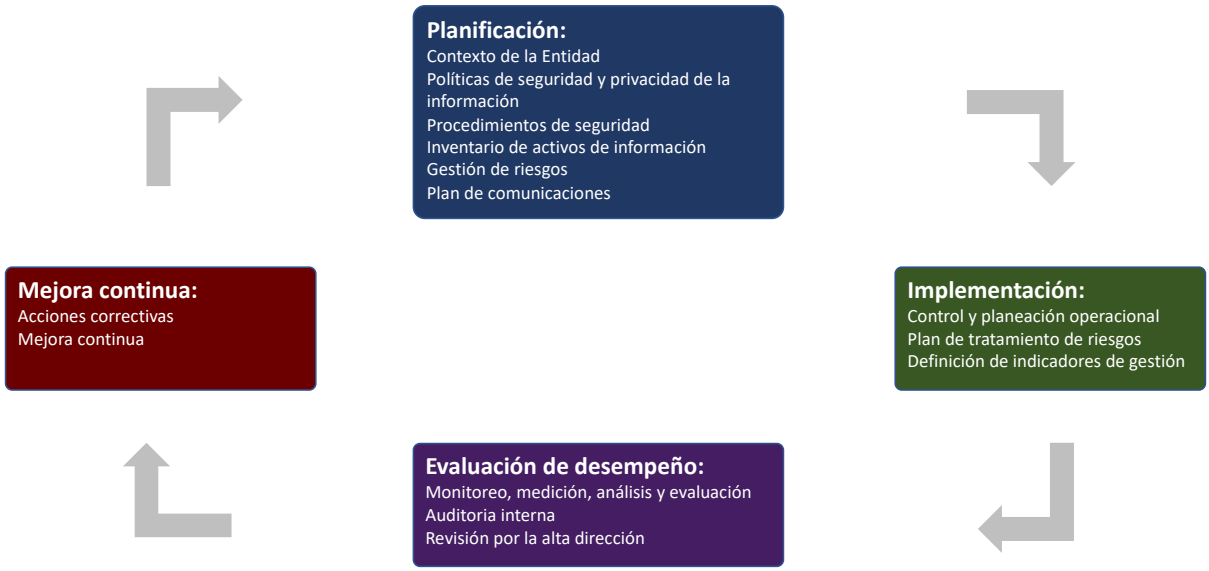

Figura 4: Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

Para dar continuidad a la implementación del Modelo de Seguridad y Privacidad de la información se deben tener en cuenta que el Subsistema de Gestión de Seguridad de la Información - SGSI hace parte del Sistema Integrado de Gestión - SIG de la Entidad, lo cual permite la articulación en:

[1] PHVA (Planear, hacer, verificar y actuar), conocido como Ciclo Deming, publicado en los años 50 por Edwards Deming

- Establecimiento del contexto de la Entidad
- Metodología para la administración de riesgos
- Revisión por la alta dirección
- Procedimientos relacionados con control de documentos, auditorías internas, generación de acciones correctivas.

Adicionalmente, la Oficina de Tecnologías de la Información de la Entidad, identifica las siguientes líneas operativas de seguridad de la información como capacidad interna para promover la implementación del MSPI.

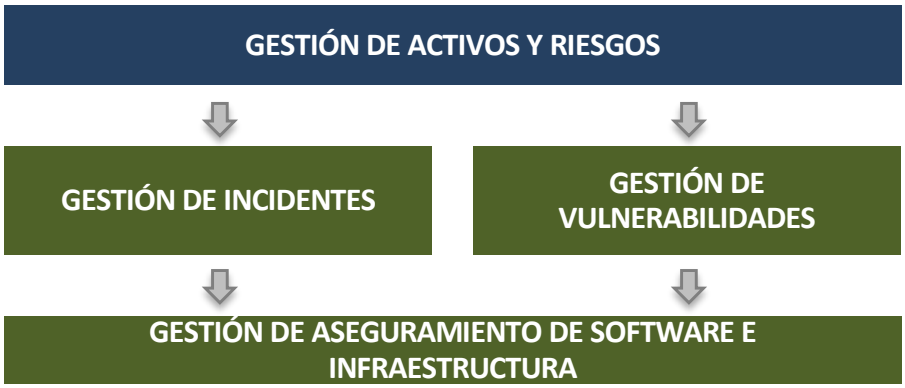

Figura 5: Líneas de operación de seguridad de la información en la Oficina de Tecnologías de la información de la Entidad

Esta estructura operativa es la encargada de la proyección de actualizaciones de políticas relacionadas con seguridad de la información, para aprobación y oficialización por parte de la línea estratégica de la Oficina de Tecnologías de la Información.

Adicionalmente, es la encargada de gestionar la implementación de controles de seguridad orientados a la protección de los datos, aplicación e infraestructura tecnológica de la Entidad, en articulación con las diferentes líneas de trabajo de la Oficina de Tecnologías de la Información y con los Enlaces del Sistema Integrado de Gestión como aliados estratégicos en la totalidad de los procesos de la Entidad.

Es importante mencionar que, lo anterior es apoyado por el plan de comunicación, sensibilización y capacitación que permitirá fomentar la aplicación de buenas prácticas de seguridad aplicables por los funcionarios, contratistas y colaboradores.

5.5. MEDICIÓN:

El Modelo de Seguridad y Privacidad de la Información, incorpora la escala de medición del nivel de madurez[2], que contempla 6 niveles:

- Nivel 1: Inexistente.
- Nivel 2: Inicial 20%: si la Entidad reconoce la necesidad de implementar el MPSI
- Nivel 3: Repetible 40%: si los procedimientos y controles se ejecutan de manera no oficial, pero regularmente.
- Nivel 4: Efectivo 60%: Si los procedimientos y controles están documentados y comunicados.
- Nivel 5: Gestionado 80%: Si se miden los procedimientos y controles.
- Nivel 6: Optimizado 100%: si los procedimientos y controles se aplican como mejor práctica y siguen la mejora continua.

Sin embargo, es importante mencionar que la medición se realizará de manera proporcional por cobertura de aplicación en los procesos, servicios, sistemas de información, bases de datos, servidores o canales de comunicación de la Entidad, relacionados con el determinado control.

Adicionalmente, la ejecución del plan de seguridad y privacidad de la información incorporará mediciones adicionales relacionadas con el grado de ejecución de las actividades definidas en este documento.

5.6. PLAN DE TRABAJO:

El logro de los objetivos específicos definidos en el presente documento requiere la definición de actividades detalladas categorizadas según el ámbito de ejecución en la siguiente estructura de plan de trabajo:

[2] Fuente MinTIC – Instrumento de evaluación del MSPI

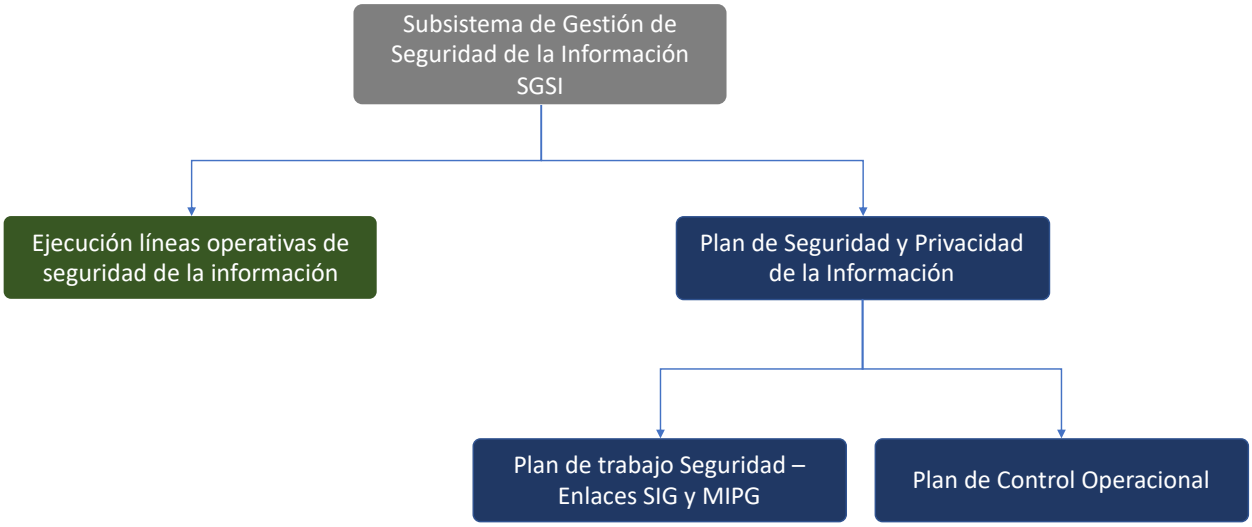

Figura 6: Estructura de plan de trabajo

Teniendo en cuenta lo anterior, a continuación, se definen los sub planes de trabajo que conforman el plan de seguridad y privacidad de la información.

5.6.1. Plan de trabajo – Enlaces SIG y MIPG:

A continuación, se listan las actividades detalladas establecidas en el marco del Sistema Integrado de Gestión y socializadas con los enlaces de cada proceso de la Entidad:

Macro Actividad	Responsable	Cobertura[3]	Plan	Fecha Inicio	Fecha Final
Gestionar la identificación y clasificación de activos de información	Procesos	Nacional	SIG	01/03/2019	30/06/2021
Identificar, valorar, definir plan de tratamiento y realizar seguimiento de riesgos de activos críticos	Procesos	Nacional	SIG	01/03/2019	30/06/2021
Gestionar el plan de continuidad de negocio	Procesos	Central	SIG	01/03/2019	30/06/2021
Gestionar las actividades complementarias para el SGSI de la vigencia.	Procesos	Central	SIG	01/03/2019	30/06/2021

[3] La cobertura será ampliada de acuerdo a las capacidades operativas para cada vigencia.

5.6.2. Plan de control operacional:

Este sub plan tiene como objetivo "*planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad y privacidad de la información que permitan implementar las acciones determinadas en el plan de tratamiento de riesgos*" (MSPI, p.30), para esto se listan las siguientes actividades:

No	Actividad	Objetivo Específico	Responsable	Cobertura	Fecha Inicio	Fecha Final
1	Actualización y socialización de políticas de seguridad de la información clasificadas por componente de aplicación (datos, aplicaciones, infraestructura, factor humano)	OE.A	Equipo de Seguridad y Riesgo informático	Nacional	01/05/2019	30/06/2021
2	Actualizar la declaración de aplicabilidad de controles en la Entidad	OE.B	Equipo de Seguridad y Riesgo informático	Nacional	1/08/2019	30/06/2021
3	Implementación de políticas de seguridad de la información a procesos, dependencias o líneas de trabajo	OE.A OE.D	Equipo de Seguridad y Riesgo informático Procesos de la Entidad	Nacional	2/09/2019	30/06/2021
4	Realizar seguimiento a la implementación del MSPI - Seguimiento a la implementación de políticas - Plan de tratamiento de riesgos	OE. C OE.D	Equipo de Seguridad y Riesgo informático	Nacional	1/11/2019	30/06/2021

6. DOCUMENTOS DE REFERENCIA

1. Ley 1448 de 2011.
2. Ley 1437 de 2011, Capítulo IV, “utilización de medios electrónicos en el procedimiento administrativo”.
3. Ley 1581 de 2012
4. Ley 1712 de 2014
5. Decreto 1413 de 2017
6. Decreto 612 de 2018
7. CONPES 3854 de 2016
8. MSPI - Modelo de Seguridad y Privacidad de la Información del MinTIC y guías complementarias
9. Norma ISO 27001:2013
10. Norma ISO 27005:2008
11. Guía para la administración de riesgos del Departamento Administrativo de la Función Pública

7. CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
1	Mayo 2018	Creación
2	Abril 2019	Retroalimentación
3	Junio 2019	Versión 1.0

Proyectó	Joaquín Rojas Palomino	
Revisó	Diana Marcela Calderón	
Aprobó 27/06/2019	Martín Cubides Rojas	

www.unidadvictimas.gov.co
Síguenos en:
Línea de atención nacional:
01 8000 91 11 19 - Bogotá: **426 11 11**
Sede administrativa:
Carrera 85D No. 46A-65
Complejo Logístico San Cayetano - Bogotá, D.C.

6. DOCUMENTOS DE REFERENCIA

1. Ley 1448 de 2011.
2. Ley 1437 de 2011, Capítulo IV, "utilización de medios electrónicos en el procedimiento administrativo".
3. Ley 1581 de 2012
4. Ley 1712 de 2014
5. Decreto 1413 de 2017
6. Decreto 612 de 2018
7. CONPES 3854 de 2016
8. MSPI - Modelo de Seguridad y Privacidad de la Información del MinTIC y guías complementarias
9. Norma ISO 27001:2013
10. Norma ISO 27005:2008
11. Guía para la administración de riesgos del Departamento Administrativo de la Función Pública

7. CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
1	Mayo 2018	Creación
2	Abril 2019	Retroalimentación
3	Junio 2019	Versión 1.0

Proyectó	Joaquín Rojas Palomino	
Revisó	Diana Marcela Calderón	D.C.
Aprobó 27/06/2019	Martín Cubides Rojas	

www.unidadvictimas.gov.co
Síguenos en:
Línea de atención nacional:
01 8000 91 11 19 - Bogotá: 426 11 11
Sede administrativa:
Carrera 85D No. 46A-65
Complejo Logístico San Cayetano - Bogotá, D.C.