TIC

# Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información

Ministerio de tecnologías de la información y las comunicaciones

MSPI

**Julián Molina Gómez** – Ministro de Tecnologías de la Información y las Comunicaciones
**Yeimi Carina Murcia Yela** - Viceministra de Transformación Digital
**Lucy Elena Urón Rincón** - Directora de Gobierno Digital
**Luis Clímaco Córdoba Gómez** - Subdirector de Estándares y Arquitectura de TI
**Danny Alejandro Garzón Aristizábal** – Contratista Subdirección de Estándares y Arquitectura de TI
**German García Filoth** – Contratista Subdirección de Estándares y Arquitectura de TI
**Johanna Marcela Forero Varela** - Profesional Especializado Subdirección de Estándares y Arquitectura de TI
**Julio Andrés Sánchez Sánchez** - Contratista Subdirección de Estándares y Arquitectura de TI
**Lourdes María Acuña Acuña -** Contratista de la Dirección de Gobierno Digital
**Tairo Elías Mendoza Piedrahita** - Profesional Especializado Dirección de Gobierno Digital
**Andrés Díaz Molina**- Jefe de la Oficina de Tecnologías de la Información
**Nelson Barrios Perdomo** – Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
**Adriana María Pedraza -** Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
**Camilo Andrés Jiménez -** Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
**Emanuel Elberto Ortiz -** Contratista Equipo de Respuesta a Emergencias Cibernéticas de Colombia – COLCERT
**Angela Janeth Cortés Hernández -** Oficial de Seguridad y Privacidad de la Información
GIT de Seguridad y Privacidad de la Información.

Ministerio de Tecnologías de la Información y las Comunicaciones
Viceministerio de Transformación Digital
Dirección de Gobierno Digital

| **Versión** | **Observaciones** |
|---|---|
| Versión 5<br>21/04/2025 | Documento Maestro del Modelo de Seguridad y Privacidad de la Información<br>Dirigida a las entidades del Estado |

Comentarios, sugerencias o correcciones pueden ser enviadas al correo electrónico: gobiernodigital@mintic.gov.co

Modelo de Seguridad y Privacidad de la Información
Documento Maestro V 5.0

# Tabla de contenido

# Listado de tablas



# 1. Listado de Ilustraciones

# 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, por lo que puede afectar su funcionamiento repercutiendo en la prestación de los servicios a la ciudadanía. Por la cual, el ministerio como entidad se encarga de diseñar, adoptar y promover políticas, planes, programas y proyectos para el uso y apropiación de las TIC, y establece lineamientos para generar confianza en el uso del entorno digital, garantizando el aprovechamiento de las tecnologías de la información y las comunicaciones. El Ministerio busca fortalecer la implementación y mejora continua de controles de seguridad de la información en las Entidades del Estado con el objetivo de: mejorar la ciberseguridad y resiliencia organizacional, promoviendo la aplicación de controles de seguridad digital para garantizar la continuidad de los servicios críticos para el Estado colombiano.

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 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 la implementación de controles físicos, lógicos y administrativos para 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 los activos de información, infraestructura critica cibernética nacional, los riesgos e incidentes de seguridad y privacidad de la información, evitando la interrupción de la prestación de los servicios de la entidad enmarcados en su modelo de operación y minimizando el impacto en caso de presentarse

Teniendo en cuenta lo anterior, el MinTIC define el Modelo de Seguridad y Privacidad de la Información – MSPI y establece los lineamientos para la implementación de la estrategia de seguridad digital, con el objetivo de formalizar al interior de las entidades un Sistema de Gestión de Seguridad y privacidad de la Información – SGSPI y seguridad digital, el cual contempla su operación basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), integrando consideraciones y controles específicos de ciberseguridad en cada una de sus etapas:

**Planear:** Se definen objetivos de seguridad y privacidad de la información y de seguridad digital, según el contexto y la valoración de riesgos.

**Hacer:** Se implementan controles de seguridad digital para proteger activos digitales e infraestructura tecnológica al mitigar riesgos.

**Verificar:** Se evalúa la efectividad de controles de seguridad de la información y seguridad digital mediante auditorías e indicadores.

**Actuar:** Se identifican desviaciones y se toman acciones correctivas y preventivas para fortalecer la seguridad y privacidad de la información y la seguridad digital.

Así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento.

El Modelo de Seguridad y Privacidad de la Información (MSPI) está estructurado en cinco (5) fases que permiten a las entidades gestionar y mantener de forma adecuada la seguridad y privacidad de sus activos de información. Estas fases se desarrollan de la siguiente manera:

1. **Diagnóstico**: La entidad debe iniciar con un diagnóstico o análisis de brechas (GAP), cuyo propósito es identificar su estado actual frente a los requisitos del MSPI. Este insumo es clave tanto para la fase de planificación como para medir avances al finalizar la fase de mejoramiento continuo.

2. **Planificación**: Se establecen las necesidades, objetivos y estrategias de seguridad y privacidad de la información, considerando el mapa de procesos, el tamaño institucional y el contexto interno y externo. Esta fase incluye la identificación, valoración y tratamiento de riesgos, siendo el pilar del ciclo de gestión.

3. **Operación**: En esta fase, la entidad implementa los controles definidos en la planificación para reducir la probabilidad y el impacto de los riesgos identificados.

4. **Evaluación del desempeño**: Se mide la efectividad del modelo a través de auditorías, revisiones y análisis de indicadores definidos previamente, permitiendo identificar avances, desviaciones o áreas de mejora.

5. **Mejoramiento continuo**: Se establecen mecanismos para detectar y corregir desviaciones, implementar acciones correctivas y prevenir su repetición, fortaleciendo así el sistema de manera progresiva.

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

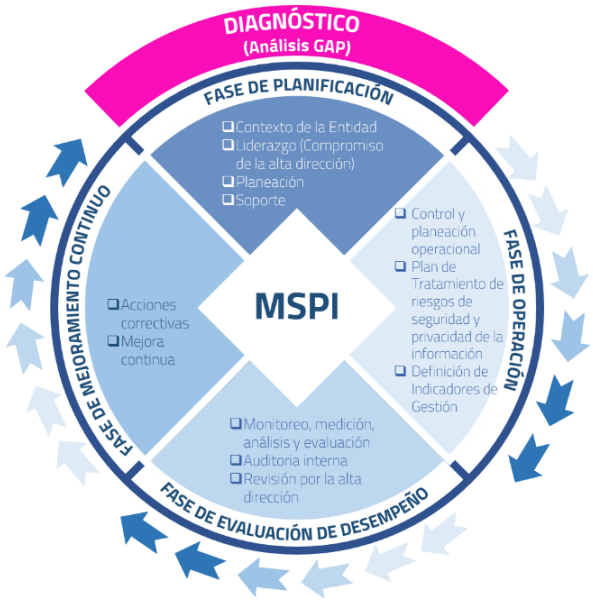


Ilustración 1 Ciclo del Modelo de Seguridad y Privacidad de la Información

La seguridad de la información debe verse como la interacción de múltiples componentes que trabajan conjuntamente para proteger no solo los sistemas tecnológicos, sino también los activos humanos, la infraestructura física, el desarrollo de software, la gestión del talento humano, la calidad, la gestión con proveedores y otros elementos clave. Esto implica la implementación de estrategias que salvaguarden la confidencialidad, integridad y disponibilidad de la información en todos los niveles de la organización, abarcando tanto aspectos técnicos como organizativos y administrativos.


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

# 2. Audiencia

El presente documento está dirigido a entidades públicas de orden nacional y territorial, así como proveedores de servicios de la Política de Gobierno Digital y estrategia de seguridad digital, terceros que deseen adoptar el Modelo de Seguridad y Privacidad de la información, entre otros, de acuerdo con la Política de Seguridad Digital y el Artículo 2. Ámbito de aplicación de la Resolución 500 de 2021, proferida por el Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC “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.”

# 3. 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 crítico:** Son aquellos elementos o componentes que hacen parte de la infraestructura crítica.

- **Activo de información:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, instalaciones, personas, etc.) que tenga valor para la organización. (ISO/IEC 27001:2022).

- **Alcance del MSPI**: Es el número del total de los procesos que serán incluidos en la implementación del MSPI.

- **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 27001:2022).

- **Amenaza cibernética:** aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado.

- **Agente de Mesa de Servicio**: Recibe la información de los Colaboradores del Ministerio, registra los casos en la herramienta de mesa de servicio y es el

- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27001:2022).

- **Ataque informático:** Conjunto de actividades realizadas por atacantes para vulnerar la seguridad informática de un sistema.

- **Ataque cibernético:** acción organizada o premeditada de una o más agentes para causar daño o problemas a un sistema a través del Ciberespacio. Este concepto se desarrolla de manera más profunda como ciberataque.

- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27001:2022).

- **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)

- **BCP (Business Continuity Planning / Plan de Continuidad de Negocios):** Es un plan logístico detallado de cómo una entidad debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

- **Ciberseguridad:** Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.

- **CERT:** (Computer Emergency Response Team) Equipo de Respuesta a Emergencias cibernéticas, por su sigla en inglés. Es el equipo que dispone de la capacidad centralizada para la coordinación de gestión de incidentes de seguridad digital.

- **Ciberespacio:** Red interdependiente de infraestructuras de tecnología de la información que incluye Internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores integrados en industrias. (Decreto 338 de 2022).

- **Ciberdefensa:** capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. La ciberdefensa implica el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética. (Conpes 3995 de 2020).

- **Ciberespionaje:** Ciberespionaje - «El Ciberespionaje se utiliza principalmente como un medio para recopilar datos sensibles o clasificados, secretos comerciales u otras formas de propiedad intelectual que pueden ser utilizados por el agresor para crear una ventaja competitiva o vendidos para obtener beneficios financieros. En algunos casos, la violación simplemente pretende causar un daño reputacional a la víctima exponiendo información privada o prácticas empresariales cuestionables.» - Crowdstrike.

- **Ciberincidente:** Cualquier acto malicioso o evento sospechoso que comprometa, o intente comprometer la Seguridad del perímetro electrónico, la Seguridad del primero físico o un activo crítico.

- **Ciberseguridad:** Es el proceso de proteger los activos de información por medio del tratamiento de las amenazas a la información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.

- **Ciberamenaza** - Cualquier circunstancia o evento con el potencial de impactar negativamente en las operaciones de la organización (incluyendo misión, funciones, imagen o reputación), activos de la organización o individuos a través de un sistema de información mediante acceso no autorizado, destrucción, divulgación, modificación de información y/o denegación de servicio. También, el potencial de una amenaza-fuente para explotar con éxito una vulnerabilidad particular del sistema de información. NIST SP 1800-15B

- **Ciberataque** - Un ataque, a través del ciberespacio, dirigido al uso del ciberespacio por parte de una empresa con el propósito de interrumpir, inutilizar, destruir o controlar maliciosamente un entorno/infraestructura informática; o destruir la integridad de los datos o robar información controlada. NIST SP 1800-10B de NIST SP 800-30 Rev.1

- **Ciberterrorismo:** es el uso del Ciberespacio, como fin o como medio, con el propósito de generar terror o miedo generalizado en la población, nación o estado trayendo como consecuencia una violación a la voluntad de las personas.

- **CSIRT:** (Computer Security lncident & Response Team) Equipo de Respuesta a Incidentes de Seguridad Cibernética, por su sigla en inglés. Es el equipo que provee las capacidades de gestión de incidentes a una organización/sector en especial. Esta capacidad permitir minimizar y controlar el daño resultante de incidentes, proveyendo la respuesta, contención y recuperación efectiva, así como trabajar en pro de prevenir la ocurrencia de futuros incidentes.

- **CSIRT Gobierno:** Equipo de Respuesta a Incidentes de Seguridad en sus siglas en inglés (Computer Security Incident & Response Team), integrado por un grupo de personas técnicas especializadas, que implementan y desarrollan medidas tendientes a prevenir y gestionar incidentes de ciberseguridad de las entidades del estado.

- **CSIRT sectorial:** Son los equipos de respuesta a incidentes de cada uno de los sectores, para el adecuado desarrollo de sus actividades económicas y sociales, a partir del uso de las tecnologías de la información y las comunicaciones.

- **CSIRT sectorial crítico:** Son los equipos de respuesta a incidentes sectoriales de cada uno de los sectores identificados como críticos.

- **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.

- **Código malicioso:** Conjunto de instrucciones o códigos informáticos que se inserta en los programas de computador, tiene la capacidad de auto replicarse y usualmente porta una carga útil que afecta el funcionamiento del computador, destruye datos, altera y pone en riesgo la información.

- **COLCERT:** Por sus siglas en inglés Computer Emergency Response Team, es el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, y tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual se encuentra enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal es la coordinación de las acciones necesarias para la protección de la infraestructura crítica cibernética del Estado Colombiano frente a emergencias de Ciberseguridad que atenten y comprometan la seguridad y defensa nacional.

- **Contención de un incidente:** Son todas aquellas actividades encaminadas a reducir el impacto inmediato de un incidente de seguridad.

- **Criterios horizontales de criticidad:** Criterios únicos a nivel país para determinar si una infraestructura estratégica es considerada crítica. Adaptación Ley 8/2011-Gobierno de España.

- **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 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, numeral 3)

- **Denegación del servicio:** Conjunto de actividades desarrolladas por atacantes informáticos para degradar o interrumpir el normal funcionamiento de un sistema servicio informático.

- **Derecho a la Intimidad:** Protege el ámbito privado del individuo y de su familia como el núcleo humano más próximo. Uno y otra están en posición de reclamar una mínima consideración particular y pública a su interioridad, actitud que se traduce en abstención de conocimiento e injerencia en la esfera reservada que les corresponde y que está compuesta por asuntos, problemas, situaciones y circunstancias de su exclusivo interés. Esta no hace parte del dominio público y, por tanto, no debe ser materia de información suministrada a terceros, ni de la intervención o análisis de grupos humanos ajenos, ni de divulgaciones o publicaciones (Sentencia C-640/10).

- **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).

- **Entorno digital:** Ambiente, tanto físico como virtual sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo

desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web. (CONPES 3854, pág. 87).

- **Entorno digital abierto:** Entorno digital en el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica. (CONPES 3854, pág. 87).

- **Evento:** Un evento es cualquier suceso observable en un sistema o red, como un usuario que se conecta a un recurso compartido de archivos, un usuario que envía un archivo electrónico o un firewall que bloquea un intento de conexión, entre otros.

- **Eventos adversos:** son aquellos que tienen consecuencias negativas, como fallos en un sistema, usos no autorizados de privilegios en un sistema, acceso no autorizados y ejecución de malware.

- **Evento de Seguridad de la Información:** Ocurrencia identificada de un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información o falla de los controles, o una situación desconocida que puede ser relevante para la seguridad. [ISO/IEC 27000:2009].

- **Defacement:** Ataque sobre un servidor web como consecuencia del cual se cambia su apariencia.

- **DoS / DDoS (Denial of Service / Distributed Denial of Service):** Se entiende como denegación de servicio, en términos de seguridad digital, a un conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca sobrecargar un servidor y de esta forma no permitir que sus legítimos usuarios puedan utilizar los servicios prestados por él. El ataque consiste en saturar con peticiones de servicio al servidor, hasta que éste no puede atenderlas, provocando su colapso.

- **DRP (Disaster Recovery Plan / Plan de Recuperación ante Desastres):** es un documento formal creado por una organización que contiene instrucciones detalladas con la definición de los procedimientos, estrategias, y roles y responsabilidades establecidos para recuperar y mantener el servicio de tecnología ante un evento de interrupción.

- **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 27001:2022).

- **Gobernanza de la seguridad digital para Colombia:** Corresponde al conjunto de interacciones y enfoques entre las múltiples partes interesadas para identificar, enmarcar, proponer, y coordinar respuestas proactivas y reactivas a posibles amenazas a la confidencialidad, integridad o disponibilidad de los servicios tecnológicos, sistemas de información, infraestructura tecnológica, redes e información que en conjunto constituyen el entorno digital.

- **Incidente:** Un incidente es una violación o amenaza inminente a las políticas de seguridad digital, políticas de uso aceptable y/o prácticas de seguridad básicas.

- **Incidente de seguridad digital:** Ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite; o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable. (Decreto 338 de 2022)

- **Infraestructura Cibernética (Ic):** Son las infraestructuras soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO).

- **Infraestructuras Críticas**: incluyen la vasta red de carreteras, puentes y túneles de conexión, ferrocarriles, servicios públicos y edificios necesarios para mantener la normalidad en la vida cotidiana de los ciudadanos. El transporte, el comercio, el agua potable y la electricidad dependen de estos sistemas críticos. Infraestructura crítica puede ser cualquier sistema, ya sea físico o virtual, que sea tan vital que si se interrumpe puede tener un impacto debilitador en la seguridad, la economía, la salud pública o la seguridad, el medio ambiente. También puede definirse como los sistemas y activos que sustentan industrias o servicios urbanos y rurales subnacionales esenciales.

    - Las infraestructuras críticas son vulnerables a innumerables amenazas o peligros, además, de manejar una relación de interdependencia entre estas mismas. Lo que significa que sus operaciones confiables son tan críticas que una interrupción o pérdida de una de estas funciones afectará directamente la seguridad y la resiliencia de la infraestructura crítica dentro y entre numerosos sectores. Lo que con el tiempo puede provocar una pérdida adicional de otras funciones.

    - Aunque parte de esta infraestructura física y cibernética esta operada por empresas estatales, normalmente el sector privado tiene un gran margen de operatividad y propiedad sobre estas mismas, especialmente en la cibernética. Por lo que se debe trabajar en sociedad con el sector público y privado para aumentar la resiliencia, reducir el riesgo y mantener la confianza en la infraestructura crítica de la nación.

- **Infraestructura Crítica Cibernética (ICC):** Sistemas y activos, físicos o virtuales, soportados por Tecnologías de la Información y las Comunicaciones, cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía. (Decreto 338 de 2022). Esta se alinea a la definición de NIST Sistema y activos, ya sean físicos o virtuales, tan vitales para los Estados Unidos que la incapacidad o destrucción de dichos sistemas y activos tendría un impacto debilitante en la seguridad, la seguridad económica nacional, la salud pública nacional o la seguridad, o cualquier combinación de estos asuntos. NIST SP 800-30 Rev.1

- **Infraestructura Estratégica (IE):** Son las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que se soporta el funcionamiento de los servicios esenciales. Adaptación Ley 8/2011-Gobierno de España.

- **Infraestructura Estratégica Cibernética (IEC):** Son las infraestructuras soportadas por Tecnologías de Información y Comunicaciones (TIC) y Tecnologías de Operación (TO), sobre las que se soporta el funcionamiento de los servicios esenciales. Fuente: Guía de IC Ministerio de Defensa.

- **Incidente de seguridad informática:** Una violación o inminente amenaza de violación de las políticas de seguridad informática, políticas de uso aceptable o prácticas estándar seguridad. En el contexto de este procedimiento, una inminente amenaza es definida como una situación en la cual la organización tiene evidencias para creer que un incidente de seguridad va a ocurrir.

- **Incidente de privacidad de la información:** Evento o serie de eventos no deseados e inesperados producto del tratamiento de los datos personales.

- **Incidentes de seguridad de la información:** Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información. [ISO/IEC 27000 2009].

- **Incidente digital:** Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el medio digital y que genera impactos sobre los objetivos. (CONPES 3854, pág. 87).

- **Información pública**. Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal. (Literal b, artículo. 6 de la Ley 1712 de 2014)

- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley. (Literal c, artículo. 6 de la Ley 1712 de 2014)

- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Ingeniería social:** Son técnicas basadas en engaños que se emplean para dirigir la conducta de una persona u obtener información sensible. El afectado es inducido a actuar de determinada forma (pulsar en enlaces, introducir contraseñas, visitar páginas, etc.) convencido de que está haciendo lo correcto cuando realmente está siendo engañado por el ingeniero social.

- **Inyección de ficheros remota:** Estado de vulnerabilidad que se crea por métodos de codificación poco seguros, y que tiene como resultado una validación de entradas inapropiada, que permite a los atacantes transferir código malicioso al sistema subyacente a través de una aplicación web.

- **Inyección SQL:** Tipo de ataque a sitios web basados en bases de datos. Una persona malintencionada ejecuta comandos SQL no autorizados aprovechando códigos inseguros de un sistema conectado a Internet. Los ataques de inyección SQL se utilizan para robar información normalmente no disponible de una base de datos o para acceder a las computadoras host de una organización mediante la computadora que funciona como servidor de la base de datos.

- **Incidente de seguridad digital - Ciberincidente:** Ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite; o que constituye una violación a las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable.

- **Infraestructura crítica cibernética:** Sistemas y activos, físicos o virtuales, soportados por Tecnologías de la Información y las Comunicaciones, cuya afectación significativa tendría un impacto grave en el bienestar social o económico de los ciudadanos, o en el funcionamiento efectivo del gobierno o la economía.

- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008, o aquella que la modifique, adicione o sustituya

- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014, o aquella que la modifique, adicione o sustituya.

- **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 y pseudominización

- **Modelo de Gobernanza de Seguridad digital:** Es el esquema de trabajo compuesto por un conjunto de políticas de operación, principios, normas, reglas, procedimientos de toma de decisiones y programas compartidos por las múltiples partes interesadas de la seguridad digital del país, con el fin de fortalecer las capacidades para la gestión de riesgos e incidentes de seguridad digital y para la respuesta proactiva y reactiva a posibles amenazas a la confidencialidad, integridad o disponibilidad de los servicios tecnológicos, sistemas de información, infraestructura tecnológica y las redes e información que, en conjunto, constituyen el entorno digital en el país. (Decreto 338-2022)..

- **Múltiples partes interesadas:** Corresponde al conjunto de actores que dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales. Comprende a las autoridades, las organizaciones privadas, los operadores o propietarios de las infraestructuras críticas cibernéticas nacionales, los prestadores de servicios esenciales, la academia y la sociedad civil.

- **NIST:** Es el Instituto Nacional de Estándares y Tecnología y busca promover la innovación y la competencia industrial mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida.

- **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.

- **Pharming:** Ataque informático que consiste en modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP legítima de una entidad de manera que en el momento en el que el usuario escribe el nombre de dominio de la entidad en la barra de direcciones, el navegador redirigirá automáticamente al usuario a otra dirección IP (Internet Protocol) donde se aloja una web (página) falsa que suplantará la identidad legítima de la entidad, obteniéndose de forma ilícita las claves de acceso de los clientes la entidad.

- **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 27001:2022).

- **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).

- **Plan de Respuesta a Ciberincidentes:** Conjunto predeterminado y ordenado de instrucciones o procedimientos para detectar, analizar, contener, erradicar y recuperar para minimizar las consecuencias de un ciberincidente.

- **Phishing:** Es un método que los ciberdelincuentes utilizan para engañar y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito, de la seguridad social y números de cuentas bancarias. Lo hacen mediante el envío de correos electrónicos fraudulentos o dirigiéndole a un sitio web falso.

- **Plan de Continuidad de la operación:** Actividades documentadas que guían a la Entidad en la respuesta, recuperación, reanudación y restauración de las operaciones a los niveles predefinidos después de un incidente que afecte la continuidad de las operaciones.

- **Ransomware:** Código malicioso para secuestrar datos, una forma de explotación en la cual el atacante cifra los datos de la víctima y exige un pago por la clave de descifrado, se propaga a través de archivos adjuntos de correo electrónico, programas infectados y sitios web comprometidos, secuestrando computadores y servidores (imposibilidad de usarlo) o cifrando los archivos, con la promesa de liberarlo tras el pago de una cantidad de dinero por el rescate.

- **RAT- Remote Access Tool:** Pieza de software que permite a un “operador” controlar a distancia un sistema como si se tuviera acceso físico al mismo. Aunque tiene usos necesarios para la administración de sistemas a distancia, el software RAT se asocia habitualmente con ciberataques o actividades criminales o dañinas. En estos casos, el malware suele instalarse sin el conocimiento de la víctima, ocultando frecuentemente un troyano.

- **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 27001:2022).

- **Riesgo de seguridad digital:** Es la combinación de amenazas y/o vulnerabilidades que se pueden materializar en el curso de cualquier actividad en el entorno digital y que puede afectar el logro de los objetivos económicos o sociales al alterar la confidencialidad, integridad y disponibilidad.

- **Rootkit:** Es una herramienta que sirve para ocultar actividades ilegítimas en un sistema. Una vez que ha sido instalado, permite al atacante actuar con el nivel de privilegios del administrador del equipo.

- **Scanner (Scanning) Escáner de vulnerabilidades:** Programa que analiza un sistema buscando vulnerabilidades. Utiliza una base de datos de defectos conocidos y determina si el sistema bajo examen es vulnerable o no.

- **Spam (correo basura):** Correo electrónico no deseado que se envía aleatoriamente en procesos por lotes. Es extremadamente eficiente y barata forma de comercializar cualquier producto. La mayoría de los usuarios que están expuestos a este correo basura que se confirma en encuestas que muestran que más del 50% de todos los e-mails son correos basura. No es una amenaza directa, pero la cantidad de e-mails generados y el tiempo que lleva a las empresas y particulares relacionarlo y eliminarlo, representa un elemento molesto para los usuarios de Internet.

- **Spear Phising:** Phishing dirigido de forma que se maximiza la probabilidad de que el sujeto objeto del ataque pique el anzuelo (suelen basarse en un trabajo previo de ingeniera social sobre la victima).

- **Spyware “spy software”:** Tipo de software malicioso que al instalarse intercepta o toma control parcial de la computadora del usuario sin el consentimiento de este último.

- **Suplantación (Spoofing):** Técnica basada en la creación de tramas TCP/IP utilizando una dirección IP falseada; desde su equipo, un atacante simula la

identidad de otra máquina de la red (que previamente ha obtenido por diversos métodos) para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del anfitrión suplantado.

- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27001:2022).

- **Seguridad digital:** Es la situación de normalidad y de tranquilidad en el entorno digital, a través de la apropiación de políticas, buenas prácticas, y mediante: (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades; que demanda la voluntad social y política de las múltiples partes interesadas. (Decreto 338 de 2022). Para el caso de estandarización de lenguaje este concepto se asocia al aceptado internacionalmente como ciberseguridad.

- **Servicio esencial:** En el marco de la gestión de riesgos de la seguridad digital es aquel servicio necesario para el mantenimiento de las actividades sociales y económicas del país, que dependen del uso de tecnologías de la información y las comunicaciones, y un incidente en su infraestructura o servicio puede generar un daño significativo que afecte la prestación de dicho servicio y la consecuente parálisis de las actividades. (Decreto 338 de 2022).

- **Servicio crítico:** Conjunto de actividades que la organización realiza, al generar un producto o en la prestación de un servicio fundamental para la organización o sector del país, que al interrumpirse afectaría su operación.
- **Suplantación de identidad:** Todas aquellas actividades realizadas por la que una persona se hace pasar por otra para llevar a cabo actividades de carácter ilegal.

- **Tecnologías de la Información:** Las tecnologías de la información se centra en el tratamiento y la gestión de datos. [1]

- **Tecnologías de Operación:** La tecnología de operación se define como el conjunto de sistemas, procesos y herramientas que permiten a las empresas gestionar y controlar sus operaciones diarias de manera eficiente.
- **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).

[1] https://www.eccouncil.org/cybersecurity-exchange/whitepaper/understanding-the-difference-between-it-and-ot-security/#:~:text=While%20IT%20focuses%20on%20data,controlling%20physical%20processes%20and%20machinery.

- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27001:2022).

- **Vulnerabilidad de seguridad digital:** Debilidad, atributo o falta de aplicación de un control que permite o facilita la actuación de una amenaza contra los servicios tecnológicos, sistemas de información, infraestructura tecnológica y las redes e información de la organización. (Decreto 338 de 2022).

- **Troyano:** Programa que aparentemente, o realmente, ejecuta una función útil, pero oculta un subprograma dañino que abusa de los privilegios concedidos para la ejecución del citado programa.

- **Virus informático / malware / software malicioso:** Programa informático que está diseñado para realizar acciones maliciosas sobre un activo informático como copiarse a sí mismo, cifrar información, recolectar y filtrar información, entre otros, sin el consentimiento del propietario

# 4. Propósitos

- Facilitar la adopción e implementación del MSPI con mecanismos y lineamientos claros.

- Desarrollar e implementar la estrategia de seguridad digital de las entidades.

- Integrar la seguridad como habilitador en la política de Gobierno Digital mediante procedimientos definidos.

- Institucionalizar la seguridad y privacidad de la información y seguridad digital en los procesos de la entidad.

- Contribuir a la transparencia en la gestión pública a través de la implementación efectiva del MSPI.

- Apoyar la implementación del plan estratégico institucional mediante el plan de seguridad y privacidad de la información.

- Asistir a las entidades en la identificación y tratamiento de riesgos de seguridad de la información y seguridad digital

# 5. 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 el que se expide el Decreto 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 Reglamentario del Sector Cultura.

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

- Decreto 1083 de 2015 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”.

- Decreto 620 de 2020. Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011. los literales e. j y literal a del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

- CONPES 3995 de 2020. Política Nacional de Confianza y Seguridad digital.

- CONPES 4144 de 2025. Política Nacional de Inteligencia Artificial

- Decreto 728 de 2017. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional

del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.

- Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

- Decreto 1008 del 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

- Decreto 338 de 2022 Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Conpes 3975 del 2019 política nacional para la transformación digital e inteligencia artificial

- 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.

- Decreto 767 de 2022. "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"

- Norma ISO/IEC 27001:2022, Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información.

- Decreto 1083 de 2015 y sus modificaciones y actualizaciones.

- Decreto 767 de 2022. “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”

- Decreto 1263 de 2022. “Por el cual se adiciona el Título 22 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías

de la Información y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Pública”

Otras normas internacionales a tener en cuenta:

**GDPR (Reglamento General de Protección de Datos):** Se recomienda adoptar prácticas inspiradas en este reglamento, especialmente en lo relacionado con derechos del titular, principios de minimización, portabilidad, notificación de brechas de seguridad y consentimiento explícito, como complemento a la Ley 1581 de 2012.

**NIST SP 800-53**: Puede ser utilizado como guía técnica para complementar los controles de seguridad del MSPI, especialmente en sistemas críticos o servicios de procesamiento masivo de datos. Su adopción es flexible, gradual y adaptada al contexto local.

Este enfoque permitirá que las entidades públicas no solo cumplan con los requerimientos normativos nacionales, sino que también avancen hacia la adopción de estándares globales que refuercen la confianza digital, la interoperabilidad y la preparación ante riesgos emergentes.

# 6. Diagnóstico

La fase de diagnóstico permite a las entidades 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, se mide el nivel de madurez de la implementación del modelo de seguridad y privacidad de la información y se obtienen insumos fundamentales para la fase de planificación.

Este autodiagnóstico se debe realizar antes de iniciar la fase de planificación y actualizar la información tras terminar la fase de evaluación de desempeño, para identificar los cambios en el nivel de madurez de la implementación del Modelo en la entidad, el resultado que se obtenga después de la fase de evaluación de desempeño se incluirá como un insumo, en la fase de mejoramiento continuo.

| | |
|---|---|
| ***Lineamiento:*** | Identificar a través de la herramienta de autodiagnóstico (instrumento de evaluación MSPI) 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 el 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. | • Documento de la herramienta de autodiagnóstico diligenciada, identificando las brechas en la implementación |

| | |
|---|---|
| • Revisar aspectos internos tales como el talento humano, procesos y procedimientos, estructura organizacional, cadena de servicio, recursos disponibles, cultura organizacional, entre otros. | del MSPI en toda la entidad, y sus acciones de mejora. |

# 7. Fase 1: Planificación

Para el desarrollo de esta fase se deben 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.
- Adoptar la Política de seguridad y privacidad de la información mediante acto administrativo con el cual la entidad lo adopto colocar el número de resolución o acto administrativo.
- 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.
- Política de Gestión de Riesgos de la entidad con los lineamientos para la gestión de riesgos de seguridad y privacidad de la información y demás documentación asociada que determinan dichos lineamientos para la administración y gestión del riesgo.
- Plan de tratamiento de riesgos de seguridad de la información.
- Declaración de aplicabilidad.
- Manual de políticas de Seguridad de la Información.
- Plan de Cambio, Cultura y Apropiación.

# 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, teniendo en cuenta procesos necesarios y sus interacciones. |
| **Propósito:** | Conocer en detalle las características de la entidad y su entorno con el fin de implementar el Modelo de Seguridad y Privacidad adaptado a las condiciones específicas de cada entidad. |

| Entradas recomendadas | Salidas |
|---|---|
| • Para establecer el contexto de las entidades, deben tener en cuenta los aspectos relacionados en el Manual Operativo MIPG.<br>• Modelo estratégico, modelo de procesos, modelo de servicios y modelo organizacional siguiendo el Marco de Referencia de Arquitectura Empresarial definido por MinTIC.<br>• Plan estratégico de la entidad<br>• Procedimientos e informes de auditoria al MSPI | Documentos obligatorios:<br>Contexto de la entidad (Política de Planeación Institucional). |

## 7.1.2.Necesidades y expectativas de los interesados

| | |
|---|---|
| **Lineamiento:** | Se deben identificar las partes interesadas internas y externas que puedan influir o verse afectadas por la seguridad y privacidad de la información, así como sus necesidades y expectativas. Esta identificación debe incluir los requisitos legales, reglamentarios y contractuales, e integrarse adecuadamente al SGSI. |

| | |
|---|---|
| **Propósito:** | Conocer las necesidades y expectativas que se tiene respecto a la implementación del modelo de seguridad y privacidad de la información para identificar las acciones y actividades necesarias para satisfacerlas. |

| Entradas recomendadas | Salidas |
|---|---|
| • 7.1.1. Comprensión de la organización y de su contexto.<br>• Política de Planeación institucional: 7.1.1. Comprensión de la organización y de su contexto.<br>• Plan Nacional de Desarrollo.<br>• Política de Gobierno Digital.<br>• Política de seguridad digital<br>• Entrevistas con los líderes de procesos de la entidad.<br>• Listado de entidades de orden nacional o territorial que se relacionan directamente el cumplimiento misional de la entidad.<br>• Listado de proveedores de la entidad.<br>• Listado de operadores de la entidad.<br>• Normatividad que le aplique a la entidad de acuerdo con funcionalidad respectivamente. | Documentos obligatorios:<br>Compendio de necesidades y expectativas de las partes interesada. (Política de Planeación Institucional).<br><br>Análisis de partes interesadas en seguridad de la información. |

# 7.1.3. Definición del alcance del MSPI

| | |
|---|---|
| **Lineamiento:** | Determinar con claridad los límites, el alcance y la aplicabilidad del MSPI en el marco del modelo de operación por procesos de la entidad. Esta definición debe especificar a qué procesos, recursos humanos, financieros, técnicos y tecnológicos se aplicará la implementación del modelo. Se recomienda iniciar con los procesos misionales, dado su |

| | |
|---|---|
| | impacto estratégico y su nivel de exposición a riesgos de seguridad y privacidad de la información. |
| **Propósito:** | Identificar qué activos de información, software, hardware, roles, sistemas de información, áreas seguras (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.<br>• 7.1.2 Necesidades y expectativas de los interesados<br>• Modelo de procesos, modelo organizacional, modelo de servicios y catálogo de servicios tecnológicos; siguiendo el Marco de Referencia de Arquitectura Empresarial definido por MinTIC.<br>• Presupuesto disponible para implementar el MSPI.<br>• 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 en el documento del Modelo de Planeación y Gestión). |

# 7.2. Liderazgo

## 7.2.1.Liderazgo y Compromiso

**Lineamiento**: Las entidades deben asignar, mediante acto administrativo, al comité institucional de gestión y desempeño (o su equivalente) las funciones relacionadas con la seguridad y privacidad de la información, asegurando la adopción, implementación y mejora continua del MSPI. En este comité debe incluirse como miembro permanente al responsable de seguridad de la información, con el fin de garantizar su implementación efectiva y el cumplimiento de acciones claves como:

- Establecer y publicar la adopción de la política general, los objetivos y las políticas específicas de seguridad y privacidad de la información.
- Garantizar la adopción de los requisitos del MSPI en los procesos de la entidad.
- Comunicar en la entidad la importancia del MSPI.
- Planear y disponer de los recursos necesarios (presupuesto, personal, tiempo etc.) para la adopción del MSPI.
- Asegurar que el MSPI consiga los resultados previstos.
- Realizar revisiones periódicas de la adopción del MSPI (al menos dos veces por año y en las que el Nominador deberá estar presente).

**Propósito**: Garantizar el liderazgo y el compromiso del comité institucional de gestión y desempeño o quien haga sus veces para conseguir los objetivos definidos para la implementación del MSPI.

| Entradas recomendadas | Salidas |
|---|---|
| • 7.1.3 Definición del alcance del MSPI según lo que arroje el autodiagnóstico de cada entidad.<br>• Modelo de procesos y modelo organizacional articulado con el Marco de Referencia de Arquitectura Empresarial definido por MinTIC.<br>• 7.1.2 Necesidades y expectativas de los interesados | • Evidencia en el acto administrativo que soporta la conformación del comité de gestión y desempeño o quien haga sus veces, señalando las funciones de seguridad y privacidad de la información. |

# 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 los lineamientos y compromisos que se adoptaran para asegurar la confidencialidad, integridad y disponibilidad de la información, 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 que permita la reevaluación y actualización periódica de las medidas de seguridad para adaptarlas a la constante evolución de los riesgos y sistemas de protección. El personal calificado de la entidad supervisará, revisará y auditará la seguridad de la información. 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.
- Ser comunicada al interior de la entidad y a los interesados que aplique.

**Propósito**: La política establece la base respecto al comportamiento 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.<br>• Necesidades y expectativas de los interesados.<br>• Definición del alcance del MSPI.<br>• Requerimientos normativos y buenas prácticas de seguridad y privacidad de la información. | • Acto administrativo o acta de aprobación del Comité Institucional de Gestión y Desempeño con la adopción de la Política de seguridad y privacidad de la información |

## 7.2.3. Roles y responsabilidades

| | |
|---|---|
| **Lineamientos:** | Articular roles y responsabilidades con las áreas de la entidad para la adopción del MSPI, asegurando el monitoreo, reporte y aprobación ante el comité institucional. Los líderes de proceso deberán gestionar los riesgos de seguridad y privacidad de la información.<br><br>Designar un responsable del MSPI con un equipo de apoyo, dependiente de un área estratégica distinta a la de Tecnología. Si no existe el cargo, deberá delegarse por acto administrativo e integrarse con voz y voto al comité de gestión institucional de gestión y desempeño y con voz al comité de control interno.<br><br>Si no hay personal de planta, varias entidades podrán compartir un responsable de seguridad mediante contrato de servicios, justificando la falta de recursos, conforme al artículo 5 de la Resolución 500 sobre Estrategia de Seguridad Digital. |
| ***Propósito:*** | Es fundamental que los funcionarios y contratistas conozcan sus responsabilidades, comprendan el impacto de sus acciones en la seguridad de la información y entiendan cómo contribuyen a la implementación efectiva del MSPI. |

| Entradas recomendadas | Salidas |
|---|---|
| • 7.1.3 Definición del alcance del MSPI<br>• 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. | • Roles y responsabilidades en seguridad de la información de las diferentes áreas o procesos de la entidad.<br>• Definición del rol de: responsable de seguridad de la información, indicando sus funciones y responsabilidades |

# 7.3. Planeación

## 7.3.1.Identificación de activos de información e infraestructura critica cibernética

| | |
|---|---|
| **Lineamiento:** | Las entidades deben definir y aplicar un proceso de identificación y clasificación de los activos de información, que permita:<br>• Identificar los activos de información que agregan valor al proceso y requieren protección, según el alcance y los procesos cubiertos por el MSPI.<br>• 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.<br>• 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.<br>• Identificar los activos de información con información personal en el inventario de activos de información.<br>• Realizar la identificación y el inventario de infraestructura crítica y servicios esenciales de la entidad**.** |
| **Propósito:** | Estructurar una metodología que permita identificar y clasificar los activos de información |

| Entradas recomendadas | Salidas |
|---|---|
| • 7.1.3 Definición del alcance del MSPI<br>• Modelo de procesos, y modelo organizacional, desarrollados para | • Procedimiento de inventario y clasificación de activos de información[2], del Modelo de |

[2] Anexo 1. Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional

| | | |
|---|---|---|
| | la Arquitectura Misional de la entidad, siguiendo el Marco de Referencia de Arquitectura Empresarial definido por MinTIC.<br><br>• Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional | Seguridad y Privacidad de la Información.<br><br>• Documento metodológico de inventario y clasificación de la información.<br><br>• Inventario de activos de información de cada proceso incluido en el alcance debidamente identificados, clasificados y valorados. |

## 7.3.2. Valoración de los riesgos de seguridad de la información

| | |
|---|---|
| **Lineamiento** | Las entidades deben definir y aplicar un proceso de valoración de riesgos de la seguridad y privacidad de la información, que permita:<br><br>• Identificar los riesgos que causen la pérdida de confidencialidad, integridad, disponibilidad, privacidad de la información, así como la continuidad de la operación de la entidad dentro del alcance del MSPI.<br><br>• Identificar los propietarios de los riesgos.<br><br>• Definir criterios para valorar las consecuencias de la materialización de los riesgos, y la probabilidad de su ocurrencia.<br><br>• Determinar el apetito de riesgos definido por la entidad.<br><br>• Establecer criterios de aceptación de los riesgos.<br><br>• Valorar los riesgos que afecten la confidencialidad, integridad y disponibilidad de la información dentro del alcance del MSPI.<br><br>• Determinar los niveles de riesgo.<br><br>• Realizar la comparación entre los resultados del análisis y los criterios de los riesgos establecidos en este mismo numeral.<br><br>• Priorización de los riesgos analizados para su tratamiento.<br><br>• Se debe asegurar que las valoraciones repetidas de los riesgos de seguridad y privacidad de la información produzcan resultados consistentes, válidos y comparables. |

- Se recomienda realizar una evaluación de riesgos específica frente a amenazas avanzadas persistentes (APT) y vulnerabilidades emergentes, con el fin de ajustar las estrategias de seguridad a los ataques de alta sofisticación.

- Se deben considerar los nuevos riesgos asociados a los dominios incluidos en la ISO/IEC 27001:2022, tales como amenazas avanzadas, entornos de nube, y riesgos en la cadena de suministro digital.

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

| Entradas recomendadas | Salidas |
|---|---|
| • 7.1.3 Definición del alcance del MSPI.<br>• 7.2.2 Política de seguridad y privacidad de la información.<br>• Directorio de servicios de componentes de información, de acuerdo con el Marco de Referencia de Arquitectura Empresarial definido por MinTIC.<br>• Inventario de activos de información de la entidad usando:<br>  ○ Proceso de valoración de riesgos de la seguridad de la información de acuerdo con lo definido en la Guía del DAPF<br>  ○ b) Reportes de debilidades o vulnerabilidades en los activos de información realizados por los colaboradores de la entidad o del resultado de auditorias | • Procedimiento y metodología de gestión de riesgos institucional incluyendo el capítulo de seguridad y privacidad de la información aprobado por el comité institucional de gestión y desempeño.<br>• Instrumento para la identificación y valoración de los riesgos de seguridad y privacidad de la información. |

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

**Lineamiento:** Las entidades deben 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 adoptados por la entidad, su estado de implementación y la justificación de posible exclusión de acuerdo con los riesgos identificados y las capacidades técnicas y humanas con las que cuenta.
- Definir un plan de tratamiento de riesgos que contenga, fechas, acciones de tratamientos de riesgos a tratar y responsables con el objetivo de realizar trazabilidad.
- Los dueños de los riesgos que deben ser los dueños de los procesos afectados por estos riesgos, o las personas designadas por ellos. Deben realizar la aprobación formal del plan de tratamiento de riesgos y la aprobación 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.<br>• 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).<br>• La aceptación de los riesgos residuales e indicación en que parte se deben aceptar.<br>• Declaración de aplicabilidad, aceptada y aprobadas en el |

| | |
|---|---|
| | comité institucional de gestión y desempeño |

# 7.4. Soporte

## 7.4.1. Recursos

| | |
|---|---|
| ***Lineamiento:*** | Las entidades deben asegurar los recursos financieros, humanos y técnicos necesarios para adoptar, implementar y mantener el MSPI como un proceso transversal conforme al alcance definido. |
| **Propósito:** | Determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del MSPI. |

| Entradas recomendadas | Salidas |
|---|---|
| • 7.1 Contexto<br>• 7.1.3 Definición del alcance del MSPI.<br>• 7.2.2 Política de seguridad y privacidad de la información.<br>• 7.2.3 Roles y responsabilidades<br>• 7.3.3 Plan de tratamiento de los riesgos de seguridad de la información.<br>• Plan de Seguridad y Privacidad de la Información.<br>• Matriz de riesgos de seguridad y privacidad de la información.<br>• Declaración de aplicabilidad.<br>• Inventarios de activos de información, sistemas de información, infraestructura de TI y de sus administradores | • Incluir dentro de los proyectos de inversión de la entidad aquellas actividades relacionadas con la adopción de MSPI de acuerdo con el alcance establecido (esto involucra también al personal de seguridad de la información a contratar para el desarrollo de las actividades del SGSI).<br>• Actualización del PETI de acuerdo con los recursos necesarios para realizar la gestión adecuada de los riesgos de seguridad de la información identificados y el plan de seguridad y privacidad de la información. |

# 7.4.2. Competencia, toma de conciencia y comunicación

**Lineamientos**

Las entidades deben 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 colaboradores de la entidad en la implementación y gestión del MSPI.
- Concientizar a los colaboradores 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.
- Tener un enfoque práctico en la respuesta a incidentes, especialmente en técnicas de phishing, ingeniería social y ciberhigiene, para fortalecer la capacidad de respuesta ante ataques dirigidos.
- Cuando proceda, tomar las acciones para adquirir y/o fortalecer la competencia de los responsables del MSPI.
- Evaluar la eficacia de las acciones de concientización y sensibilización realizadas.

**Propósito**

Garantizar una correcta comunicación, sensibilización y concientización con respecto a la seguridad y privacidad de la información, en la que todos los funcionarios conozcan la política, su rol en el MSPI y las implicaciones de no aplicar las reglas de seguridad y privacidad.

**Entradas recomendadas**

- 7.1.3 Definición del alcance del MSPI.
- 7.2.3 Roles y responsabilidades
- Manual de funciones de la entidad.

**Salidas**

- 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 capacitación Institucional. | Plan de comunicaciones del modelo de seguridad y privacidad de la información |

# 7.4.3. Información documentada

| | |
|---|---|
| **Lineamiento:** | El modelo de seguridad y privacidad de la información de la entidad debe incluir:<br>• Información documentada de los lineamientos establecidos.<br>• Documentos que la entidad considere necesarios para la eficacia del SGSI.<br>• Reglas claras para crear y actualizar documentos: identificación, formato, soporte, y control de versiones.<br>• La información documentada debe estar disponible y ser adecuada para su uso, donde y cuando se necesite además de estar adecuadamente protegida |
| **Propósito:** | Mantener una documentación adecuada para que pueda ser consultada en cualquier momento por las partes interesadas y le permita conocer los detalles del sistema de gestión de seguridad de la información. |

| Entradas recomendadas | Salidas |
|---|---|
| • Lineamientos de las diferentes Fases del MSPI | • Políticas, manuales, procesos procedimientos guías, entre otros.<br>• Inventario de activos, matriz de riesgos, planes de tratamiento, declaración de aplicabilidad, proceso de gestión de eventos, vulnerabilidades. |

# 8. Fase 2: Operación

Tras finalizar la fase 7 de planeación del MSPI, se iniciará la implementación de los procesos de seguridad de la información: gestión de activos, riesgos, incidentes, vulnerabilidades, tratamiento y evaluación de controles. Se fomentará la cultura de seguridad y se definirán criterios de cumplimiento y mecanismos de control para procesos y servicios externos relevantes, asegurando su alineación con el SGSI. Los documentos que se deben generar en esta fase son:

- Actualización del inventario de información.
- Actualización de la matriz de riesgos de seguridad de la información.
- Plan de implementación de controles de seguridad.
- Actualización de la gestión de eventos e incidentes de seguridad de la información.
  Actualización de la gestión de vulnerabilidades.
  Evidencia de la implementación de los controles de seguridad de la información.

# 8.1. Control y planeación operacional

| | |
|---|---|
| **Lineamiento:** | Las entidades deben realizar la planificación e implementación de las acciones determinadas en el plan de tratamiento de riesgos y el plan de Seguridad y Privacidad de la Información, esta información debe estar documentada para cada proceso según lo planificado, los planes de tratamiento deben ser definidos y aprobados por los lideres de proceso, Los proyectos o controles de seguridad que no pueden implementarse en el corto plazo o mediano plazo se deben escalar al comité institucional de gestión y desempeño para toma de decisiones y asignación de recursos. Las acciones que la entidad considere relevantes deben ser aprobadas por el comité institucional de gestión y desempeño. De igual manera, deben reforzar los mecanismos de monitoreo continuo, incluyendo la implementación de sistemas de alerta temprana que permitan a las entidades detectar y responder a incidentes en tiempo real, garantizando la resiliencia frente a ciberataques. |
| **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.<br>• Anexo A 27001:2022 | • Plan de seguridad y privacidad de la información que defina la implementación de controles de seguridad y privacidad de la información y contenga como mínimo: controles, actividades, |

| | |
|---|---|
| • Plan de 7.3.3 Plan de tratamiento de los riesgos de seguridad de la información.<br><br>• Plan de Seguridad y Privacidad de la Información | fechas, responsable de implementación y presupuesto.<br><br>• Evidencia de la implementación de los controles de seguridad y privacidad de la información. |

# 8.2. Plan de tratamiento de riesgos

**Lineamiento:**

- La entidad debe realizar evaluaciones de riesgos de seguridad de la información a intervalos planificados o cuando se propongan u ocurran cambios significativos.
- La entidad debe conservar información documentada de los resultados de las evaluaciones de riesgos de seguridad de la información.
- La entidad debe implementar el plan de tratamiento de riesgos de seguridad de la información.
- La entidad debe conservar información documentada de los resultados del tratamiento de riesgos de seguridad de la información.

**Propósito:** Establecer un proceso formal de identificación, evaluación y tratamiento de los riesgos de seguridad de la información

| Entradas recomendadas | Salidas |
|---|---|
| • Inventario de activos de información<br><br>• Incidentes de seguridad de la información<br><br>• Eventos y reportes de amenazas y vulnerabilidades de seguridad e la información | • Matriz de riesgos de seguridad de la información.<br><br>• Planes de tratamiento de los riesgos de seguridad e la información. |

## 8.3. Definición de indicadores de gestión

| | |
|---|---|
| **Lineamiento:** | La entidad debe definir indicadores que le permitan medir la evolución y avance en el nivel de madurez de la seguridad de la información. |
| **Propósito:** | Establecer indicadores para medir la gestión y madurez de la entidad en la implementación del modelo de seguridad y privacidad de la información |

| Entradas recomendadas | Salidas |
|---|---|
| • Política de seguridad de la información | • Indicadores de gestión de seguridad de la información |

# 9. Fase 3: Evaluación de desempeño

Una vez culminada las actividades de la fase de operación 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. Seguimiento, medición, análisis y evaluación

| | |
|---|---|
| ***Lineamiento:*** | Las entidades deben conocer sus avances en la implementación del modelo de Gobierno Digital, estableciendo tiempos y recursos para su monitoreo y reporte ante el Comité de Gestión y Desempeño, conforme al MIPG<br><br>Es importante incluir dentro del plan de auditorías los temas relacionados con seguridad digital como lo establece el MIPG. Los mecanismos utilizados para medir, analizar, monitorizar, evaluar y realizar seguimiento a la eficacia del Sistema deben ser comparables y reproducibles.<br><br>Deberán incluir retroalimentación periódica que recoja la percepción de seguridad y las vulnerabilidades encontradas por los usuarios en cada entidad. |
| **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.<br>• Documento con los resultados del tratamiento de riesgos de seguridad de la información.<br>• Resultado de la implementación de controles<br>• Diagnóstico del MSPI<br>• Plan de seguridad y privacidad de la información<br>• Plan de concientización y sensibilización.<br>• Reporte de incidentes presentados | • 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.<br>• Informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos. |

[3] Para la definición de los indicadores se puede utilizar como guía los lineamientos de Indicadores de Gestión de Seguridad de la Información

# 9.2. Auditoría Interna

| | |
|---|---|
| **Lineamiento:** | Realizar mínimo una auditoría interna al año con el fin de obtener información sobre el cumplimiento del MSPI. |
| **Propósito:** | Identificar no conformidades, desviaciones y oportunidades de mejora del MSPI |

| Entradas recomendadas | Salidas |
|---|---|
| • Todos los documentos producto de las salidas de las fases anteriores del MSPI.<br>• El informe de los resultados de las evaluaciones independientes, seguimientos y auditorías.<br>• Informes y compromisos adquiridos en los comités institucional de gestión y desempeño.<br>• El informe de los incidentes de seguridad y privacidad de la información reportados y la solución de estos.<br>• 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.<br>• Indicadores definidos y aprobados para la evaluación del MSPI. | • Resultados de las auditorías internas.<br>• No conformidades, hallazgos u oportunidades de mejora de las auditorías internas.<br>• 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. |

[4] Factores análisis PESTEL (Factores políticos, factores económicos, factores sociales, factores tecnológicos, factores legales)

## 9.3. Revisión por la dirección

| | |
|---|---|
| **Lineamiento:** | La Política y el Manual de Seguridad y Privacidad deben ser revisados y aprobados por el Comité de Gestión y Desempeño o por decisión del nominador, considerando los cambios en las necesidades de las partes interesadas. |
| **Propósito:** | Revisar el MSPI de la entidad, por parte de la alta dirección (comité Institucional de Gestión y Desempeño), en los intervalos planificados, que permita determinar su conveniencia, adecuación y eficacia. |

| Entradas recomendadas | Salidas |
|---|---|
| • Los documentos de alto nivel del MSPI deberán ser aprobados, incluyendo los actos administrativos que se necesiten para constituirlos al interior de la entidad. | • Revisión a la implementación.<br>• Acta y documento de Revisión por la Dirección.<br>• Compromisos de la Revisión por la Dirección. |

# 10. Fase 4: Mejoramiento continuo

Una vez culminadas las actividades del MSPI de la fase evaluación y desempeño, se deben 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 continua

| | |
|---|---|
| **Lineamiento:** | Las entidades deben contar con un plan de mejoramiento continuo que integre oportunidades de mejora, no conformidades y desviaciones, con acciones correctivas claras, responsables, tiempos y recursos definidos para fortalecer el 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. | • Plan anual de mejora del MSPI que incluya los controles de seguridad a implementar, oportunidades de mejora, no conformidades y demás desviaciones identificadas en la |

| | |
|---|---|
| • Resultados de auditorías y revisiones independientes al MSPI. | gestión de los diferentes procesos de seguridad y privacidad de la información que componen el SGSI.<br>• Plan estratégico de seguridad y privacidad de la información actualizado. |

# 10.2. Acciones Correctivas y no conformidades

| | |
|---|---|
| **Lineamiento:** | Ante una no conformidad, la entidad debe corregirla, mitigar sus efectos y evaluar acciones para evitar su repetición. |
| **Propósito:** | Identificar las no conformidades asociadas a la evaluación del MSPI y de los procesos. |

| Entradas recomendadas | Salidas |
|---|---|
| • Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI. | • Plan anual de mejora del MSPI que incluya los controles de seguridad a implementar |
| • Resultados de auditorías y revisiones independientes al MSPI. | • Plan estratégico de seguridad y privacidad de la información actualizado. |
| • Incidentes de seguridad de la información | • Planes de acción para la remediación de las no conformidades |

# 11. Anexo

## 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 27001:2022, los cuales tratan los 4 temas en los que se agrupan los 93 controles de seguridad de la información y se estructurarán tal como lo muestra la Tabla 1:

| | Políticas especificas | | | |
|---|---|---|---|---|
| **Núm.** | **Nombre** | **Seleccionado / Excepción** | **Tema** | **Descripción / Justificación** |
| | Nombre | Control | #Proteccion | |
| | ... | | | |

*Tabla 1 Estructura de los controles*

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 27001:2022.

- 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.

- Tema: Este campo describe a que tipo de control pertenece (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.

| Núm. | Nombre | Descripción / Justificación |
|---|---|---|
| A.5 | Controles organizacionales | |
| A.5.1 | 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, que integren controles de ciberseguridad específicos para detectar y responder a incidentes, para garantizar un enfoque coordinado en la protección del ciberespacio |
| A.5.2 | Roles y responsabilidades de 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.5.3 | Segregación de funciones | Control: Deben segregarse los deberes conflictivos y las áreas conflictivas de responsabilidad. |
| A.5.4 | Responsabilidades de la dirección | Control: La gerencia debe exigir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y los procedimientos específicos del tema de la organización. |
| A.5.5 | Contacto con las autoridades | Control: Se deben mantener los contactos apropiados con las autoridades pertinentes. |
| A.5.6 | 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.5.7 | Inteligencia de amenazas | Control: La información relacionada con las amenazas a la seguridad de la información debe recopilarse y analizarse para generar información sobre amenazas. Se sugiere establecer un procedimiento formal de Inteligencia de amenazas de la seguridad de la información. |
| A.5.8 | 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.5.9 | Inventario de activos de información y otros asociados a la misma | Control: Se debe desarrollar y mantener un inventario de información y otros activos asociados, incluidos los propietarios |
| A.5.10 | Uso aceptable de activos de información y otros asociados a la misma | 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.5.11 | 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.5.12 | Clasificación de la información | Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada. |

| Núm. | Nombre | Descripción / Justificación |
|---|---|---|
| A.5.13 | Etiquetado de la información | Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización. |
| A.5.14 | Transferencia de información | Control: Deben existir reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes. |
| A.5.15 | Control de Acceso | Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información. |
| A.5.16 | Gestión de la identidad | Control: Debe gestionarse el ciclo de vida completo de las identidades. |
| A.5.17 | Información de autenticación | Control: La asignación de la información secreta se debe controlar por medio de un proceso de gestión formal, además se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta. |
| A.5.18 | Derechos de acceso | Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado. |
| A.5.19 | Seguridad de la información en la relación con proveedores | Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deberían documentar. |
| A.5.20 | Abordar la seguridad de la información en los acuerdos con proveedores | Control: Los requisitos de seguridad de la información pertinentes deben establecerse y acordarse con cada proveedor en función del tipo relación con el proveedor. |
| A.5.21 | Gestión de la seguridad de la información en la cadena de suministro de las TIC (Tecnologías de Información y Comunicación) | Control: Deben definirse e implementarse procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC |
| A.5.22 | Seguimiento, Revisión y Gestión de Cambios de Servicios de Proveedores | Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos. |
| A.5.23 | Seguridad de la información para el uso de servicios en la nube (cloud) | Control: Los procesos de adquisición, uso, gestión y salida de los servicios en la nube deben establecerse de acuerdo con los requisitos de seguridad de la información de la organización. |

| Núm. | Nombre | Descripción / Justificación |
|---|---|---|
| A.5.24 | Planificación y preparación de la gestión de incidentes de seguridad de la información | Control: Los procesos de adquisición, uso, gestión y salida de los servicios en la nube deben establecerse de acuerdo con los requisitos de seguridad de la información de la organización. |
| A.5.25 | Evaluación y decisión sobre los eventos de seguridad de la información | Control: Los eventos de seguridad de la información se deben evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información. |
| A.5.26 | Respuesta a los incidentes de seguridad de la información | Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados. |
| A.5.27 | Aprendizaje sobre los incidentes de seguridad de la información | Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros. |
| A.5.28 | Recopilación de pruebas | Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia. |
| A.5.29 | Seguridad de la información durante interrupciones | Control: La organización debe planificar cómo mantener la seguridad de la información en un nivel adecuado durante la interrupción. |
| A.5.30 | Preparación de las TIC para la continuidad de negocio | Control: La preparación de las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC. |
| A.5.31 | Requisitos legales, estatutarios, regulatorios y contractuales | Control: 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.5.32 | 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.5.33 | 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.5.34 | Privacidad y protección de la PII (Información Identificable Personal) | Control: La organización deberá identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y reglamentos aplicables y los requisitos contractuales. Se recomienda incluir dentro del procedimiento de gestión de incidentes las actividades pertinentes para atender de manera diligente los |

| Núm. | Nombre | Descripción / Justificación |
|---|---|---|
| | | incidentes relacionados con información personal de acuerdo a lo establecido en la ley 1581 del 2012. |
| A.5.35 | 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.5.36 | Cumplimiento de políticas, normas y estándares de seguridad de la información | 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.5.37 | Procedimientos operacionales documentados | Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten. |
| A.6 | Controles de personas | |
| A.6.1 | Revisión de antecedentes | Control: Los controles de verificación de antecedentes de todos los candidatos para convertirse en personal deben llevarse a cabo antes de unirse a la organización y de manera continua, teniendo en cuenta las leyes, regulaciones y ética aplicables, y deben ser proporcionales a los requisitos comerciales, la clasificación de la información a la que se accede y los riesgos percibidos. |
| A.6.2 | Términos y condiciones de 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.6.3 | Concientización, educación y entrenamiento en 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.6.4 | Proceso disciplinario | Control: Se debe contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra colaboradores que hayan cometido una violación a la seguridad de la información. |
| A.6.5 | Responsabilidades después de la finalización o cambio de 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.6.6 | Acuerdos de confidencialidad o no divulgación | Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información. |

| Núm. | Nombre | Descripción / Justificación |
|---|---|---|
| A.6.7 | Trabajo remoto | 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 trabajo remoto. |
| A.6.8 | Reportes de eventos de seguridad de la información | Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible. |
| A.7 | Controles físicos | |
| A.7.1 | Perímetros 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.7.2 | Entrada física | Control: Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado. |
| A.7.3 | Aseguramiento de oficinas, salas e instalaciones | Control: Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones. |
| A.7.4 | Supervisión de la seguridad física | Control: Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones. |
| A.7.5 | Protección contra amenazas físicas y ambientales | Control: Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes. |
| A.7.6 | Trabajar en áreas seguras | Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras. |
| A.7.7 | Escritorio despejado y pantalla despejada | 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.7.8 | Ubicación y Protección del equipo | 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.7.9 | Seguridad de los 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.7.10 | Medios de almacenamiento | Control: Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización. |
| A.7.11 | Servicios de apoyo | Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. |
| A.7.12 | Seguridad del cableado | Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta |

| Núm. | Nombre | Descripción / Justificación |
|---|---|---|
| | | servicios de información debe estar protegido contra interceptación, interferencia o daño. |
| A.7.13 | Mantenimiento de equipos | Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas. |
| A.7.14 | Eliminación 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.8 | Controles tecnológicos | |
| A.8.1 | Dispositivos de punto final de usuario | 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.8.2 | Derechos de acceso privilegiado | Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado. |
| A.8.3 | Restricción de acceso a la información | Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso. |
| A.8.4 | Acceso al código fuente | Control: Se debe restringir el acceso a los códigos fuente de los programas. |
| A.8.5 | Autenticación segura | Control: Las tecnologías y los procedimientos de autenticación segura deben implementarse en función de las restricciones de acceso a la información y la política específica del tema sobre el control de acceso. |
| A.8.6 | Gestión de la 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.8.7 | Protección contra malware | Control: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos. |
| A.8.8 | Gestión de vulnerabilidades técnicas | Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado. |
| A.8.9 | Gestión de la configuración | Control: Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, monitorearse y revisarse. |
| A.8.10 | Eliminación de información | Control: La información almacenada en sistemas de información, dispositivos o en cualquier otro medio de almacenamiento debe ser eliminada cuando ya no sea necesaria. |
| A.8.11 | Enmascaramiento de datos | Control: Cuando sea aplicable, se deben asegurar la privacidad y la protección de la información de datos |

| Núm. | Nombre | Descripción / Justificación |
|---|---|---|
| | | personales, como se exige en la legislación y la reglamentación pertinentes. Se deben aplicar medidas como el cifrado, el control de acceso y el monitoreo del acceso y uso de estos datos, en alineación con legislaciones de privacidad relevantes ej: GDPR en Europa. Además, se deben aplicar técnicas de anonimización de datos cuando sea posible, siguiendo los lineamientos de la guía de anonimización de datos estructurados del archivo general de la nación u otras guías aplicables al respecto, reduciendo la cantidad de información personal que se almacena o se transmite innecesariamente. |
| A.8.12 | Prevención de fuga de datos | Control: Las medidas de prevención de fuga de datos deben aplicarse a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información confidencial. |
| A.8.13 | Copia de seguridad de la información | Control: Se deben hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada. |
| A.8.14 | Redundancia de las 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.8.15 | Registro | Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información. |
| A.8.16 | Actividades de seguimiento | Control: Se deben producir, almacenar, proteger y analizar registros que registren actividades, excepciones, fallas y otros eventos relevantes. |
| A.8.17 | Sincronización del reloj (clock) | Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo. |
| A.8.18 | Uso de programas de utilidad privilegiados | Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones. |
| A.8.19 | Instalación de software en sistemas operativos | Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos. |
| A.8.20 | Seguridad en redes | Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones. |
| A.8.21 | Seguridad de los servicios de red | Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los |

| Núm. | Nombre | Descripción / Justificación |
|---|---|---|
| | | servicios se presten internamente o se contraten externamente. |
| A.8.22 | Segregación de redes | Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes. |
| A.8.23 | Filtrado web | Control: El acceso a sitios web externos debe administrarse para reducir la exposición a contenido malicioso. |
| A.8.24 | Uso de criptografía | Control: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información. |
| A.8.25 | Ciclo de vida de desarrollo seguro | Control: Deben establecerse y aplicarse reglas para el desarrollo seguro de software y sistemas. |
| A.8.26 | Requisitos de seguridad de la aplicación | Control: Los requerimientos relacionados con seguridad de la información se deben incluir en los requerimientos para nuevos sistemas de información o para mejoras a los sistemas de información existentes. |
| A.8.27 | Arquitectura del sistema seguro y principios de ingeniería | Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información. |
| A.8.28 | Codificación segura | Control: Los principios de codificación segura deben aplicarse al desarrollo de software. |
| A.8.29 | Pruebas de seguridad en desarrollo y aceptación | Control: La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados. |
| A.8.30 | Desarrollo subcontratado | Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente. |
| A.8.31 | Separación de los entornos de desarrollo, prueba y producción | 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. |
| A.8.32 | 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.8.33 | Información de prueba | Control: Asegurar la protección de los datos usados para pruebas. |
| A.8.34 | Protección de sistemas de información durante pruebas de auditoría | Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio. |

*Tabla 2: Controles del Anexo A del estándar ISO/IEC 27001:2022 y dominios a los que pertenece*