ALCALDÍA MAYOR DE BOGOTÁ D.C.
MOVILIDAD
Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial

FORMATO DE APROBACIÓN DOCUMENTAL

CÓDIGO: DESI-FM-008 | **VERSIÓN: 11**

FECHA DE APLICACIÓN: MAYO 2019

INFORMACIÓN DOCUMENTADA:		CÓDIGO:		VERSIÓN:		JUSTIFICACIÓN:		
TIPO	NOMBRE	ANTERIOR	VIGENTE	ANTERIOR	VIGENTE	ELABORA	ACTUALIZA	ANULA
Plan	Plan de Seguridad y Privacidad de la Información	EGTI-PL-003	EGTI-PL-003	2	3		X	

DESCRIPCIÓN DE LA JUSTIFICACIÓN:

Se actualiza el plan para presentar los temas y actividades que contempla desarrollar la UMV en su Plan de Seguridad y Privacidad de la información.

AVALA: LÍDER DE PROCESO *(Puede ser el Líder Estratégico o Líder Operativo dependiendo del proceso)*	ELABORA/ACTUALIZA/ANULA: *(Colaborador del proceso en compañía del enlace)*	ACOMPAÑAMIENTO: ASESOR OAP *(Colaborador de la Oficina Asesora de Planeación a cargo de procesos)*
(Firma)	*(Firma)*	*(Firma)* Andrea del P. Zambrano.
Nombre: Martha Patricia Aguilar Copete	*Nombre: Gloria Méndez/ Jeison Medina/ Yuly González*	*Nombre: Andrea del Pilar Zambrano Barrios*
Cargo: Secretaria General (E)	*Cargo: Contratistas Proceso EGTI*	*Cargo: Contratista Proceso DESI*

TRÁMITE DE APROBACIÓN DOCUMENTAL (DILIGENCIADO POR LA OFICINA ASESORA DE PLANEACIÓN)	¿ES APROBADO?	FECHA DE APROBACIÓN:	RESPONSABLE DEL SISTEMA DE GESTIÓN DE CALIDAD
	SI [X] NO [ ]	30-01-2020	(Firma) Martha Patricia Aguilar Copete REPRESENTANTE DE LA ALTA DIRECCIÓN
	OBSERVACIONES:		

ALCALDÍA MAYOR DE BOGOTÁ D.C.

MOVILIDAD

Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Bogotá, D.C.,
(ENERO DE 2020)

CONTENIDO

1. INTRODUCCION

El presente documento corresponde a la validación de las actividades del estado actual de la seguridad de la información en la UNIDAD ADMINISTRATIVA ESPECIAL DE REHABILITACIÓN Y MANTENIMIENTO VIAL (UAERMV). Para la evaluación se tiene como referencia las normas ISO 27001:2013, 27002, los lineamientos dados por MINTIC.

Dichos lineamientos están enmarcados para asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad de la información.

Así mismo, se debe formular, aprobar y hacer seguimiento a la implementación de la estrategia de gobierno digital y seguridad de la información en la UNIDAD ADMINISTRATIVA ESPECIAL DE REHABILITACIÓN Y MANTENIMIENTO VIAL (UAERMV).

Este plan define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales, los cuales son los elementos fundamentales de la Seguridad y privacidad de la Información, de la Arquitectura y de los Servicios Ciudadanos Digitales, que a través de la implementación de estándares, guías, recomendaciones y buenas prácticas permiten el desarrollo de los componentes y el logro en la implementación de la Política de Gobierno Digital en la Entidad.

2. OBJETIVO GENERAL

Establecer las actividades que contempla el Modelo de Seguridad y Privacidad de la Información, alineadas con la norma NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y la Continuidad de los servicios, para la implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) en la UNIDAD ADMINISTRATIVA ESPECIAL DE REHABILITACION Y MANTENIMIENTO VIAL (UAERMV).

3.OBJETIVOS ESPECÍFICOS DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD.

- Establecer las orientaciones, directrices e instrumentos que le permitan a la UMV gestionar la seguridad de la información.
- Identificar los controles de seguridad de la información definidos en el anexo A de la norma ISO 27001:2013 que se aplican actualmente a la UMV.
- Identificar los controles y mecanismos de seguridad que utilizan actualmente los sistemas de información de la UMV.
- Identificar y gestionar los riesgos de seguridad asociados a los recursos tecnológicos a los que está expuesta la UMV.
- Realizar los análisis a las vulnerabilidades que se identifiquen en la UMV, para mitigar los incidentes de seguridad.
- Describir los principales problemas de seguridad que se presentan en la Entidad.
- Definir las medidas de seguridad más apropiadas a aplicarse.
- Definir las políticas de seguridad encaminadas a minimizar los riesgos a los que está expuesta la información de la Entidad.
- Plantear un SGSI para la UMV bajo la norma ISO/IEC 27001 con el fin de garantizar confidencialidad, integridad y disponibilidad de la información.
- Implementar un SGSI para la UMV que permita proteger los activos de información de la Entidad.
- Establecer la guía que deben aplicar los usuarios para mantener un correcto uso de los recursos tecnológicos.
- Definir los lineamientos para contribuir a garantizar la seguridad de la información en la UAERMV.
- Lograr un adecuado nivel de confidencialidad, integridad y disponibilidad de la información que se produce o recibe en la Entidad.
- Cumplir con los principios de seguridad de la información.
- Apoyar e impulsar la innovación tecnológica en la Entidad.
- Proteger los activos de información, tecnológicos y de seguridad digital.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de la seguridad de la información en los servidores públicos, terceros, y demás usuarios externos de la UAERMV.

- Garantizar la continuidad del negocio frente a incidentes de seguridad.

4. ALCANCE

Este plan aplica a todos los niveles de la UNIDAD ADMINISTRATIVA ESPECIAL DE REHABILITACION Y MANTENIMIENTO VIAL (UAERMV), como a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de la Entidad, compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, Entidades relacionadas que acceden, ya sea interna o externamente a cualquier archivo de información, independientemente de su ubicación. Así mismo, esta Política aplica sobre toda la información creada, procesada o utilizada por la UNIDAD ADMINISTRATIVA ESPECIAL DE REHABILITACION Y MANTENIMIENTO VIAL (UAERMV), sin importar el medio, formato, presentación o lugar en el cual se resguarde.

Con el fin, de cumplir con los objetivos de la institución relacionados con la seguridad de la información y la seguridad informática, se han definido las políticas y lineamientos de seguridad y privacidad de la información, de acuerdo con el alcance previamente definido:

- ✓ Políticas de seguridad: definen los controles que proporcionen directivas y consejos de gestión que contribuyan a mejorar la seguridad de los activos de información.
- ✓ Políticas de navegación en internet: establecen la configuración de perfiles de navegación para optimizar el uso del canal de internet y reducir el riesgo de descarga de software nocivo.
- ✓ Políticas de tratamiento y manejo de datos personales: dictan los lineamientos para el manejo y tratamiento de los datos personales de acuerdo con la Ley 1581 de 2012 de la SIC (Superintendencia de Industria y Comercio).
- ✓ Políticas de seguridad de activos de información: definen los controles para catalogar los activos de información y protegerlos eficazmente.

- ✓ Política de protección y respaldo de la información: establecen los lineamientos para garantizar la realización de las copias o respaldos de la información.
- ✓ Política del escritorio limpio y bloqueo de pantalla: instituye los lineamientos para proteger los documentos ubicados en los escritorios y el bloqueo de los equipos de cómputo, cuando el usuario no se encuentre en su puesto de trabajo.
- ✓ Política de seguridad para gestión de contraseñas: establece los lineamientos para la gestión segura de las credenciales (usuario y contraseña) en los aplicativos y equipos de cómputo.
- ✓ Política de responsabilidades operacionales y control de cambios: define los lineamientos para cuando se requieren hacer cambios importantes en la infraestructura tecnológica o sistemas de información que pueden afectar la continuidad de la operación.
- ✓ Política de protección contra software nocivo: establece los lineamientos para evitar la descarga, instalación y propagación de software nocivo (virus y sus variantes)
- ✓ Política de gestión de riesgos: define los lineamientos para la identificación y mitigación de los riesgos asociados a los activos de información de la entidad.
- ✓ Política para el buen uso del correo electrónico institucional: implementa los lineamientos para el uso eficiente y seguro del correo electrónico de la entidad.
- ✓ Política de registro histórico de actividades (log): establece los lineamientos para almacenar los logs de los aplicativos críticos de la entidad, para que en caso de presentarse un incidente de seguridad sea posible realizar un análisis forense de la situación.
- ✓ Política sobre el uso de equipos de cómputo y el acceso a la red: instituye los lineamientos para el buen uso de los equipos de cómputo y la protección del acceso a la red LAN o wifi de la Entidad

5. PLAN PARA LA IMPLEMENTACION DEL SGSI EN LA ENTIDAD.

A continuación, se listan los HITOS definidos para la implementación del SGSI.

Tabla 1. Hitos implementación SGSI

Descripción	Actividad	Entregables
Hito N.º 1	Diagnóstico	• Diagnóstico de Seguridad de la Información. • Propuesta del Alcance del SGSI
Hito N.º 2	Establecimiento y Estructura del SGSI, Definición del Alcance	• Generación parcial de Políticas del SGSI. • Generación de formatos aplicables. • Inventario de activos. • Generación de SoA (documento de aplicabilidad) • Documentación básica inicial del SGSI. • Comunicación y socialización a los usuarios de la entidad.
Hito N.º 3	Gestión de Riesgos	• Matriz de Gestión de Riesgos. • Metodología de la Gestión de Riesgos • Definición del Plan de Tratamiento de Riesgos. • Informe de Gestión de Riesgos. • Comunicación y socialización a los usuarios de la entidad.
Hito N.º 4	Implementación y Operación del SGSI	• Actualización de documentación vigente. • Informe de Medición del SGSI. • Seguimiento del SGSI. • Políticas específicas del SGSI.

Descripción	Actividad	Entregables
Hito N.º 5	Monitorear y Revisar	• Seguimiento de los controles de seguridad de la información. • Manual del SGSI. • Medición, Métricas de procedimientos de seguridad. • Comunicación y socialización a los usuarios de la entidad. • Informe de auditoría interna. • Planes de acción de auditoria del SGSI. • Mejora continua. • Acciones Correctivas y de mejora.
Hito N.º 6	Mantener y Mejorar	• Implementar Mejoras. • Generar acciones correctivas. • Comunicación y socialización a los usuarios de la entidad.
Hito N.º 7	Acompañamiento en la Auditoría Externa (*)	• Preauditoria. • Cierre de hallazgos • Revisión, planes de acción, análisis y seguimiento a los hallazgos del Ente Certificador

DOMINIOS DE CONTROL

La norma ISO 27001:2013 en su anexo A tomado de la norma ISO 27002 para su aplicación se encuentra organizada, de la siguiente manera:

- 14 dominios.
- 10 cláusulas o capítulos.
- 114 controles.
- 35 objetivos de control.

Los lineamientos y buenas prácticas para la implementación de los controles que se definen en la norma ISO 27001:2013 que apliquen a la entidad de acuerdo con los procesos y procedimientos establecidos para cada (proceso o dependencia de ésta).

Según MINTIC, la UMV para finales del año 2017 debería haber tenido una calificación del 60% sobre 100% de acuerdo con la aplicación de los 14 dominios que menciona la norma, revisando los controles de seguridad que se han aplicado en la entidad, se obtuvo una calificación de 6,57% del 60% que se debería tener implementado, de acuerdo con lo establecido por MINTIC, esto evidencia la brecha entre lo que se tiene y lo requerido, sin embargo, la meta es cumplir el 100% de los controles de seguridad, alineados a la implementación del SGSI ver tabla 2 (Dominios de control).

Tabla 2. Dominios de control de la ISO 27001:2013

NOMBRE DOMINIOS DE CONTROL	RESULTADO	CALIFICACIÓN OBJETIVO
Políticas de seguridad de la información	10	60
Organización de la seguridad de la información	3	60
Seguridad de los recursos humanos	7	60
Gestión de activos	6	60
Control de acceso	14	60
Criptografía	0	60
Seguridad física y del entorno	23	60
Seguridad de las operaciones	9	60
Seguridad de las comunicaciones	9	60
Adquisición, desarrollo y mantenimiento de sistemas	0	60
Relación con los proveedores	0	60
Gestión de incidentes de seguridad de la información	0	60

Aspectos de la seguridad de la información de la gestión de la continuidad del negocio	0	60
Cumplimiento	9	60

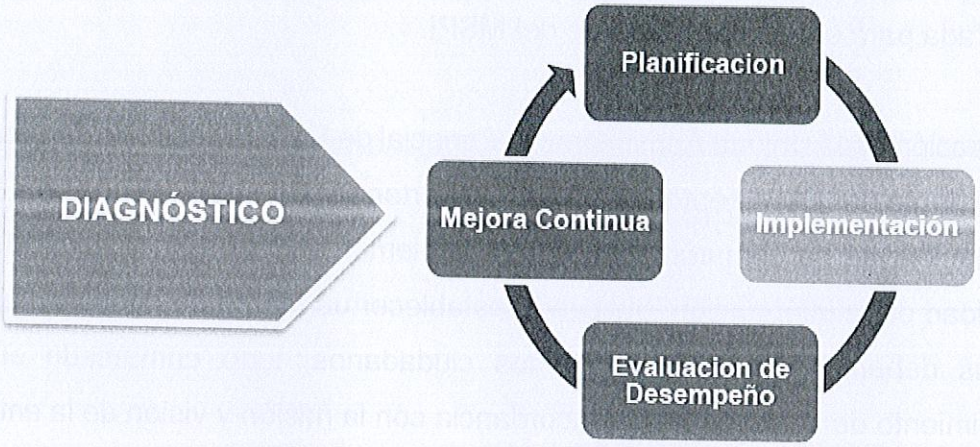
6. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA UEARMV

A continuación, se describen los componentes del modelo de seguridad que se implementarán en la Unidad Administrativa Especial de Rehabilitación Y Mantenimiento Vial (UEARMV) para el Sistema de Gestión de la Seguridad de la Información (SGSI) basado en el del Modelo de Seguridad y Privacidad de la Información (MSPI) definido por MINTIC, el cual a su vez está alineado a la norma ISO27001:2013 y a la metodología de gestión de riesgos del Departamento Administrativo de la Función Pública (DAFP).

Para gestionar la seguridad de la información enfocada a preservar la integridad, disponibilidad y confidencialidad de la información y contribuir con esto al cumplimiento de la misión y los objetivos estratégicos, la UMV debe adoptar un modelo cíclico de operación que comprende en su totalidad cinco (5) fases que le permitan contar con un sistema de gestión sostenible al interior de esta.

Estas fases se muestran en la siguiente ilustración:

Ilustración 1 Fases de la adopción del MSPI



Fuente: Modelo de Seguridad y Privacidad de la Información – MSPI de MinTIC.

De acuerdo con la figura anterior, la fase de diagnóstico ha sido ejecutada en la UMV como parte del dominio de seguridad. En el presente documento se abordarán los elementos requeridos en la fase de **planificación** y parte de la **implementación.**

Dentro de la fase de planificación, la UMV contempla los siguientes elementos:

6.1. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La política general de seguridad de la información debe ser un documento de alto nivel que incluya la voluntad de la alta dirección de la Entidad para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información. Esta política debe contener una declaración general por parte de la administración, donde se especifiquen sus objetivos, alcance y nivel de cumplimiento, y debe ser aprobada y divulgada al interior de la entidad.

A continuación, se presenta el contenido sugerido de la política general de seguridad y privacidad de la información para la UMV, este contenido está basado en la guía elaborada para este fin en el marco del MSPI.

La dirección de la Unidad Administrativa Especial de Rehabilitación y Mantenimiento Vial, en adelante la UMV, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información, buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

La presente Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de la UMV con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

La UMV, para asegurar la dirección estratégica, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.

- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la UMV.
- Garantizar la continuidad del negocio frente a incidentes.

Alcance/Aplicabilidad

- Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros, así como a la ciudadanía en general.

Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento a la política en un 100%.

A continuación, se establecen los principios de seguridad que soportan el SGSI en la UMV:

- La UMV ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios, contratistas o terceros.
- La UMV protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de estos.

- La UMV protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de ésta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- La UMV protegerá su información de las amenazas originadas por parte de sus funcionarios, contratistas y terceros.
- La UMV protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- La UMV controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La UMV implementará el control de acceso a la información, sistemas y recursos de red.
- La UMV garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La UMV garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- La UMV garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos que los puedan afectar.
- La UMV garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

6.2. POLÍTICAS COMPLEMENTARIAS DE SEGURIDAD DE LA INFORMACIÓN

De acuerdo con las recomendaciones del MSPI y la norma ISO27001 en su versión 2013, a continuación, se definen las políticas (o grupos de políticas) de seguridad que la UMV está adoptando dentro de su proceso de implementación del SGSI.

6.2.1. Políticas de gestión de activos

Este grupo de políticas debe contemplar las directrices frente a la identificación, uso, administración y responsabilidad sobre los activos de Información, las políticas relacionadas con gestión de activos deben contemplar como mínimo:

- **Identificación y clasificación de activos de información**: Esta política debe determinar la periodicidad con la cual se va a realizar al interior de la Entidad la identificación y/o actualización del inventario de activos de Información, la política debe determinar el responsable de realizar la actividad, se debe determinar bajo que instrumento se va a realizar la actividad, dicho instrumento debe permitir identificar el propietario del activo de información.

  En el numeral 7.5- "Inventario de activos de información" del presente documento se detalla la Clasificación de activos de información.

- **Etiquetado de la Información:** Esta política debe determinar el mecanismo, responsable y obligatoriedad para el etiquetado o rotulación de Activos (ver numeral 7.5, literal f- "Etiquetado de la información").

- **Devolución de los Activos:** Esta política debe determinar el instrumento y responsable del cumplimiento, mediante el cual se genera obligatoriedad para que los funcionarios, contratistas y/o terceros realicen la entrega de activos físicos y de la información una vez finalizado el empleo o contrato que se tenga con la Entidad.

- **Gestión de medios removibles:** Esta política debe contemplar los usos y permisos que tienen los usuarios y/o funcionarios de la Entidad frente a los medios removibles, entendiendo como medio removible a todos aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de los computadores (USB, discos externos, tarjetas de memoria, CD, DVD, etc.). Esta política debe describir detenidamente los casos en los cuales se autoriza y en cuales no, el uso de medios removibles y los procedimientos que se deben seguir para realizar dichas autorizaciones; adicionalmente, debe describir el responsable de las autorizaciones, y las responsabilidades de quienes reciben la autorización para el uso de dicho medio. El uso de medios removibles en la entidad debe estar alineado a la clasificación de activos establecida en la Entidad.

- **Disposición de los activos:** Esta política debe determinar la obligatoriedad para la construcción y cumplimiento de un procedimiento mediante el cual se realice de forma segura y correcta la eliminación, retiro, traslado o reúso de los activos de la entidad, cuando estos ya no se requieran para la operación. Esta política debe especificar, de ser necesaria, la toma de copias de respaldo y posterior eliminación de la información contenida en los activos, evitando así el acceso no autorizado a la misma, la política debe indicar quién es el responsable de emitir las correspondientes autorizaciones y debe aplicar tanto para medios removibles como activos de procesamiento y/o almacenamiento de información.
- **Dispositivos móviles:** Esta política debe determinar los funcionarios, contratistas o terceros que pueden tener acceso a las redes inalámbricas y quiénes pueden hacer uso de chats corporativos y/o correos electrónicos de la entidad en este tipo de dispositivos, adicionalmente debe describir las responsabilidades que deben tener los funcionarios o contratistas frente al uso de la información almacenada en los dispositivos móviles, así como los controles de seguridad que la entidad utilizará para proteger, mitigar, supervisar y monitorear los riesgos asociados al acceso y divulgación no autorizada de dicha información.

6.2.2. Políticas de control de acceso

Este grupo de políticas debe hacer referencia a todas aquellas directrices mediante las cuales la entidad determina los mecanismos de protección, los límites y procedimientos frente a la administración y responsabilidad, relacionados con los accesos a la información, sin importar si estos accesos sean electrónicos o físicos; las políticas relacionadas con el control de acceso deben contemplar como mínimo:

- **Control de acceso con usuario y contraseña:** Se debe elaborar una política sobre control de acceso a redes, aplicaciones, y/o sistemas de información de la

entidad, mediante la cual se determinen los responsables y los procedimientos formales de autorización de creación, modificación, suspensión o eliminación de usuarios (ID) y contraseñas. La política debe enunciar las responsabilidades que los funcionarios, contratistas o terceros tienen al contar con un usuario o contraseña de la entidad, se debe estipular que los usuarios (ID) y contraseñas son personales e intransferibles y no deben prestarse, ni compartirse. La entidad debe establecer que por cada funcionario, contratista o tercero debe tenerse un usuario y una contraseña para el acceso.

- **Suministro del control de acceso:** Esta política debe determinar los procedimientos formales y directrices que se deben construir para la gestión de asignación, modificación, revisión o revocación de derechos y/o privilegios a cada uno de los usuarios (ID) creados, también debe tenerse en cuenta en esta política los casos especiales como lo son usuarios (ID) con privilegios superiores utilizados para la administración de infraestructura, aplicaciones y sistemas de información de la entidad.
- **Gestión de Contraseñas:** Esta política debe definir los lineamientos mínimos en cuanto a calidad que deben tener las contraseñas para ser utilizadas como mecanismo de autenticación en los accesos a la red, aplicaciones y/o sistemas de información de la entidad. Esta política debe indicar a los funcionarios, contratistas y/o terceros los parámetros mínimos para que una contraseña sea considera como fuerte y debe establecer que los accesos a la red, las aplicaciones y sistemas de información deben requerir un usuario (ID) y una contraseña fuerte para que realice la correspondiente autenticación y acceso a la información de forma segura. De igual forma debe establecer normas de cambio de contraseña, indicando la periodicidad con la que se debe exigir a los usuarios que realicen el cambio de la contraseña, estableciendo reglas mínimas de uso histórico de

contraseñas (que no se asigne la misma contraseña, que se haya usado en los últimos 3 cambios, por ejemplo)

6.2.3. No repudio

La política de seguridad y privacidad debe comprender la capacidad de no repudio con el fin de contar con evidencias respecto a la comunicación a nivel interno y externo, de forma que se obtenga información suficiente sobre la ocurrencia de un evento o comunicación, el momento en el que ocurrió y las partes que intervinieron. Con el fin de evitar que una de las partes niegue haber realizado alguna acción.

La política deberá incluir mínimo los siguientes aspectos:

- **Trazabilidad:** La política debe establecer reglas para que, por medio de la trazabilidad de las acciones, se haga seguimiento a la creación, origen, recepción, entrega de información y otros.
- **Retención:** La política debe indicar el periodo de retención o almacenamiento de las acciones realizadas por los usuarios, el cual deberá ser informado a los funcionarios, contratistas y/o terceros de la Entidad.
- **Auditoría:** La política debe especificar la ejecución de auditorías continuas, como procedimiento para asegurarse que las partes implicadas nieguen haber realizado una acción.
- **Intercambio electrónico de información:** La política de indicar, en los casos que aplique, que los servicios de intercambio electrónico de información son garantía de no repudio.

6.2.4. Privacidad y confidencialidad

Esta política debe contener una descripción de las políticas de tratamiento y protección de datos personales que deben ser aplicados en la UMV, conforme a lo establecido en la Ley 1581 de 2012 y el Decreto 1377 de 2013. La política de privacidad debe contener como mínimo lo siguiente:

a. Ámbito de aplicación.
b. Excepción al ámbito de aplicación de las políticas de tratamiento de datos personales
c. Principios del tratamiento de datos personales.
    - Principio de la Legalidad: El tratamiento de datos personales debe estar sujeto a lo establecido en la Ley 1581 de 2012 y su decreto regulatorio.
    - Principio de finalidad: Indicar la finalidad del tratamiento de datos personales, la cual debe ser informada al titular.
    - Principio de libertad: El tratamiento sólo puede hacerse con el consentimiento previo, expreso e informado del titular de los datos.
    - Principio de veracidad o calidad: La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
    - Principio de transparencia: Garantizar al titular de los datos el derecho a obtener información que le concierna del encargado del tratamiento.
    - Principio de acceso y circulación restringida: El tratamiento sólo podrá hacerse por personas autorizadas por el titular o por personas previstas en la normatividad vigente.
    - Principio de seguridad: La información sujeta a tratamiento, se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento

- Principio de confidencialidad: Todas las personas que participen en el Tratamiento de Datos Personales deben garantizar la reserva de dicha información.

d. Derechos de los titulares

La política debe indicar los derechos de los titulares de los datos, tales como:

- Conocer, actualizar y rectificar sus datos personales.
- Solicitar la prueba de su autorización para el tratamiento de sus datos personales.
- Ser informado respecto del uso que se les da a sus datos personales.
- Revocar la autorización y/o solicitar la supresión de sus datos personales de las bases de datos o archivos cuando el titular lo considere, siempre y cuando no se encuentren vigentes con el Banco los servicios o productos que dieron origen a dicha autorización.
- Presentar quejas ante la entidad administrativa encargada de la protección de los datos personales.

e. Autorización del titular

La política debe indicar cómo obtener autorización del titular para el tratamiento de sus datos personales, así como los casos en los cuales no se requiere autorización del titular.

f. Deberes de los responsables del Tratamiento

La política debe indicar cuáles son los deberes de los responsables y/o encargados del tratamiento de los datos personales.

La política de confidencialidad debe contener un compromiso o acuerdo de confidencialidad, por medio del cual todo funcionario, contratista y/o tercero vinculado a la entidad, adquiera el compromiso, mediante la firma del acuerdo, de no divulgar la información interna y externa que conozca de la Entidad, así como la relacionada con las

funciones que desempeña en la misma. La firma del acuerdo implica que la información conocida por todo funcionario, contratista y/o tercero, en ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente, sin contar con previa autorización.

La política deberá indicar el momento en el que se debe firmar el acuerdo de confidencialidad, así como la vigencia de este.

6.2.5. Política de controles criptográficos y gestión de llaves:

Esta política deberá especificar cómo se asegura la confidencialidad y autenticidad de la información que circula o se genera a través de los diferentes sistemas de información. La política debe establecer los casos en los que se hace necesario hacer uso de controles criptográficos para la protección de la información al igual que para la protección y tiempo de vida de las llaves criptográficas.

6.2.6. Disponibilidad del servicio y de la información

La UMV debe contar con un plan de continuidad del negocio con el fin de asegurar, recuperar o restablecer la disponibilidad de los procesos que soportan el Sistema de Gestión de Seguridad de la Información y procesos misionales de la Entidad, ante el evento de un incidente de seguridad de la información.

La política de disponibilidad debe incluir como mínimo los siguientes aspectos:

- **Niveles de disponibilidad:** Esta política debe velar por el cumplimiento de los niveles de disponibilidad de servicios e información acordados con usuarios, proveedores y/o terceros en función de las necesidades de la Entidad, los acuerdos de nivel de servicios ofrecidos y evaluaciones de riesgos.

- **Planes de recuperación:** La política debe incluir los planes de recuperación que tengan en cuenta las necesidades de disponibilidad del negocio.
- **Interrupciones:** La política debe velar por la gestión de interrupciones de mantenimiento de los servicios que afecten la disponibilidad de este, teniendo en cuenta los acuerdos de niveles de servicios (ANS).
- **Segregación de ambientes:** Esta política debe establecer la separación de ambientes para minimizar los riesgos asociados a la ejecución de cambios en los servicios y nuevos desarrollos, con el fin de asegurar que los cambios que se apliquen en los ambientes de producción han sido verificados y validados con anticipación en entornos de la UMV.
- **Gestión de Cambios:** La política debe incluir gestión de cambios para que los pasos a producción afecten mínimamente la disponibilidad y se realicen bajo condiciones controladas.
- **Copias de respaldo:** Esta política debe establecer las reglas de ejecución de copias de respaldo de la información, los requerimientos de almacenamiento de dichas copias y las reglas para la validación de la efectividad de estas.

6.2.7. Registro y auditoría

Esta política debe velar por el mantenimiento de las evidencias de las actividades y acciones que afectan los activos de información.

Esta política debe contener:

- **Responsabilidad:** Incluir la responsabilidad de la Oficina de Control Interno, acerca de la responsabilidad de llevar a cabo las auditorías periódicas a los sistemas y actividades relacionadas a la gestión de activos de información, así como la responsabilidad de dicha Oficina de informar los resultados de las auditorías.

- **Almacenamiento de registros:** La política debe incluir el almacenamiento de los registros de las copias de seguridad en la base de datos correspondiente y el correcto funcionamiento de estas. Los registros de auditoría deben incluir toda la información registro y monitoreo de eventos de seguridad.
- **Normatividad:** La política de auditoría debe velar porque las mismas sean realizadas acorde a la normatividad y requerimientos legales que le apliquen a la UMV.
- **Garantía cumplimiento:** La política de auditoría debe garantizar la evaluación de los controles, la eficiencia de los sistemas, el cumplimiento de las políticas y procedimientos de la entidad, así como las recomendaciones que puedan surgir a partir de dicha evaluación.
- **Periodicidad:** La política debe determinar la revisión periódica de los niveles de riesgos a los cuales está expuesta la Entidad, lo cual se logra a través de auditorías periódicas alineada a los objetivos estratégicos y gestión de procesos de la Entidad.

6.2.8. Gestión de incidentes de seguridad de la información

La entidad deberá documentar una política general de gestión de eventos, incidentes y vulnerabilidades de seguridad de la información. Esta política debe ir dirigida a todos los usuarios que tienen un acceso autorizado a cualquier sistema de información.

La política debe contemplar para su elaboración los siguientes parámetros:

- Debe estar aprobada por la alta dirección, certificando así el compromiso con el proceso.
- **Visión general:** ¿Qué se debe reportar? ¿A quién debe reportarse?, ¿Qué medios pueden emplearse para hacer el reporte?
- **Definir responsables:** Se deben mencionar de manera muy general quienes serán los responsables de gestionar los eventos.

- **Actividades:** Explicar de manera general en que consiste el proceso de gestión de incidentes desde el reporte hasta la resolución.
- **Documentación:** Se debe hacer referencia sobre la documentación del esquema de gestión y los procedimientos.
- **Descripción del equipo que manejará los incidentes:** Se debe indicar como está compuesta la estructura general para la gestión de incidentes y vulnerabilidades de seguridad.
- **Aspectos legales:** Deben citarse los aspectos legales que se deben tener en cuenta o los cuales debe darse cumplimiento.
- **Bitácora de Incidentes**: Se debe contar con formato donde reposen todas las incidencias reportadas, y así poder sacar un récord de cada cuanto ocurren, cuáles y de qué tipo de incidentes.

6.2.9. Capacitación y sensibilización en seguridad de la información

Esta política se deberá centrar en la formación de los funcionarios de la entidad en temas relacionados con la seguridad de la información, cuya finalidad es disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano.

Dicha política debe contener los siguientes aspectos:

- El compromiso de la alta dirección en destinar los recursos suficientes para desarrollar los programas de capacitación y sensibilización que se determinen como requeridos.
- ¿Quiénes deberán ser entrenados? ¿Quiénes deberán ser sensibilizados?
- La obligación de los usuarios a asistir a los eventos o cursos de capacitación.
- Revisión periódica de resultados de capacitaciones para mejoramiento de los procesos.

- Definir los roles y responsabilidades de quienes diseñarán los programas, quienes los comunicarán.
- Documentación sobre planes de estudio y desarrollo de los programas.
- Compromisos y obligaciones por parte del personal capacitado.

6.2.10. Políticas de Seguridad Física y del entorno

- **Perímetros de Seguridad:** Esta política debe definir los perímetros físicos de seguridad donde se encuentra información crítica, sensible o se realice almacenamiento y/o procesamiento de información a los cuales los funcionarios, contratistas o terceros, tienen acceso y a cuáles no, la política debe definir los responsables de autorizar ingresos a las áreas delimitadas como de acceso restringido.
- **Política de Escritorio Limpio:** Esta política debe establecer las reglas para el manejo de documentos y dispositivos removibles que utilizan los funcionarios o contratistas en los puestos de trabajo de la UMV, con el finde evitar accesos no autorizados, perdida o daño de información o de activos de información. De igual forma, debe establecer reglas de bloqueo de pantalla durante la ausencia de los funcionarios de su puesto de trabajo y reglas para mantener el escritorio de las estaciones de trabajo libre de archivos.

6.3. PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

Los procedimientos de seguridad de la información deben indicar cómo se realizará la implementación de las políticas de seguridad de la información que se establezcan. A continuación, se listan los procedimientos aplicables a la UMV y recomendados por el MSPI, por cada dominio de la norma ISO27001:2013, definidos en el Anexo A de esa norma.

6.3.1. Seguridad del recurso humano

En este dominio relacionado con el personal que labora para la UMV (funcionarios y contratistas), se podrían definir los siguientes procedimientos:

a. **Procedimiento de capacitación y sensibilización del personal:** Indica la metodología empleada por la entidad para realizar la capacitación y sensibilización del personal en temas de seguridad de la información teniendo en cuenta los diferentes roles y responsabilidades, la periodicidad de dichas capacitaciones y sensibilizaciones etc.
b. **Procedimiento de ingreso y desvinculación del personal:** Este procedimiento debe indicar la manera como la entidad gestiona de manera segura el ingreso y desvinculación, incluyendo temas como verificación de antecedentes, firma de acuerdos de confidencialidad, recepción de entregables requeridos para generar paz y salvos entre otras características.

Este procedimiento va de la mano con el área de gestión de recursos humanos y contratación puede generarse con su colaboración.

6.3.2. Gestión de activos

En este dominio relacionado con la identificación y clasificación de activos de acuerdo con su criticidad y nivel de confidencialidad se pueden definir los siguientes procedimientos:

a. **Procedimiento de identificación y clasificación de activos:** En este procedimiento se debe indicar la manera en que los activos de información son identificados e inventariados por la entidad, así como también se debe especificar como son

clasificados de acuerdo con su nivel de confidencialidad o criticidad, como se asignan y se devuelven los activos una vez se termina la relación laboral con la entidad.

b. **Procedimiento de disposición de activos:** Este procedimiento debe explicar cómo se debe realizar una correcta disposición de los activos cuando ya no se requieran y su transferencia hacia otros lugares de manera segura.

6.3.3. Control de acceso

En este dominio relacionado con el acceso a la información y a las instalaciones de procesamiento de la información, se pueden generar los siguientes procedimientos.

a. **Procedimiento para ingreso seguro a los sistemas de información:** En este procedimiento la entidad debe indicar como gestiona el acceso a sus sistemas de información de manera segura, empleando métodos preventivos contra ataques de fuerza bruta, validando los datos completos para ingreso a los sistemas y/o empleando métodos para cifrar la información de acceso a través de la red entre otros.

b. **Procedimiento de gestión de usuarios y contraseñas:** En este procedimiento, la entidad deberá indicar como realiza la creación de usuarios y la asignación de contraseñas (las cuales deberán tener un nivel de seguridad aceptable, con base a una política de contraseñas seguras definida previamente), prohibiendo su reutilización posterior, permitiendo a los usuarios cambiarla regularmente, llevando un registro de estos. Este procedimiento debe aplicar a todos los sistemas de información, también se debe tener en cuenta el rol que cada usuario requiera en los determinados sistemas, para brindar el acceso necesario.

6.3.4. Criptografía

En este dominio está relacionado con el buen uso de la criptografía para garantizar la disponibilidad, integridad y confidencialidad de la información, así como también el correcto uso de las llaves criptográficas durante todo su ciclo de vida (creación, uso, recuperación, distribución, retiro y destrucción. Se pueden generar los siguientes procedimientos:

a. **Procedimiento de controles criptográficos:** En este procedimiento deberá especificarse como se utilizará la criptografía dentro de los sistemas de información de la organización para garantizar su integridad, disponibilidad y confidencialidad.

   Debe especificarse la complejidad de los controles criptográficos a emplear, dependiendo de la criticidad de la información que circulará a través de la red o se encontrará alojada en un sistema determinado.

b. **Procedimiento de gestión de llaves criptográficas:** Este procedimiento deberá describir el ciclo de vida de las llaves criptográficas dentro de la entidad (si aplica), desde que se crean hasta que se distribuyen a cada usuario o aplicación de manera segura. Deben mencionarse aspectos como la creación de las llaves, obtención de certificados, almacenamiento seguro de las llaves, actualización o cambio, revocación y recuperación de llaves.

6.3.5. Seguridad física y del entorno

Este dominio está relacionado con la prevención del acceso a áreas no autorizadas, el daño a la infraestructura, las instalaciones o de la información. Se pueden generar los siguientes procedimientos, en acuerdo con el área administrativa de la entidad.

a. **Procedimiento de control de acceso físico:** En este procedimiento se debe describir cómo se ejecutan los diferentes pasos para garantizar el control de acceso seguro a las instalaciones al personal autorizado. Este procedimiento puede incluir registros de fecha y hora de ingreso, seguimiento de los libros o plataforma de registro. Se debe contemplar la solicitud de permisos a áreas restringidas, quien los otorga y que debe hacerse para poder tener acceso a éstas.

b. **Procedimiento de protección de activos:** Este procedimiento debe contener los pasos con los cuales los equipos son protegidos por la entidad. Se recomienda que este procedimiento indique como se determina la ubicación de los equipos que procesan información confidencial, como se aseguran dichas instalaciones, los controles que se aplican para minimizar riesgos de desastres naturales, amenazas físicas, daños por polvo, agua, interferencias, descargas eléctricas etc.

c. **Procedimiento de retiro de activos:** En este procedimiento debe especificarse como los activos son retirados de la entidad con previa autorización. Se debe indicar el flujo de las solicitudes, autorizaciones y el control que tendrá el activo fuera de la entidad, así como también los controles de seguridad que deberá incluir el equipo cuando esté por fuera (controles criptográficos, cifrado de discos etc.)

d. **Procedimiento de mantenimiento de equipos:** Este procedimiento debe especificar como se ejecutan mantenimientos preventivos o correctivos dentro de la entidad, indicando los intervalos en que estos deberán realizarse, con base a las sugerencias de los proveedores o en el caso de que existan seguros atados a los equipos y los mantenimientos sean requisitos. Se debe especificar el modo en que los

mantenimientos se llevarán a cabo y el personal que deberá ejecutarlo, llevando el registro apropiado.

6.3.6. Seguridad de las operaciones

Este dominio busca asegurar las operaciones correctas dentro de las instalaciones de procesamiento de información:

a. **Procedimiento de gestión de cambios:** Este procedimiento deberá indicar como se realiza el control de cambios en los servicios tecnológicos y los sistemas de información de manera segura. Se deben especificar aspectos como la identificación y registro de cambios significativos, planificación y pruebas previas de los cambios a realizar, valoración de impactos, tiempos de no disponibilidad del servicio, comunicación a las áreas pertinentes, procedimientos de rollback (reversa) entre otros.
b. **Procedimiento de gestión de capacidad:** Se debe especificar como la organización realiza la gestión de la capacidad para los servicios tecnológicos y sistemas de información críticos, en especial si los recursos requeridos son escasos, demorados en su adquisición o contratación, o son costosos. La entidad puede realizar acciones como la eliminación de datos obsoletos, cierre de aplicaciones, ambientes y sistemas en desuso, restricción de ancho de banda etc.
c. **Procedimiento de separación de ambientes:** Con el fin de evitar problemas operacionales que pueden desencadenar en incidentes críticos, es necesario desarrollar un procedimiento de separación de ambientes que permita realizar una transición de los diferentes sistemas desde el ambiente de desarrollo hacia el de producción. Dentro de los aspectos más importantes a considerar se encuentran la implementación de un ambiente de pruebas para las aplicaciones, definición de los

requerimientos para la transición entre ambientes, la compatibilidad de los desarrollos con diferentes sistemas entre otros.

d. **Procedimiento de protección contra códigos maliciosos:** La entidad debe indicar por medio de este procedimiento cómo realiza la protección contra códigos maliciosos teniendo en cuenta, qué controles utiliza (hardware o software), cómo se instalan y se actualizan las plataformas de detección, la definición de procedimientos o instructivos específicos sobre el modo de operación de la plataforma, reporte y recuperación de ataques contra software malicioso.

6.3.7. Seguridad de las comunicaciones

Este dominio busca el aseguramiento y la protección de la información a través de los diferentes servicios de comunicaciones de la organización.

a. **Procedimiento de aseguramiento de servicios en la red:** Este procedimiento explica la manera en que la entidad protege la información en las redes, indicando los controles de seguridad (cómo se cifran los datos a través de la red por ejemplo) que se aplican para acceder a la red cableada e inalámbrica, con miras a proteger la privacidad de la información que circula a través de estos medios, también se debe incluir el uso de registros (logs) que permitan realizar seguimiento a acciones sospechosas.
b. **Procedimiento de transferencia de información:** En este procedimiento la entidad deberá indicar cómo realiza la transmisión o transferencia de la información de manera segura dentro de la entidad o con entidades externas, donde se apliquen métodos para proteger la información de interceptación, copiado, modificación y/o destrucción.

Se deben tener en cuenta acuerdos de confidencialidad y no divulgación, que deberán ser actualizados y revisados constantemente, donde se incluyan condiciones sobre la información que se va a proteger, la duración del acuerdo, responsabilidades, propietarios de la información, acciones en caso de incumplimiento, entre otros.

6.3.8. Relaciones con los proveedores

Este dominio está relacionado con la protección de los activos de la organización a los cuales los proveedores o terceros tienen acceso.

a. **Procedimiento para el tratamiento de la seguridad en los acuerdos con los proveedores:** Este procedimiento debe indicar cómo la entidad establece, acuerda, aprueba y divulga los requerimientos y obligaciones relacionados con la seguridad de la información. Dichos acuerdos deben tener características como: Aspectos legales, descripción de la información a la que ambas partes tendrán acceso, reglas de uso aceptable e inaceptable de la información, requerimientos en gestión de incidentes, resolución de conflictos, informes periódicos por parte del proveedor, auditorías al servicio y gestión de cambios.

6.3.9. Adquisición, desarrollo y mantenimiento de sistemas de información

a. **Procedimiento adquisición, desarrollo y mantenimiento de software:** Este procedimiento deberá describir cómo se realiza la gestión de la seguridad de la información en los sistemas desarrollados internamente (inhouse) o adquiridos a un tercero, verificando que cada uno de ellos preserve la confidencialidad, integridad y disponibilidad de la información de la entidad. Dicha gestión y control también debe ser especificada para los sistemas ya existentes que son actualizados o modificados en la entidad.

b. **Procedimiento de control software:** En este procedimiento la entidad deberá indicar como realiza el control de instalación de software, es decir, como limita el uso o instalación de software no autorizado dentro de la entidad, quienes están autorizados para realizar la instalación de software, como se realizaría la gestión de las solicitudes de instalación de software para los usuarios, cómo se realiza el inventario de software dentro de la entidad entre otros aspectos.

6.3.10. Gestión de incidentes de seguridad de la información

a. **Procedimiento de gestión de incidentes de seguridad de la información:** Este procedimiento debe indicar cómo responde la entidad en caso de presentarse algún incidente que afecte alguno de las 3 características fundamentales de la información: Disponibilidad, Integridad o Confidencialidad. Deben especificarse los roles, las responsabilidades y acciones requeridas para identificar, contener, documentar, recolectar evidencias y mejorar la respuesta ante un incidente de seguridad de la información, así mismo, deberá indicar en qué casos sería necesario pasar a la activación de los planes de continuidad del negocio, dependiendo de la criticidad de la información.

6.3.11. Aspectos de seguridad de la información de la gestión de continuidad de negocio

a. **Procedimiento de gestión de la continuidad de negocio:** En este procedimiento la entidad debe indicar la manera en que la entidad garantizará la continuidad para todos sus procesos (de ser posible o por lo menos los misionales), identificando los procesos críticos que tendrán mayor prioridad en las fases de recuperación ante algún desastre o incidente crítico.

El procedimiento debe indicar los pasos a seguir cuando existan estas situaciones adversas, quienes deberán actuar (incluyendo las terceras partes o proveedores), los tiempos a cumplir, los procesos alternos o que permitan continuar con el proceso de manera temporal.

6.4. ROLES Y RESPONSABILIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La UMV definió mediante un acto administrativo (resolución, circular, decreto, entre otros), los roles y las responsabilidades de seguridad de la información en los diferentes niveles (Directivo, de procesos y Operativos) que permitan la correcta toma de decisiones y una adecuada gestión que permita el cumplimiento de los objetivos de seguridad de la Entidad.

De acuerdo con el modelo de seguridad y privacidad y la norma ISO 27001, se deben definir los siguientes roles y responsabilidades para la seguridad de la información.

6.4.1. Responsable de Seguridad de la Información para la entidad

La UMV debe designar un responsable de seguridad de la información denominado Oficial de Seguridad, el cual debe liderar el proyecto de implementación del SGSI.

Las responsabilidades del líder del proyecto deben ser:

- Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades propias del proyecto, de manera que cumpla o exceda las necesidades y expectativas de los interesados en el mismo.

- Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la entidad.
- Generar el cronograma de la implementación del Modelo de Seguridad y privacidad de la información.
- Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma que se defina para el proyecto.
- Gestionar el equipo de proyecto de la entidad, definiendo roles, responsabilidades, entregables y tiempos.
- Coordinar las actividades diarias del equipo y proporcionar apoyo administrativo
- Encarrilar el proyecto hacia el cumplimiento de la implementación del Modelo de Seguridad y privacidad de la Información para la entidad.
- Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos del proyecto para darle solución oportuna y escalar al Comité de seguridad en caso de ser necesario.
- Monitorear el estado del proyecto en términos de calidad de los productos, tiempo y los costos.
- Trabajar de manera integrada con el grupo o áreas asignadas.
- Asegurar la calidad de los entregables y del proyecto en su totalidad.
- Velar por el mantenimiento de la documentación del proyecto, su custodia y protección.
- Contribuir al enriquecimiento del esquema de gestión del conocimiento sobre el proyecto en cuanto a la documentación de las lecciones aprendidas.
- Liderar la programación de reuniones de seguimiento y velar por la actualización de los indicadores de gestión del proyecto.

6.4.2. Equipo del Proyecto

Con el objetivo de buscar asegurar que el proyecto de implementación del modelo de seguridad y privacidad se realice de forma transversal en la UMV, se propone que el equipo del proyecto esté formado por:

- Encargado(a) de seguridad de la información.
- Un representante del área de tecnología.
- Un representante de la oficina de control interno.
- Un representante de la oficina asesora de planeación.
- Un representante de la oficina asesora jurídica.
- Encargado(a) del sistema de Gestión de Calidad.
- Funcionarios, proveedores, y ciudadanos

Entre las responsabilidades del equipo del proyecto deben estar:

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

6.4.3. Comité de seguridad de la información

Se creará mediante acto administrativo, el comité de seguridad de la información, el cual debe estar conformado por:

i) Promover la difusión y sensibilización de la seguridad de la información dentro de la Entidad.

j) Poner en conocimiento de la entidad, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma.

k) Las demás funciones inherentes a la naturaleza del Comité.

6.5. INVENTARIO DE ACTIVOS DE INFORMACIÓN

La UMV desarrollará una metodología de gestión de activos que le permita generar un inventario de activos de información exacto, actualizado y consistente, que a su vez permita definir la criticidad de los activos de información, sus propietarios, custodios y usuarios.

La clasificación de activos de información se debe realizar acorde con el alcance definido para la implementación del SGSI (es decir a los procesos en los que se implementará seguridad de la información) la gestión de activos debe estar alineada con el Dominio 8 Gestión de Activos del anexo A de la norma ISO 27001:2013, y la guía de controles del modelo de seguridad y privacidad de la información, para garantizar el cumplimiento de los puntos descritos a continuación:

a. **Inventario de activos:** Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.

b. **Propiedad de los activos:** Los activos mantenidos en el inventario deben tener un propietario.

c. **Uso aceptable de los activos:** Se debe identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.

- El Director de la Entidad.
- Jefe de la Oficina Asesora de Planeación
- Jefe de la Oficina Asesora Jurídica
- Responsable de Seguridad de la Información de la Entidad.
- La Secretaria General
- Delegado de Gestión Documental
- Delegado del Área de Tecnología
- Jefe de la Oficina de Control Interno

Las funciones del comité de seguridad deben ser:

a) Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la UMV.
b) Revisar los diagnósticos del estado de la seguridad de la información en la UMV.
c) Acompañar e impulsar el desarrollo de proyectos de seguridad.
d) Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la UMV.
e) Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.
f) Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
g) Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
h) Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.

d. **Devolución de activos:** Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

e. **Clasificación de la información**: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

La clasificación de activos de información tiene como objetivo asegurar que la información recibe los niveles de protección adecuados, ya que con base en su valor y de acuerdo con otras características particulares requiere un tipo de manejo especial.

De acuerdo con el MSPI, la UMV puede realizar la clasificación de los activos de acuerdo con los siguientes criterios:

- **Clasificación de acuerdo con la confidencialidad**

La confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados, se sugieren tres (3) niveles alineados con los tipos de información declarados en la ley 1712 del 2014:

Tabla 3 Clasificación de los activos de información - Confidencialidad

Tipo	Descripción
INFORMACIÓN PÚBLICA RESERVADA	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
INFORMACIÓN PÚBLICA CLASIFICADA	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de esta. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.

Tipo	Descripción
INFORMACIÓN PÚBLICA	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA.

Fuente. MSPI

- **Clasificación de acuerdo con la integridad**

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

Tabla 4 Clasificación de los activos de información - Integridad

Nivel	Descripción
A (ALTA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
M (MEDIA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.
B (BAJA)	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.

Fuente. MSPI

- **Clasificación de acuerdo con la disponibilidad**

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

El MSPI recomienda el siguiente esquema de clasificación de tres (3) niveles:

Tabla 5 Clasificación de los activos de información - Disponibilidad

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

Fuente. MSPI

Para cada activo de información se debe definir la clasificación de acuerdo con estos tres criterios, lo que determinará en su conjunto el nivel de clasificación del activo, de acuerdo con las siguientes tablas:

Tabla 6 Criterios de clasificación de activos de información

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PÚBLICA RESERVADA	A (ALTA)	1 (ALTA)

INFORMACIÓN PÚBLICA CLASIFICADA	M (MEDIA)	2 (MEDIA)
INFORMACIÓN PÚBLICA	B (BAJA)	3 (BAJA)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Fuente. MSPI

Tabla 7 Niveles de clasificación de activos de información

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

Fuente. MSPI.

De acuerdo con el nivel de clasificación de cada activo se deberá priorizar la gestión de riesgos de este, la gestión de riesgos para los activos de información será revisada en el artefacto 03-TO-BE-SG-ART-Pro-MSPR-V2.

f. **Etiquetado de la información:** Se debería 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 entidad.

Para realizar el etiquetado de los Activos de Información en esta guía se proponen una seria de ítems que podrían ser tenidos en cuenta para realizar este proceso y se deberían tener en cuenta las siguientes pautas generales:

- Se etiquetarán todos los Activos de Información que estén clasificados según el esquema clasificación en Confidencialidad, Integridad y disponibilidad.
- Se etiquetará el nivel de clasificación con relación a Confidencialidad, Integridad y Disponibilidad.
- Si un Activo de Información en formato impreso no se encuentra etiquetado debe ser tratado en todos sus niveles (Confidencialidad, Integridad y Disponibilidad) como NO CLASIFICADA.
- Cada Activo de Información debe ser etiquetado teniendo en cuenta el esquema de clasificación, y en el campo correspondiente diligenciar la clasificación de la siguiente forma: {Clasif.Confidencialidad} - {Clasif.Integridad} - {Clasif.Disponibilidad}
- Para los activos clasificados en confidencialidad como INFORMACIÓN PÚBLICA RESERVADA se podría utilizar la etiqueta IPR, INFORMACIÓN PÚBLICA CLASIFICADA IPC e INFORMACION PUBLICA, IPB.
- Para los activos clasificados en integridad como ALTA se utilizará la etiqueta A, MEDIA, M y BAJA, B.
- Para los activos clasificados en disponibilidad como ALTA se utilizará la etiqueta 1, MEDIA, 2 y BAJA, 3.

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

g. **Manejo de activos:** Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.

La identificación del inventario de activos de información permite clasificar los activos a los que se les debe brindar mayor protección, pues identifica claramente sus características y rol al interior de un proceso.

Las actividades que debe llevar a cabo la UMV para obtener un inventario de activos de información son: Definición, Revisión, Actualización y Publicación, las cuales se deben reflejar documentalmente en la Matriz de Inventario y Clasificación de Activos de Información. A continuación, se detalla cada una de estas actividades.

6.5.1. Definición del inventario de activos de información

Consiste en determinar qué activos de información van a hacer parte del inventario, para esta tarea debe existir un equipo que realice la gestión de activos de información al interior de la entidad y por medio del líder del cada proceso (o quien haga sus veces… Líder requerido en gestión de calidad) ayude en realización de la actividad.

En segunda instancia los líderes de procesos o quien haga sus veces deben, solicitar la revisión de la definición de los activos por parte del propietario del activo de información designado, custodio y usuario de este, para que validen si son las partes interesadas o la parte de la entidad adecuadas para tener este rol.

Es recomendable que la definición del inventario se lleve a cabo por lo menos una vez al año. A continuación, se describe la información que se debe obtener para cada activo de información:

Información básica

a) La información básica hace referencia a aquellas características del activo y para realizar la etapa de definición podría incluir como mínimo la siguiente información.

b) Identificador: Número consecutivo único que identifica al activo en el inventario.

c) Proceso: Nombre del proceso al que pertenece el activo.

d) Nombre Activo: Nombre de identificación del activo dentro del proceso al que pertenece.

e) Descripción/Observaciones: Es un espacio para describir el activo de manera que sea claramente identificable por todos los miembros del proceso.

f) Tipo: Define el tipo al cual pertenece el activo. Para este campo se utilizan los siguientes valores:

- Información: Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.
- Software: Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.
- Recurso humano: Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información.
- Servicio: Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.
- Hardware: Equipos de cómputo y de comunicaciones que por su criticidad son considerados activos de información, no sólo activos fijos.

- Otros: activos de información que no corresponden a ninguno de los tipos descritos anteriormente, pero deben ser valorados para conocer su criticidad al interior del proceso.

g) Ubicación: Describe la ubicación tanto física como electrónica del activo de información.

h) Clasificación: Hace referencia a la protección de información de acuerdo con los criterios de Confidencialidad, Integridad y Disponibilidad definidos para cada activo de información, Ver numeral 7.5, literal e, para detalle de clasificación de activos de información.

i) Justificación: Para cada valoración, describe el impacto que causaría la pérdida de la propiedad (Confidencialidad, Integridad y Disponibilidad), o el argumento del porque se asignó dicha valoración.

j) Criticidad: Es un cálculo automático que determina el valor general del activo, de acuerdo con la clasificación de la Información. Ver numeral 7.5, literal e, para detalle de clasificación de activos de información.

Propiedad

a) Propietario: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos

b) asociados con el proceso se clasifican adecuadamente. Deben definir y revisar periódicamente las restricciones y clasificaciones del acceso.

c) Custodio: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de hacer efectivos las restricciones y clasificaciones de acceso definidos por el propietario. (Para sistemas de información o información consignada o respaldada, generalmente es TI o para información física, los

custodios pueden ser los funcionarios o el proceso de archivo o correspondencia, el custodio generalmente se define donde reposa el activo original).

Acceso

a. Usuarios: Son quienes generan, obtienen, transforman, conservan, eliminan o utilizan la información, en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información.

Gestión

a) Fecha ingreso del Activo: Fecha de ingreso del activo de información en el inventario

b) Fecha salida del Activo: Fecha de exclusión del activo de información del inventario.

6.5.2. Revisión del inventario de activos de información

La actividad de revisión se refiere a la verificación que se lleva a cabo para determinar si un activo de información continua o no siendo parte del inventario, o si los valores de evaluación asignados en el inventario y clasificación de activos de Información deben ser modificados.

En general, el inventario de activos puede ser revisado o validado en cualquier momento en que el líder del proceso (o quien haga sus veces) así lo solicite, o si el equipo de gestión de activos lo solicita a algún líder de proceso o el oficial de seguridad de la información si así lo requiere.

Las razones por las cuales debería realizarse una revisión o validación son:

a) Actualizaciones al proceso al que pertenece el activo.

b) Adición de actividades al proceso.

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

d) Inclusión de un nuevo activo.

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

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

g) Cambios físicos de la ubicación de activos de información.

6.5.3. Actualización del inventario de activos de información

Una vez se ha definido qué cambios se realizarían en el inventario, desde cada proceso, se procede a actualizar el inventario de activos de información.

6.5.4. Publicación del inventario de activos de información

El inventario de activos de información debe ser un documento clasificado como "***Confidencial"***, y no debe tener características que lo permitan modificar por los usuarios autorizados. Sólo debe tener acceso de modificación a este documento el líder del proceso con previa autorización del oficial de seguridad de la información o quien hagas sus veces.

6.6. PLAN DE DIAGNÓSTICO DE TRANSICIÓN DE IPV4 A IPV6.

De acuerdo con los lineamientos del MSPI, la UMV inicio un proceso de adopción del protocolo IPv6, para este proceso, y entendiendo que quizá las entidades estatales no cuenten con infraestructura tecnológica que soporte este protocolo, el Ministerio de las Tecnologías de Información y Comunicaciones plantea varias fases para el proceso de transición de IPv4 a IPv6.

La primera de estas fases es la **planeación de la transición**, la cual pretende realizar un diagnóstico del estado de preparación de la entidad para implementar el protocolo IPv6, generando luego un plan detallado que incluye la estrategia de transición. De acuerdo con la guía del MSPI, en esta fase la UMV debe realizar las siguientes actividades:

- Elaborar y mantener el inventario de hardware y software actual, identificando claramente cuáles equipos y servicios soportan IPv6, cuales requieren actualizarse y cuáles no lo soportan.
- Identificar la topología actual de la red y su funcionamiento y establecer el nuevo diseño de red sobre IPv6.
- Validar el estado actual de los sistemas de información, los sistemas de comunicaciones, los sistemas de almacenamiento y evaluar la interacción entre ellos cuando se adopte el protocolo IPv6.
- Establecer el protocolo de pruebas para la validación de aplicativos, equipos de comunicaciones, equipos de cómputo, plan de seguridad y coexistencia de los protocolos IPv4 e IPv6 en la entidad, a este respecto se debe planear la ejecución y configuración de las pruebas piloto IPv6, analizando el comportamiento de cada dispositivo de la red de comunicaciones, agregando carga de tráfico, servicios y usuarios finales, teniendo en cuenta que las pruebas realizadas deben estar sujetas a las mejores prácticas y metodologías de transición a IPv6 con la técnica de Doble Pila o *Dual Stack.*
- Planear la migración de los siguientes servicios tecnológicos: Servicio de Resolución de Nombres (DNS), Servicio de Asignación Dinámica de Direcciones IP (DHCP), Directorio Activo, Servicios WEB, Servicios geográficos. Realizando la validación del soporte de IPv6 para el Servicio de Correo Electrónico en la nube, el Servicio de telefonía IP, servicios de hosting físico y virtual; así mismo revisar los procedimientos

de implementación de estos servicios y las aplicaciones identificadas en esta fase, con base en los estándares de la RFC de IPv6.

- Identificar la configuración y los esquemas de seguridad de la red de comunicaciones y sistemas de información.
- Generar el plan detallado del proceso de transición de protocolo IPv4 a IPv6, teniendo en cuenta la recomendación de utilizar la técnica de Doble Pila, la cual consiste en mantener los dos protocolos en operación, habilitando el protocolo IPv6 en aquellos equipos que lo soporten permitiendo que se realice la interacción entre los servicios y dispositivos utilizando el protocolo soportado por ambos.
- Establecer los acuerdos de confidencialidad que sean necesarios sobre el tratamiento de la información ante terceros al momento de ejecutar el plan de transición.
- Evaluar opciones de capacitación de los funcionarios del área de TI de conformidad con los planes de capacitación establecidos para el protocolo IPv6 e iniciar un proceso de sensibilización a las personas de toda la organización a fin de dar a conocer el nivel de impacto de la adopción del nuevo protocolo.
- Se recomienda revisar las políticas de enrutamiento para IPv6 entre los segmentos de red internos, de tal manera que el tráfico IPv6 generado internamente este plenamente controlado a través de zonas desmilitarizadas desde el *firewall* respectivo de cada entidad.

Una vez realizadas estas actividades, se deben obtener los siguientes entregables.

- Plan de trabajo para la adopción de IPv6 en toda la organización.
- Plan de diagnóstico que debe contener los siguientes componentes: Inventario de TI (Hardware y software) de la Entidad diagnosticada, Informe de la Infraestructura de red de comunicaciones, recomendaciones para adquisición de elementos de comunicaciones, de cómputo y almacenamiento con el cumplimiento de IPv6, plan

de direccionamiento en IPv6, plan de manejo de excepciones, definiendo las acciones necesarias en cada caso particular con aquellos elementos de hardware y software (aplicaciones y servicios) que sean incompatibles con IPv6, Informe de preparación (*Readiness*) de los sistemas de comunicaciones, bases de datos y aplicaciones.

- Documento que define los lineamientos al implementar la seguridad en IPv6 en concordancia con la política de seguridad de las entidades.
- Plan de capacitación en IPv6 a los funcionarios de las Áreas de TI de la Entidad y el plan de sensibilización al total de funcionarios de la Entidad.

En general, para iniciar el proceso de adopción del protocolo IPv6, se recomienda realizar un inventario de los activos de información, revisar su actual infraestructura de computación y de comunicaciones, validar todos los componentes de hardware y software de que se disponga, revisar los servicios que se prestan, los sistemas de información, revisión de estándares y políticas para conocer el impacto de adopción de la nueva versión del protocolo IP, a fin de facilitar las labores de planeación e implementación de IPv4 a IPv6, garantizando que las operaciones continúen funcionando normalmente dentro de las entidades del estado.

Luego de finalizada la fase de diagnóstico, se debe abordar la **fase de implementación del protocolo IPv6**, finalizando el proceso de transición con la **fase de pruebas de funcionalidad IPv6.**

6.7. INDICADORES DE GESTIÓN DE SEGURIDAD PARA LA UMV.

Los siguientes son los indicadores que van alineados por IT4+ en el documento "Guía de indicadores de gestión para la seguridad de la información

5482_G9_Indicadores_Gestion_Seguridad" para la gestión de seguridad y que desde el área de seguridad de la información propone como referencia para iniciar la evaluación de la implementación del MSPI.

INDICADOR INDSG01 - ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN.			
IDENTIFICADOR	INDSG01		
DEFINICIÓN			
El indicador permite determinar y hacer seguimiento, al compromiso de la dirección, en cuanto a seguridad de la información, en lo relacionado con la asignación de personas y responsabilidades relacionadas a la seguridad de la información al interior de la entidad			
OBJETIVO			
Hacer un seguimiento a la asignación de recursos y responsabilidades en gestión de seguridad de la información, por parte de la alta dirección.			
TIPO DE INDICADOR			
Indicador de Gestión			
DESCRIPCIÓN DE VARIABLES		**FÓRMULA** (VSG01/VSG02) *100	**FUENTE DE INFORMACIÓN**
VSG01: Número de personas con su respectivo rol definido según el modelo de operación.		(VSG01/VSG02) *100	Capítulo 2 de la guía del modelo de operación del marco de seguridad y privacidad de la información
VSG02: Número de personas con su respectivo rol definido con un año de asignación			Documento de asignación de personal.
METAS			
SATISFACTORIA	80- 90%	**SOBRESALIENTE**	100%

INDICADOR INDSG02 - TRATAMIENTOS DE EVENTOS RELACIONADOS EN MARCO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
IDENTIFICADOR	INDSG02
DEFINICIÓN	

INDICADOR INDSG02 - TRATAMIENTOS DE EVENTOS RELACIONADOS EN MARCO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		
El indicador permite determinar la eficiencia en el tratamiento de eventos relacionados a la seguridad de la información. Los eventos serán reportados por los usuarios o determinadas en las auditorías planeadas para el sistema.		
OBJETIVO		
El objetivo del indicador es mostrar la gestión y evolución del modelo de seguridad y privacidad de la información al interior de una entidad		
TIPO DE INDICADOR		
Indicador de Gestión		
DESCRIPCIÓN DE VARIABLES	**FÓRMULA**	**FUENTE DE INFORMACIÓN**
VSG03: Número de anomalías cerradas.	(VSI03/VSI04) *100	Auditorías internas, herramientas de monitoreo
VSG04: Número total de anomalías encontradas.		Auditorías internas, herramientas de monitoreo
METAS		
SATISFACTORIA 80- 90%	**SOBRESALIENTE** 100%	

INDICADOR INDSG03 – CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA ENTIDAD		
IDENTIFICADOR	INDSG03	
DEFINICIÓN		
Cumplimiento de políticas de seguridad de la información en la entidad		
OBJETIVO		
Busca identificar el nivel de estructuración de los procesos de la entidad orientados a la seguridad de la información.		
TIPO INDICADOR		
Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES	**FÓRMULA** = 1 (SÍ se evidencia) = 0 (NO se evidencia)	**FUENTE DE INFORMACIÓN**
VSG05: ¿La entidad ha definido una política general de seguridad de la información?	VSI0X = 1 (SÍ se	Modelo de Operación / Usuarios UMV

VSG06: ¿La entidad ha definido una organización interna en términos de personas y responsabilidades con el fin de cumplir las políticas de seguridad de la información y documenta estas actividades?	evidencia) VSIOX = 0 (NO se evidencia)	Modelo de Operación / Usuarios UMV	
VSG07: ¿La entidad cumple con los requisitos legales, reglamentarios y contractuales con respecto al manejo de la información?		Modelo de Operación / Usuarios UMV	
METAS			
CUMPLE	1	**NO CUMPLE**	**0**

INDICADOR INDSG04 – IDENTIFICACIÓN DE LINEAMIENTOS DE SEGURIDAD DE LA ENTIDAD		
IDENTIFICADOR	INDSG04	
DEFINICIÓN		
Grado de la seguridad de la información y los equipos de cómputo.		
OBJETIVO		
Busca medir el nivel de preparación del recurso humano y su apropiación en cuanto a la seguridad de la información y los equipos de cómputo.		
TIPO INDICADOR		
Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES	**FORMULA** = 1 (SÍ se evidencia) = 0 (NO se evidencia)	**FUENTE DE INFORMACIÓN**
VSG08: ¿La entidad ha definido lineamientos de trabajo a través del comité o responsable de seguridad para que sus funcionarios cumplan las políticas de seguridad y evalúa periódicamente su pertinencia?	VSI0X = 1 (SÍ se evidencia)	Usuarios UMV.
VSG09: ¿La entidad ha definido lineamientos en cuanto a la protección de las instalaciones físicas, equipos de cómputo y su entorno para evitar accesos no autorizados y minimizar riesgos de la información de la entidad?	VSIOX = 0 (NO se evidencia)	Usuarios UMV.
METAS		

INDICADOR INDSG04 – IDENTIFICACIÓN DE LINEAMIENTOS DE SEGURIDAD DE LA ENTIDAD			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

INDICADOR INDSG05 – VERIFICACIÓN DEL CONTROL DE ACCESO			
IDENTIFICADOR	INDSG05		
DEFINICIÓN			
Grado control de acceso en la entidad.			
OBJETIVO			
Busca identificar la existencia de lineamientos, normas o estándares en cuanto al control de acceso en la entidad.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**
VSG10: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar el acceso de los usuarios a sus servicios de Gobierno en línea y a sus redes de comunicaciones?		= 1 (SÍ se evidencia) = 0 (NO se evidencia)	Usuarios UMV.
VSG11: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar el uso y el acceso a los sistemas de información, las aplicaciones y los depósitos de información con las que cuenta la entidad?			Usuarios UMV.
VSG12: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar las terminales móviles y accesos remotos a los recursos de la entidad?			
METAS			
CUMPLE	1	**NO CUMPLE**	0

INDICADOR INDSG06 – IMPLEMENTACIÓN DE LOS PROCESOS DE REGISTRO Y AUDITORÍA			
IDENTIFICADOR	INDSG06		
DEFINICIÓN			
Grado de existencia de lineamientos, normas o estándares en cuanto registro y auditoría para la seguridad de la información.			
OBJETIVO			
Busca identificar la existencia de lineamientos, normas o estándares en cuanto registro y auditoría para la seguridad de la información.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES	**FORMULA** = 1 (SÍ se evidencia) = 0 (NO se evidencia)	**FUENTE DE INFORMACIÓN**	
VSG13: ¿La entidad ha definido lineamientos, normas y/o estándares para el registro y control de eventos que sucedan sobre sus sistemas, redes y servicios?	VSI0X = 1 (SÍ	Usuarios UMV.	
VSG14: ¿La entidad verifica de manera interna y/o a través de terceros, periódicamente sus procesos de seguridad de la información y sistemas para asegurar el cumplimiento del modelo?		Usuarios UMV.	
VSG15: ¿La entidad verifica de manera interna y/o a través de terceros, periódicamente sus procesos de seguridad de la información y sistemas para asegurar el cumplimiento del modelo?		Usuarios UMV.	
METAS			
CUMPLE	1	**NO CUMPLE**	0

INDICADOR INDSG07 – POLÍTICAS DE PRIVACIDAD Y CONFIDENCIALIDAD	
IDENTIFICADOR	INDSG07
DEFINICIÓN	
Grado de implementación de políticas privacidad y confidencialidad de la entidad.	
OBJETIVO	

Busca identificar el nivel de implementación de políticas privacidad y confidencialidad de la entidad.		
TIPO INDICADOR		
Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES	**FORMULA** = 1 (SÍ se evidencia) = 0 (NO se evidencia)	**FUENTE DE INFORMACIÓN**
VSG16: ¿La entidad ha implementado lineamientos, normas y/o estándares para proteger la información personal y privada de los ciudadanos que utilicen sus servicios?	VSI0X = 1 (SÍ se evidencia)	Usuarios UMV.
VSG17: ¿La entidad ha implementado lineamientos, normas y/o estándares para proteger la información privada de las entidades que utilicen sus servicios?	VSIOX = 0 (NO se evidencia)	Usuarios UMV.

METAS			
CUMPLE	1	**NO CUMPLE**	0

INDICADOR INDSG08 – ATAQUES INFORMÁTICOS A LA ENTIDAD.	
IDENTIFICADOR	INDSG08
DEFINICIÓN	
Porcentaje de ataques informáticos recibidos en la entidad que impidieron la prestación de alguno de sus servicios.	
OBJETIVO	
Busca conocer el número de ataques informáticos que recibe la entidad	
TIPO INDICADOR	
Indicador de Cumplimiento	

DESCRIPCIÓN DE VARIABLES	**FORMULA** = 1 (SÍ se evidencia) = 0 (NO se evidencia)	**FUENTE DE INFORMACIÓN**
VSG18: ¿Cuántos ataques informáticos recibió la entidad en el último año?	VSI0X = 1	Herramientas de Monitoreo/Usuarios UMV.

VSG19: ¿Cuántos ataques recibió la entidad en el último año que impidieron la prestación de algunos de los servicios que la entidad ofrece a los ciudadanos y empresas?	(SÍ se evidencia) VSIOX = 0 (NO se evidencia)	Herramientas de Monitoreo/Usuarios UMV.	
METAS			
CUMPLE	1	**NO CUMPLE**	0

6.8. ACTIVIDADES GENERALES DE RENDIMIENTO Y MEDICIÓN.

Las siguientes son las actividades generales que soportan la etapa de Evaluación del Desempeño del MSPI (Modelo de Seguridad y Privacidad de la Información) y que se sugiere sean tenidas en cuenta en el proceso de Gestión de Seguridad de la información en la UMV:

- Revisión de la eficacia del MSPI.
- Medición de la efectividad de Controles.
- Revisión de las valoraciones de los riesgos.
- Medición de los indicadores de gestión del MSPI.
- Realización de auditorías.
- Revisiones del MSPI por parte de la dirección.
- Actualizar los planes de seguridad.
- Registro de las actividades del MSPI.
- Revisiones de Acciones o Planes de Mejora (Respuesta a no conformidades).

Desde el punto de vista del desarrollo de estas actividades, su cumplimiento deberá estar asociado con la mejora de los procesos de la UMV, donde se debe relacionar la gestión de la organización y actividades de verificación, se sugiere tener en cuenta las siguientes:

- Consolidar indicadores periódicamente.
- Evaluar indicadores frente a las metas.
- Graficar los Indicadores.
- Analizar causas de las desviaciones.
- Evaluar las No Conformidades ocurridas y su impacto en el cumplimiento de las metas y objetivos del MSPI.

FUENTES DE INFORMACIÓN

1. Modelo de seguridad y privacidad de la información de MINTIC y sus guías asociadas.
2. NTC ISO27001:2013

REVISIÓN Y APROBACIÓN:

Elaborado y/o Actualizado por:	Validado por RESPONSABLE DIRECTIVO del Proceso:	Aprobado Representante de la Alta Dirección:
JEISON MEDINA VALDEZ / GLORIA MÉNDEZ Contratista / Proceso EGTI		
Revisado por:		
ANDREA DEL PILAR ZAMBRANO Contratista/ Proceso DESI	Firma: MARTHA PATRICIA AGUILAR COPETE Secretaría General (E)	Firma: MARTHA PATRICIA AGUILAR COPETE Representante de la Alta Dirección

CONTROL DE CAMBIOS:

VERSIÓN	DESCRIPCIÓN	FECHA	APROBADO Representante de la Alta Dirección SIG
1	Elaborada por el Ing. Omar Fdo. Garzón Giraldo (especialista en seguridad de la información), versión inicial del documento conforme a los requerimientos de MINTIC.	Febrero 2019	Jefe Oficina Asesora de Planeación
2	Se modifica la codificación del documento para adecuarlo a la estructura de documental de la nueva plataforma estratégica y debido a que el código EGTI-PL-001 se asignó en primera instancia al Plan Estratégico de Tecnologías de la Información PETI.	Mayo de 2019	Jefe Oficina Asesora de Planeación
3	Se actualiza el plan para presentar los temas y actividades que contempla desarrollar la UMV en su Plan de Seguridad y Privacidad de la información.	Enero 2020	Jefe Oficina Asesora de Planeación