Diario Oficial Año CLVI No. 51.619 Edición de 52 páginas • Bogotá, D. C., miércoles, 17 de marzo de 2021

RESOLUCIÓN 500 DE 2021

(marzo 10)

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.

[Ocultar]

Fecha de expedición de la norma	10/03/2021
Fecha de publicación de la norma	17/03/2021
Fecha de entrada en vigencia de la norma	17/03/2021

La Ministra de Tecnologías de la Información y las Comunicaciones, en ejercicio de sus facultades legales, en especial las que le confiere el parágrafo del artículo 16 del Decreto número 2106 de 2019, y

CONSIDERANDO QUE

Conforme al principio de “masificación del gobierno en línea” hoy Gobierno Digital, consagrado en el numeral 8 del artículo 2° de la Ley 1341 de 2009, las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones.

De acuerdo con el artículo 2.2.9.1.2.1 del Decreto número 1078 de 2015 (DUR-TIC), *por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones*, la Política de Gobierno Digital será definida por MinTIC 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.

Según el numeral 2, del artículo anteriormente citado, los habilitadores transversales de la Política de Gobierno Digital, son los elementos fundamentales de Seguridad y privacidad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los componentes y el logro de los propósitos de dicha Política.

El parágrafo del artículo 16 del Decreto número 2106 de 2019, *por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública*, señala que las autoridades deberán disponer de una estrategia de seguridad digital, para la gestión documental electrónica y preservación de la información, siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

Por lo anterior, es necesario que MinTIC establezca 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.

En mérito de lo expuesto,

RESUELVE:

Artículo 1°. *Objeto.* La presente resolución 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.

Artículo 2°. *Ámbito de aplicación.* Serán sujetos obligados de la presente resolución los señalados en el artículo 2.2.9.1.1.2. del Decreto número 1078 de 2015 (DUR-TIC), *por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones*.

Artículo 3°. *Lineamientos generales.* Los sujetos obligados deben adoptar medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al plan de seguridad y privacidad de la información y así mitigar riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital. Las entidades deben contar con políticas, procesos, procedimientos, guías, manuales y formatos para garantizar el cumplimiento al ciclo PHVA del MSPI. En ese sentido, deben adoptar los lineamientos del MSPI, guía de riesgos y gestión de incidentes de seguridad digital que se relacionan en el Anexo 1 de la presente resolución.

Para todos los procesos, trámites, sistemas de información, infraestructura tecnológica e infraestructura crítica de los sujetos obligados, se deben adoptar medidas de seguridad eficientes alienadas al MSPI, para prestar servicios de confianza, generando protección de la información de los ciudadanos, gestionando los riesgos y los incidentes de seguridad digital.

Artículo 4°. *Sistema de gestión de seguridad de la información y seguridad digital.* Los sujetos obligados deben aplicar los modelos, guías, y demás documentos técnicos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones a través del habilitador de seguridad y privacidad de la información en el marco de la Política de Gobierno Digital y propenderán por la incorporación de estándares internacionales y sus respectivas actualizaciones o modificaciones, al igual que otros marcos de trabajo que defina mejores prácticas en la materia.

Artículo 5°. *La estrategia de seguridad digital.* Los sujetos obligados deben adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital. Dicha estrategia se debe incluir en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos artículo 2.2.22.3.14. del Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto número 1083 de 2015, Único Reglamentario del Sector de Función Pública, o la norma que la modifique, adicione, subrogue o derogue.

El Plan de Seguridad y Privacidad de la Información contempla la protección de la información digital, medios impresos y físicos digitales y no digitales.

La estrategia de seguridad digital debe definirse en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes de seguridad digital, incorporadas en el Anexo 1 de la presente resolución y estar debidamente articulada al habilitador de seguridad y privacidad de la Política de Gobierno Digital.

Adicionalmente, la estrategia de seguridad digital debe:

1. Ser aprobada a través de un acto administrativo de carácter general.

2. Contar con un análisis y tratamiento de riesgos de seguridad digital e implementar controles que permitan gestionarlos.

3. Establecer los roles y responsabilidades al interior de la entidad asociados a la seguridad digital.

4. Establecer e implementar los principios, lineamientos y estrategias para promover una cultura para la seguridad digital y de la información que incluya actividades de difusión, capacitación y concientización tanto al interior de la entidad como frente a usuarios y terceros que ésta considere relevantes para mejorar habilidades y promover conciencia en la seguridad de la información. Estas actividades deben realizarse anualmente y pueden incluirse, adicionalmente, en el Plan Institucional de Capacitaciones (PIC), o el que haga sus veces.

5. La estrategia debe incluir todas las tecnologías de la información y las comunicaciones que utiliza la organización, incluida la adopción de nuevas tecnologías o tecnologías emergentes.

6. Aplicar las demás consideraciones que a juicio de la entidad contribuyan a elevar sus estándares de seguridad digital.

Parágrafo 1°. Los sujetos obligados deben adoptar el Modelo de Seguridad y Privacidad de la Información (MSPI) señalado en el Anexo 1 de la presente resolución, como habilitador de la política de Gobierno Digital.

Parágrafo 2°. El Modelo de Seguridad y Privacidad de la Información (MSPI) señalado en el Anexo 1 será actualizado por el MinTIC a través de las sucesivas versiones de cada uno de los documentos que lo componen y previo informe del equipo técnico. La actualización se publicará en la sede electrónica de MinTIC.

Artículo 6°. *La gestión de la seguridad de la información, seguridad digital y la gestión de riesgos de la entidad.* Los sujetos obligados deben determinar e implementar controles para mitigar los riesgos que pudieran afectar la seguridad digital y física de acuerdo con el resultado del análisis y evaluación de riesgos y cumplir con las siguientes características y responsabilidades:

1. Definir controles considerando aspectos tales como la estructura, tamaño, canales de atención, volumen transaccional, número de usuarios, evaluación del riesgo y servicios prestados por la entidad.

2. Realizar una gestión efectiva de la seguridad de la información y la seguridad digital en la entidad.
3. Reportar los resultados del análisis de riesgos y gestión de incidentes al comité institucional de gestión y desempeño o quien haga sus veces.

4. Estar al tanto de las nuevas modalidades de ciberataques que pudieran llegar a afectar a la entidad, según las políticas que establezca la entidad de acuerdo con su evaluación de riesgo y atendiendo criterios de razonabilidad.

5. Establecer las capacitaciones que recibirán los funcionarios de la entidad en temas relacionados con seguridad digital y mantenerlos actualizados sobre las nuevas amenazas cibernéticas.

6. Realizar el monitoreo del cumplimiento de las políticas y procedimientos que se establezcan en materia de seguridad de la información y sin perjuicio de aquellas tareas que realizan las autoridades de control.

7. Asesorar a la dirección de la entidad sobre seguridad de la información y seguridad digital para que pueda hacer seguimiento y tomar las decisiones adecuadas en esta materia.

8. Realizar un análisis de riesgo para determinar la pertinencia de contratar o implementar el servicio de un equipo especializado para atender incidentes de seguridad digital. El análisis debe identificar las características del proveedor, herramientas, servicios y privacidad de la información, entre otros.

9. Determinar los recursos técnicos, humanos y administrativos de seguridad de la información y seguridad digital, necesarios para la entidad. Dichos recursos deben manejarse de manera diferenciada a los de operaciones y tecnología de la información.

10. Implementar y gestionar un Sistema de Gestión de Seguridad de la Información de acuerdo a lo establecido en el Modelo de Seguridad y Privacidad de la Información, que permita gestionar los riesgos de seguridad de la información de la entidad de una manera adecuada y oportuna.

11. Cumplir los lineamientos de gestión del riesgo establecidos en la guía para la administración del riesgo y el diseño de controles en entidades públicas expedida en el marco del modelo integrado de planeación y gestión.

Artículo 7°. *Operaciones seguras*. Los sujetos obligados deben implementar mecanismos de gestión y monitoreo que protejan la infraestructura de TI de amenazas físicas y digitales.

Artículo 8°. *Controles e interoperabilidad*. Los sujetos obligados deben implementar controles y procesos que habiliten la integración al servicio ciudadano digital de interoperabilidad de forma segura y cumpliendo de los lineamientos dados sobre el particular en el marco de la política de gobierno digital.

Artículo 9°. *Gestión de incidentes de seguridad digital*. Los sujetos obligados deben establecer un procedimiento de gestión de incidentes de seguridad digital, para realizar el tratamiento, investigación y gestión de los incidentes de seguridad digital que se presente en relación con los activos de información de cada proceso, para lo cual deben:

1. Gestionar los incidentes de seguridad digital, según el procedimiento establecido por MinTIC, para lo cual deben crear una bitácora que contenga la descripción de cada una de las actividades desarrolladas en la gestión de estos.

2. Designar dentro de la entidad los responsables de gestionar y dar respuesta a los incidentes de seguridad digital, liderado por el responsable de seguridad digital.

3. Una vez identificado el incidente de seguridad digital se deberá reportar ante el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Digital) de Gobierno, los incidentes catalogados como Muy Grave y Grave por la entidad, para el respectivo apoyo y coordinación en la gestión de estos a través del formato de reporte establecido por el CSIRT Gobierno, el cual estará disponible por los canales de comunicación del CSIRT Gobierno.

4. Los incidentes catalogados por el responsable de seguridad digital de la entidad, como Menos Grave y Menor, deben ser comunicados al CSIRT Gobierno en el formulario establecido una vez sea gestionado, con el fin de poder llevar una estadística de los incidentes y conocer las tipologías de estos.

5. Los sujetos obligados, según el análisis e investigación de los incidentes y teniendo en cuenta la causa raíz, deben realizar los respectivos planes de mejoramiento, para lo cual el responsable de seguridad digital de la entidad supervisará y hará seguimiento a su cumplimiento.

Artículo 10. ***Privacidad de la información.*** Los sujetos obligados deben definir una estrategia que permita brindar servicios, controles y condiciones de protección de la privacidad de la información de la Entidad y los ciudadanos acorde con lo exigido en la Ley 1581 de 2012 y los decretos reglamentarios.

Artículo 11. ***Mecanismos de autenticación.*** Los sujetos obligados deben emplear mecanismos para la autenticación y segregar las funciones y responsabilidades de los usuarios con privilegios de administrador o que brindan soporte remoto, para mitigar los riesgos de seguridad de la información. Para ello, deben seguir el modelo de servicios ciudadanos digitales en particular el modelo de autenticación digital.

Artículo 12. ***Retención y destrucción final de información.*** Los sujetos obligados deben establecer procesos y procedimientos para la retención y destrucción final de la información digital, para ello seguirán las normas de gestión documental digital dispuestas por el Archivo General de la Nación.

Artículo 13. ***Seguridad digital desde el proceso de desarrollo de software.*** Los sujetos obligados deben integrar la seguridad digital, dentro del ciclo de vida del desarrollo del software para todos los sistemas de información, aplicaciones web y móviles, así como cualquier otro sistema que almacene, transmita o presente información, desde las etapas iniciales como el diseño y el levantamiento de requerimientos, hasta las pruebas de seguridad una vez el software se encuentre en producción, teniendo en cuenta los riesgos asociados a cada sistema de información. Dicho proceso deberá quedar documentado y estar alineado con las normas de responsabilidad demostrada en el tratamiento de datos personales señaladas en la Ley 1581 de 2012, el Decreto número 1074 de 2015 y demás normas que las desarrollan, adicionen o modifiquen.

Artículo 14. ***Terceros, colaboradores y seguridad digital.*** Los sujetos obligados deben incluir en su estrategia de seguridad digital y su plan de Seguridad y privacidad de la información las medidas y obligaciones pertinentes para la adopción y el cumplimiento de políticas y controles para la gestión de los riesgos de seguridad y privacidad de la información por parte de terceros y colaboradores.

Artículo 15. ***Control de las actividades incluidas en la estrategia de seguridad digital y gestión de riesgos.*** Los sujetos obligados deben establecer los mecanismos de control al interior de la entidad que permitan verificar el cumplimiento de las disposiciones establecidas en la política de seguridad de la información que hayan aprobado internamente, realizando auditorías de seguridad de la información al menos una vez al año, que contemplen aspectos técnicos de la seguridad digital como análisis de vulnerabilidades a sistemas de información críticos, entre otros.

Así mismo, deberán contar con indicadores para medir la eficacia, efectividad y eficiencia de la gestión de la seguridad de la información y la seguridad digital.

Artículo 16. ***Seguridad digital y responsabilidad.*** Los sujetos obligados podrán incluir en su estrategia de seguridad digital los elementos de valoración que se requerirán para determinar la conveniencia de contar con garantías que cubran los costos asociados a ataques cibernéticos.

Artículo 17. ***Etapas generales de la gestión de incidentes de seguridad digital.*** Los sujetos obligados deben incluir en su estrategia de seguridad digital las actividades a realizar en las etapas de prevención; protección y detección; respuesta y comunicación; recuperación y aprendizaje, como mínimo deberán incorporar:

1. **Prevención**

La función de prevención admite la capacidad de limitar o contener el impacto de un posible incidente de seguridad digital. En esta etapa, los sujetos obligados deben cuando menos:

1.1. Establecer, mantener y documentar los controles de acceso (lógicos, físicos y procedimentales), protección de infraestructura y gestión de identidades, privacidad y protección de la información.
1.2. Adoptar políticas, procedimientos y mecanismos para evitar la fuga de datos e información.
1.3. Gestionar y documentar la seguridad de la plataforma tecnológica.
1.4. Contar con los recursos tecnológicos necesarios para realizar una adecuada gestión de seguridad de la información y la ciberseguridad.
1.5. Identificar, y gestionar los riesgos de seguridad de la información que puedan llegar a afectar a la entidad y establecer controles para su mitigación.
1.6. Considerar dentro del plan de continuidad del negocio la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques de seguridad de la información.
1.7. Realizar pruebas del plan de continuidad del negocio que simulen la materialización de ataques de seguridad de la información.
1.8. Determinar la necesidad de contar con herramientas o servicios que permitan hacer correlación de eventos que puedan alertar sobre incidentes de seguridad, entre otros, SIEM (Gestión de eventos de información de seguridad) o SOC (Centro de operaciones de seguridad).
1.9 De acuerdo con la estructura, infraestructura, canales de atención, volumen transaccional y número de clientes, monitorear diferentes fuentes de información institucionales oficiales tales como sistemas de información, infraestructuras críticas, correos electrónicos, sitios web, blogs, dispositivos y perfiles oficiales de redes sociales con el propósito de identificar posibles ataques cibernéticos contra la entidad.
1.10. Colaborar y articular con las autoridades que hacen parte del modelo nacional de gestión de ciberseguridad en los proyectos que se adelanten con el propósito de fortalecer la gestión de la ciberseguridad a nivel nacional.

2. **Protección y detección**

La función de protección y detección permite el descubrimiento oportuno de eventos e incidentes de ciberseguridad y cómo protegerse ante los mismos. Los sujetos obligados deben:

1. 1. Adoptar procedimientos y mecanismos para identificar y analizar los incidentes de seguridad que se presenten.

1.2. Gestionar las vulnerabilidades de aquellas infraestructuras críticas o plataformas que soporten activos de información críticos y que estén expuestos en el ciberespacio.

1.3. Realizar un monitoreo continuo a su plataforma tecnológica e infraestructura crítica con el propósito de identificar y predecir comportamientos inusuales que puedan evidenciar ataques contra la entidad.

1.4. Implementar tecnologías que permitan a la Entidad identificar el origen de los ataques, tipos de ataques, comportamientos y la detección predictiva de amenazas.

1.5. Realizar periódicamente auditorías de seguridad de la información tanto para los aspectos de gestión como para los aspectos técnicos, como podrían ser: auditorías internas y externas al modelo de Seguridad y Privacidad de la Información, análisis de vulnerabilidades, Hacking ético, pruebas de penetración a sistemas informático y pruebas de ingeniería social entre otras.

3. Respuesta y comunicación

Aún con las medidas de seguridad adoptadas, los sujetos obligados deben desarrollar e implementar planes de respuesta a incidentes de seguridad digital. Para hacerle frente a esta situación los sujetos obligados deben:

1. 1. Establecer planes y procedimientos de respuesta a incidentes digitales y de seguridad de la información.

1. 2. Establecer los procedimientos para reportar, cuando se considere pertinente, al Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT) o quien haga sus veces, a través del CSIRT sectorial, los incidentes de seguridad Digital que requieran de su gestión.

1. 3. Comunicar a las autoridades competentes después de una fuga o afectación a la privacidad de la información de la Entidad o ciudadanos.

1. 4. Dar un tratamiento adecuado a las evidencias forenses para que las áreas de seguridad digital y las autoridades puedan realizar su identificación, recolección, embalaje y disposición en las investigaciones correspondientes.

4. Recuperación y aprendizaje

Desarrollar e implementar actividades apropiadas para definir y mantener los planes de recuperación, resiliencia y restauración de las infraestructuras críticas, servicios, sistemas de información, procesos o en general de un activo de información que se haya deteriorado debido a un incidente de seguridad digital. Los sujetos obligados deben:

1. 1. Adoptar los mecanismos necesarios para recuperar los sistemas de información e infraestructuras al estado en que se encontraban antes del ataque de seguridad.

1. 2. Ajustar sus sistemas de gestión de riesgo y de seguridad de la información como consecuencia de los incidentes presentados, adoptando los controles que resulten pertinentes.

1. 3. Socializar, cuando la entidad lo considere pertinente, las lecciones aprendidas al interior de la organización y con las entidades de su sector.

Artículo 18. ***Vigencia*****.** La presente resolución rige a partir de la fecha de su publicación en el ***Diario Oficial***.

Publíquese y cúmplase.

Dada en Bogotá, D. C., a 10 de marzo de 2021.

La Ministra de Tecnologías de la Información y las Comunicaciones,

Karen Abudinen Abuchaibe.

Modelo de Seguridad y Privacidad de la Información

Karen Cecilia Abudinen Abuchaibe - Ministra de Tecnologías de la Información y las Comunicaciones
Germán Camilo Rueda - Viceministro de Transformación Digital
Aura María Cifuentes Gallo - Directora de Gobierno Digital
Gersson Jair Castillo Daza- Subdirector de Estándares y Arquitectura de TI
Angela Janeth Cortés Hernández – Líder del equipo de Seguridad y Privacidad de la Información
Danny Alejandro Garzón – Asesor del equipo de Seguridad y Privacidad de la Información
Andrés Díaz Molina - Oficial de Seguridad y Privacidad de la Información
Juan Carlos Noriega – Líder del equipo de Política
Marco E. Sánchez Acevedo – Abogado del equipo de Política
Ministerio de Tecnologías de la Información y las Comunicaciones
Viceministerio de Transformación Digital
Dirección de Gobierno Digital

Versión	Observaciones
Versión 4 22/02/2021	**Documento Maestro del Modelo de Seguridad y Privacidad de la Información** Dirigida a las Entidades del Estado

Contenido

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

01. Introducción

El Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, es consecuente con la realidad de que las entidades públicas están cada vez más expuestas a sufrir incidentes de seguridad digital, lo cual, puede afectar su funcionamiento repercutiendo en la prestación de los servicios a la ciudadanía. Razón por la cual el ministerio como entidad encargada de diseñar, adoptar y promover políticas, planes, programas y proyectos en el uso y apropiación de las TIC, establece lineamientos con el objetivo de generar confianza en el uso del entorno digital, garantizando el máximo aprovechamiento de las tecnologías de la información y las comunicaciones.

La política de gobierno digital tiene como objetivo promover lineamientos, planes, programas y proyectos en el uso y apropiación de las TIC para generar confianza en el uso del entorno digital, propendiendo por el máximo aprovechamiento de las tecnologías de la información y las comunicaciones. Además establece como habilitador transversal la seguridad y privacidad de la información, mediante el cual se definen de manera detallada la implementación de controles de seguridad físicos y lógicos con el fin de asegurar de manera eficiente los trámites, servicios, sistemas de información, plataforma tecnológica e infraestructura física y del entorno de las Entidades públicas de orden nacional y territorial, gestionando de manera eficaz, eficiente y efectiva los activos de información, infraestructura critica, los riesgos e incidentes de seguridad y privacidad de la información y así evitar la interrupción en la prestación de los servicios de la Entidad enmarcados en su modelo de operación por procesos.

Teniendo en cuenta lo anterior, el MinTIC elaboró el Modelo de Seguridad y Privacidad de la Información – MSPI y define los lineamientos para la implementación de la estrategia de seguridad digital, con el objetivo de formalizar al interior de de los sujetos obligados un sistema de gestión de seguridad de la información – SGSI y seguridad digital, el cual contempla su operación basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento; el modelo consta de cinco (5) fases las cuales permiten que las Entidades puedan gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información. Por ello, los sujetos obligados deben abordar las siguientes fases:

1. Diagnóstico: Realizar un diagnóstico o un análisis GAP, cuyo objetivo es identificar el estado actual de la Entidad respecto a la adopción del MSPI. Se recomienda usar este diagnóstico al iniciar el proceso de adopción, con el fin de que su resultado sea un insumo para la fase de planificación y luego al finalizar la Fase 4 de mejora continua.

2. Planificación: Determinar las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta su mapa de procesos, el tamaño y en general su contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo.

3. Operación: Implemetar los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.

4. Evaluación de desempeño: Determinar el sistema y forma de evaluación de la adopción del modelo.

5. Mejoramiento Continuo: Establecer procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición.

Cada una de las fases se dará por completada, cuando se cumplan todos los requisitos definidos en cada una de ellas.

Ilustración 1 Ciclo del Modelo de Seguridad y Privacidad de la Información

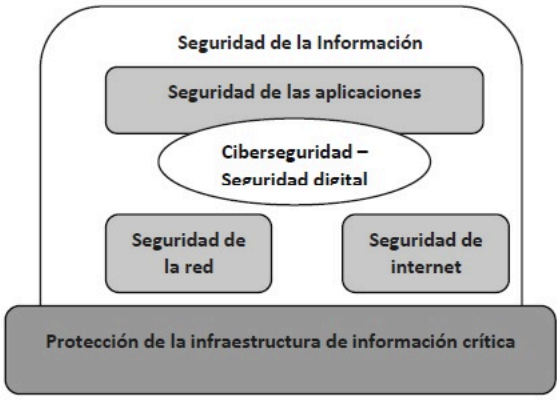

Ilustración 2. Relación entre la ciberseguridad y otros ámbitos de la seguridad (Fuente: ISO/IEC 27032)

02. Audiencia

El presente documento está dirigido a los sujetos señalados en el artículo 2.2.9.1.1.2. del Decreto 1078 de 2015 (DUR-TIC), "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"

03. Definiciones

A los efectos de la presente guía se deberán atender las siguientes definiciones:

- Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

- Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).

- Activos de Información y recursos: se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 20116).

- Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

- Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).

- Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

- Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

- Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

- Ciberseguridad: Protección de activos de información, mediante el tratamiento de las amenazas que ponenn en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.
- Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

- Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las Entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

- Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

- Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

- Datos Personales Mixtos: Para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.

- Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

- Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

- Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3) x Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- 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 la Ley 1712 de 2014. (Ley 1712 de 2014, art 6) x 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 la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.

- Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.

- Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las Entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

- Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

- Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

- Responsabilidad Demostrada: Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

- Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3).

- Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).

- Seguridad digital: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

- Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

- 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).

- Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o Entidad. (ISO/IEC 27000).

- Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

- Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

04. Propósitos

- Proporcionar a los sujetos obligados mecanismos, lineamientos e instrumentos de implementación claros que les permitan adoptar, implementar y apropiar el MSPI con mayor facilidad.

- Aportar en el desarrollo e implementación de la estrategia de seguridad digital de las Entidades.

- Establecer procedimientos de seguridad que permitan a las Entidades apropiar el habilitador de seguridad en la política de Gobierno Digital.

- Institucionalizar la seguridad y privacidad de la información en los procesos y procedimientos de las Entidades.

- Mediante la implementación eficiente, eficaz y efectiva del MSPI, se busca contribuir al incremento de la transparencia en la gestión pública.

- Contribuir en el desarrollo y ejecución del plan estratégico institucional, de cada entidad, a través del plan de seguridad y privacidad de la información.

05. Marco jurídico

- Conforme con lo establecido en la normatividad vigente el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, hace referencia a las siguientes normas, que se deben tener en cuenta para el desarrollo de la apropiación del MSPI en la Entidad:

- Constitución Política de Colombia. Artículos 15, 209 y 269.

- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.

- Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.

- Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

- Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.

- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Decreto 1080 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura.

- Decreto 1081 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.

- Decreto 1083 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.

- CONPES 3854 de 2016. Política Nacional de Seguridad digital.

- Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

- Decreto 612 de 2018. Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

- Decreto 2106 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

- Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario

06. Diagnóstico

La fase de diagnóstico permite a los sujetos obligados establecer el estado actual de la implementación de la seguridad y privacidad de la información, para tal fin se debe realizar un Diagnóstico” utilizando el “instrumento de evaluación MSPI” con el que se identifica de forma específica los controles implementados y faltantes y así tener insumos fundamentales para la fase de planificación.

Este autodiagnóstico se debe realizar antes de iniciar la fase de planificación, y actualizarlo posterior al término de la fase de evaluación de desempeño, esto con el fin de identificar los avances en la implementación del Modelo en la entidad, el resultado que se obtenga posterior a la fase de evaluación de desempeño será incluido como un insumo, en la fase de mejoramiento continuo.

Lineamiento:	Identificar a través de la herramienta de autodiagnóstico (Análisis GAP) el estado actual de la Entidad respecto a la Seguridad y privacidad de la Información.
Propósito:	Identificar el nivel de madurez de seguridad y privacidad de la información en que se encuentra la Entidad, como punto de partida para la implementación del MSPI.

Entradas recomendadas	Salidas
• Para la identificación del estado de implementación del MSPI, se debe utilizar la herramienta de autodiagnóstico del MSPI. • Revisar aspectos internos tales como el talento humano, procesos y procedimientos, estructura organizacional, cadena de servicio, recursos disponibles, cultura organizacional, entre otros.	• Documento con el resultado de la herramienta de autodiagnóstico, identificando la brecha en la implementación del MSPI en toda la Entidad, y sus acciones de mejora.

07. Planificación

Para el desarrollo de esta fase se debe utilizar los resultados de la fase anterior y proceder a elaborar el Plan de Seguridad y Privacidad de la Información con el objetivo de que la Entidad realice la planeación del tiempo, recursos y presupuesto de las actividades que va a desarrollar relacionadas con el MSPI.
Los documentos que se deben generar en esta fase son:

- Alcance MSPI

- Acto administrativo con las funciones de seguridad y privacidad de la información.

- Política de seguridad y privacidad de la información.
- Documento de roles y responsabilidades asociadas a la seguridad y privacidad de la información
- Procedimiento de inventario y Clasificación de la Información e infraestructura crítica
- Metodología de inventario y clasificación de la información e infraestructura crítica
- Procedimiento de gestión de riesgos de seguridad de la información
- Plan de tratamiento de riesgos de seguridad de la información
- Declaración de aplicabilidad
- Manual de políticas de Seguridad de la Información
- Plan de capacitación, sensibilización y comunicación de seguridad de la información

7.1 Contexto

7.1.1 Comprensión de la organización y de su contexto

Lineamiento:	Determinar los elementos externos e internos que son relevantes con las actividades que realiza la Entidad en el desarrollo de su misión y que podrían influir en las capacidades para lograr los objetivos del modelo, alineado con los objetivos estratégicos de la Entidad
Propósito:	Conocer en detalle las características de la Entidad y su entorno, que permitan implementar el Modelo de Seguridad y Privacidad adaptado a las condiciones específicas de cada Entidad.

Entradas recomendadas	Salidas
H Para establecer el contexto de la Entidad **debe tener en cuenta los aspectos relacionados en el Manual Operativo MIPG.** H Modelo estratégico, modelo de procesos, modelo de servicios y modelo organizacional siguiendo el Marco de Referencia de Arquitectura Empresarial definido por MinTIC. • **Plan estratégico de la Entidad**	**Documentos obligatorios:** Contexto de la entidad (Política de Planeación Institucional).

7.1.2 Necesidades y expectativas de los interesados

Lineamiento: Se debe determinar partes interesadas internas o externas como las personas, entidades u organizaciones que pueden influir directamente en la seguridad y privacidad de la información de la Entidad o que pueden verse afectados en caso de que estas se vean comprometidas. Adicionalmente se deberán determinar sus necesidades y/o expectativas (intereses) relacionados con la seguridad y privacidad de la información. Los requisitos de las partes interesadas deberán incluir los requisitos legales, reglamentarios y contractuales.

Propósito: Conocer las expectativas que se tiene respecto a la implementación del modelo de seguridad y privacidad de la información, para asegurar que el modelo garantizará su cumplimiento.

Entradas recomendadas	Salidas
• 7.1.1 Comprensión de la organización y de su **contexto** • Política de Planeación institucional**7.1.1 Comprensión de la organización y de su contexto** • Plan Nacional de Desarrollo. • Política de Gobierno Digital. • Entrevistas con los líderes de procesos de la Entidad. • Listado de entidades de orden nacional o territorial que se relacionan directamente el cumplimiento misional de la Entidad. • Listado de proveedores de la Entidad. • Listado de operadores de la Entidad. • Normatividad que le aplique a la Entidad de acuerdo con funcionalidad respectivamente.	**Documentos obligatorios:** Partes interesadas. (Política de Planeación Institucional).

7.1.3 Definición del alcance del MSPI

Lineamiento:
- Determinando los límites y la aplicabilidad del MSPI en el marco del modelo de operación por proceso de la Entidad. Determinando a qué procesos y recursos tecnológicos se realizará la implementación del MSPI.

Propósito:
- Identificar qué información (generada o utilizada en los procesos de la Entidad) será protegida mediante la adopción del MSPI.

Entradas recomendadas	Salidas
• 7.1.1 Comprensión de la organización y de su **contexto** (numeral 0)**7.1.1 Comprensión de la organización y de su contexto** • 7.1.2 Necesidades y expectativas de los **interesados** (numeral 0) • Modelo de procesos, modelo organizacional, modelo de servicios y catálogo de servicios tecnológicos; siguiendo el Marco de Referencia de Arquitectura Empresarial definido por MinTIC. • Presupuesto disponible para implementar el MSPI. • Listado de las sedes físicas donde opera la Entidad.	• Alcance del MSPI, (Este alcance puede estar integrado al Manual del Sistema Integrado de Gestión, o

7.2 Liderazgo

7.2.1 Liderazgo y Compromiso

Lineamiento: Cada sujeto obligado debe incluir dentro del
- desempeño o quien haga sus veces, las funci
- privacidad de la información, adoptando,
- mejorando continuamente el MSPI, por medio
- propósito de garantizar el éxito de su in
- cumplimento entre otras, a las siguientes accion
  - Establecer y publicar la adopción de la p políticas específicas de seguridad y privacida
  - Garantizar la adopción de los requisitos del
  - Comunicar en la Entidad la importancia del
  - Planear y disponer de los recursos necesar etc.) para la adopción del MSPI.
  - Asegurar que el MSPI consiga los resultados
  - Realizar revisiones periódicas de la adopció año y en las que el Nominador deberá estar

Propósito: Garantizar el liderazgo y el compromiso del
- desempeño o quien haga sus veces para conse
- implementación del MSPI.

Entradas recomendadas	
• 7.1.3 Definición del alcance del **MSPI** (numeral 0) • Modelo de procesos y modelo organizacional articulado con el Marco de Referencia de Arquitectura Empresarial definido por MinTIC. • **7.1.2 Necesidades y expectativas de los interesados** (numeral 8.1.2)	• Evid sopo gesti vece segu infor

7.2.2 Política de seguridad y privacidad de la información

Lineamiento: Se debe establecer en la política de seguridad y privacidad de la información, que establezca el enfoque de la entidad, para ello debe tener en cuenta:

- Misión de la Entidad
- Normatividad vigente la cual se debe contar para el funcionamiento de la Entidad
- Establecer compromiso del cumplimiento de los requisitos relacionados con la seguridad y privacidad de la información, así como también el de la mejora continua una vez el MSPI sea adoptado
- Estar alineada con el contexto de la Entidad, así como la identificación de las áreas que hacen parte de la implementación de seguridad de la información.
- Se deben asignar los roles y responsabilidades que se identifiquen.
- Ser incluidos y aprobados los temas de seguridad de la información y seguridad digital en el comité gestión y desempeño institucional, modificando el acto administrativo de conformación de este, aprobado por el mismo comité y expedido por el nominador o máxima autoridad de la Entidad.
- Ser comunicada al interior de la Entidad y a los interesados que aplique.

Propósito: La política establece la base respecto al comportamiento de personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la Entidad.
Orientar y apoyar por parte de la alta dirección de la Entidad a través del comité de gestión institucional, la gestión de la seguridad de la información de acuerdo con la misión de la entidad, normatividad y reglamentación pertinente.

Entradas recomendadas	Salidas
• Comprensión de la organización y de su contexto • Necesidades y expectativas de los interesados • Definición del alcance del MSPI • **Requerimientos normativos.**	• Acto administrativo con la adopción de la Política de seguridad y privacidad de la información.

7.2.3 Roles y responsabilidades

Lineamiento: Articular con las áreas o dependencias de la l
necesarios para la adopción del MSPI, el mo
seguimiento ante el comité institucional de
aprobados y comunicados dentro de la Entid
Se debe delegar a un responsable de la segu
el equipo humano necesario para coordina
cargo no existe en la Entidad deberá ser deleg
depender de un área estratégica que no sea
(se recomienda el despacho de nominador),
deberá ser incluida como miembro del comi
voto y en el comité de control interno con vo

Propósito: Hay que asegurar que los funcionarios de la
ellos, cuál es su impacto en la seguridad
contribuyen con la adopción del MSPI.

Entradas recomendadas	Salidas
• **7.1.3 Definición del alcance del** • Modelo de procesos, y modelo organizacional, desarrollados para la Arquitectura Misional de la Entidad, siguiendo el Marco de Referencia de Arquitectura Empresarial definido por MinTIC. • **¡Error! No se encuentra el origen de la referencia.**	Roles y re

7.3 Planificación

7.3.1 Identificación de activos de información e infraestructura critica

Lineamiento: Las entidades deben definir y aplicar un proceso de identificación y clasificación de la información, que permita:

- Determinar o identificar qué activos de información van a hacer parte del Inventario, que aportan valor agregado al proceso y por tanto necesitan ser protegidos de potenciales riesgos.
- Clasificar los activos de información de acuerdo con los tres principios de seguridad de la información, integridad, confidencialidad y disponibilidad para garantizar que la información recibe los niveles de protección adecuados.
- Actualizar el inventario y la clasificación de los activos por los propietarios y custodios de los activos de forma periódica o toda vez que exista un cambio en el proceso.

Propósito: Estructurar una metodología que permita identificar y clasificar los activos de información

Entradas recomendadas	Salidas
• **7.1.3 Definición del alcance del MSPI** • Modelo de procesos, y modelo organizacional, desarrollados para la Arquitectura Misional de la Entidad, siguiendo el Marco de Referencia de Arquitectura Empresarial definido por MinTIC. • Guía para la Gestión y Clasificación de Activos de Información	• Procedimiento de inventario y clasificación de la información.[1]. • Documento metodológico de inventario y clasificación de la información.

[1] *Anexo 1. Guía para la Gestión y Clasificación de Activos de Información*

7.3.2 Valoración de los riesgos de seguridad de la i

Lineamiento: Las entidades deben definir y aplicar un proce seguridad y privacidad de la información, que pe

- Identificar los riesgos que causer integridad, disponibilidad, privacida continuidad de la operación de la En
- Identificar los dueños de los riesgos.
- Definir criterios para valorar las con los riesgos, y la probabilidad de su oc
- Determinar el apetito de riesgos defi
- Establecer criterios de aceptación de
- Aplicar el proceso de valoración del riesgos asociados a la perdida disponibilidad de la información que
- Determinar los niveles de riesgo.
- Realizar la comparación entre los res los riesgos establecidos en este misn
- Priorización de los riesgos analizados

Se debe asegurar que las valoraciones repeti privacidad de la información produzcan re comparables.

Propósito: Estructurar una metodología que permita ges privacidad de la información.

Entradas recomendadas	
• 7.1.3 Definición del alcance del **MSPI** • • 7.2.2 Política de seguridad y **privacidad de la información** • Directorio de servicios de componentes de información, de acuerdo con el Marco de Referencia de Arquitectura Empresarial definido por MinTIC. • Inventario de activos de información de la Entidad usando: o ¡Error! No se encuentra el origen de la referencia. • Proceso de valoración de riesgos de la seguridad de la información definido por medio de: o Lineamientos para la Gestión del Riesgo de Seguridad Digital en	• Pro ges incl priv por con

[2] *Anexo 1. Guía para la gestión de riesgos de seguridad digital.*

Entidades Públicas - Guía riesgos vigente.

7.3.3 Plan de tratamiento de los riesgos de seguridad de la información

Lineamiento:

- La Entidad debe definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información, que permita:
- Seleccionar las opciones (controles) pertinentes y apropiadas para el tratamiento de riesgos.
- Elaborar una declaración de aplicabilidad que contenga: los controles necesarios, su estado de implementación y la justificación de posible exclusión.
- Definir un plan de tratamiento de riesgos que contenga, fechas y responsables con el objetivo de realizar trazabilidad.
- Los dueños de los riesgos deben realizar la aprobación formal del plan de tratamiento de riesgos y esta aceptación debe llevarse a la revisión por dirección en el Comité Institucional y de Desempeño, o quien haga sus veces.

Propósito:

- Estructurar una metodología que permita definir las acciones que debe seguir la Entidad para poder gestionar los riesgos de seguridad y privacidad de la información

Entradas recomendadas	Salidas
• Inventario de activos de información de la Entidad. • 7.3.2 Valoración de los riesgos de seguridad de la **información**	• Plan de tratamiento de riesgos, aprobado por los dueños de los riesgos y el comité institucional de gestión y desempeño (Decreto 612 de 2018 Publicación antes de 31 de enero de cada vigencia). • Declaración de aplicabilidad, aceptada y aprobadas en el comité de gestión institucional.

7.4 Soporte

7.4.1 Recursos

Lineamiento: La Entidad debe determinar y proporcionar l MSPI, teniendo en cuenta que es un proces que se disponga de los recursos fin horas/hombre) de sus colaboradores y en g la adopción, implementación, mantenimien

Determinar y proporcionar los recursos implementación, mantenimiento y mejora c

Propósito:

Entradas recomendadas
• 7.1 **Contexto** • 7.1.3 Definición del alcance del **MSPI** • 7.2.2 Política de seguridad y privacidad **de la información** • 7.2.3 Roles y **responsabilidades** • 7.3.3 Plan de tratamiento de los riesgos de seguridad de la **información**

7.4.2 Competencia, toma de conciencia y comunicación

Lineamiento

La Entidad debe definir un plan de comunicación, capacitación, sensibilización y concientización para:

- Asegurar que las personas cuenten con los conocimientos, educación y formación o experiencia adecuada para la implementación y gestión del modelo de seguridad y privacidad de la información.
- Involucrar al 100% de los funcionarios de la entidad en la implementación y gestión del MSPI.
- Concientizar a los funcionarios y partes interesadas en la importancia de la protección de la información.
- Identificar las necesidades de comunicaciones internas y externas relacionadas con la seguridad y privacidad de la información. Se deberá definir qué será comunicado, cuándo, a quién, quién debe comunicar y finalmente definir los procesos para lograrlo.

Propósito:

Garantizar una correcta comunicación, sensibilización y concientización con respecto a la seguridad y privacidad de la información, en la que todos sus funcionarios estén al tanto de la política de seguridad y privacidad, cuál es su rol en el cumplimiento del MSPI, beneficios y consecuencias de no poner en práctica las reglas definidas en el modelo (desde el punto de vista de seguridad y privacidad de la información).

Entradas recomendadas	Salidas
• 7.1.3 Definición del alcance del **MSPI** (numeral 0) • 7.2.3 Roles y **responsabilidades** (numeral 0) • Manual de funciones de la Entidad. • Plan de capacitación Institucional.	• Plan de cambio, cultura, apropiación, capacitación y sensibilización de Seguridad y Privacidad de la Información y seguridad digital. Este se puede incluir en el Plan Institucional de Capacitaciones - PIC. • Plan de comunicaciones del modelo de seguridad y privacidad de la información.

08. Fase 2: Operación

Una vez culminada las actividades del MSPI de la fase de 7.3 Planificación, se llevará acabo la implementación de los controles, con el fin de dar cumplimiento con los requisitos del MSPI.

Los documentos que se deben generar en esta fase son:

- Plan de implementación de controles de seguridad y privacidad de la información

- Evidencia de la implementación de los controles de seguridad y privacidad de la información

8.1 Planificación e implementación

Lineamiento: **La Entidad debe realizar la planificación e implementación de las acciones determinadas en el plan de tratamiento de riesgos, esta información debe estar documentada por proceso según lo planificado. Estos documentos deben ser aprobados por el comité institucional** de gestión y desempeño.

Propósito:

Implementar los planes y controles para lograr los objetivos del MSPI

Entradas recomendadas	Salidas
• 7.3.2 Valoración de los riesgos de seguridad de la **información** • Plan de 7.3.3 Plan de tratamiento de los riesgos de seguridad **de la información**	• Plan de implementación de controles de seguridad y privacidad de la información que contenga como mínimo: controles, actividades, fechas, responsable de implementación y presupuesto. • Evidencia de la implementación de los controles de seguridad y privacidad de la información.

09. Fase 3: Evaluación de desempeño

Una vez culminada las actividades del MSPI, se evalúa la efectividad de las acciones tomadas a través de los indicadores definidos en la fase de implementación que debe incluir la correcta interacción entre el MSPI, MIPG y los requerimientos de la Ley 1581 de 2012 “Protección de datos personales”, Ley 1712 de 2014 “Ley de Transparencia y Acceso a la Información Pública”, Decreto 2106 de 2019 o cualquier norma que las reglamente, adicione, modifique o derogue.

9.1.1 Seguimiento, medición, análisis y evaluación

Lineamiento: Es importante que las Entidades conozcan de manera permanente los avances en su gestión, los logros de los resultados y metas propuestas, para la implementación del modelo habilitador de la Política de Gobierno Digital. Para tal fin es importante establecer los tiempos, recursos previstos para el monitoreo, desempeño, resultados y aceptación de estos en el comité de gestión institucional y desempeño, como lo establece el MIPG. Es importante incluir dentro del plan de auditorías los temas relacionados con seguridad digital como lo establece el MIPG.

Propósito: Evaluar el desempeño de seguridad de la información y la eficacia del MSPI.

Entradas recomendadas	Salidas
• Documento con los resultados de la valoración de los riesgos • Documento con los resultados del tratamiento de riesgos de seguridad de la información • Resultado de la implementación de controles	• Hoja de vida de indicadores[3], los cuales deben incluirse en el tablero de control del plan de acción, tal como lo ordena el decreto 612 de 2018. • Informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos.

9.1.2 Auditoría Interna

Lineamiento: Realizar las auditorías internas con el fin de obtener información sobre el cumplimiento del MSPI.

Entradas recomendadas	Salidas
• Todos los documentos producto de las salidas de las fases anteriores del MSPI. • El informe de los resultados de las evaluaciones independientes, seguimientos y auditorías. • Informes y compromisos adquiridos en los comités institucional de gestión y desempeño.	• Resultados de las auditorías internas. • No conformidades de las auditorías internas. • Plan de auditorías que evidencia la programación de las auditorias de seguridad y privacidad de la información, este plan debe estar aprobado por el Comité de Coordinación de Control Interno.

[3] *Para la definición de los indicadores se puede utilizar como modelo la Guía - Indicadores Gestión de Seguridad de la Información*

• El informe de los incidentes de seguridad y privacidad de la información reportados y la solución de estos. • Informe sobre los cambios PESTEL[4] (legales, procesos, reglamentarios, regulatorios, tecnológicos, ambientales, o aquellos en el marco del contexto de la organización) en la Entidad. • Indicadores definidos y aprobados para la evaluación del MSPI.	

9.1.3 Revisión por la dirección

Lineamiento: Los temas de seguridad y privacidad de la información, seguridad digital y en especial la Política y el Manual de Políticas de Seguridad y Privacidad de la Información deben ser tratados y aprobados en el comité institucional de gestión y desempeño, o cuando el nominador lo determine.

Propósito: Revisar el MSPI de la Entidad, por parte de la alta dirección (comité de gestión institucional), en los intervalos planificados, que permita determinar su conveniencia, adecuación y eficacia.

Entradas recomendadas	Salidas
• Todos los documentos del MSPI deberán **ser aprobados,** incluyendo los actos administrativos que se necesiten para constituirlos al interior de la Entidad.	• Revisión a la implementación • Acta y documento de Revisión por la Dirección. • Compromisos de la Revisión por la Dirección.

10 Fase 4: Mejoramiento continuo

Una vez culminada las actividades del MSPI de la fase evaluación y desempeño, se debe consolidar los resultados obtenidos de la fase de evaluación de desempeño y diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

10.1 Mejora

Lineamiento:	Es importante que las Entidades elaboren un plan de mejoramiento continuo con el fin de realizar acciones correctivas, optimizar procesos o controles y mejorar el nivel de madurez del MSPI.
Propósito:	Identificar las acciones asociadas a la mejora continua del MSPI y de los procesos.

Entradas recomendadas	Salidas
• Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI. • Resultados de auditorías y revisiones independientes al MSPI.	• Plan anual de mejora del MSPI

11. ANEXOS

11.1 Controles y objetivos de control

La siguiente tabla muestra los controles de seguridad detallando cada uno de los dominios establecidos en el anexo A de la norma NTC: ISO/IEC 27001, los cuales tratan de los objetivos de control, y se estructurarán tal como lo muestra la Tabla 1:

Tabla 1 – Estructura de los controles.

Políticas especificas			
Núm.	Nombre	Seleccionado / Excepción	Descripción / Justificación
	Nombre	Control	
	...		

Cada uno de los campos de la tabla anterior se definen de la siguiente manera:

- Núm.: Este campo identifica cada uno de los controles correspondientes al Anexo A de la norma NTC: ISO/IEC 27001.
- Nombre: Este campo hace referencia al nombre del control que se debe aplicar para dar cumplimiento a la política definida.
- Control: Este campo describe el control que se debe implementar con el fin de dar cumplimiento a la política definida.
- Dominio: Este campo describe si el control aplica para uno o múltiples dominios.
- Seleccionado / Excepción: El listado de controles además debe incluir un campo que permita ser utilizado para la generación de la declaración de aplicabilidad, donde cada uno de los controles es justificado tanto si se implementa como si se excluye de ser implementado, lo cual ayuda a que la Entidad tenga documentado y de fácil acceso el inventario de controles.
- Descripción / Justificación: El listado de controles cuenta con la descripción de cada control en la tabla. Adicionalmente, es posible utilizarlo para la generación de la declaración de aplicabilidad, donde cada uno de los controles es justificado tanto si se implementa como si se excluye de ser implementado.

Tabla 2: Controles del Anexo A del estándar ISO/IEC 27001:2013 y dominios a los que pertenece.

Núm.	Nombre	Descripción / Justificación
A.5	Políticas de seguridad de la información	
A.5.1	Directrices establecidas por la dirección para la seguridad de la información	Lineamiento: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.
A.5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.
A.5.1.2	Revisión de las políticas para seguridad de la información	Control: Las políticas para seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.
A.6	Organización de la seguridad de la información	
A.6.1	Organización interna	Lineamiento: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.
A.6.1.1	Roles y responsabilidades para la seguridad de información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
A.6.1.3	Contacto con las autoridades	Control: Se deben mantener los contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especial	Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
A.6.1.5	Seguridad de la información en la gestión de proyectos	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A.6.2	Dispositivos móviles y teletrabajo	Lineamiento: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.
A.6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.6.2.2	Teletrabajo	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
A.7	Seguridad de los recursos humanos	
A.7.1	Antes de asumir el empleo	Lineamiento: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.
A.7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
A.7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A.7.2	Durante la ejecución del empleo	Lineamiento: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.
A.7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberán recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
A.7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
A.7.3	Terminación o cambio de empleo	Lineamiento: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.
A.7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deben definir, comunicar al empleado o contratista y se deberían hacer cumplir.
A.8	Gestión de activos	
A.8.1	Responsabilidad por los activos	Lineamiento: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
A.8.1.1	Inventario de activos	Control: Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.
A.8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.
A.8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A.8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
A.8.2	Clasificación de la información	Lineamiento: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.
A.8.2.1	Clasificación de la información	Control: La información se debe clasificar en func criticidad y susceptibilidad a divulgación o a modi
A.8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implement procedimientos para el etiquetado de la informac clasificación de información adoptado por la orga
A.8.2.3	Manejo de activos	Control: Se deben desarrollar e implementar p activos, de acuerdo con el esquema de clasificaci organización.
A.8.3.1	Gestión de medios removibles	Control: Se deben implementar procedimien removibles, de acuerdo con el esquema d organización.
A.8.3.2	Disposición de los medios	Control: Se debe disponer en forma segura de los utilizando procedimientos formales.
A.8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información s autorizado, uso indebido o corrupción durante el
A.9	Control de acceso	
A.9.1	Requisitos del negocio para control de acceso	Lineamiento: Limitar el acceso a información y a información.
A.9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisa con base en los requisitos del negocio y de seguri
A.9.1.2	Política sobre el uso de los servicios de red	Control: Solo se debe permitir acceso de los usua para los que hayan sido autorizados específicame
A.9.2	Gestión de acceso de usuarios	Lineamiento: Asegurar el acceso de los usuarios autorizado a sistemas y servicios.
A.9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso form registro de usuarios, para posibilitar la asignación
A.9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de usuarios para asignar o revocar los derechos de a todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asigna privilegiado.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de la información secreta proceso de gestión formal.
A.9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben re usuarios, a intervalos regulares.
A.9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los em información y a las instalaciones de procesamien al terminar su empleo, contrato o acuerdo, o se cambios.
A.9.3	Responsabilidades de los usuarios	Lineamiento: Hacer que los usuarios rindan c información de autenticación.
A.9.3.1	Uso de la información de autenticación secreta	Control: Se debe exigir a los usuarios que cumpl para el uso de información de autenticación secr
A.9.4	Control de acceso a sistemas y aplicaciones	Lineamiento: Evitar el acceso no autorizado a sist
A.9.4.1	Restricción de acceso Información	Control: El acceso a la información y a las f aplicaciones se debe restringir de acuerdo con la
A.9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de contro aplicaciones se debe controlar mediante un proc
A.9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseña asegurar la calidad de las contraseñas.
A.9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictame que pudieran tener capacidad de anular el sistem
A.9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos
A.10	Criptografía	

Núm.	Nombre	Descripción / Justificación
A.10.1	Controles criptográficos	Lineamiento: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.
A.10.1.1	Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.10.1.2	Gestión de llaves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
A.11	Seguridad física y del entorno	
A.11.1	Áreas seguras	Lineamiento: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.
A.11.1.1	Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.
A.11.1.2	Controles físicos de entrada	Control: Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Control: Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
A.11.1.4	Protección contra amenazas externas y ambientales	Control: Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.1.5	Trabajo en áreas seguras	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.
A.11.1.6	Áreas de despacho y carga	Control: Se deben controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
A.11.2	Equipos	Lineamiento: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.
A.11.2.1	Ubicación y protección de los equipos	Control: Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.
A.11.2.2	Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
A.11.2.3	Seguridad del cableado	Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debe estar protegido contra interceptación, interferencia o daño.
A.11.2.4	Mantenimiento de equipos	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
A.11.2.5	Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
A.11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
A.11.2.8	Equipos de usuario desatendidos	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les dé protección apropiada.
A.11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
A.12	Seguridad de las operaciones	
A.12.1	Procedimientos operacionales y responsabilidades	Lineamiento: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.
A.12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.
A.12.1.2	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
A.12.1.3	Gestión de capacidad	Control: Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.

Núm.	Nombre	Descripción / Justificación
A.12.2	Protección contra códigos maliciosos	Lineamiento: Asegurarse de que la información y de información estén protegidas contra códigos m
A.12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de recuperación, combinados con la toma de concier proteger contra códigos maliciosos.
A.12.3	Copias de respaldo	Lineamiento: Proteger contra la perdida de datos
A.12.3.1	Respaldo de información	Control: Se deben hacer copias de respaldo d imágenes de los sistemas, y ponerlas a prueba política de copias de respaldo aceptada.
A.12.4	Registro y seguimiento	Lineamiento: Registrar eventos y generar evidenc
A.12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar re actividades del usuario, excepciones, fallas y even
A.12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de r alteración y acceso no autorizado.
A.12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y de registrar, y los registros se deberían proteger y re
A.12.4.4	sincronización de relojes	Control: Los relojes de todos los sistemas d pertinentes dentro de una organización o ámbito con una única fuente de referencia de tiempo.
A.12.5	Control de software operacional	Lineamiento: Asegurar la integridad de los sistem
A.12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos software en sistemas operativos.
A.12.6	Gestión de la vulnerabilidad técnica	Lineamiento: Prevenir el aprovechamiento de las
A.12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente informa técnicas de los sistemas de información que se organización a estas vulnerabilidades, y tomar las riesgo asociado.
A.12.6.2	Restricciones sobre la instalación de software	Control: Se debe establecer e implementar las re por parte de los usuarios.
A.12.7	Consideraciones sobre auditorias de sistemas de información	Lineamiento: Minimizar el impacto de las activida operacionales.
A.12.7.1	Información controles de auditoría de sistemas	Control: Los requisitos y actividades de auditoría sistemas operativos se deben planificar y acorda las interrupciones en los procesos del negocio.
A.13	Seguridad de las comunicaciones	
A.13.1	Gestión de la seguridad de las redes	Lineamiento: Asegurar la protección de la i instalaciones de procesamiento de información d
A.13.1.1	Controles de redes	Control: Las redes se deben gestionar y controla sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de los requisitos de gestión de todos los servicios de servicios de red, ya sea que los servicios se pre externamente.
A.13.1.3	Separación en las redes	Control: Los grupos de servicios de información, se deben separar en las redes.
A.13.2	Transferencia de información	Lineamiento: Mantener la seguridad de la infor organización y con cualquier Entidad externa.
A.13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debe contar con políticas, procedimi formales para proteger la transferencia de inform de instalaciones de comunicación.
A.13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deben tener en cuenta la tr del negocio entre la organización y las partes exte
A.13.2.3	Mensajería electrónica	Control: Se debe proteger adecuadamente la inf electrónica.

A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Control: Las instalaciones de procesamiento de información se debe implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
A.18	Cumplimiento	
A.18.1	Cumplimiento de requisitos legales y contractuales	Lineamiento: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.
A.18.1.2	Derechos de propiedad intelectual	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
A.18.1.3	Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A.18.1.4	Privacidad y protección de datos personales	Control: Cuando sea aplicable, se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.
A.18.1.5	Reglamentación de controles criptográficos	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
A.18.2	Revisiones de seguridad de la información	Lineamiento: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.
A.18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
A.18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

11.2. Guía - Roles y responsabilidades

11.2.1 Definición de roles y responsabilidades

Los sujetos obligados deben definir internamente las responsabilidades para ejecutar las actividades específicas de seguridad de la información designando al equipo que corresponda.

El mayor aporte que genera una definición de roles es que se tendrán establecidas las tareas que realizará cada uno de los miembros del equipo del MSPI, dejando un campo muy pequeño a que se presenten imprecisiones con referencia a las responsabilidades que cada integrante tiene.

Partiendo de este punto, las entidades tendrán asegurado que cada actividad establecida dentro de la etapa de planeación del MSPI, tenga un responsable claro y de igual forma que cada uno de los miembros del equipo responsable de la ejecución entiendan claramente sus roles y responsabilidades.

11.2.2 Identificación de los responsables

En primer lugar, se genera la necesidad de vincular de forma más efectiva al personal de alto nivel que estará vinculado al proceso de desarrollo del MSPI en las entidades para que el apoyo se vaya garantizandodesde el principio de la planeación del proyecto e ir marcando un punto de partida de éxito con la implementación del modelo de gestión de seguridad de la información planteado para la entidad.
Los representantes de alto nivel de la entidad deben identificar y establecer, sin perjuicio de lo establecido en la Ley 489 de 1998, en el menor tiempo posible (cada entidad establecerá los términos en los cuales se puede cumplir con esta obligación) organizar el grupo de trabajo responsable para implementar el Modelo de seguridad de la información en las entidades del Estado, definiendo el perfil y rol de conformdad con lo establecido en su documento de política.

Teniendo en cuenta lo anterior, al final del ejercicio el equipo directivo que lidera la implementación del MSPI, debe dar a conocer el perfil y responsabilidades de cada integrante.

1. Equipo de gestión al interior de cada una de las entidades

El equipo de gestión del proyecto en cada una de las entidades se encarga de tomar las medidas necesarias para planear, implementar y hacer seguimiento a todas las actividades necesarias para adoptar el Modelo de Seguridad de la Información al interior de su entidad, así como planear las actividades necesarias para una adecuada administración y sostenibilidad de este.

1. Perfiles y responsabilidades

A continuación, se proponen las siguientes actividades asociadas a la seguridad y privacidad de la información:

1. Responsable de Seguridad de la Información para la entidad

El Responsable de Seguridad de la información será el lider de la implementación del Modelo de seguridad y privacidad de la información en la Entidad y velará por el cumplimiento de las siguientes actividades:

- Fomentar la implementación de la Política de Gobierno Digital
- Asesorar a la Entidad en el diseño, implementación y mantenimiento del Modelo de Seguridad y privacidad de la Información para la entidad de conformidad con la regulación vigente.
- Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación actual de la entidad.
- Realizar la estimación, planificación y cronograma de la implementación del MSPI.
- Liderar la implementación y hacer seguimiento a las tareas y cronograma definido.
- Definir, elaborar e implementar las políticas, procedimientos, estándares o documentos que sean
- De su competencia para la operación del MSPI.
- Realizar el acompañamiento a los procesos y /o proyectos en materia de seguridad y privacidad de la información.
- Liderar y brindar acompañamiento a los procesos de la entidad en la gestión de riesgos de seguridad y privacidad de la información, así como los controles correspondientes para su mitigación y seguimiento al plan de tratamiento de riesgos, de acuerdo con las disposiciones y metodologías en la materia.
- Proponer la formulación de políticas y lineamientos de seguridad y privacidad de la información.

- Definir e implementar en coordinación con las dependencias de la Entidad, las estrategias de sensibilización y divulgaciones de seguridad y privacidad de la información para servidores públicos y contratistas.

- Apoyar a los procesos de la Entidad en los planes de mejoramiento para dar cumplimiento a los planes de acción en materia de seguridad y privacidad de la información.

- Definir, socializar e implementar el procedimiento de Gestión de Incidentes de seguridad de la información en la entidad.

- Efectuar acompañamiento a la alta dirección, para asegurar el liderazgo y cumplimiento de los roles y responsabilidades de los líderes de los procesos en seguridad y privacidad de la información.

- Poner en conocimiento de las dependencias con competencia funcional, cuando se detecten irregularidades, incidentes o prácticas que atentes contra la seguridad y privacidad de la información de acuerdo con la normativa vigente.

1. Comité Institucional de Gestión y Desempeño Institucional – Comité de Seguridad y privacidad de la información

Asegurar la implementación y desarrollo de políticas de gestión y directrices en materia de seguridad y privacidad de la información, mediante el cumplimiento de las siguientes actividades:

- Aprobación seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarios para la implementación interna de las políticas de seguridad y privacidad de la información.

- Socializar la importancia de adoptar la cultura de seguridad y privacidad de la información a los procesos de la entidad.

- Aprobar acciones y mejores prácticas que en la implementación del MSPI.

- Adoptar las decisiones que permitan la gestión y minimización de riesgos críticos de seguridad de la información.

- Las demás que tengan relación con el estudio, análisis y recomendaciones en materia de seguridad y privacidad de la información.

11.2.7. Oficina asesora Jurídica

- Brindar asesoría a los procesos de la Entidad en temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información.

- Brindar asesoría al Comité Institucional de Gestión y Desempeño en materia de temas normativos, jurídicos y legales vigentes que involucren acciones ante las autoridades competentes relacionados con seguridad y privacidad de la información.

- Verificar que los contratos o convenios de ingreso que por competencia deban suscribir los sujetos obligados, cuenten con cláusulas de derechos de autor, confidencialidad y no divulgación de la información según sea el caso.

- Representar a la Entidad en procesos judiciales ante las autoridades competentes relacionados con seguridad y privacidad de la información.

- Apoyar y asesorar a los procesos en la elaboración del Índice de Información clasificada y reservada de los activos de información de acuerdo con la regulación vigente.

11.2.8. Gestión del Talento Humano

- Controlar y salvaguardar la información de datos personales del personal de planta de la Entidad, en concordancia con la normatividad vigente.

- Realizar la gestión de vinculación, capacitación, desvinculación del personal de planta dando cumplimiento a los controles y normatividad vigente relacionada con seguridad y privacidad de la información.

11.2.9. Control Interno

Dentro de la definición de responsables en cada uno de los Dominios entregados en el Marco de arquitectura Empresarial, está contemplado el papel del responsable de seguridad y privacidad de la información de la entidad, de esta forma se tienen las siguientes responsabilidades específicas de acuerdo con el Dominio:

Tabla 3: Responsabilidades – Marco de Arquitectura Empresarial

DOMINIO	RESPONSABILIDADES
SERVICIOS TECNOLÓGICOS	- Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de información de la institución. - Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información. - Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad. - Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias.
	- Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. - Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.
ESTRATEGIA TI	- Definir la estrategia informática que permita lograr los objetivos y minimizar de los riesgos de la institución. Es el encargado de guiar la prestación del servicio y la adquisición de bienes y servicios relacionados y requeridos para garantizar la seguridad de la información.
GOBIERNO TI	- Seguir y controlar la estrategia de TI, que permita el logro de los objetivos y la minimización de los riesgos del componente de TI. Encargado monitorear y gestionar la prestación del servicio y la adquisición de bienes y/o servicios relacionados y requeridos para garantizar la seguridad de información.
SISTEMAS DE INFORMACIÓN	- Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la entidad. - Apoyar la implementación segura de los sistemas de información, de acuerdo con el modelo de seguridad y privacidad de la información del estado colombiano. - Desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información. - Liderar el proceso de gestión de incidentes de seguridad, así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados. - Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.
DE INFORMACIÓN	- Supervisar que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes de información implementados. - Verificar el cumplimiento de las obligaciones legales y regulatorias del estado relacionadas con la seguridad de la información.

USO Y APROPIACIÓN	- Desarrollar el plan de formación y sensibilización de la entidad incorporando el componente de seguridad de la información en diferentes niveles. - Supervisar los resultados del plan de formación y sensibilización establecido para la entidad, con el fin de identificar oportunidades de mejora. - Participar en la elaboración de los planes de gestión de cambio, garantizando la inclusión del componente de seguridad de la información en la implementación de los proyectos de TI.

Teniendo en cuenta la naturaleza de la entidad, debe conformarse un equipo para el desarrollo del proyecto al cual deben pertenecer miembros directivos y representantes de las áreas misionales, con el propósito de asegurar que toda la información más relevante de la entidad esté disponible oportunamente. De esta forma, se busca asegurar que sea una iniciativa de carácter transversal a la entidad, y que no dependa exclusivamente de la oficina o área de TI.

Una de las tareas principales del líder del proyecto es entregar y dar a conocer los perfiles y responsabilidades de cada Integrante al grupo de trabajo e identificar las personas idóneas para tomar cada rol. De esta forma, y de manera general se pone a consideración el siguiente listado para que las entidades analicen de acuerdo con su composición orgánica cuales deben ser los miembros del equipo de seguridad y privacidad de la información, de acuerdo con los siguientes perfiles:

- Personal de seguridad de la información.
- Un representante del área de Tecnología.
- Un representante del área de Control Interno.
- Un representante del área de Planeación.
- Un representante de sistemas de Gestión de Calidad.
- Un representante del área Jurídica.
- Funcionarios, proveedores, y ciudadanos

Es importante resaltar nuevamente la necesidad del compromiso de la Alta dirección de la entidad, de esta forma se presenta la figura No. 01, en la cual se presentan los perfiles de manera genérica el nivel al cual pertenecerían según lo propuesto.

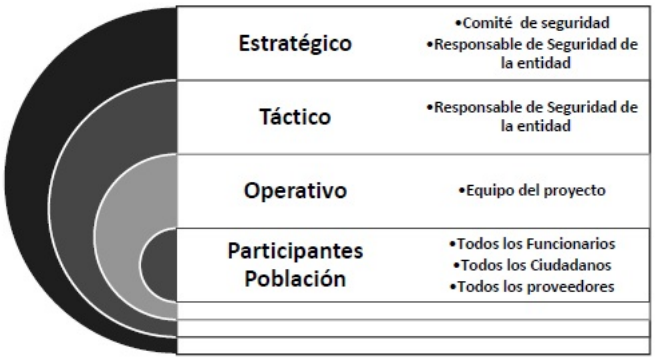

Ilustración 2: Equipo de Gestión de Seguridad de la Información en las entidades

RESPONSABILIDADES DEL EQUIPO DEL PROYECTO:

- Apoyar al líder de proyecto al interior de la entidad.
- Oficiar como consultores de primer nivel en cuanto a las dudas técnicas y de procedimiento que se puedan suscitar en el desarrollo del proyecto.
- Ayudar al líder de proyecto designado, en la gestión de proveedores de tecnología e infraestructura.
- Asistir a las reuniones de seguimiento o de cualquier otra naturaleza planeadas por el líder de proyecto.
- Las que considere el líder del proyecto o el comité de seguridad de la entidad.

De manera particular se resaltan dos perfiles que deben estar participando de manera activa durante el desarrollo del proyecto, a pesar de que el proyecto no es de responsabilidad exclusiva del área de TI su papel es fundamental, y de acuerdo con la Ley de Protección de Datos Personales se debe tener muy presente el rol de responsable del tratamiento de los datos personales.

Teniendo en cuenta que el responsable del tratamiento de datos personales en la entidad, es quien tiene decisión sobre las bases de datos que contengan este tipo de datos y que el responsable es quien direcciona las actividades de los encargados de los datos personales (quien realiza el tratamiento directamente), como se mencionaba anteriormente, adicional a las responsabilidades arriba citadas se tendrán en cuenta que de acuerdo a la Ley 1581 de 2012 Protección de Datos Personales los deberes y responsabilidades de los responsables y/o encargados del tratamiento de los datos personales son:

- Informar y garantizar el ejercicio de los derechos de los titulares de los datos personales.
- Tramitar las consultas, solicitudes y reclamos.
- Utilizar únicamente los datos personales que hayan sido obtenidos mediante autorización, a menos que los mismos no la requieran.
- Respetar las condiciones de seguridad y privacidad de información del titular.
- Cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente.

COMITÉ DE SEGURIDAD:

Las funciones de este comité pueden ser incluidas por el comité Institucional de desarrollo administrativo, como instancia orientadora de la implementación de la estrategia de Gobierno en línea de acuerdo con el señalado en el Art. 2.2.9.1.2.4. Responsable de orientar la implementación de la Estrategia de Gobierno en Línea; ó si la Entidad así lo estima conveniente, se debe crear un comité de Seguridad de la Información para la Entidad.
A continuación, se presenta un ejemplo de plantilla que podría servir como base para la generación de la resolución para la creación del comité de seguridad de la información para las entidades, se reitera que está sujeta a las condiciones orgánicas y misionales de cada entidad.

RESOLUCIÓN XX DE XXXX

"Por la cual se conforma el Comité de Seguridad de la Información de nombre de la entidad y se definen sus funciones"

EL CARGO DE DIRECTIVO DE QUIEN TIENE LA FACULTAD DE LA NOMBRE DE LA ENTIDAD,

en ejercicio de sus facultades legales, en especial las conferidas por ..., y

CONSIDERANDO

Que....

...Que, en mérito de lo expuesto,

RESUELVE:

Artículo 1°. Conformación del Comité de Seguridad de la Información. Créase el Comité de Seguridad de la Información de Nombre de la entidad. El Comité estará integrado así:

1. El Directivo del área de informática o su delegado.

2. El Directivo del área de Planeación o su representante.

3. El Directivo del área Jurídica (según corresponda por distribución Orgánica de la entidad) o su delegado.

4. El Directivo encargado de los sistemas de Gestión de Calidad (según corresponda por distribución Orgánica de la entidad) o su delegado

5. El Directivo encargado de la Gestión Documental (según corresponda por distribución Orgánica de la entidad) o su delegado.

6. El Directivo encargado (según corresponda por distribución Orgánica de la entidad) de Control Interno o su delegado.

7. El responsable de Seguridad de la información de la entidad.

Parágrafo 1º. El Comité podrá invitar a cada sesión, con voz y sin voto, a aquellas personas que considere necesarias por la naturaleza de los temas a tratar.

Artículo 2º. Objetivo del Comité de Seguridad de la Información. El Comité deberá asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en el organismo, así como de la formulación y mantenimiento de una política de seguridad de la información a través de todo el organismo.

Artículo 3°. Funciones del comité. El Comité de Seguridad de la Inf entidad tendrá dentro de sus funciones las siguientes:

1. Coordinar la implementación del Modelo de Seguridad y pr interior de la entidad.
2. Revisar los diagnósticos del estado de la seguridad de la ir entidad.
3. Acompañar e impulsar el desarrollo de proyectos de seguri
4. Coordinar y dirigir acciones específicas que ayuden a pro establecer los recursos de información que sean consisten de Nombre de la entidad.
5. Recomendar roles y responsabilidades específicos que se re la información.
6. Aprobar el uso de metodologías y procesos específicc información.
7. Participar en la formulación y evaluación de planes de acci riesgos.
8. Realizar revisiones periódicas del SGSI (por lo menos u resultados de esta revisión definir las acciones pertinentes.
9. Promover la difusión y sensibilización de la seguridad de entidad.
10. Poner en conocimiento de la entidad, los documentos gen de seguridad de la información que impacten de manera tra
11. Las demás funciones inherentes a la naturaleza del Comité.

Parágrafo. Una vez conformado el Comité de Seguridad de la Inforn reglamento, en el cual fijará el alcance de cada una de las funcio presente artículo.

Artículo 5°. Secretaria Técnica: La Secretaría Técnica del Comité se y el secretario elegido será remplazado cada XXXX (X) meses.

Artículo 6°. Funciones de la Secretaría Técnica. Las funciones de la siguientes:

1. Elaborar las actas de las reuniones del Comité y verificar su formalización por parte de sus miembros.
2. Citar a los integrantes del Comité a las sesiones ordinarias o extraordinarias
3. Remitir oportunamente a los miembros la agenda de cada comité.
4. Llevar la custodia y archivo de las actas y demás documentos soportes.
5. Servir de interlocutor entre terceros y el Comité.
6. Realizar seguimiento a los compromisos y tareas pendientes del Comité.
7. Presentar los informes que requiera el Comité.
8. Las demás que le sean asignadas por el Comité.

Artículo 7°. Reuniones del Comité de Seguridad de la Información. El Comité de Seguridad de la Información – deberá reunirse (según periodicidad definida por la entidad), previa convocatoria del Secretario Técnico del Comité.

Artículo 8°. Sesiones Extraordinarias. Los miembros que conforman el Comité podrán ser citados a participar de sesiones extraordinarias de trabajo cuando sea necesario, de acuerdo con temas de riesgos, incidentes o afectaciones de continuidad dentro del Sistema de Gestión de Seguridad de la Información.

Artículo 9°. Vigencia y Derogatoria: La presente Resolución rige a partir de la fecha de su expedición.

PUBLÍQUESE Y CÚMPLASE

Dado en XXXX, a los X días del mes de XXXX de XXXX

Directivo Responsable de la entidad

Cargo

11.3. Guía -Gestión inventario clasificación de activos e infraestructura critica

Esa guía presenta los lineamientos básicos que debe tener en cuenta para realizar una adecuada identificación, gestión y clasificación de activos de información e infraestructura critica de cada Entidad, asi:

- Establecer las responsabilidades de los funcionarios y contratistas de la entidad con los Activos de
- Información.

- Garantizar que los activos de información de la entidad reciban un adecuado nivel de protección
- de acuerdo con su valoración.

- Proporcionar una herramienta que visualice de manera fácil los activos de información de la Entidad.

- Sensibilizar y promover la importancia de los activos de información de la entidad.

- Proveer las pautas requeridas y necesarias para la adecuada identificación, clasificación y valoración de los activos de información de la Entidad.

- Cumplir con la organización y publicación de los activos de información, respetando tanto las normas como los procedimientos que se deben cumplir.

El inventario y clasificación de activos hace parte de las actividades más relevantes e importantes del Modelo de Seguridad y Privacidad de la Información y está compuesta por las fases:

- Identificación y Tipificación de los Activos de Información: Corresponde a la etapa en donde la Dependencia como propietario y custodio de la información, identifica y clasifica la información producida, de acuerdo con: Activos de información puros, de Tecnologías de la Información, de Talento humano y Servicios.

- Clasificación de los activos de Información: Corresponde a la etapa en donde la Dependencia propietario y custodio de la información califica los activos de información de acuerdo con lo establecido en el Artículo 6º de la Ley 1712 de 2014: Información Pública, Clasificada o Reservada.

- Revisión y Aprobación: Corresponde a la Etapa en donde se valida la clasificación y valoración dada a los activos de información, para la presentación y aprobación por el Comité MIG.

- Publicación de los Activos de Información: Corresponde a la etapa de publicación de la información en la página web de la Entidad, Link de transparencia y acceso a la Información Pública, Portal de Datos Abiertos del estado colombiano o el sitio que lo modifique o sustituya.

11.3.1 Identificación y tipificación de los activos de información

De acuerdo con las directrices del Archivo General de la Nación, que implementan la metodología apropiada sobre el tratamiento de los “tipos de información y documentos físicos y electrónicos, así como los sistemas, medios y controles asociados a la gestión”, la identificación y tipificación de los activos de información se deben articular de igual forma.

Los propietarios y custodios de la información producida en el área, deben identificar, clasificar y valorar los activos de información de acuerdo con la siguiente compilación de Activos de Información teniendo en cuenta lo establecido en la norma técnica ISO/IEC 27000: (Información; Software como programa informático; Hardware como computadora; servicios; personas, y sus calificaciones, habilidades y experiencia; intangibles como reputación e imagen).

De igual forma, se deben tomar como fuente de información, las Tablas de Retención Documental actualizadas de la entidad, que contemplan las series, sub-series y tipos documentales de la información producida, su medio de conservación y preservación. Las fuentes de información no contemplados en este documento, deben ser complementadas e identificadas por los Gestores, con los jefes de las áreas, Oficina TI (sistemas de información y tecnologías) y servidores (funcionarios y/o contratistas).

Información básica

La información básica hace referencia a aquellas características mínimas del activo que deben identificarse durante esta fase:

- Identificador: Número consecutivo único que identifica al activo en el inventario.
- Proceso: Nombre del proceso al que pertenece el activo.
- Nombre Activo: Nombre de identificación del activo dentro del proceso al que pertenece.
- Descripción/Observaciones: Es un espacio para describir el activo de manera que sea claramente identificable por todos los miembros del proceso.
- Ubicación: Describe la ubicación tanto física como electrónica del activo de información.
- Propietario: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con el proceso se clasifican adecuadamente. Deben definir y revisar periódicamente las restricciones y clasificaciones del acceso.
- Custodio: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de hacer efectivos las restricciones y clasificaciones de acceso definidos por el propietario. (Para sistemas de información o información consignada o respaldada, generalmente es TI o para información física, los custodios pueden ser los funcionarios o el proceso de archivo o correspondencia, el custodio generalmente se define donde reposa el activo original).
- Tipo: Define el tipo al cual pertenece el activo. Para este campo se utilizan los siguientes valores:

TIPIFICACIÓN DEL ACTIVO	DESCRIPCIÓN	COMPONENTES
Información	Corresponden a este tipo datos e información almacenada o procesada electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.	
Hardware	Se consideran los medios materiales físicos destinados a soportar directa o indirectamente los servicios que presta la Entidad.	Servidores, routers, módems Computadores (portátiles, escritorio), impresoras, Celulares Tablet, Teléfonos IP
Software	Se refiere a los programas, aplicativos, sistemas de información que soportan las actividades de la Entidad y la prestación de los servicios.	Software de aplicación, correo electrónico, sistema operativo, etc.
Servicios	Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.	
Recurso Humano	Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información	Contratistas, funcionarios, proveedores.
Instalaciones	Los lugares donde se almacenan o resguardan los sistemas de información y comunicaciones.	Centros de computo, centros de cableado, Datacenter.
Infraestructura crítica cibernética nacional	se entiende por aquella infraestructura soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública.	

Las razones por las cuales debería realizarse una actualización del inventario de activos son:

- Actualizaciones al proceso al que pertenece el activo.
- Adición de actividades al proceso.

- Inclusión de nuevos registros de calidad, nuevos registros de referencia o procesos y procedimientos.

- Inclusión de un nuevo activo.

- Desaparición de un área, proceso o cargo en la entidad que tenía asignado el rol de propietario o custodio (Cambios Organizacionales).

- Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados.

- Cambios físicos de la ubicación de activos de información.

11.3.2 Clasificación de Activos de Información

La clasificación de activos de información tiene como objetivo asegurar que la información recibe los niveles de protección adecuados, de acuerdo con sus características particulares.
El sistema de clasificación definido se basa en la Confidencialidad, la Integridad y la Disponibilidad de cada activo. Asimismo, contempla el impacto que causaría la pérdida de alguna de estas propiedades.

Para cada propiedad se establecieron criterios específicos y lineamientos para el tratamiento adecuado del activo. Así mismo en esta guía se definieron tres (3) niveles que permiten determinar el valor general o criticidad del activo en la entidad (es importante aclarar que los niveles pueden ser definidos a criterio de la entidad): Alta, Media y Baja, con el fin identificar qué activos deben ser tratados de manera prioritaria
(ver Tabla: Niveles de evaluación).

Tabla 4: Criterios de Clasificación

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Tabla 5: Niveles de Clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

11.3.3. Clasificación de acuerdo con la confidencialidad

La confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados, Esta se debe definir de acuerdo con las características de los activos que se manejan en cada entidad, a manera de ejemplo en la guía se definieron tres (3) niveles alineados con los tipos de información declarados en la ley 1712 del 2014:
Tabla 6: Esquema de clasificación por confidencialidad

INFORMACION PUBLICA RESERVADA	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
INFORMACION PUBCLCA CLASIFICADA	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
INFORMACION PÚBLICA	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA.

11.3.4 Clasificación de acuerdo con la Integridad

La integridad se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción. En esta guía se recomienda el siguiente esquema de clasificación de tres (3) niveles:

Tabla 7: Esquema de clasificación por Integridad

A (ALTA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
M (MEDIA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.
B (BAJA)	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.

NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.

11.3.5 Clasificación de acuerdo con la Disponibilidad

La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona, entidad o proceso autorizada cuando así lo requiera está, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso.

En esta guía se recomienda el siguiente esquema de clasificación de tres (3) niveles:

Tabla 8: Esquema de clasificación por Disponibilidad

1 (ALTA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
2 (MEDIA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
3 (BAJA)	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.

11.3.6 Revisión y aprobación de los activos de información

Posterior a la identificación, clasificación y valoración de los activos de información compilados en la Matriz de Activos de Información, validados y aprobados por los jefes de cada dependencia, deben enviar al área correspondiente los activos de información para su consolidación y validación por parte de la Oficina Asesora Jurídica para posteriormente presentar ante el Comité MIG y proceder con la publicación correspondiente.

La aprobación por parte del Comité MIG de los activos de información de la Entidad, se encuentra establecido en la Resolución MinTIC No. 911 del 26 de marzo de 2018, siendo este “la instancia orientadora del MIG en donde se tratan los temas referentes a las políticas de gestión y desempeño institucional, y demás componentes del modelo, promoviendo sinergias entre las dependencias, Iniciativas, estrategias y proyectos que redunden en beneficios institucionales y en la satisfacción de la ciudadanía, usuarios y grupos de interés del Ministerio/Fondo TIC.” Este Comité hará las veces del Comité de Gestión y Desempeño Institucional del que habla el artículo 2.2.22.6 del Decreto 1083 de 2015”.

11.3.7 Publicación de los activos de información

El área, proceso, grupo interno, funcionario o rol responsable de la custodia del inventario de activos de información debe enviar a la Oficina Asesora de Prensa o quien haga sus veces en la Entidad el consolidado del inventario de Activos de Información para la respectiva publicación de la información en la página web de la Entidad, Link de transparencia y acceso a la Información Pública, Portal de Datos Abiertos del estado colombiano o el sitio que lo modifique o sustituya.

11.3.8 Etiquetado de los Activos de Información

Para realizar el etiquetado de los Activos de Información se proponen los siguientes lineamientos:

- Se deben etiquetar todos los Activos de Información que estén clasificados según el esquema clasificación en Confidencialidad, Integridad y disponibilidad de la Entidad.
- Si un Activo de Información en formato impreso no se encuentra etiquetado debe ser tratado en todos sus niveles (Confidencialidad, Integridad y Disponibilidad) como NO CLASIFICADA.
- Para los activos clasificados en confidencialidad como INFORMACION PUBLICA RESERVADA se podría utilizar la etiqueta IPR, INFORMACION PUBLICA CLASIFICADA IPC y INFORMACION PUBLICA, IPB.
- Para los activos clasificados en integridad como ALTA se utilizara la etiqueta A, MEDIA, M y BAJA, B.
- Para los activos clasificados en disponibilidad como ALTA se utilizara la etiqueta 1, MEDIA, 2 y BAJA, 3.

De esta manera se realizarían las combinaciones de acuerdo con los criterios de clasificación de la información.

11.4 Guía para la gestión de riesgos de seguridad de la información (Anexo 4. DAFP)

https://www.funcionpublica.gov.co/documents/28587410/34298398/2020-12-16_Guia_administracion_riesgos_dise%C3%B1o_controles_final.pdf/fa179c5e-45bb-dffd-027c-043d4733c834 t=1609857497641

11. Guía - Indicadores Gestión de Seguridad de la Información

1. Objetivo de la medición

La creación de indicadores de gestión está orientada principalmente en la medición de efectividad, eficiencia y eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, indicadores que servirán como insumo para el componente de mejora continua, permitiendo adoptar decisiones de mejora.

Los objetivos de estos procesos de medición en seguridad de la información son:

- Evaluar la efectividad de la implementación de los controles de seguridad
- Evaluar la eficiencia del Modelo de Seguridad y Privacidad de la Información al interior de la entidad.
- Proveer estados de seguridad que sirvan de guía en las revisiones del Modelo de Seguridad y Privacidad de la Información, facilitando mejoras en seguridad de la información y nuevas entradas a auditar.
- Comunicar valores de seguridad al interior de la entidad.
- Servir como insumos al plan de análisis y tratamiento de riesgos.

11.5.2. Construcción de indicadores

Acorde con la Guía para Diseño, Construcción e Interpretación de Indicadores del DANE, para la construcción de indicadores se debe tener en cuenta un tratamiento adecuado de la información que será la base del proceso de revisión control y mejora, de esta forma, dentro de la elaboración de indicadores se tienen definidos cuatro etapas específicas, como se menciona a continuación:

1. IDENTIFICACIÓN DEL OBJETO DE LA MEDICIÓN

En este primer paso los encargados de la implementación del MSPI, deben tener en cuenta el Plan de Seguridad de la Información que se ha definido y de esta manera se desarrolla el objeto de medición sobre los aspectos que consideren más relevantes para evaluar, determinar qué tan fácil es recolectar la información asociada y que herramientas estoy empleando para obtener dicha información.

2. DEFINICIÓN DE LAS VARIABLES

Una vez determinado el objeto de la medición, se pasa a definir los aspectos que van a precisar los datos que se recolectarán en el levantamiento de la información, de esta forma se determinarán los insumos, puntos de control, herramientas usadas y la relación que se puede presentar entre estos aspectos o variables de medición.
En este sentido, las variables, una vez identificadas, deben ser definidas con la mayor rigurosidad, asignándole un sentido claro, para evitar que se originen ambigüedades y discusiones sobre sus resultados.
Así mismo, se debe tener claridad de quién y cómo produce dicha información para de esta forma mejorar el criterio de confiabilidad.5

3. SELECCIÓN DE INDICADORES Y CALIDAD DE LOS DATOS

El punto inicial es determinar si el indicador que se está eligiendo es de interés para la alta dirección, si va a permitir al líder del proyecto (el encargado de la seguridad de la información de la entidad) identificar la efectividad no solo del avance en la implementación, sino que, con esta recolección, medición y seguimiento del proyecto se logra demostrar cómo éste aporta al objetivo misional de la entidad.
Finalmente es importante que el indicador sea sencillo de expresar, leer e interpretar, y como se menciona en la guía del DNP, metodológicamente, debe ser elaborado de forma sencilla, automática, sistemática y continua.

4. DISEÑO DEL INDICADOR

Con el diseño del indicador también deben surtirse algunas actividades o pasos a tener en cuenta para el proceso definitivo en la construcción de los indicadores, de esta forma, una vez superados los pasos precedentes,

Tabla 9: Criterios para selección de indicadores

Criterio de selección	Pregunta a tener en cuenta	Objetivo
Pertinencia	¿El indicador expresa qué se quiere medir de forma clara y precisa?	Busca que el indicador permita describir la situación o fenómeno determinado, objeto de la acción.
Funcionalidad	¿El indicador es monitoreable?	Verifica que el indicador sea medible, operable y sensible a los cambios registrados en la situación inicial
Disponibilidad	¿La información del indicador está disponible?	Los indicadores deben ser construidos a partir de variables sobre las cuales exista información estadística de tal manera que puedan ser consultados cuando sea necesario.
Confiabilidad	¿De donde provienen los datos?	Los datos deben ser medidos siempre bajo ciertos estándares y la información requerida debe poseer atributos de calidad estadística.
Utilidad	¿El indicador es relevante con lo que se quiere medir?	Que los resultados y análisis permitan tomar decisiones.

Fuente: Guía para Diseño, Construcción e Interpretación de Indicadores. Metodología línea base de indicadores, DANE 2009.

11.5.3 Indicadores propuestos

A continuación, se definen una serie de indicadores para medir la gestión y el cumplimiento en el avance de implementación del Nuevo Modelo de Seguridad y Privacidad de la Información, esperando que sirva de base para que los encargados de la seguridad de la información de los sujetos obligadosy sea un ejemplo para apoyarlos en esta labor.

Dichos indicadores son:

INDICADOR 01- ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN.					
IDENTIFICADOR	SGIN01				
DEFINICIÓN					
El indicador permite determinar y hacer seguimiento, al compromiso de la dirección, en cuanto a seguridad de la información, en lo relacionado con la asignación de personas y responsabilidades relacionadas a la seguridad de la información al interior de la entidad					
OBJETIVO					
Hacer un seguimiento a la asignación de recursos y responsabilidades en gestión de seguridad de la información, por parte de la alta dirección.					
TIPO DE INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES			**FORMULA**	**FUENTE DE INFORMACIÓN**	
VSI01: Número de personas con su respectivo rol definió según el modelo de operación capítulo 2			(VSI01/VSI02)*100	Capítulo 2 de la guía del modelo de operación del marco de seguridad y privacidad de la información	
VSI02: Número de personas con su respectivo rol definió después de un año				Actas de asignación de personal.	
METAS					
MÍNIMA	**75-80%**	**SATISFACTORIA**	80- 90%	**SOBRESALIENTE**	100%
OBSERVACIONES					
De acuerdo a lo establecido en el capítulo 2 de la guía del modelo de operación del marco de seguridad y privacidad de la información, es necesario crear nuevos cargos y asignar responsabilidades en los actuales, por lo tanto, el indicador está enfocado, no solo a la contratación de nuevas personas, sí no a la asignación de responsabilidades.					

INDICADOR 02 - CUBRIMIENTO DEL SGSI EN ACTIVOS DE INFORMACIÓN.	
IDENTIFICADOR	SGIN02
DEFINICIÓN	
El indicador permite determinar y hacer seguimiento al cubrimiento que se realiza a nivel de activos **críticos** de información de una entidad y los controles aplicados.	
OBJETIVO	
Hacer un seguimiento a la inclusión de nuevos activos críticos de información y su control, dentro del marco de seguridad y privacidad de la información.	
TIPO DE INDICADOR	

Indicador de Gestión		
DESCRIPCIÓN DE VARIABLES	**FORMULA**	**FUENTE DE INFORMACIÓN**
VSI03: Número de activos críticos de información incluidos en el alcance de implementación del modelo, incluidos en la zona de riesgo inaceptable y la implementación del control no requiere adquisición de elementos de hardware o software.	(VSI03/VSI04)*100	Alcance del SGSI, Inventario de Activos de información, plan de tratamiento, matriz de riesgos
VSI04: Número de activos críticos de información incluidos en el alcance de implementación del modelo; activos incluidos en la zona de riesgo inaceptable.		Inventario de Activos de información, nuevos

METAS					
MÍNIMA	75-80%	**SATISFACTORIA**	80- 90%	**SOBRESALIENTE**	100%

OBSERVACIONES
El indicador de cada proceso debe ser recolectado y promediado para construir un indicador que refleje el estado a nivel empresa. El terminó "incluir un activo" debe ser entendido como realizar la correcta clasificación del activo, tratamiento, evaluación de riesgos sobre el mismo y determinación de controles para minimizar el riesgo calculado. Para este indicador, solo se tienen en cuenta los controles que no implican adquisición de hardware o software.

INDICADOR 03 - TRATAMIENTOS DE EVENTOS RELACIONADOS EN MARCO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
IDENTIFICADOR	SGIN03
DEFINICIÓN	
El indicador permite determinar la eficiencia en el tratamiento de eventos relacionados la seguridad de la información. Los eventos serán reportados por los usuarios o determinadas en las auditorías planeadas para el sistema.	
OBJETIVO	
El objetivo del indicador es reflejar la gestión y evolución del modelo de seguridad y privacidad de la información al interior de una entidad	
TIPO DE INDICADOR	
Indicador de Gestión	

DESCRIPCIÓN DE VARIABLES	**FORMULA**	**FUENTE DE INFORMACIÓN**
VSI05: Número de anomalías cerradas.	(VSI05/VSI06)*100	Auditorías internas, herramientas de monitoreo
VSI06: Número total de anomalías encontradas.		Auditorías internas, herramientas de monitoreo

METAS					
MÍNIMA	75-80%	**SATISFACTORIA**	80- 90%	**SOBRESALIENTE**	100%

INDICADOR – PLAN DE SENSIBILIZACIÓN	
IDENTIFICADOR	SGIN04
DEFINICIÓN	
El indicador permite medir la aplicación de los temas sensibilizados en por parte de los usuarios finales. Estas mediciones se podrán realiz especializadas en el tema o de forma aislada por parte de los respo sensibilización.	
OBJETIVO	
El objetivo del indicador es establecer la efectividad de u sensibilización previamente definido como medio para el control de in	
TIPO INDICADOR	
Indicador de Gestión	

DESCRIPCIÓN DE VARIABLES	**FORMULA**	**FU**
VSI07: Número de fallas o no cumplimientos encontrados en las sensibilizaciones programadas o eventos realizados para evaluar el tema.	(VSI07/VSI08)*100	Ofi Info inte list
VSI08: Total de personal a capacitar.		Tot ent

METAS				
MÍNIMA	75-80%	**SATISFACTORIA**	80- 90%	**SOBRE**

OBSERVACIONES
Para el levantamiento de la información que permita obtener datos pa debe idear planes, laboratorios o actividades periódicas que perm divulgado.

INDICADOR – CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD DE ENTIDAD	
IDENTIFICADOR	SGIN05
DEFINICIÓN	
Cumplimiento de políticas de seguridad de la información en la entida	
OBJETIVO	
Busca identificar el nivel de estructuración de los procesos de la entid de la información.	
TIPO INDICADOR	
Indicador de Cumplimiento	

DESCRIPCIÓN DE VARIABLES	**FORMULA**	**FUENT**
VSI09: ¿La entidad ha definido una política general de seguridad de la información?	VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Guía d Usuari
VSI10: ¿La entidad ha definido una organización interna en términos de personas y responsabilidades con el fin de cumplir las		Guía d Usuari

políticas de seguridad de la información y documenta estas actividades?		
VSI11: ¿La entidad cumple con los requisitos legales, reglamentarios y contractuales con respecto al manejo de la información?		Guía del Modelo de Operación / Usuarios Internos
METAS		
CUMPLE	1	**NO CUMPLE** 0
OBSERVACIONES		

INDICADOR – IDENTIFICACIÓN DE LINEAMIENTOS DE SEGURIDAD DE LA ENTIDAD			
IDENTIFICADOR	SGIN06		
DEFINICIÓN			
Grado de la seguridad de la información y los equipos de cómputo.			
OBJETIVO			
Busca medir el nivel de preparación del recurso humano y su apropiación en cuanto a la seguridad de la información y los equipos de cómputo.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**
VSI12: ¿La entidad ha definido lineamientos de trabajo a través del comité o responsable de seguridad para que sus funcionarios cumplan las políticas de seguridad y evalúa periódicamente su pertinencia?		VSI0X = 1 (SÍ se evidencia)	Usuarios Internos.
VSI13: ¿La entidad ha definido lineamientos en cuanto a la protección de las instalaciones físicas, equipos de cómputo y su entorno para evitar accesos no autorizados y minimizar riesgos de la información de la entidad?		VSIOX = 0 (NO se evidencia)	Usuarios Internos.
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

INDICADOR – VERIFICACIÓN DEL CONTROL DE ACCESO	
IDENTIFICADOR	SGIN07
DEFINICIÓN	
Grado control de acceso en la entidad.	
OBJETIVO	
Busca identificar la existencia de lineamientos, normas o estándares en cuanto al control de acceso en la entidad.	
TIPO INDICADOR	
Indicador de Cumplimiento	
DESCRIPCIÓN DE VARIABLES	**FORMULA**
VSI14: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar el acceso de los usuarios a sus servicios de Gobierno en línea y a sus redes de comunicaciones?	VSI0X = 1 (SÍ se evidencia)
VSI15: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar el uso y el acceso a los sistemas de información, las aplicaciones y los depósitos de información con las que cuenta la entidad?	VSIOX = 0 (NO se evidencia)
VSI16: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar las terminales móviles y accesos remotos a los recursos de la entidad?	
METAS	
CUMPLE 1	**NO CUMPLE**
OBSERVACIONES	

INDICADOR – ASEGURAMIENTO EN LA ADQUISICIÓN Y MANTENIMIEN	
IDENTIFICADOR	SGIN08
DEFINICIÓN	
Grado de protección de los servicios de la entidad.	
OBJETIVO	
Busca identificar la existencia de lineamientos, normas o estándares en desarrollo de aplicaciones.	
TIPO INDICADOR	
Indicador de Cumplimiento	
DESCRIPCIÓN DE VARIABLES	**FORMULA**
VSI17: ¿La entidad ha definido lineamientos, normas y/o estándares para el desarrollo o adquisición de software, sistemas y aplicaciones?	VSI0X = 1 (SÍ se evidencia)
VSI18: ¿La entidad ha definido lineamientos, normas y/o estándares para la gestión de incidentes relacionados con el servicio?	VSIOX = 0 (NO se evidencia)
METAS	
CUMPLE 1	**NO CUMPLE**
OBSERVACIONES	

INDICADOR – IMPLEMENTACIÓN DE LOS PROCESOS DE REGISTRO Y AU

IDENTIFICADOR	SGIN09		
DEFINICIÓN			
Grado de existencia de lineamientos, normas o estándares en cuanto registro y auditoría para la seguridad de la información.			
OBJETIVO			
Busca identificar la existencia de lineamientos, normas o estándares en cuanto registro y auditoría para la seguridad de la información.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**
VSI19: ¿La entidad ha definido lineamientos, normas y/o estándares para el registro y control de eventos que sucedan sobre sus sistemas, redes y servicios?		VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Usuarios Internos.
VSI20: ¿La entidad verifica de manera interna y/o a través de terceros, periódicamente sus procesos de seguridad de la información y sistemas para asegurar el cumplimiento del modelo?			Usuarios Internos.
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

INDICADOR – DETECCIÓN DE ANOMALÍAS EN LA PRESTACIÓN DE LOS SERVICIOS DE LA ENTIDAD			
IDENTIFICADOR			
DEFINICIÓN	SGIN10		
Grado de implementación de los mecanismos encaminados a la detección de anomalías e irregularidades.			
OBJETIVO			
Busca medir el nivel de mecanismos encaminados a la detección de anomalías e irregularidades			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES			
VSI21: VAPRSG005: ¿La entidad ha implementado mecanismos para detectar periódicamente vulnerabilidades de seguridad en el funcionamiento de: a) su infraestructura, b) redes, c) sistemas de información, d) aplicaciones y/o e) uso de los servicios?		**FORMULA**	**FUENTE DE INFORMACIÓN**
			Usuarios Internos, No Conformidades
METAS			

		VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	
CUMPLE			
OBSERVACIONES	1	**NO CUMPLE**	

INDICADOR – POLÍTICAS DE PRIVACIDAD Y CONFIDENCIALIDAD			
IDENTIFICADOR	SGIN11		
DEFINICIÓN			
Grado de implementación de políticas privacidad y confidencialidad de			
OBJETIVO			
Busca identificar el nivel de implementación de políticas privacidad entidad.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE**
VSI22: ¿La entidad ha implementado lineamientos, normas y/o estándares para proteger la información personal y privada de los ciudadanos que utilicen sus servicios?		VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Usuario
VSI23: ¿La entidad ha implementado lineamientos, normas y/o estándares para proteger la información privada de las entidades que utilicen sus servicios?			Usuario
METAS			
CUMPLE	1	**NO CUMPLE**	
OBSERVACIONES			

INDICADOR – VERIFICACIÓN DE LAS POLÍTICAS DE INTEGRIDAD DE LA			
IDENTIFICADOR	SGIN12		
DEFINICIÓN			
Grado de implementación de mecanismos para la integridad de la infor			
OBJETIVO			
Busca identificar el nivel de implementación de políticas privacidad entidad.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE**

VSI24: ¿La entidad ha implementado lineamientos contra modificación o pérdida accidental de información?	VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Usuarios Internos.	
VSI25: ¿La entidad ha implementado lineamientos, normas y/o estándares para recuperar información en caso de modificación o pérdida intencional o accidental?		Usuarios Internos.	
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

INDICADOR – POLÍTICAS DE DISPONIBILIDAD DEL SERVICIO Y LA INFORMACIÓN			
IDENTIFICADOR	SGIN13		
DEFINICIÓN			
Grado de cumplimiento de las políticas de disponibilidad del servicio y la información.			
OBJETIVO			
Busca identificar el nivel de implementación de políticas de disponibilidad del servicio y la información.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES	**FORMULA**	**FUENTE DE INFORMACIÓN**	
VSI26: ¿La entidad verifica que los lineamientos, normas y/o estándares orientados a la continuidad en la prestación de los servicios se cumplan?	VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Usuarios Internos.	
VSI27: ¿La entidad ha implementado mecanismos para que los servicios de Gobierno en línea tengan altos índices de disponibilidad?		Usuarios Internos.	
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

INDICADOR – ATAQUES INFORMÁTICOS A LA ENTIDAD.	
IDENTIFICADOR	SGIN14
DEFINICIÓN	
Porcentaje de ataques informáticos recibidos en la entidad que impidieron la prestación de alguno de sus servicios.	
OBJETIVO	
Busca conocer el número de ataques informáticos que recibe la entidad	
TIPO INDICADOR	
Indicador de Cumplimiento	

DESCRIPCIÓN DE VARIABLES	**FORMULA**	**FUENTE I**	
VSI28: ¿Cuántos ataques informáticos recibió la entidad en el último año?	VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Herramie Monitore	
VSI29: ¿Cuántos ataques recibió la entidad en el último año que impidieron la prestación de algunos de los servicios que la entidad ofrece a los ciudadanos y empresas?		Herramie Monitore	
METAS			
CUMPLE	1	**NO CUMPLE**	
OBSERVACIONES			

INDICADOR – PORCENTAJE DE DISPONIBILIDAD DE LOS SERVICIO DE PRESTA LA ENTIDAD			
IDENTIFICADOR	SGIN15		
DEFINICIÓN			
Porcentaje de disponibilidad de los servicios que presta la entidad			
OBJETIVO			
Busca identificar el nivel de disponibilidad del servicio y la información.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES	**FORMULA**	**FUENTE I**	
VSI30: La entidad tiene definidos ANS para los servicios de Gobierno en Línea que presta	VSI0X = 1 (SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Usuarios	
VSI31: Porcentaje de disponibilidad de los servicio de Gobierno en línea que presta la entidad en base a los ANS del punto anterior.		Usuarios	
METAS			
CUMPLE	1	**NO CUMPLE**	
OBSERVACIONES			

INDICADOR – PORCENTAJE DE IMPLEMENTACIÓN DE CONTROLES			
IDENTIFICADOR	SGIN16		
DEFINICIÓN			
grado de avance en la implementación de controles de seguridad			
OBJETIVO			
Busca identificar el grado de avance en la implementación de controles			
TIPO INDICADOR			
Indicador de Gestión			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENT**
VSI32: Número de Controles Implementados		(VSI032/VSI33)*100	Plan d

VSI33: Número de Controles que se planearon implementar				Plan de Tratamiento de riesgos.	
METAS					
MÍNIMA	75-80%	**SATISFACTORIA**	80- 90%	**SOBRESALIENTE**	100%

DERECHOS DE AUTOR

Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de la Información son derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones -MINTIC.

De igual forma, son derechos reservados por parte del MinTIC, todas las referencias a las políticas, definiciones o contenido relacionados con los documentos del MSPI publicadas en el compendio de las normas técnicas colombianas vigentes.

En consecuencia, el MinTIC goza de los derechos de autor6 establecidos en la ley 23 de 1982 y demás normas concordantes y complementarias, respecto de los documentos del MGRSD y su contenido.

Las reproducciones, referencias o enunciaciones de estos documentos deberán ir siempre acompañadas por el nombre o seudónimo del titular de los derechos de autor (Ministerio de Tecnologías de la Información y las Comunicaciones).

Lo anterior, sin perjuicio de los derechos reservados por parte de entidades tales como la International Standard Organization (ISO), ICONTEC, entre otras, respecto de referencias, definiciones, documentos o contenido relacionado en el MGRSD y sus documentos o anexos que son de su autoría o propiedad.

AUDIENCIA

El presente documento está dirigido a los sujetos obligados señalados en el artículo 2.2.9.1.1.2. del Decreto 1078 de 2015 (DUR-TIC), "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"

HERRAMIENTAS DE APOYO

los sujetos obligados, podrán acceder a las herramientas que se han desarrollado con el objetivo de apoyar en el proceso de implementación del MSPI para los encargados de seguridad de la Información y así obtener una guía más práctica en temas específicos que se podrán encontrar en el siguiente link:

https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Iniciativas/