COLOMBIA POTENCIA DE LA VIDA

Transporte

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión 01 - 2024

UPIT
UNIDAD DE PLANEACIÓN DE INFRAESTRUCTURA DE TRANSPORTE

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La información es un activo esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada. Esto es importante en un entorno cada vez más interconectado. Como resultado de esta interconexión creciente, la información se expone a un gran número y variedad de amenazas y vulnerabilidades.

La información puede existir en diversas formas, se puede imprimir o escribir en papel, almacenar electrónicamente, transmitir por correo o por medios electrónicos, presentar en películas, o expresarse en la conversación. Cualquiera que sea su forma o medio por el que se comparte o almacena, siempre debería tener protección adecuada.

La seguridad de la información protege estos activos contra varias amenazas, con el fin de asegurar la continuidad del negocio, minimizar el riesgo y maximizar el retorno de inversiones y oportunidades.

La seguridad de la información se logra implementando un conjunto apropiado de controles, incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Los controles necesitan ser establecidos, implementados, monitoreados, revisados y mejorados, donde sea necesario, para asegurar que se cumplen los objetivos específicos de seguridad de la organización. Esto debería hacerse en conjunto con otros procesos de gestión. Argumento por el cual se realiza el documento, describir las razones, naturaleza e interés del documento y si es necesario referenciar el marco normativo.

2. JUSTIFICACIÓN

La seguridad de la información es importante tanto para los negocios del sector público como del privado y para proteger la infraestructura crítica. En ambos sectores, la seguridad de la información actuará como un elemento facilitador para lograr, por ejemplo, gobierno en línea (e-government) o negocios electrónicos (e-business) y evitar o reducir los riesgos pertinentes. La interconexión de las redes públicas y privadas y compartir los recursos de información incrementan la dificultad para lograr el control del acceso. La tendencia hacia la computación distribuida también ha debilitado la eficacia del control central y especializado.

La definición, implementación y seguimiento del plan de seguridad de la información en la Unidad de Planeación de Infraestructura de Transporte – UPIT permitirá tomar decisiones oportunas, encaminadas a desarrollar seguridad y privacidad de la información de manera apropiada, derivada de la evaluación de riesgos, el cumplimiento normativo y los requisitos de la entidad para procesar la información que apoya su misión.

3. OBJETIVOS

A. Definir el plan de seguridad y privacidad de la información en la Unidad de Planeación de Infraestructura de Transporte – UPIT, que permita realizar el seguimiento en la implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información - SGSI, considerando los lineamientos y directrices establecidas en el Modelo

de Seguridad y Privacidad de la Información – MSPI y el Modelo de Planeación y Gestión – MIPG.

B. Establecer responsabilidades en la definición, operación, seguimiento y mejora de las políticas institucionales relacionadas con la seguridad de la información en la entidad.

C. Orientar a los funcionarios, contratistas y terceros sobre la responsabilidad en el uso y buen manejo de los activos de la información y de la infraestructura tecnológica que soporta la operación de la entidad.

D. Fomentar la conciencia sobre la importancia en el aseguramiento de la información institucional, la cual debe adoptarse como una cultura organizacional.

4. ALCANCE

El plan de seguridad y privacidad de la información aplica para la definición, implementación, mantenimiento y mejora de los lineamientos, directrices, políticas y controles de seguridad de la información que permiten a la Unidad de Planeación de Infraestructura de Transporte – UPIT, contar con niveles apropiados de seguridad de los activos de información.

5. RESPONSABILIDADES

La Oficina de Gestión de la Información es responsable de realizar seguimiento, actualización, mantenimiento y mejora del plan de seguridad y privacidad de la información de la Unidad de Planeación de Infraestructura de Transporte – UPIT.

5.1. COMITÉ DE SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN

Se recomienda crear un comité de sistemas y seguridad de la información para realizar el seguimiento de los objetivos y proyectos estipulados en el plan.

5.2. RESPONSABLE DEL TRATAMIENTO DE LOS DATOS PERSONALES

En cumplimiento de los lineamientos establecidos en la Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”, y la Política de Tratamiento de Datos Personales, se define como responsable del tratamiento de datos personales la Unidad de Planeación de Infraestructura de Transporte – UPIT identificada con NIT: 860.034.604-5.

5.3. EQUIPO DE GESTIÓN

El equipo de gestión del plan se encarga de tomar las medidas para planear, implementar y hacer seguimiento a todas las actividades necesarias para adoptar el Modelo de Seguridad y Privacidad de la Información, así como planear las actividades necesarias para una adecuada administración y sostenibilidad de este.

En el marco del desarrollo de las actividades asociadas al SGSI, la Oficina de Gestión de la Información, es responsable de definir, implementar, mantener y mejorar el SGSI.

5.4. ROLES Y RESPONSABLES EQUIPO DE GESTIÓN

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

5.4.1. Administrador de infraestructura tecnológica

Garantizar la continuidad en la prestación de los sistemas y servicios informáticos que apoyan el cumplimiento de los objetivos y la misión de la Entidad, a través de la administración (configuración, pruebas, puesta en operación, migración, actualización, mantenimiento) de la infraestructura tecnológica IT que soportan la operación informática institucional.

El responsable de la administración de los activos de IT, debe mantener actualizada la documentación requerida para garantizar la disponibilidad de los servicios informáticos críticos (sistemas de información, recursos compartidos, servidores de almacenamiento), que incluye manuales de usuario, manuales de configuración y despliegue, medios de instalación, códigos fuente (cuando aplique) y la información para la puesta en operación (IP, servidores, motores de DB y sistemas operativos).

En desarrollo de la administración de los activos de IT que soportan la operación informática de la entidad, se deben establecer estrategias que permitan contar con respaldo del recurso humano (backup), quién podrá, de ser necesario, solucionar inconvenientes técnicos asociados a los dispositivos de tecnologías de información y comunicaciones.

El administrador de la IT debe gestionar (documentar) los incidentes de seguridad de la información materializados, que puedan comprometer la confidencialidad, integridad y disponibilidad de los activos de información, así como alimentar la base de conocimiento de las acciones adelantadas para restaurar la operación.

Responsable: Profesional o contratista de temas de TIC.

5.4.2. Seguridad informática

Garantizar el aseguramiento de la información institucional digital, creada, procesada, modificada y alojada en la infraestructura tecnológica de la entidad, a través de la definición e implementación del SGSI, MSPI, seguimiento, monitoreo, mantenimiento y mejora continua de los controles, lineamientos y directrices de seguridad informática en concordancia con las normas técnicas

internacionales como por ejemplo NTC-ISO-IEC 27001:2013 y la normatividad vigente y aplicable.

Ilustración 1. *Responsabilidades seguridad y privacidad de la información*

El oficial de seguridad de la información es el encargado de la ejecución de campañas de socialización que busquen generar una cultura alrededor de la seguridad de la información en la UPIT, y del seguimiento a la implementación del modelo de seguridad y privacidad de la información (MSPI).

➔ **Responsable:** Profesional o contratista de temas TIC.

5.4.3. Administrador redes de comunicaciones

Los servicios informáticos, red de datos y de comunicaciones deben contar con altos niveles de disponibilidad, que se reflejen en oportunidad de la información institucional de manera eficiente y efectiva, para lo cual se debe gestionar el recurso humano calificado para adelantar actividades de administración, configuración, mantenimiento y operación de los equipos de comunicaciones de la entidad. Es responsabilidad del administrador de las redes de datos (networking) y los equipos que la soportan, implementan, mantienen y mejoran las mejores prácticas y estándares para la gestión de infraestructura tecnológica.

Ilustración 2. *Modelo red de datos UPIT*

El administrador de redes debe ejecutar las acciones necesarias asociadas a la continuidad en la prestación de los servicios informáticos en la entidad, adelantando tareas de respaldo de la configuración de los equipos activos, así como gestionar garantías sobre los activos de infraestructura tecnológica clasificados y valorados como críticos.

- Se deben proponer alternativas de operación en caso de materialización de incidentes de seguridad que comprometan total o parcialmente la operación informática.

➔ **Responsable.** Profesional o contratista temas TIC.
➔ **Apoyo.** Contratistas de TIC, Terceros.

5.4.4. DBA - Administrador de bases de datos

Garantizar la protección de los datos creados, procesados y/o modificados que se encuentran alojados en los sistemas de información de la entidad, a partir de la implementación, mantenimiento y mejora de controles de seguridad que permitan niveles apropiados de integridad y confiabilidad de la información resultado de la operación informática misional de la entidad.

La responsabilidad en la administración de las bases de datos misionales de la entidad es asumida desde la Oficina de Gestión de la Información, considerando como un factor crítico las tareas de procesamiento y manejo de la información institucional usada en la toma de decisiones encaminadas a cumplir metas, objetivos y la misión de la UPIT.

El administrador de las bases de datos debe garantizar que exista una única fuente de información institucional, para lo cual se establecerá un único sistema de reportes misionales, operado a través del documento institucional vigente ´Procesamiento de Datos´. La asignación de un único DBA en la UPIT, permite a la entidad contar con niveles de confiabilidad de la información reportada a los entes de control, reportes de metas y demás instancias que lo requieran.

➔ **Responsable.** Profesional o contratista de temas TIC
➔ **Apoyo.** Contratistas de TIC, Terceros.

5.4.5. Administración sistema de información misional

Uno de los logros de la Política de Gobierno Digital, se relaciona con los sistemas de información y busca potenciar los procesos y servicios que presta la entidad a través de la gestión de los sistemas de información.

Ilustración 3. *Administración sistema de información misional*

Es responsabilidad del administrador de las herramientas misionales, contar con la documentación (modelo entidad relación (ER), diccionario de datos, manuales de usuario, manuales de configuración…) debidamente actualizada y controlada, teniendo en cuenta los lineamientos de seguridad de la información para la publicación de documentos y requisitos del modelo integrado de planeación y gestión.

Las necesidades de ajustes, desarrollos nuevos e implementación de funcionalidades sobre las herramientas misionales identificados y requeridos desde cada uno de los procesos (áreas, dependencias), deben ser evaluados y aprobados por el líder de desarrollo de software de la entidad, previa comunicación oficial por parte del área solicitante.

Los cambios a las funcionalidades de las herramientas misionales deben ser aprobados por el líder de la Oficina de Gestión de la Información, previa validación y documentación de las pruebas realizadas, así como los planes de contingencia y recuperación.

El sistema de información misional es la fuente oficial de información institucional relacionada con la población objeto, por lo que las solicitudes de procesamiento de información deben canalizarse a través de los medios oficiales para este fin, siendo responsabilidad del administrador de este sistema dar estricto cumplimiento a los lineamientos dispuestos por el Comité de Sistemas y Seguridad de la Información, referentes al procesamiento de datos (generación de reportes).

➔ **Responsable.** Profesional o contratista de temas TIC

5.4.6. Administrador sistemas de información administrativos

El equipo de sistemas de la Oficina de Gestión de la Información designará a los responsables de la administración, configuración y puesta en operación (cuando sea requerido) de los aplicativos que apoyan los procesos administrativos de la entidad, como nomina, inventarios, almacén, cartera y tesorería entre otros.

Ilustración 4. *Administración sistema de información administrativa y financiera*

El administrador de los sistemas de información es responsable de realizar seguimiento a la documentación requerida para su configuración, despliegue y puesta en operación, que permitan la oportuna recuperación frente a la materialización de un evento de seguridad informática que comprometa su operación.

Se deben aplicar procedimientos de copias de respaldo que permitan niveles apropiados de integridad de la información contenida en las bases de datos de los servicios informáticos administrativos, así como la ejecución de simulacros de restauración programados y controlados, que verifiquen la funcionalidad de las copias realizadas, para lo cual el administrador del sistema de información administrativa verificará los recursos (hardware, software, medios) necesarios y realizará la documentación de los resultados.

Importante: el equipo de sistemas de la Oficina de gestión de la Información, es responsable de ejecutar acciones para preservar la disponibilidad de los sistemas de información administrativos, así como de velar por la protección de la información derivada de su uso. Los directores, jefes de área, y jefes directos son responsables del uso de las herramientas, informando oportunamente a la Oficina de Gestión de la Información a través del documento institucional vigente, roles y responsabilidades de los funcionarios designados.

El uso de las funcionalidades de las herramientas informáticas de apoyo es responsabilidad de los usuarios autorizados, al igual que el manejo que den a las contraseñas asignadas, en cumplimiento de los lineamientos de seguridad de los activos de información de la UPIT, evitando exponerla a daño, modificación, destrucción accidental o intencional, robo o alteración.

➔ **Responsable.** Profesional o Contratista de temas TIC

5.4.7. Responsable gestión documental

Los lideres de Gestión Documental, deben velar por la clasificación de la información institucional. El responsable del proceso debe gestionar la implementación de un sistema de gestión documental que permita contar con seguimiento y trazabilidad en el flujo de información.

Ilustración 5. *Modelo gestión documental*

5.4.8. Control de documentos – SIG

El equipo del SIG es responsable de garantizar el control de los documentos que consolidan el Sistema Integrado de Gestión de la UPIT, y deberá verificar la estructura y forma de los documentos allegados por las diferentes dependencias de la entidad, antes de avalar la publicación de estos.

Ilustración 6. *Modelo control documental*

Es responsabilidad del equipo del SIG garantizar el control de los documentos generados al interior de la entidad, informando oportunamente a las áreas sobre la información vigente, a través de los medios electrónicos dispuestos.

5.4.9. Responsable plan de sensibilización

Considerando la importancia de generar una cultura alrededor de la seguridad de la información en La Unidad de Planeación de Infraestructura de Transporte – UPIT, desde la Oficina de Gestión de la Información, el equipo de Comunicaciones y demás áreas delegadas por el Comité de Sistemas y Seguridad de la Información, se debe establecer, actualizar y ejecutar un plan de

comunicación que permita a la entidad conocer los lineamientos y directrices relacionadas al SGSI.

Ilustración 7. *Socialización seguridad de la información*

Es responsabilidad del equipo de Comunicaciones apoyar el desarrollo de los planes de comunicación del SGSI y MSPI.

6. DESARROLLO

6.1. COMPONENTES DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A continuación, se relacionan puntos críticos en donde se pueden encontrar los componentes principales del Sistema de Gestión de Seguridad de la Información en la entidad.

- **Estructura organizacional de seguridad de la información:**

Una vez conformado y oficializado el Comité de Sistemas y Seguridad de la Información, será responsable de la dirección estratégica del Sistema de Gestión de Seguridad de la Información. El oficial o encargado de seguridad de la información, es el responsable de la gestión del sistema, y un conjunto de responsabilidades separadas entre las áreas de tecnología y las áreas usuarias para el apropiado apoyo a la gestión de la seguridad de la información en la entidad.

- **Clasificación de información:**

La Oficina de Gestión de la Información debe adoptar un instructivo para la clasificación de los activos de información, el cual proporciona los niveles de clasificación de la información, el formato para establecer el inventario de activos de información, software, hardware y servicios.

- **Políticas y procedimientos de la gestión de seguridad:**

El Manual del Subsistema de Gestión de Seguridad de la Información describe las políticas que soportan el SGSI, y que se establecen para alcanzar niveles apropiados de seguridad de los

activos de información del Instituto para la Unidad de Planeación de Infraestructura de Transporte – UPIT.

- **Controles:**

Los controles para implementar y la justificación de su selección o no, descritos en la declaración de aplicabilidad, alineados con la norma NTC-ISO-IEC 27001:2013.

- **Gestión del recurso humano:**

Se deben definir los roles y responsabilidades por los diferentes estándares de gestión de la seguridad de la información para los encargados de la seguridad de la información, y se debe garantizar una socialización y concientización al personal de la entidad sobre el conocimiento de las amenazas y responsabilidades para salvaguardar la confidencialidad, integridad y disponibilidad de la información.

- **Monitoreo y revisión de la gestión de seguridad:**

  El Sistema Integrado de Gestión será el encargado de considerar los componentes para el seguimiento y mejora continua del Sistema de Gestión de Seguridad de la Información. Se debe fortalecer el esquema de control de registros de auditoría de los diferentes sistemas de información, así como la gestión y monitoreo centralizado de los activos de infraestructura tecnológica.

6.2. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Política general del sistema de gestión de seguridad de la información

La Dirección de La Unidad de Planeación de Infraestructura de Transporte – UPIT, consciente del crecimiento de los riesgos de seguridad digital, derivados del uso y masificación de las tecnologías de información y comunicaciones y considerando que la información es un activo esencial para la toma de decisiones encaminadas al cumplimiento de su misionalidad, se compromete a definir, implementar, mantener y mejorar un sistema de gestión de seguridad de la información que le permita contar con niveles apropiados de integridad, confidencialidad y disponibilidad de sus activos de información, en el marco del cumplimiento de las leyes, decretos, normas y lineamientos del orden Nacional.

La Unidad de Planeación de Infraestructura de Transporte – UPIT, gestionará a través del comité de seguridad de la información los recursos necesarios para minimizar el impacto sobre los activos de la información, a partir de una adecuada gestión de riesgo, promoviendo el compromiso y participación del talento humano y la mejora continua para apropiar una cultura de seguridad de la información en el marco de su misión y objetivos institucionales.

Es obligación de todos los funcionarios, contratistas y terceros con acceso autorizado a la infraestructura tecnológica, servicios de red, aplicaciones y a los activos de información institucional, dar estricto cumplimiento a la política de seguridad y privacidad de la información de

la Unidad de Planeación de Infraestructura de Transporte – UPIT, una vez sea oficializada y aprobada la política.

Objetivos del sistema de gestión de seguridad de la información

- Establecer lineamientos, directrices, controles y en general la intención de la Dirección de la Unidad de Planeación de Infraestructura de Transporte – UPIT, de consolidar el uso apropiado de los servicios de procesamiento de información, que permitan la protección de los activos de información institucional.

- Definir la responsabilidad en la definición, operación, seguimiento y mejora de las políticas institucionales relacionadas con la seguridad de la información en la entidad al Comité Sistemas y Seguridad de la Información una vez estos estén oficializados y conformados.

- Orientar a los funcionarios, contratistas y terceros sobre la responsabilidad de uso y buen manejo de los activos de la información y de la infraestructura tecnológica que soporta la operación informática de la entidad.

- Definir aspectos a ser tenidos en cuenta por la entidad, relacionados con el talento humano y su responsabilidad en el uso de la información institucional antes, durante y en la terminación del vínculo laboral.

- Establecer directrices para la protección física de los activos de infraestructura tecnológica de la entidad.

- Establecer responsabilidades, controles y lineamientos para proteger los sistemas y servicios informáticos, por los cuales se procesa la información institucional que garantiza la operación informática de la entidad.

- Fomentar la importancia en el aseguramiento de la información institucional la cual debe ser adoptada como una cultura organizacional.

Alcance del sistema de gestión de seguridad de la información

El presente plan de seguridad y privacidad de la información, así como la definición, implementación, mantenimiento y mejora de los controles de la seguridad informática, cubren todos los activos de infraestructura tecnológica (servidores, equipos de cómputo, equipos de comunicaciones, entre otros) y los activos de información (bases de datos, documentos, SIG, servicios informáticos, documentos, registros), con el propósito de proteger la información institucional digital contra daño, pérdida, sustracción, modificación accidental o intencional, describiendo buenas prácticas en el uso de los sistemas y servicios informáticos, así como los activos de tecnologías de la información y las comunicaciones, dispuestos por la Unidad de Planeación de Infraestructura de Transporte – UPIT, a los usuarios para el cumplimiento de sus funciones.

Plan de implementación del MSPI

La implementación del plan del Modelo de Seguridad y Privacidad de la Información – MSPI comprende las siguientes actividades.

Tabla 1. *Plan de implementación MSPI*

Actividades	Tareas	Responsable	Fecha	
1. DIAGNÓSTICO ESTADO ACTUAL MSPI				
Determinar estado actual del MSPI	1. Revisión de la información actual. 2. Diligenciamiento del instrumento de diagnóstico de MSPI del MinTIC.	Oficina de Gestión de la Información	01/03/2024	31/03/2024
2. GESTIÓN DE ACTIVOS DE INFORMACIÓN				
Lineamientos para la gestión de activos de la información	1. oficializar el instructivo de clasificación de activos de la información.	Oficina de Gestión de la Información	01/04/2024	30/04/2024
Levantamientos de activos de la información	1. Socialización de la documentación para la gestión de activos. 2. Actualización de inventarios de activos de información existentes. 3. Elaboración de inventario de activos para otros procesos. 4. Revisión de inventarios de activos de información.	Oficina de Gestión de la Información	16/04/2024	15/05/2024
Publicación de activos de información	1. Validar y aceptar los activos de información por parte de los líderes de los procesos. 2. Consolidar los inventarios de activos de información. 3. Publicar los inventarios de activos de información.	Oficina de Gestión de la Información	15/05/2024	31/05/2024
Registro de activos de información según Ley 1712 de 2014	1. Actualizar el instrumento de registro de activos de información. 2. Revisar viabilidad jurídica del instrumento para publicación. 3. Publicación del instrumento de registro de activos de información.	Oficina de Gestión de la Información - Gestión Jurídica	01/06/2024	15/06/2024

Actividades	Tareas	Responsable	Fecha	
Reporte de bases de datos personales	1. Reportar al área encargada las bases de datos personales identificadas en el inventario de activos de información.	Oficina de Gestión de la Información	16/06/2024	30/06/2024
3. GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL				
Revisión y actualización de los lineamientos para la administración del riesgo.	1. Actualización de la política de administración del riesgo. 2. Actualización de la metodología para la gestión del riesgo. 3. Actualización de Formato Mapa de Riesgos.	Oficina de Gestión de la Información	16/06/2024	31/06/2024
Plan de formación y sensibilización.	1. Socialización y entrenamiento a los encargados sobre el proceso de administración de riesgos de seguridad digital.	Oficina de Gestión de la Información	01/07/2024	31/07/2024
Proceso de administración de riesgos de seguridad digital.	1. Identificación del riesgo. 2. Análisis del riesgo inherente. 3. Evaluación del riego inherente. 4. Definición de controles existentes. 5. Análisis del riesgo residual. 6. Selección de la opción de tratamiento del riesgo. 7. Definición del plan de tratamiento. 8. Realimentación, revisión y verificación de los riesgos identificados (Ajustes).	Líderes de procesos-Direcciones	01/07/2024	31/07/2024
Aceptación de los riesgos residuales y aprobación del plan de tratamiento.	**1.** Generar documento con la aceptación de los riesgos residuales. **2.** Generar documento con la aprobación del plan del tratamiento.	Líderes de procesos	01/08/2024	31/08/2024
Comunicación del riesgo.	1. Presentar a las partes interesadas los resultados del proceso de	Oficina de Gestión de la Información	01/09/2024	30/09/2024

Actividades	Tareas	Responsable	Fecha	
	administración o gestión del riesgo.			
Seguimiento al plan de tratamiento.	1. Realizar seguimiento al estado de implementación de los planes de tratamiento de riesgos y verificación de evidencias.	Oficina de Gestión de la Información	01/10/2024	31/10/2024
Evaluación de la efectividad de los controles.	1. Evaluación de riesgos residuales	Oficina de Gestión de la Información	01/11/2024	15/11/2024
Mejora continua.	1. Identificación de las oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de la efectividad de los controles del plan de tratamiento.	Oficina de Gestión de la Información	16/11/2024	30/11/2024
Monitoreo y revisión.	1. Generación, presentación y reporte de indicadores del plan de tratamiento.	Oficina de Gestión de la Información	01/10/2024	30/12/2024
3. MARCO DOCUMENTAL				
Procedimientos	Oficializar Procedimientos relacionados con la seguridad de la Información	Oficina de Gestión de la Información	22/04/2024	30/06/2024
Políticas y manuales	1. Oficializar políticas y manuales relacionados con la seguridad de la Información: • Política para el tratamiento de datos personales. • Manual seguridad de la información. • Política Cifrado de la Información • Política Control Acceso Físico • Política Control Acceso Lógico • Política Cumplimiento • Política Escritorios Limpios y Bloqueo de Pantallas • Política de Gestión de Riesgos • Política de Gestión de Terceros.	Oficina de Gestión de la Información	22/04/2024	30/06/2024

Actividades	Tareas	Responsable	Fecha	
	• Política de Organización de SI. • Política Red Segura • Política de Clasificación de la Información. • Política de Concientización en SI. • Política de Continuidad del Negocio. • Política de Copias de Seguridad. • Política de Desarrollo Seguro. • Política Gestión Medios Removibles • Política de Gestión de Activos de Información. • Política de Seguridad en Gestión Humana. • Política Gestión de Contraseñas. • Política Gestión de Vulnerabilidades Técnicas.			
Declaración de aplicabilidad	1. Revisión y actualización de declaración de aplicabilidad.	Oficina de Gestión de la Información	22/04/2024	30/06/2024
Normograma de seguridad de la información	1. Identificación de la legislación aplicable. 2. Consolidación normograma de seguridad de la información. 3. Verificación del cumplimiento de los requisitos legales de seguridad de la información.	Oficina de Gestión de la Información	22/04/2024	30/06/2024
4. PLAN DE SENSIBILIZACIÓN				
Plan de comunicación, sensibilización y capacitación para la entidad	1. Ejecución de actividades de comunicación, sensibilización y capacitación. 2. Ejecución de pruebas de ingeniería social.	Oficina de Gestión de la Información	01/03/2024	31/12/2024

Actividades	Tareas	Responsable	Fecha	
5. EVALUACIÓN DEL DESEMPEÑO				
Indicadores de desempeño y eficacia SGSI	1. Revisión y actualización de las métricas de seguridad de la información.	Oficina de Gestión de la Información	22/04/2024	30/06/2024
Revisión de la seguridad de la información	1. Revisión independiente de la seguridad de la información. 2. Verificación del cumplimiento de las políticas y normas de seguridad.	Oficina de Gestión de la Información	01/11/2024	30/11/2024
6. MEJORA CONTINUA				
Acciones correctivas y de mejora	1. Definición del plan de mejoramiento. 2. Ejecución de las acciones correctivas y de mejora. 3. Seguimiento al plan de mejoramiento.	Oficina de Gestión de la Información	01/12/2024	31/12/2024

7. MARCO NORMATIVO

- **Constitución Política de Colombia.** Artículo 15.
- **Ley 44 de 1993.** Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).
- **Ley 527 de 1999.** Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- **Ley 594 de 2000.** Por la que se expide la Ley General de Archivos.
- **Ley 850 de 2003.** Por la que se reglamentan las veedurías ciudadanas
- **Ley 1266 de 2008.** Por la cual se dictan las disposiciones generales del Habeas 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 1221 del 2008.** Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- **Ley 1273 de 2009.** Por la que se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- **Ley 1341 de 2009.** Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones – TIC - Se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
- **Ley 1437 de 2011.** Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.

- **Ley 1474 de 2011.** Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- **Ley 1581 de 2012.** Por la que 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.
- **Ley 1915 de 2018.** Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- **Ley 1952 de 2019.** Por medio de la cual se expide el código general disciplinario
- **Decreto 2609 de 2012.** Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- **Decreto 0884 del 2012.** Por el cual se reglamenta parcialmente la Ley 1221 del 2008.
- **Decreto 1377 de 2013.** Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Decreto compilado en el Decreto Único Reglamentario del sector Industria, Comercio y Turismo 1074 de 2015.
- **Decreto 886 de 2014.** Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- **Decreto 103 de 2015.** Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- **Decreto 1074 de 2015.** Por la que se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- **Decreto 1078 de 2015.** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 728 de 2017.** Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico
- **Decreto 1499 de 2017.** Por la que se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- **Decreto 1008 del 2018.** Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- **CONPES 3701 de 2011.** Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- **CONPES 3854 de 2016.** Política Nacional de Seguridad digital.
- **CONPES 3995 de 2020.** Política Nacional de Confianza y Seguridad Digital.
- **ISO/IEC 27001:2013**. Information Technology Security Techniques - Information Security Management Systems- Requirements.
- **ISO/IEC 27002.** (Information Technology Security Techniques- Code of Practice for Information Security Management.

8. CONTROL DE CAMBIOS

Versión Generada	Fecha	Descripción del Cambio o Modificación
1	30/01/2024	Documento Inicial

Elaboró	Revisó	Aprobó
Gabino Hernández- Contratista Oficina de Gestión de la Información	Bismark Benjamín Buenaños Mosquera - Asesor Dirección General UPIT	Elkin Mauricio Escobar Sarmiento - Jefe Oficina de Gestión de la Información UPIT