MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión: 1
Unidad de Planeación de Infraestructura de Transporte
Bogotá D.C., agosto de 2024

TABLA DE CONTENIDO

1. Introducción

La gestión de la seguridad de la información está enfocada en la preservación de la confidencialidad, integridad, disponibilidad y privacidad de los diferentes activos de información que soportan los procesos de la UPIT. El objetivo fundamental del Sistema de Gestión de Seguridad de la Información (SGSI) es prevenir la materialización de riesgos que afecten la seguridad de la información mediante controles diseñados para contrarrestar los diversos tipos de amenazas. El diseño, implementación, mantenimiento y mejora del sistema de gestión de seguridad de la información en la UPIT permite una gestión ordenada y controlada del modelo de seguridad y privacidad de la información recomendado por la política de gobierno digital recomendada por el Ministerio de Tecnologías de la Información y las Comunicaciones.

Mediante el Manual del SGSI se presentan las actividades fundamentales del ciclo: Planear, Hacer, Verificar y Actuar dentro del marco de trabajo de la norma técnica Colombiana NTC ISO/IEC 27001.

Entre los beneficios que la UPIT puede alcanzar con la implementación de su SGSI, se pueden citar: mejorar las capacidades institucionales para gestionar amenazas informáticas, cumplir con los requerimientos de protección de la información institucional y personal que está bajo la responsabilidad de la entidad, cumplir requisitos legales de seguridad de la información e integrar el habilitador de seguridad y privacidad de la información a la arquitectura empresarial de la UPIT.

2. ¿Para qué debo aplicar el documento?

El Manual del Sistema de Gestión de Seguridad de la Información tiene como objetivo planificar el diseño de las acciones y controles que mitigarán los riesgos de seguridad de la información a los que pueden estar expuestos los activos de información de la UPIT, y para lograrlo, anualmente la entidad aplica los procedimientos descritos en el presente manual con el fin de identificar adecuadamente el contexto de la seguridad, identificar riesgos de seguridad digital y establecer un plan de seguridad y privacidad de la información que facilite la implementación de las acciones que preserven la confidencialidad, integridad, privacidad y disponibilidad de la información de la UPIT.

Todas las acciones del plan anual de seguridad y privacidad de la información forman parte integral de la planificación institucional y el plan de acción anual de las diferentes dependencias.

3. ¿Cuál es la aplicación del documento?

El presente Manual describe las acciones del ciclo PHVA de la gestión de la seguridad de la información en la UPIT, iniciando con la identificación del contexto institucional de la seguridad digital, diseñando el plan de tratamiento de riesgos, realizando seguimiento a la implementación de los controles de seguridad, y finalizando con las actividades evaluación de la efectividad del sistema, sus controles y planes de tratamiento de riesgos.

El Manual del SGSI es de aplicación obligatoria para todos los funcionarios y contratistas de la UPIT, en particular para el responsable de la seguridad de la información designado por el Jefe de la Oficina de Gestión de Información de la UPIT.

Los controles de seguridad aplicados al elaborar el plan de seguridad y privacidad de la información son obligatorios para todos los colabores que prestan sus servicios a la UPIT, incluidos servidores públicos, funcionarios, contratistas y proveedores de servicios contratados por la UPIT.

4. ¿Qué conceptos debo tener claros para comprender el documento?

Para los propósitos de este manual, son aplicables los términos, definiciones y abreviaturas señalados en la Norma Técnica Colombiana ISO 27001:2022 o su versión vigente y, además, las siguientes:

Definiciones:

Amenaza: Es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio.

Confidencialidad: Propiedad de que la información no se haga disponible o revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad que permite que la información este accesible y utilizable por parte de las entidades o personas debidamente autorizadas.

Integridad: Propiedad de precisión y completitud.

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Colaboradores: Servidores públicos y contratistas de la Unidad de Planeación de Infraestructura de Transporte.

Siglas:

ISO: *International Standardization Organization* (Organización Internacional de Estandarización por sus siglas en inglés)

MINTIC: Ministerio de Tecnologías de la Información y las Comunicaciones.

SGSI: Sistema de Gestión de Seguridad de la Información.

5. ¿Qué normatividad afecta el documento?

El conjunto detallado de las normas aplicables a la gestión de la seguridad de la información se encuentra disponible en el normograma institucional, a continuación, se citan las normas que por especial relevancia se deben considerar cuando se aplique el Manual del SGSI:

- Constitución Política de Colombia, artículos 15 y 23.
- Ley 1266 de 2008, *"Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones"*.
- Ley 1581 de 2012, *"Por medio de la cual se dictan disposiciones generales para la protección de datos personales".*
- Ley 1712 de 2014, *"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones"*.
- Decreto 103 de 2015, *"Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones".*
- Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Resolución No. 746 de 2022 del MINTIC, *"Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución número 500 de 2021"*.
- Resolución No. 500 de 2021 del MINTIC, *"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".*

- Norma Técnica Colombiana NTC ISO/IEC Colombiana 27001:2022. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

6. ¿Qué documentos externos requiero en la ejecución?

Los siguientes documentos externos deben ser considerados cuando se aplique el Manual del SGSI:

- Política de gobierno digital, Ministerio de Tecnologías de la Información y las Comunicaciones.
- Manual Operativo del Modelo Integrado de Planeación y Gestión V5, marzo 2023 – Función Pública

7. ¿Qué documentos internos requiero en la ejecución?

Tema	Tipo documental	Nombre del documento
Gestión de riesgos	Manual	Manual para la administración de los riesgos, Unidad de Planeación de Infraestructura de Transporte.

8. Desarrollo del documento

Contexto organizacional

Generalidades

La Unidad de Planeación de Infraestructura de Transporte, UPIT, es una unidad administrativa especial adscrita al Ministerio de Transporte, la cual nace como una solución ante la necesidad de una visión integral para planear el desarrollo articulado de la infraestructura de transporte en Colombia, así como una estrategia de largo plazo que guíe y priorice las inversiones requeridas en esta materia.

La UPIT, se creó el 21 de mayo de 2014, mediante el Decreto 946 de 2014; sin embargo, fue hasta el año 2020 que se lograron las condiciones presupuestales y administrativas para establecer y financiar la planta de personal de la Entidad mediante la expedición del Decreto 1819 de 2020.

El 12 de octubre de 2021 en compañía de la vicepresidenta de la República, la ministra de Transporte, el Departamento Nacional de Planeación, y Directivos del sector transporte, en un sencillo evento presentaron a la ciudadanía la nueva entidad.

Finalmente, la UPIT inicia actividades a finales del 2021, como una Entidad orientada al desarrollo de la infraestructura de transporte del país con una visión técnica, intermodal que dé respuestas eficientes, innovadoras y resilientes a las necesidades territoriales y nacionales.

Misión

Planear el desarrollo sostenible de la infraestructura de transporte del país conectando a los colombianos de manera integral, promoviendo la competitividad y la movilidad para el desarrollo del territorio nacional.

Visión

A 2030, seremos el referente de planeación de infraestructura de transporte para todos los colombianos. Nuestra estrategia está orientada a la consolidación de una red intermodal de transporte que dé respuestas eficientes, innovadoras y resilientes a las necesidades territoriales y nacionales.

Construcción del contexto de la seguridad de la información

Las actividades de gestión de la seguridad de la información en la UPIT deben iniciarse anualmente con el análisis del contexto interno y externo institucional. El Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones evalúa los factores internos y externos que pueden afectar la seguridad de la información institucional y el sistema de gestión de seguridad la información.

El análisis del contexto interno y externo permite identificar las situaciones que tienen el potencial de afectar positiva o negativamente el logro de los objetivos de la seguridad, los requerimientos de las partes interesadas sobre la seguridad de la información o los riesgos de seguridad de la información.

Este análisis se realiza mediante la metodología de análisis de Fortaleza, Oportunidades, Debilidades y Amenazas los resultados integran al análisis de contexto del sistema integrado de gestión institucional.

Para el análisis del contexto, el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones puede considerar, entre otros, los siguientes factores:

Factores Externos:

1) Entorno tecnológico actual e iniciativas de desarrollo tecnológico de la UPIT.
2) Cambios normativos, reglamentarios o institucionales que afecten a la Entidad.
3) Aspectos presupuestales, financieros y de mercado que limiten o posibiliten las adquisiciones de servicios o productos tecnológicos orientados a soportar la gestión de seguridad, la ciberseguridad y protección de datos personales.
4) Otros factores que a juicio de la Oficina de gestión de información son externos y pueden afectar las capacidades en materia de seguridad de la información, ciberseguridad y protección de datos personales.

Factores Internos:

1) Cambios en la estructura orgánica o de funciones de la UPIT.
2) Cambios en la plataforma estratégica institucional como: visión, objetivos institucionales, PETI.
3) Cambios en el Sistema Integrado de Gestión de la UPIT.
4) Elementos socio culturales como el nivel de conciencia en seguridad y competencias en materia de seguridad de la información de los colaboradores de la UPIT.
5) Relaciones contractuales con proveedores o contratistas.
6) Otros que a juicio de la Oficina de Gestión de la Información son internos y pueden afectar las capacidades en materia de seguridad de la información, ciberseguridad y protección de datos personales.

Compresión de las necesidades y expectativas de las partes interesadas

Anualmente el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones, identifica las necesidades y expectativas de seguridad de la información de las partes interesadas en la gestión de seguridad de la UPIT como entes de control, entidades vinculadas, ciudadano, caracterización de grupos de valor y clientes internos, para establecer requisitos, necesidades y expectativos de seguridad de la información, ciberseguridad y protección de datos personales. El análisis se realiza mediante mesas técnicas en donde se aplican metodologías de recolección y análisis de información como espina de pescado, lluvia de ideas, juicio experto y otras técnicas de facilitación e ideación. Los resultados del análisis de

necesidades en materia de seguridad se consolidan en la matriz de necesidades de seguridad, ciberseguridad y protección de datos personales.

Respecto a las obligaciones legales en materia de seguridad de la información los mismos se consignan en el normograma del Sistema Integrado de Gestión Institucional.

Las necesidades identificadas en materia de seguridad, ciberseguridad y protección de datos personales se evalúan para identificar estrategias que permitan su satisfacción. Las diferentes estrategias se consolidan en el plan de seguridad y privacidad de la información.

Determinación del alcance del Sistema de Gestión de Seguridad de la Información

El alcance de la implementación del Sistema de Gestión de Seguridad de la Información se verifica anualmente para determinar su pertinencia y adecuación a las necesidades de la Entidad. Para la determinación del alcance del SGSI de la UPIT se deben considerar:

- Resultados del análisis de contexto de la seguridad de la información.
- Necesidades y expectativas en materia de seguridad, ciberseguridad y protección de datos personales de las partes interesadas identificadas.
- Dependencias entre los procesos institucionales, requerimientos tecnológicos y planes estratégicos institucionales.
- El Sistema de Gestión de Seguridad de la Información de la UPIT cubre todos los procesos institucionales en su sede Bogotá, y fue formalmente adoptado por el Comité Institucional de Gestión y Desempeño de la UPIT

Liderazgo

Liderazgo y compromiso

La Unidad de Planeación de Infraestructura de Transporte a través del Comité Institucional de Gestión y Desempeño ejerce su liderazgo y compromiso respecto a la gestión de la seguridad de la información por medio de:

a) La adopción formal de la Política de Gestión de Seguridad de la Información.

Ver Política de protección de datos personales seguridad de la información, política de seguridad de la información

b) Asegurando que el Sistema de seguridad de la información forma parte del Sistema Integrado de Gestión Institucional.

c) Asignando los recursos de personal, económicos y técnicos necesarios para la adecuada gestión de la seguridad de la información, la ciberseguridad y la protección de datos personales.

d) Comunicando a todas las partes interesadas internas y externas la importancia de mantener una gestión eficaz de la seguridad de la información, la necesidad de cumplir los requisitos normativos e institucionales y la importancia de proteger todos los activos de información que están bajo responsabilidad de los colaboradores de la UPIT.
Ver Plan de Seguridad y Privacidad de la Información.

e) Revisando anualmente el desempeño de la gestión de la seguridad de la información, para asegurarse que se logren los objetivos y resultados previstos.

f) Dirigiendo y orientando a todos los colaboradores de la UPIT para que contribuyan en la mejora de la eficacia, a través de la adopción de políticas, procedimientos y controles que soporten la preservación de la seguridad de la información, la ciberseguridad y la protección de datos personales.

g) Revisando y evaluando periódicamente acciones de mejora que contribuyan al fortalecimiento del Sistema de Gestión de Seguridad de la Información Institucional.

h) Definiendo los roles y responsabilidades necesarias en el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones que permita establecer, implementar, mantener y mejorar continuamente la gestión de la seguridad de la información.

Política de Seguridad de la Información

La Unidad de Planeación de Infraestructura de Transporte gestiona los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad y privacidad de toda la información necesaria para planear el desarrollo sostenible de la infraestructura de transporte del país, a través de su sistema de gestión de seguridad de la información, el cual mejorará continuamente con:

1. La implementación de las acciones que permitan cumplir los requisitos legales y normativos en materia de seguridad de la información que sean aplicables a su misionalidad.
2. La adopción de los controles de seguridad de la información que faciliten y aseguren las actividades de sus diferentes procesos institucionales.
3. El entrenamiento a todos sus colaboradores en materia de seguridad de la información.
4. La Identificación, valoración y tratamiento de los riesgos de seguridad de la información.

Como objetivos del Sistema de Gestión de Seguridad de la Información, la UPIT se compromete a:

1. Mantener los riesgos que puedan afectar la seguridad de la información dentro de los limites tolerables definidos en la política institucional de gestión de riesgos.
2. Sensibilizar a los colaboradores de la UPIT y a las partes interesadas pertinentes en los aspectos relevantes en materia de seguridad de la información necesarios para impedir la materialización de incidentes de seguridad de la información que afecten a la Entidad.
3. Fomentar la adopción de la cultura de autogestión en la protección de la información institucional en todos los colabores de la UPIT a través de acciones que mejoren el cumplimiento de las políticas, procedimientos y controles de seguridad y privacidad de la información.
4. Mantener y mejorar la infraestructura tecnológica y los controles necesarios para garantizar la disponibilidad, confidencialidad e integridad de la información institucional.

Organización de la seguridad, roles y responsabilidades

La gestión de la seguridad de la información es liderada por el Comité Institucional de Gestión y Desempeño quien es la máxima autoridad del Sistema Integrado de Gestión. La implementación técnica de las políticas, procedimientos y controles, así como la designación de los diferentes roles y responsabilidades en materia de seguridad de la información es coordinada por el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones. Las responsabilidades en materia de seguridad de la información se establecen en las políticas técnicas de seguridad de la información, en resoluciones institucionales y en las cláusulas de los contratos celebrados con proveedores y contratistas de la UPIT.

Los diferentes roles y responsabilidades de la seguridad de la información se definen siguiendo los lineamientos del Modelo Integrado de Planeación y Gestión, dimensión de control interno así:

a. Línea Estratégica: Corresponderá a la Alta Dirección establecer desde el Direccionamiento Estratégico los lineamientos necesarios para que los controles definidos para la Entidad tengan un enfoque basado en riesgos y evaluarlos de forma sistemática en el marco del Comité Institucional de Control Interno.
b. 1ª Línea de Defensa: Corresponde a los servidores en sus diferentes niveles la aplicación de los controles tal como han sido diseñados, como parte del día a día y autocontrol de las actividades de la gestión a su cargo.
c. 2ª Línea de Defensa: Corresponde a la Media y Alta Gerencia, como son la Oficina de Planeación o quien haga sus veces, los Líderes de Proceso, Coordinadores, Supervisores o Interventores de contratos o proyectos entre otros, establecer mecanismos que les permitan ejecutar un seguimiento o autoevaluación permanente de la gestión, orientando y generando alertas a la 1ª línea de Defensa.
d. 3ª Línea de Defensa: Corresponde a la Oficina de Control Interno o quien haga sus veces hacer el seguimiento objetivo e independiente de la gestión, utilizando los mecanismos y herramientas de auditoría interna, así como estableciendo cursos de acción que le permitan generar alertas y recomendaciones a la administración, a fin de evitar posibles incumplimientos o materializaciones de riesgos en los diferentes ámbitos de la entidad.

Planeación

Acciones para tratar riesgos y oportunidades

Generalidades

La planificación de las acciones de tratamiento de riesgos del del Sistema de Gestión de Seguridad de la Información se realiza de acuerdo con el Manual para la Administración de los Riesgos de la UPIT.

Valoración de riesgos

Los riesgos de seguridad de la información, ciberseguridad y protección de datos personales se valoran siguiendo el Manual para la Administración de los Riesgos de la UPIT.

Los riesgos de seguridad de la información, la ciberseguridad y la protección de datos personales se identifican mediante mesas de trabajo con las diferentes dependencias, el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones lidera el análisis periódico de los riesgos de seguridad de la información y sus planes de mitigación en coordinación con los líderes de las diferentes dependencias y procesos institucionales.

Los resultados del análisis de riesgos se registran en la herramienta de gestión de riesgos del sistema integrado de gestión.

Las actividades de evaluación y priorización de los riesgos son lideradas por el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones, quien orienta a las dependencias en la aplicación de los criterios y lineamientos de la política de gestión de riesgos.

Tratamiento de riesgos

Para realizar el tratamiento de los riesgos de seguridad de la información, la UPIT ejecuta las siguientes acciones lideradas por el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones:

- Selecciona opciones apropiadas de tratamiento de riesgos de acuerdo con los resultados de la valoración de riesgos, estas opciones contemplan: mitigar,

transferir, evitar los riesgos considerados inaceptables o aceptar formalmente los riesgos que cumplan con los niveles de tolerancia del riesgo en la UPIT. Igualmente evalúa y adopta en los casos que sean pertinentes, las oportunidades de mejora que fortalezcan el sistema de gestión de seguridad de la información.

- Identifica los controles de seguridad de la información que permitan la implementación de las opciones de tratamiento de riesgos seleccionadas. Los diferentes controles de seguridad se seleccionan a partir de las recomendaciones de las mejores prácticas de seguridad de la información, ciberseguridad, controles definidos para la protección de los datos personales.

- Compara los controles seleccionados con los controles recomendados por el Anexo A de la Norma ISO 27001 para verificar que no se pasen por alto controles necesarios.

  Con los resultados de la selección de controles se produce la declaración de aplicabilidad de controles de seguridad de la información que permite realizar seguimiento a los controles seleccionados para el tratamiento de los riesgos identificados.

- Formula el plan de tratamiento de riesgos de seguridad de la información, que permite dar cumplimiento a las obligaciones definidas por el Decreto 612 de 2018 por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

Una vez formulado el plan de tratamiento de riesgos de seguridad de la información el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones, socializa la propuesta con las diferentes dependencias para obtener de parte de los respectivos dueños de riesgo, la aprobación del plan y la aceptación del riesgo residual de acuerdo con lo definido en el Manual para la Administración de los riesgos.

Los resultados de las actividades de valoración y tratamiento de riesgos se documentan siguiendo los lineamientos del Sistema Integrado de Gestión Institucional y se mantienen en la herramienta de gestión de riesgos.

Objetivos de la seguridad de la información

Anualmente la UPIT realiza la revisión de sus objetivos de seguridad de la información y su pertinencia de acuerdo con la planeación estratégica institucional para confirmar su continuidad o formular mejoras. La UPIT fija los siguientes objetivos en materia de seguridad de la información:

1) Mantener todos los riesgos que puedan afectar la seguridad de la información dentro de los limites tolerables definidos en el manual para la administración de los riesgos.
2) Sensibilizar a los colaboradores y a las partes interesadas pertinentes en los aspectos relevantes en materia de seguridad de la información necesarios para impedir la materialización de incidentes de seguridad de la información que afecten a la UPIT.
3) Mantener y mejorar la infraestructura tecnológica y los controles necesarios para garantizar la disponibilidad, confidencialidad e integridad de la información institucional.

Planificación y control de cambios

Cuando se identifican cambios sobre el Sistema de Gestión de Seguridad de la Información, el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones es la dependencia responsable de realizar la planificación de los planes de manejo del cambio y sustentar ante el Comité Institucional de Gestión y Desempeño su aplicación. Dentro de los cambios que deben ser sometidos a evaluación del comité se incluyen entre otros:

- Modificación del alcance del SGSI.
- Ajuste de objetivos.
- Cambios las actividades de gestión de riesgos de seguridad de la información.
- Cambios a las políticas de operación para la administración del riesgo.
- Cambios en las responsabilidades para la gestión de la seguridad de la información y otros que a juicio del Comité deban ser aprobados por esta instancia.

Soporte

Recursos

Los recursos de personal, económicos, de infraestructura tecnológica y demás necesarios para establecer, implementar, mantener, y mejorar el sistema de gestión de seguridad de la información, se identifican a partir de:

- Análisis de resultados del contexto interno y externo.
- Identificación de necesidades y expectativas de las partes interesadas.
- Alcance del Sistema de Gestión de Seguridad de la Información.
- Resultados de las actividades de valoración y tratamiento de riesgos.
- Formulación del plan de tratamiento de riesgos de seguridad de la información.
- Resultados de la ejecución del plan de formación y sensibilización en seguridad de la información.
- Resultados de la medición, análisis y evaluación del desempeño de la gestión de la seguridad.
- Resultados las auditorías internas y externas.
- Resultados de la revisión por parte de la dirección del estado del SGSI.
- Actividades de mejoramiento continuo de la seguridad de la información, ciberseguridad y protección de datos personales.

La información recopilada en estas fuentes permite la construcción del Plan de Seguridad y Privacidad de la Información que permite dar cumplimiento a las obligaciones definidas por el Decreto 612 de 2018 por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

Competencias

Las competencias, habilidades y conocimientos necesarios en materia de seguridad de la información para la planta de personal de la UPIT se documentan a través del Manual de Funciones y Competencias Laborales, los conocimientos y habilidades específicas en materia de seguridad de la información del personal vinculado mediante la modalidad de contrato por prestación de servicios, son definidas por el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones y se documentan a través de los contratos suscritos por la Entidad con los contratistas.

Toma de conciencia

Con el fin de mejorar los niveles de toma de conciencia y sensibilización respecto a la importancia de la aplicación de buenas prácticas de gestión de la seguridad de la información, la UPIT prepara anualmente el plan institucional de capacitación en al cual se integran las actividades de sensibilización en seguridad digital. Dentro de los aspectos que se incluyen en las actividades de sensibilización en seguridad de la información están:

a) Política de seguridad de la información
b) Beneficios del sistema de gestión de seguridad de la información.
c) Contribución personal a la mejora de la efectividad de la seguridad de la información.
d) Implicaciones del incumplimiento de los requisitos, políticas y controles del Sistema de Gestión de Seguridad de la Información.
e) Políticas técnicas de seguridad de la información.
f) Amenazas informáticas.

Comunicación

Anualmente el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones prepara el Plan de Seguridad y Privacidad de la Información que permite dar cumplimiento a las obligaciones definidas por el Decreto 612 de 2018 por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado. Dentro de plan de seguridad y privacidad de la información se incorporan entre otras las actividades de necesarias para:

a) Mejorar la conciencia de todos los colaboradores de la UPIT sobre aspectos como: política de seguridad de la información, controles de seguridad, implicaciones de las no conformidades con los requisitos del Sistema de seguridad de la información y buenas prácticas de gestión de seguridad de la información.
b) Socializar los resultados de la mejora continua y desempeño del Sistema de seguridad de la información.
c) Fomentar la aplicación de los controles de seguridad para prevenir perdida de confidencialidad, integridad y disponibilidad, y la materialización de riesgos.

Información documentada

Generalidades

La documentación del Sistema de Gestión de Seguridad de la Información debe cumplir con la estructura documental establecida en el Sistema Integrado Gestión de la UPIT, lo que permite asegurar el control sobre la creación, aprobación, distribución, utilización y actualización de los documentos y registros utilizados en el SGSI.

El siguiente conjunto de documentos soportan específicamente las acciones para establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información:

- Manual del Sistema de Gestión de Seguridad de la Información como requisito del modelo de seguridad y privacidad de la información de MINTIC.
- Política de seguridad de la información como requisito del modelo de seguridad y privacidad de la información de MINTIC.
- Políticas técnicas de seguridad de la información como requisito del modelo de seguridad y privacidad de la información de MINTIC.
- Manual para la administración de los riesgos como requisito del modelo integrado de planeación y gestión del DAFP (Departamento Administrativo de la Función Pública).
- Declaración de aplicabilidad de controles de seguridad de la información como requisito del modelo de seguridad y privacidad de la información de MINTIC.
- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información como obligación del decreto 612 de 2018 del DAFP.
- Plan de Seguridad y Privacidad de la Información como obligación del Decreto 612 de 2018 del DAFP.

Creación y actualización de documentación

La creación y actualización de la documentación del Sistema de Gestión de Seguridad de la Información, se realiza según el Manual Gestión y Control de la Información Documentada, disponible en el banco de documentos del repositorio institucional.

Control de la información documentada

Para garantizar que la información del Sistema de Gestión de Seguridad de la Información esté debidamente protegida y siempre esté disponible y sea adecuada para su uso donde y cuando se necesite, el responsable de gestión de seguridad de la información debe aplicar el Manual Gestión y Control de la Información del Sistema Integrado de Gestión Institucional.

Operación del sistema de gestión de la seguridad de la información

Planificación y control operacional

Mediante la elaboración el Plan de Seguridad y Privacidad de la Información, la UPIT planifica, implementa y controla las acciones necesarias para cumplir los requisitos de seguridad de la información, implementar las acciones de tratamiento de riesgos y gestionar los controles necesarios para prevenir la materialización de eventos no deseados que afecten la confidencialidad, integridad y disponibilidad de la información institucional.

Mediante el procedimiento de gestión de cambios el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones gestiona los cambios planificados y revisa las consecuencias de los cambios no previstos sobre la infraestructura tecnológica institucional. El procedimiento contempla la definición de acciones de mitigación de los efectos adversos de los cambios.

El control de las actividades de gestión de seguridad subcontratadas con proveedores de servicios es realizado a través del proceso de Gestión de Tecnologías de la Información.

Valoración de riesgos

A través del Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones, la UPIT realiza la valoración anual de los riesgos de seguridad de la información aplicando el Manual para la Administración de los Riesgos.

Igualmente, cuando se presentan cambios significativos o eventos de seguridad calificados como incidentes de seguridad de la información se revisa la valoración de riesgos de seguridad de la información, ciberseguridad y protección de datos personales.

Los resultados de la valoración periódica de los riesgos de seguridad se registran en el instrumento de gestión de riesgos del sistema integrado de gestión.

Tratamiento de riesgos de seguridad de la información

Mediante los resultados de la valoración periódica de riesgos, el Grupo Interno de Trabajo de Gestión de Tecnologías de la Información y las Comunicaciones, define las acciones necesarias para mitigar, transferir, evitar los riesgos considerados inaceptables o aceptar formalmente los riesgos que cumplan con los lineamientos de las Políticas de Operación para la Administración del Riesgo.

El tratamiento de los riesgos de seguridad sigue las acciones definidas en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, los resultados de las acciones de tratamiento de riesgos se registran en el instrumento de gestión de riesgos del sistema integrado de gestión.

Evaluación del desempeño

Seguimiento, medición, análisis y evaluación

La medición de la eficacia del Sistema de Gestión de Seguridad de la Información permite identificar oportunidades de mejora que propenden por la evolución continua del mismo.

La medición se desarrolla mediante la gestión de indicadores que miden tanto la eficacia del sistema en general como de los controles implementados. Los indicadores de desempeño del SGSI se registran en la caracterización del proceso de gestión de tecnología.

Auditoría a la gestión de la seguridad

Auditoría interna

Mediante los procedimientos del Sistema Integrado de Gestión se planifican las auditorías internas al SGSI, los resultados de la planificación de las auditorías se registran en el Plan anual de Auditorías Institucional.

Revisión por parte de la dirección

Anualmente el Comité Institucional de Gestión y Desempeño realiza la revisión del Sistema Integrado de Gestión, dentro del cual se evalúan los resultados y desempeño del SGSI.

La revisión por la alta dirección del Sistema de Gestión de Seguridad de la Información considera:

a) Estado de las acciones con relación a las revisiones previas al sistema.
b) Cambios en cuestiones externas e internas que sean pertinentes al sistema de gestión de seguridad de la información, estos cambios se identifican a partir de los resultados del análisis del contexto interno y externo institucional.
c) Retroalimentación sobre el desempeño de la seguridad de la información incluyendo:
    - No conformidades y acciones correctivas aplicadas.
    - Seguimiento y resultados de las mediciones de indicadores de la gestión de la seguridad de la información.
    - Resultados de las auditorías internas.
    - Cumplimiento de los objetivos de la seguridad.
d) Retroalimentación de las partes interesadas, la cual se obtiene mediante la encuesta anual de satisfacción de los servicios de seguridad de la información.
e) Resultados de la valoración de riesgos y estado del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
f) Oportunidades de mejora en materia de seguridad de la información.

Mejoramiento

Mejoramiento continuo

La UPIT implementa acciones de mejoramiento continuo sobre su Sistema de Gestión de Seguridad de la Información, a través de:

a) Revisión anual del contexto interno y externo de la seguridad de la información.
b) Valoración de riesgos de seguridad de la información.
c) Evaluación del desempeño de los indicadores del SGSI.
d) Ejecución del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan de Seguridad y Privacidad de la Información.
e) Resultados de las auditorías al SGSI.

f) Implementación de las decisiones de la alta dirección como resultado de la revisión anual del SGSI.
g) Implementación de las acciones de mejora identificadas durante del tratamiento de no conformidades y acciones correctivas.

No conformidades y acciones correctivas

La UPIT aplica los procedimientos de tratamiento de no conformidades del Sistema Integrado de Gestión cuando ocurren no conformidades sobre el SGSI.

El procedimiento contempla las acciones necesarias para:

- Reaccionar a la no conformidad.
- Evaluar la necesidad de acciones para eliminar las causas de la no conformidad con el fin de que no vuelva a ocurrir y no ocurra en otra parte.

9. Bibliografía

- Resolución No. 00500 de marzo 10 de 2021 MINTIC, *"por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".*
- Norma técnica colombiana NTC-ISO/IEC 27001, Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos.

10. ¿Qué cambios ha tenido el documento?

Versión Generada	Fecha	Descripción del Cambio o Modificación
01	12/08/2024	Creación del documento

Elaboró	Revisó	Aprobó
Juan Carlos Alarcón Suescún Contratista GIT de Gestión de Tecnologías de la Información y las Comunicaciones	Bismark Benjamín Buenaños Mosquera Coordinador GIT de Gestión de Tecnologías de la Información y las Comunicaciones	