empoduitama
acueducto alcantarillado

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PROFESIONAL ESPECIALIZADO EN SISTEMAS

MIPG

Modelo integrado de Planeación y Gestión

Contenido

1. INTRODUCCIÓN

La seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno en línea, permite alinearse al componente de TIC para la Gestión al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad.

La Seguridad y Privacidad de la Información se alinea al componente de TIC para Servicios apoyando el tratamiento de la información utilizada en los trámites y servicios que ofrece la Entidad, observando en todo momento las normas sobre protección de datos personales, así como otros derechos garantizados por la Ley que exceptúa el acceso público a determinada información.

El componente de TIC para Gobierno Abierto se alinea con el componente de Seguridad y Privacidad de la Información que permite la construcción de un estado más transparente, colaborativo y participativo al garantizar que la información que se provea tenga controles de seguridad y privacidad, de tal forma que los ejercicios de interacción de información con el ciudadano, otras entidades y la empresa privada sean confiables.

2. OBJETIVOS

2.1. Objetivo General

Definir buenas prácticas en Seguridad y Privacidad para la EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE DUITAMA “EMPODUITAMA S.A E.S.P.” con el fin de garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad, por medio de acciones transversales definidas, tendientes a proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.

2.1.1 Objetivos específicos

- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.

- Implementar mejores prácticas de seguridad que permitan identificar infraestructuras críticas en la entidad.
- Contribuir a mejorar los procesos de intercambio de información pública.
- Orientar a las entidades en las mejores prácticas en seguridad y privacidad.
- Optimizar la gestión de la seguridad de la información al interior de las entidades.

2.2. ALCANCE

Este plan empieza con el establecimiento del Modelo de Seguridad y Privacidad de la Información y termina con el plan de mejora de éste.

Se extiende a todos los procesos que ejecuta la empresa.

2. DEFINICIONES:

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC27000).
- **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).
- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).
- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).
- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente Pagina 6 de 12 ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).
- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

- **Datos Personales Mixtos:** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).
- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3).
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los

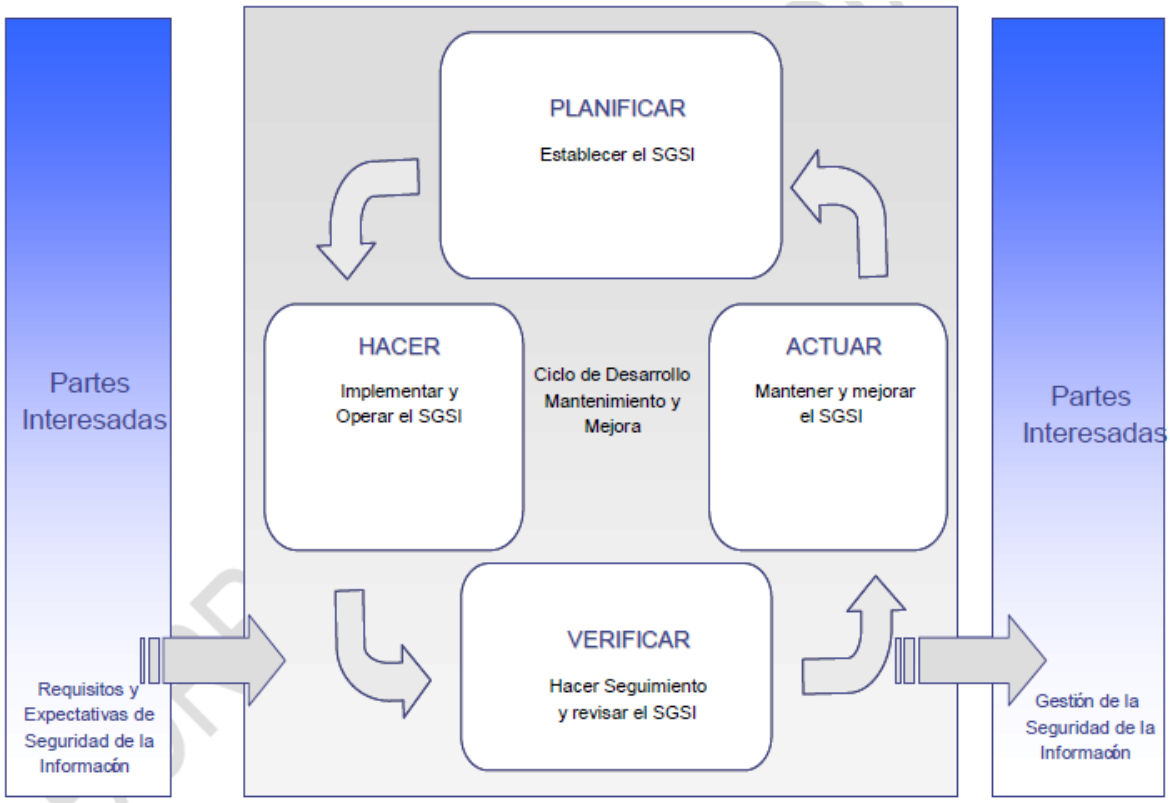
requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008.
- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.
- **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25).
- **Responsabilidad Demostrada:** Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
- **Responsable del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).
- **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
- **Partes interesadas (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

3. REQUISITOS GENERALES

La EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE DUITAMA “EMPODUITAMA S.A E.S.P.” Por medio del Comité de Gestión y Desempeño institucional, creado por resolución 196 DEL 26 DE AGOSTO DE 2018, impulsará la implementación del Modelo de Seguridad y Privacidad de la Información MSPI, en el contexto de las actividades globales de la entidad y de los riesgos que enfrenta. Para llevar a cabo este propósito, se basará en el modelo PHVA.



Fuente: Guía PESI MinTIC

PLANIFICAR: Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar los activos y el riesgo buscando mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.

HACER: Implementar y operar la política, los controles, procesos y procedimientos del MSPI.

VERIFICAR: Evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.

ACTUAR: Emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del MSPI y la revisión por la dirección, para lograr la mejora continua del MSPI.

4. ESTABLECIMIENTO Y GESTIÓN DEL MSPI (Modelo de Seguridad y Privacidad de la Información)

4.1. Establecimiento del MSPI

4.1.1. Política de Seguridad y Privacidad de la Información

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de la EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE DUITAMA "EMPODUITAMA S.A E.S.P." 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, 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 EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE DUITAMA "EMPODUITAMA S.A E.S.P.", para asegurar la dirección estratégica de la Entidad, 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 EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE DUITAMA "EMPODUITAMA S.A E.S.P."
- Garantizar la continuidad del negocio frente a incidentes.

Alcance/Aplicabilidad

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros de la EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE DUITAMA "EMPODUITAMA S.A E.S.P." y la ciudadanía en general.

Nivel de cumplimiento

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

A continuación, se establecen las 12 políticas de seguridad que soportan el SGSI de la EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE DUITAMA "EMPODUITAMA S.A E.S.P.":

- La EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE DUITAMA "EMPODUITAMA S.A E.S.P." 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 empleados, contratistas o terceros.
- La EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE DUITAMA "EMPODUITAMA S.A E.S.P." protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
- La EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE DUITAMA "EMPODUITAMA S.A E.S.P." 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 esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- La EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE DUITAMA "EMPODUITAMA S.A E.S.P." protegerá su información de las amenazas originadas por parte del personal.
- La EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE DUITAMA "EMPODUITAMA S.A E.S.P." protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- La EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE DUITAMA “EMPODUITAMA S.A E.S.P.” controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE DUITAMA “EMPODUITAMA S.A E.S.P.” implementará control de acceso a la información, sistemas y recursos de red.
- La EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE DUITAMA “EMPODUITAMA S.A E.S.P.” garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE DUITAMA “EMPODUITAMA S.A E.S.P.” 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 EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE DUITAMA “EMPODUITAMA S.A E.S.P.” garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.
- La EMPRESA DE SERVICIOS PÚBLICOS DOMICILIARIOS DE DUITAMA “EMPODUITAMA S.A E.S.P.” garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere. La documentación generada deberá acogerse a los parámetros del Sistema Integrado de Gestión y deberá ser controlado por este medio. Se debe llevar registro de los incidentes de seguridad significativos.

4.2. Implementación y operación del MSPI

El Plan de implementación para la dimensión de Seguridad y Privacidad de la Información comprende el siguiente cronograma

Gestión	Actividades	Tareas	Fechas Programación Tareas	
			Fecha Inicio	Fecha Final
Activos de Información	Definir lineamientos para el levantamiento de activos de información	Actualización de metodología e instrumento de levantamiento de activos de información	Mar/2021	Mayo./2021
	Levantamiento Activos de Información	Socializar la guía de activos de Información.	Jun/2021	Jul./2021
		Validar activos de información en el instrumento levantado en la vigencia anterior	Jul/2021	Ago./2021
		Identificar nuevos activos de información en cada dependencia	Jul/2021	Ago./2021
		Consolidar el instrumento de activos de Información.	Ago/2021	Ago/2021
Gestión de Riesgos	Actualización de lineamientos de riesgos	Actualizar política de seguridad y privacidad de la información	Jun/2021	Ago./2021
	Sensibilización	Socialización Gestión de Riesgos de Seguridad y privacidad de la Información y Seguridad Digital	Jun/2021	Ago/2021
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital	Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital	Ago/2021	Sep/2021
	Matriz de riesgos	Realizar y socializar Matriz de riesgos de privacidad y seguridad la información	Sep/2021	Nov/2021
Protección de datos personales	Revisión de bases de datos	Revisar la información recolectada por las áreas para el registro de las bases de datos	Jun/2021	Oct/2021
	Registro y actualización de las bases de datos	Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información	Oct/2021	Dic/2021

4.3. Seguimiento y revisión del MSPI

Se harán revisiones para determinar cambios en los controles si éstos no son eficientes, ya sea que esta decisión se motive por medio de las auditorías internas o la experiencia del proceso de Gestión de las TIC.

4.4. Mantenimiento y mejora del MSPI

La entidad debe, regularmente:

- Implementar las mejoras identificadas en el MSPI.
- Emprender las acciones correctivas y preventivas adecuadas, aplicando las lecciones aprendidas de las experiencias de seguridad de otras organizaciones y las de la propia organización.
- Comunicar las acciones y mejoras a todas las partes interesadas, con un nivel detalle apropiado a las circunstancias y en donde sea pertinente, llegar a acuerdos sobre cómo proceder.
- Asegurar que las mejoras logran los objetivos previstos.

5. REQUISITOS DE DOCUMENTACION

La documentación del MSPI debe incluir registros de las decisiones de la dirección, asegurar que las acciones sean trazables a las decisiones y políticas de la alta dirección, y que los resultados registrados sean reproducibles.

Es importante estar en capacidad de demostrar la relación entre los controles seleccionados y los resultados del proceso de valoración y tratamiento de riesgos al igual que con la política y objetivos del MSPI. Lo anterior se cumplirá con actos administrativos donde se acoge la política de Seguridad y Privacidad de la Información y los procedimientos o guías de gestión de archivos y riesgos.

6. RESPONSABILIDADES DE LA DIRECCION

6.1. Compromiso de la dirección

La dirección de la entidad debe bridar evidencia de su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del MSPI:

- Mediante el establecimiento de una política del MSPI.
- Asegurando que se establezcan los objetivos y planes del MSPI. Con respecto a este requerimiento se establecerá un calendario de actividades.
- Estableciendo funciones y responsabilidades de seguridad de la información. Estas responsabilidades se establecen a través de las políticas que deben ser aprobadas.
- Comunicando a la organización la importancia de cumplir los objetivos de seguridad de la información y de la conformidad con la política de seguridad de la información, sus responsabilidades bajo la ley, y la necesidad de la mejora continua.
- Brindando los recursos suficientes para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un MSPI.
- Decidiendo los criterios para aceptación de riesgos y los niveles de riesgo aceptables. Esto se hará por medio del desarrollo del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- Asegurando que se realizan auditorías internas del MSPI.
- Efectuando las revisiones por la dirección (representada por el comité de gestión y desempeño institucional), del MSPI.

7. AUDITORIAS INTERNAS DEL MSPI

La entidad debe llevar a cabo auditoria internas del MSPI cuando se den cambios de normatividad que afecten la estructura del Modelo o cuando se actualicen las herramientas para la gestión de la seguridad comprendidas objetivos de control, controles, procesos y procedimientos del MSPI, con el fin de evaluar si:

- Cumplen los requisitos de la presente norma y de la legislación o reglamentaciones pertinentes.
- Cumplen los requisitos identificados de seguridad de la información.
- Están implementados y se mantienen eficazmente.
- Tienen un desempeño acorde con lo esperado.

8. REVISION DEL MSPI POR LA DIRECCIÓN

8.1. Generalidades

El comité de gestión y desempeño institucional de EMPODUITAMA debe revisar el MSPI de la organización por lo menos una vez al año, para asegurar su conveniencia, suficiencia y eficacia. Esta revisión debe incluir la evaluación de las oportunidades de mejora y la necesidad de cambios del MSPI, incluidos la política de seguridad y los objetivos de seguridad. Los resultados de las revisiones se deben documentar claramente y se deben llevar registros.

8.2. Información para la revisión

Las entradas para la revisión por el comité de gestión y desempeño institucional deben incluir:

- Resultados de las auditorias y revisiones del MSPI.
- Retroalimentación de las partes interesadas.
- Técnicas, productos o procedimientos que se pueden usar en la organización para mejorar el desempeño y eficacia del MSPI.
- Vulnerabilidades o amenazas no tratadas adecuadamente en la valoración previa de los riesgos.
- Acciones de seguimiento resultante de revisiones anteriores por el comité de gestión y desempeño institucional.
- Cualquier cambio que pueda afectar el MSPI.
- Recomendaciones para mejoras.

8.3. Resultados de la revisión

Los resultados de la revisión por el comité de gestión y desempeño institucional deben incluir cualquier decisión y acción relacionada con:

- La mejora de la eficacia del MSPI.
- La actualización de la evaluación de riesgos y del plan de tratamiento de riesgos.
- La modificación de los procedimientos y controles que afectan la seguridad de la información, según sea necesario, para responder a eventos internos o externos que pueden tener impacto en el MSPI, incluidos cambios a:

  - Los requisitos de la organización
  - Los requisitos de seguridad
  - Los procesos del organismo que afectan los requisitos del negocio existentes.
  - Los requisitos reglamentarios o legales.
  - Las obligaciones contractuales.
  - Los niveles de riesgo y/o niveles de aceptación de riesgos.
- Los recursos necesarios.
- La mejora a la manera en que se mide la eficacia de los controles.

9. MEJORA DEL MSPI

9.1. Mejora continua

Luego de la puesta en marcha de la primera versión de este plan y los controles y auditorías pertinentes, la entidad debe mejorar continuamente la eficacia del MSPI mediante

- El uso de la política de seguridad de la información.
- Los objetivos de seguridad de la información.
- Los resultados de la auditoría.
- El análisis de los eventos a los que se les ha hecho seguimiento.

10. COMPATIBILIDAD DEL MSPI CON OTROS SISTEMAS DE GESTION

El MSPI está alineado con la norma NTC/IEC ISO 27001 y con la NTC-ISO 9001:2000, con el fin de apoyar la implementación y operación, consistentes e integradas con sistemas de gestión relacionados.