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 - 2022

TABLA DE CONTENIDO

1. INTRODUCCIÓN

En Colombia, en el año 2011 se estableció la Ley 1448, prorrogada hasta el 10 de junio de 2031 por medio de la Ley 2078 de 2021, permitiendo continuar con 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, a través de la ejecución del Plan de Seguridad y Privacidad de la Información 2019-2021, permitiendo avanzar progresivamente en adopción de la política de seguridad digital, por tal razón se ilustran las mediciones realizadas por el Departamento Administrativo de la Función Pública del avance en esta política y se actualiza el plan de seguridad y privacidad de la información para la Entidad hasta la vigencia 2022, prorrogando las macro actividades definidas en el ciclo PHVA, correspondiente al Planear, Hacer, Verificar y Actuar, del Sistema de Gestión de Seguridad de la Información.

Es importante mencionar que, la definición del plan de seguridad y privacidad de la información se realiza con base en las directrices del MinTIC, en el marco de la política de Gobierno Digital, así como de 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 mantiene dos (2) líneas de trabajo:

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

Las 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

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.

escenario de responsabilidad compartida para el aseguramiento de la información de la población víctima del conflicto armado en Colombia.

2. DEFINICIONES:

Activo de información: Es la información que tiene valor para la organización y los elementos relacionados con la misma. Por ejemplo: Los sistemas de información, elementos de hardware, personas e instalaciones.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A ISO/IEC 27002:2015

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:

A continuación se presenta la normatividad vigente relacionada con el adecuado tratamiento de la información manejada por la Entidad en términos de confidencialidad, integridad y disponibilidad. Entre otras se citan:

- Artículo 15 de la Constitución Política establece que: "*Todas las personas tienen derecho a su intimidad personal, familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen*

derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas"

- Ley 1273 de 2009 "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones (…)"

- Artículo 1 de la Ley Estatutaria No 1712 de 2014 relacionada con la Transparencia y el Derecho de Acceso a la Información Pública Nacional, tiene por objeto: "*regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información."*

- Literal a) del artículo 6 ibídem define la información como: " un *conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen";* y así mismo en los literales que se relacionan a continuación realiza la siguiente clasificación:

    - *"b)* ***Información pública.*** *Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal;*

    - *c)* ***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 semiprivado 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;*

    - *d)* ***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 Estatutaria No 1581 de 2012 "Por la cual se dictan disposiciones

generales para la protección de datos personales" reviste un tratamiento especial y conforme al artículo 17 de dicha normatividad se señalan los deberes del responsable respecto al tratamiento de datos dentro de los cuales se destacan los siguientes literales:

> "a) *Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data*"
> (…)
> (…)
> "*d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento".*

- 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" en su artículo 166, crea 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 a través del artículo 29 dispone que:

  > "(…)
  > *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".*

- El artículo 2.2.9.1.1.1 del Decreto 1078 de 2015 subrogado por el artículo 1 del Decreto 1008 de 2018 señala: *"los lineamientos generales de la Política de Gobierno Digital para Colombia, antes estrategia de Gobierno en Línea, la cual desde ahora debe ser entendida como: 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".*

- El artículo 2.2.9.1.2.1 del Decreto 1078 de 2015 subrogado por el artículo 1 del Decreto 1008 de 2018 dispone que: "la Política de Gobierno Digital será definida por el Ministerio de Tecnologías de la Información y las Comunicaciones y se desarrollará a través de componentes y habilitadores transversales que, acompañados de lineamientos y estándares, permitirán el logro de propósitos que generarán valor público en un entorno de confianza digital a partir del

aprovechamiento de las TIC, conforme se describe a continuación:

"(…)

1. Componentes de la Política de Gobierno Digital: Son las líneas de acción que orientan el desarrollo y la implementación de la Política de Gobierno Digital, a fin de lograr sus propósitos. Los componentes son:

1.1. TIC para el Estado: Tiene como objetivo mejorar el funcionamiento de las entidades públicas y su relación con otras entidades públicas, a través del uso de las Tecnologías de la Información y las Comunicaciones.

1.2. TIC para la Sociedad: Tiene como objetivo fortalecer la sociedad y su relación con el Estado en un entorno confiable que permita la apertura y el aprovechamiento de los datos públicos, la colaboración en el desarrollo de productos y servicios de valor público, el diseño conjunto de servicios, la participación ciudadana en el diseño de políticas y normas, y la identificación de soluciones a problemáticas de interés común.

2. Habilitadores Transversales de la Política de Gobierno Digital: Son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

3. Lineamientos y estándares de la Política de Gobierno Digital: Son los requerimientos mínimos que todos los sujetos obligados deberán cumplir para el desarrollo de los componentes y habilitadores que permitirán lograr los propósitos de la Política de Gobierno Digital.

***4. Propósitos de la Política de Gobierno Digital**: Son los fines de la Política de Gobierno Digital, que se obtendrán a partir del desarrollo de los componentes y los habilitadores transversales, estos son:*

4.1. Habilitar y mejorar la provisión de servicios digitales de confianza y calidad.

4.2. Lograr procesos internos, seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información.

4.3. Tomar decisiones basadas en datos a partir del aumento, el uso y aprovechamiento de la información.

4.4. Empoderar a los ciudadanos a través de la consolidación de un Estado Abierto.

4.5. Impulsar el desarrollo de territorios y ciudades inteligentes para la solución de retos y problemáticas sociales a través del aprovechamiento de las TIC"

- El artículo 2.2.9.1.1.3 del Decreto 1008 de 2018 "Por el cual se establecen 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 número 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones" establece los principios de la Política de Gobierno Digital siendo uno de ellos, la Seguridad de la Información que busca:

  "*crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano".*

- El documento CONPES 3854 de 2016 establece la Política Nacional de Seguridad Digital, la cual contiene entre otros, principios fundamentales relacionados con: "*PF1. Salvaguardar los derechos humanos y los valores fundamentales de los ciudadanos en Colombia, incluyendo la libertad de expresión, el libre flujo de información, la confidencialidad de la información y las comunicaciones, la protección de la intimidad y los datos personales y la privacidad, así como los principios fundamentales consagrados en la Constitución Política de Colombia. (…)* y "*PF4. Adoptar un enfoque basado en la gestión de riesgos, que permita a los individuos el libre, seguro y confiable desarrollo de sus actividades en el entorno digital. (…)".*

- El CONPES 3995 de 2020 establece la Política Nacional de Confianza y Seguridad Digital, la cual tiene como objetivo: "*Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías*"

- El artículo 2.2.9.1.2.1 del Decreto 1008 de 2018 "Por el cual se establecen 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 número 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones" al señalar la

estructura respecto a la Política de Gobierno Digital establece la seguridad de la información como elemento fundamental y habilitador transversal de la referida política.

- La Directiva Presidencial 03 de 2021 señala entre otros aspectos, los lineamientos de Seguridad Digital, siendo relevantes:

  "3.1. "*Dar cumplimiento a las directrices en materia de seguridad digital y de la información que expida el MinTIC y las que se expidan en el marco de la política nacional de confianza y seguridad digital del Gobierno Nacional (…)*
  3.2. (…) fortalecer las medidas en materia de seguridad digital considerando las dinámicas que ha incorporado el uso de medios digitales: (…)"
- El artículo 1 de la Resolución 500 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital" expedida por el MINTIC tiene por objeto: "*establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establecer los lineamientos y estándares para la estrategia de seguridad digital.*

- La Resolución No 569 de 2018 de la Unidad para la Atención y Reparación Integral a las Víctimas, mediante la cual adoptó y actualizó el Sistema Integrado de Gestión involucrando varios sistemas dentro de los cuales se encuentra el Sistema de Seguridad de la Información bajo la Norma Técnica ISO 27001:2013.

Adicionalmente, es importante indicar que los datos e información que se genere obtengan, use o se almacene, custodie, distribuya, envie, intercambie y/ o modifique en la Unidad para la Atención y Reparación Integral a las Víctimas, en cada uno de sus procesos misionales, de apoyo y estratégicos son sensibles y deben manejarse en condiciones que garantice su confiabilidad, oportunidad y seguridad.

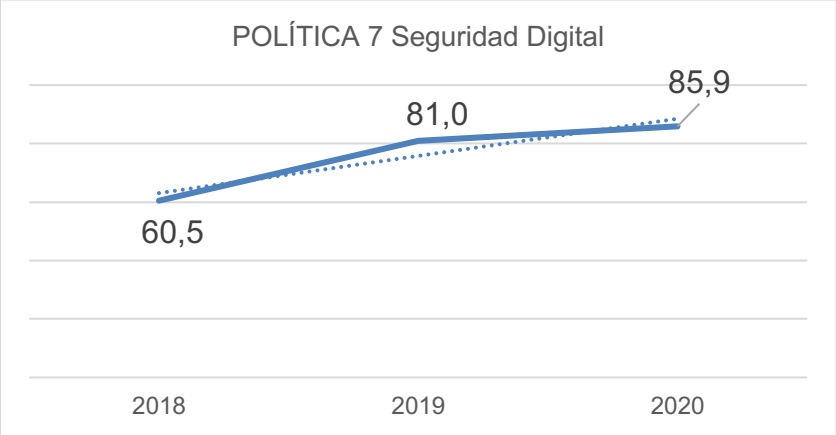
Por lo anterior, la Unidad para la Atención y Reparación Integral a las Víctimas debe implementar, en el marco de la mejora continua, las acciones orientadas a la protección de la información que gestiona, realizando la identificación y tratamiento de riesgos de la información de los activos críticos 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. POLÍTICA DE SEGURIDAD DIGITAL

Para los años 2018 al 2020, en el marco del Modelo Integrado de Planeación y Gestión – MIPG, el Departamento Administrativo de la Función Pública, ha realizado tres (3) mediciones de la adopción de la política de Gobierno Digital. En este sentido, la Unidad para la Atención y Reparación Integral a las Víctimas ha logrado el avance progresivo de la implementación de la estrategia de Seguridad Digital, a través de la política 7 "Seguridad digital", de la siguiente manera:



Fuente: https://www.funcionpublica.gov.co/web/mipg/resultados-medicion

El incremento en la mencionada medición se ha logrado a partir del establecimiento y ejecución del Plan de Seguridad y Privacidad de la Información 2019-2021, permitiendo la identificación y priorización de actividades que generan capacidades para la identificación, gestión y tratamiento de los riesgos de seguridad digital en la Entidad.

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, actualiza el documento 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 DEL SGSI (OE):

a. Proteger la información y sistemas de información, según estándares que salvaguarden la confidencialidad, integridad y disponibilidad, de los activos de la Entidad.

b. Implementar los controles de seguridad de la información para mitigar, reducir o eliminar la divulgación, pérdida o modificación no controlada de los activos de la Entidad.

c. Realizar seguimiento a los eventos e incidentes de seguridad para obtener lecciones aprendidas y mejorar periódicamente el sistema de gestión de Seguridad de la Información.

d. Promover, mantener y establecer la cultura de seguridad de la información en la Unidad para las Víctimas y partes interesadas.

e. Incrementar la disponibilidad de servicios de TI y de operación, a través del plan de continuidad de negocio.

f. Suministrar información confiable, íntegra, oportuna, accesible y de valor a la población Víctima.

5.2.1. INDICADORES RELACIONADOS:

A continuación, se relacionan los indicadores relacionados con cada objetivo específico del Sistema de Gestión de Seguridad de la Información:

No	Objetivo	Ecuación del Indicador	Meta
1	Proteger la información y sistemas de información, según estándares que salvaguarden la confidencialidad, integridad y disponibilidad, de los activos de la Entidad.	No. De Riesgos con nivel de riesgo residual bajo/Total de Riesgos identificados	85%
		No de Activos críticos con nivel riesgo residual Bajo /No. de Activos Críticos	70%
		No. Planes de tratamiento cerrados a conformidad al cierre de la vigencia /No. Planes de tratamiento	100%
2	Implementar los controles de seguridad de la información, para mitigar, reducir o eliminar la divulgación, pérdida o modificación no controlada de los activos de la Entidad.	Promedio efectividad de controles del Instrumento MSPI del MinTIC	80%
3	Realizar seguimiento a los eventos e incidentes de seguridad, para obtener lecciones aprendidas y mejorar periódicamente el sistema de gestión de Seguridad de la Información.	Suma de vulnerabilidades gestionadas y solucionadas / Suma de vulnerabilidades priorizadas remitidas a los dominios	>= 80%
		Número de tickets de mesa de servicios tecnológicos de seguridad resueltos / Número de tickets de mesa de servicios tecnológicos escalados al equipo de seguridad	100%
		Número de eventos reportados por los colaboradores internamente/ Número de eventos Totales	50%
4	Promover, mantener y establecer la cultura en seguridad de la información en la Unidad para las Víctimas y partes interesadas.	Promedio Calificaciones Obtenidas en evaluaciones de Seguridad de la Información y Ciberseguridad	4,5

No	Objetivo	Ecuación del Indicador	Meta
		Número de participantes en campañas de concientización / Número de funcionarios y contratistas totales	80%
		Número de participantes en campañas de concientización / Número de funcionarios y contratistas totales	80%
5	Incrementar la disponibilidad de servicios de TI y de operación, a través del plan de continuidad de negocio.	No. Simulacros Éxitos en gestión de continuidad del negocio /No. simulacros en gestión de continuidad del negocio	100%
6	Suministrar información confiable, íntegra, oportuna, accesible y de valor a la población Víctima.	Porcentaje de disponibilidad de la infraestructura tecnológica	99,9%

Indicadores SGSI – Relación con objetivos

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 la red de procesos de la Unidad para la Atención y Reparación Integral a las Víctimas y sus partes interesadas, relacionadas directamente con el Sistema de Gestión de Seguridad de la Información.

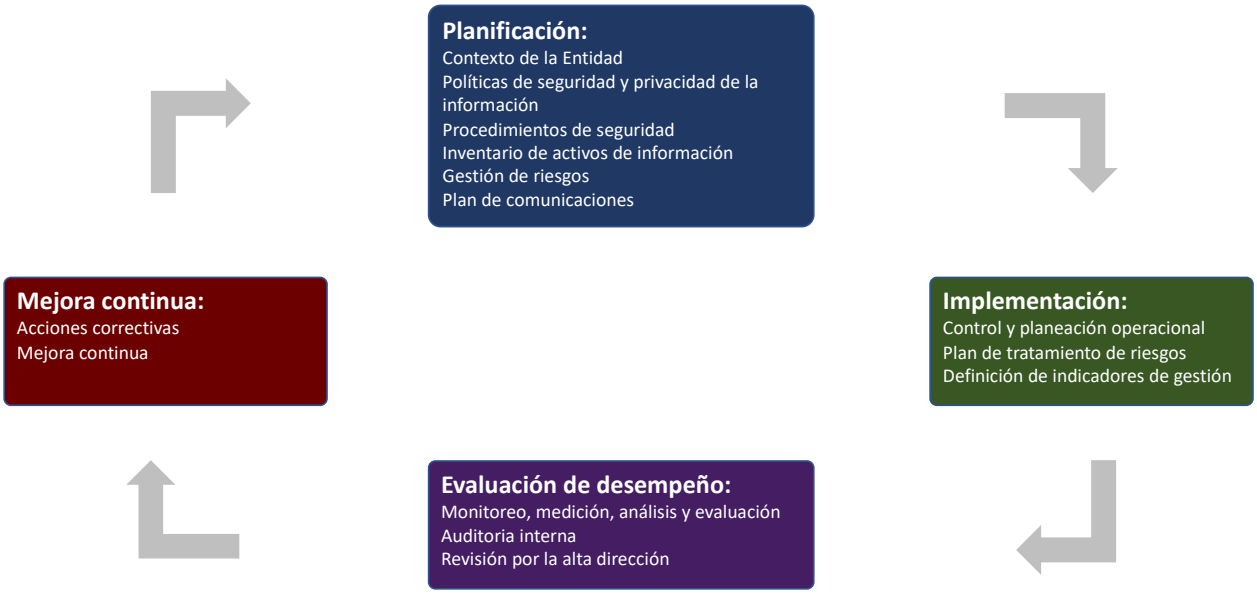
En este sentido, el Plan de Seguridad y Privacidad de la Información contempla como alcance los 18 procesos de la Entidad que gestionan, controlan y salvaguardan la confidencialidad, integridad y disponibilidad de la información de la población víctima y del recurso humano (funcionario o contratista) vinculado con la entidad.

5.4. DISEÑO:

El plan de seguridad y privacidad de la información se construye en el marco del Sistema 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 el ciclo de operación, tomando como referencia el Modelo de Seguridad y Privacidad de la Información del MinTIC:



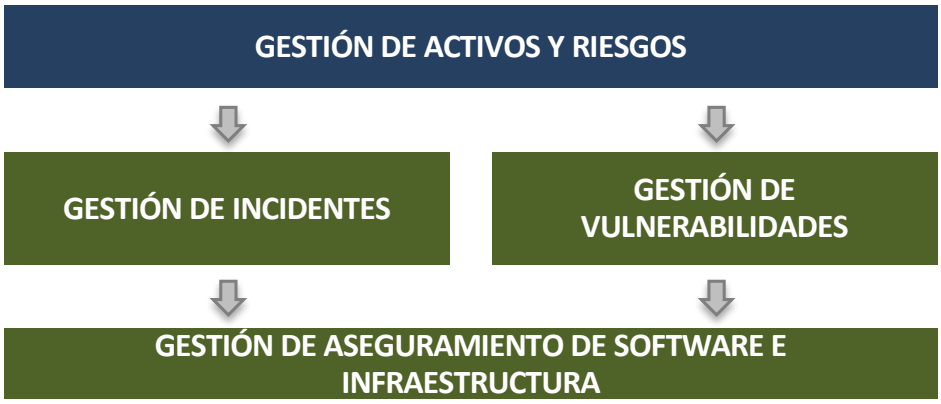
Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

Para dar continuidad a la implementación del Modelo de Seguridad y Privacidad de la información se deben tener en cuenta que el Sistema 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:

- 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.

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

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.



Líneas de operación de seguridad de la información en la Oficina de Tecnologías de la información de la Entidad

En el marco de estas líneas operativas, se realiza 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, se gestiona la implementación de controles de seguridad orientados a la protección de los datos, sistemas de información e infraestructura tecnológica de la Entidad, en articulación con las diferentes líneas de trabajo de la Oficina de Tecnologías de la Información y en articulación 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 con el diseño y ejecución de actividades de comunicación, sensibilización y capacitación que permiten fomentar la aplicación de buenas prácticas de seguridad aplicables por los funcionarios, contratistas y colaboradores.

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.

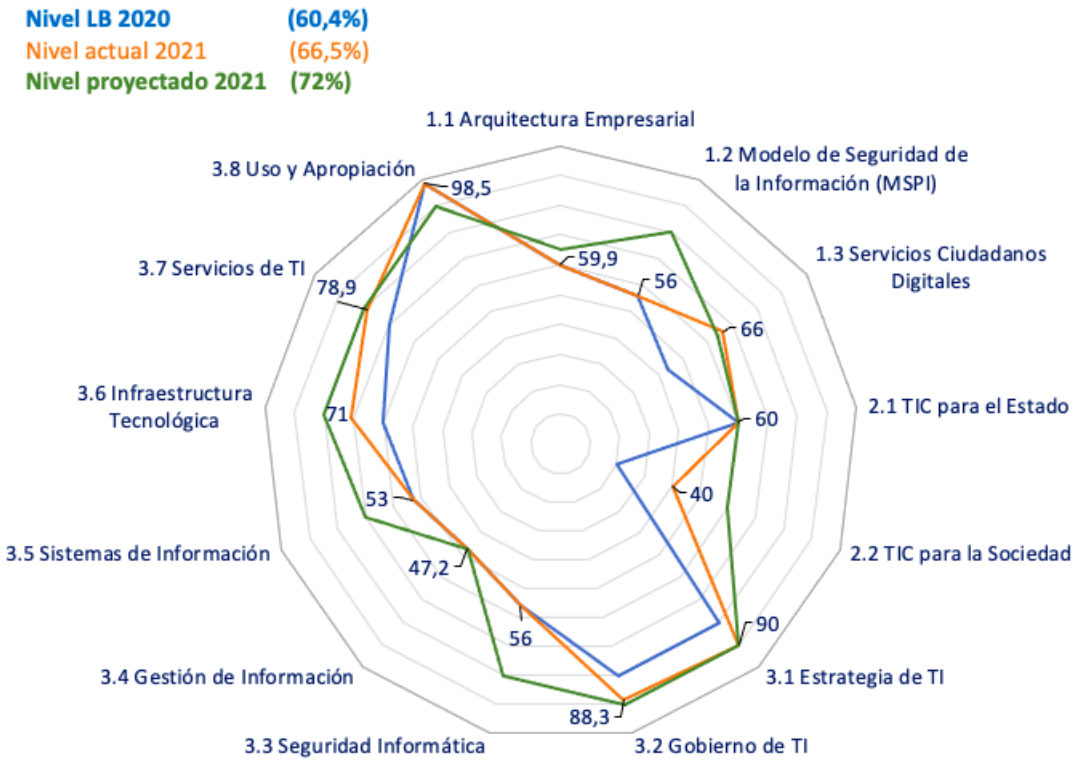
5.5. MEDICIÓN:

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.

Es importante indicar que, el nivel de madurez del Modelo de Seguridad y Privacidad de la Información se realiza en el marco del Plan Estratégico de Tecnologías de la Información, liderado por la Oficina de TI de la Entidad, cuyo avance a corte septiembre de 2021, se registra en un 56%.

[2] Fuente MinTIC – Instrumento de evaluación del MSPI



Medición Nivél de madurez – Plan Estratégico de Tecnologías de la Información

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:

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.

Estructura de plan de trabajo

Teniendo en cuenta lo anterior, a continuación, se definen los 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 marco actividades establecidas en el marco del Sistema Integrado de Gestión y socializadas con los enlaces de cada proceso de la Entidad:

Macro Actividad	Objetivo Específico	Responsable	Cobertura[3]	Plan	Fecha Inicio	Fecha Final
Gestionar la identificación y clasificación de activos de información	OE.A	Procesos	Nacional	SIG	01/03/2019	31/07/2022
Identificar, valorar, definir plan de tratamiento y realizar seguimiento de	OE.B	Procesos	Nacional	SIG	01/03/2019	31/07/2022

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

Macro Actividad	Objetivo Específico	Responsable	Cobertura[3]	Plan	Fecha Inicio	Fecha Final
riesgos de activos críticos						
Gestionar el plan de continuidad de negocio	OE.E	Procesos	Central	SIG	01/03/2019	31/07/2022
Gestionar las actividades complementarias para el SGSI de la vigencia.	OE.D	Procesos	Central	SIG	01/03/2019	31/07/2022

5.6.2. Plan de control operacional:

Este 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 de la Información - OTI	Nacional	01/05/2019	31/07/2022
2	Actualizar la declaración de aplicabilidad de controles en la Entidad	OE.B	Equipo de Seguridad de la Información - OTI	Nacional	1/08/2019	31/07/2022

No	Actividad	Objetivo Específico	Responsable	Cobertura	Fecha Inicio	Fecha Final
3	Implementación de políticas de seguridad de la información a procesos, dependencias o líneas de trabajo	OE.A OE.B OE.F	Equipo de Seguridad de la Información – OTI Procesos de la Entidad	Nacional	2/09/2019	31/07/2022
4	Realizar seguimiento a la implementación del MSPI - Seguimiento a la implementación de políticas - Plan de tratamiento de riesgos	OE. B	Equipo de Seguridad de la Información - OTI	Nacional	1/11/2019	31/07/2022
5	Realizar la atención y seguimiento a los eventos e incidentes de seguridad de la información	OE.C	Equipo de Seguridad de la Información - OTI	Nacional	1/11/2021	31/07/2022

6. DOCUMENTOS DE REFERENCIA

1. Ley 1448 de 2011.
2. Ley 1581 de 2012
3. Ley 1712 de 2014
4. Decreto 1008 de 2018
5. CONPES 3854 de 2016
6. CONPES 3995 de 2020
7. Resolución 500 de 2021 del MinTIC
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
4	Octubre 2021	Versión 2.0. Actualización de la justificación, objetivos acorde a lo establecido en el Sistema Integrado de Gestión, indicadores, alcance y prórroga de la fecha final de las actividades establecidas en el plan.

Proyectó	Joaquín Rojas Palomino	
Aprobó 20/10/2021	Víctor Edgardo Durán Martínez