PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Secretaría TIC, Innovación y Gobierno Abierto

2025

TABLA DE CONTENIDO

1. INTRODUCCIÓN.

La información es considerada el activo más importante y valioso para todas las organizaciones, y un recurso indispensable para el desarrollo y cumplimiento de sus objetivos misionales, esta puede llegar a ser vulnerable, sensible o crítica y por lo tanto requiere de una evaluación para determinar su nivel de protección necesario para mitigar o evitar posibles situaciones de riesgo e impacto asociado a la pérdida de su disponibilidad, integridad o confidencialidad.

Para la Gobernación de Nariño es indispensable establecer un modelo de gestión de seguridad y privacidad de la información, para salvaguardar de posibles afectaciones a la información que soportan los procesos y la gestión diaria de la entidad en el desempeño de sus funciones y en todos sus aspectos, garantizando la seguridad de los datos, el cumplimiento de las normas legales, las políticas de seguridad digital y continuidad del servicio de MinTIC, la norma NTC/IEC ISO 27001:2013 y el Modelo Integrado de Planeación y Gestión MIPG de la entidad.

El Sistema de Seguridad y Privacidad de la información, está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la Entidad, todo con el objetivo de preservar la confidencialidad, disponibilidad e integridad de los activos de la información, garantizando su buen uso y la privacidad de los datos, todo esto enmarcado en el ciclo PHVA (Planear, Hacer, Verificar y Actuar), para crear condiciones de uso confiable en el entorno digital y físico de la información, mediante un enfoque basado en la gestión de riesgos e implementación de un conjunto de actividades, estrategias, herramientas y controles de seguridad de la información.

Todo esto con base al marco normativo del nivel nacional en donde la implementación del Sistema de Gestión de Seguridad y Privacidad de la Información surge en el contexto de lo expuesto en el Decreto Presidencial 1008 de 2018 referido a las obligaciones de los sujetos obligados en el artículo 2.2.9.1.1.2. para la implementación del habilitador de seguridad de la información, en atención a las orientaciones definidas en el Manual de Gobierno Digital, relacionadas con la adopción e implementación del Modelo de Seguridad y Privacidad de la Información, refrendadas y actualizadas a través del Decreto Presidencial 767 de 2022 en lo referente al habilitador de seguridad y privacidad de la información, el cual derogó el Decreto 1008 de 2018.

Así mismo, la resolución 0500 de marzo 10 del 2021 expedida por el Ministerio de Tecnologías de Información y de las Comunicaciones, que tiene como objeto establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información, la guía de gestión de riesgos de Seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y establecer los lineamientos y estándares para la estrategia de seguridad digital. La resolución en mención precisa la necesidad de que los sujetos obligados deban adoptar las medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al Plan de Seguridad y Privacidad de la Información y así mitigar los riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital.

Es precisamente a través del artículo 5 de la resolución 0500 que se precisa la necesidad de adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital, e incluirla en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos del artículo 2.22.22.3.14 del capítulo 3 del título 22 de la parte 2 del libro 2 del decreto 1083 de 2015

Con el Decreto Presidencial 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", en su artículo 1, adiciona al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto Presidencial 1083 de 2015, Único Reglamentario del Sector de Función Pública, agregando al anterior Decreto el artículo 2.2.22.3.14, por medio del cual se integran los planes institucionales y estratégicos al Plan de Acción, considerando en su numeral 11 y 12 como obligación la elaboración anual del "Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información" y del "Plan de Seguridad y Privacidad de la Información" respectivamente de cada Entidad, y lo señalado en la 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, señala en su artículo 74 denominado "Plan de acción de las entidades públicas", el cual indica que a partir de la vigencia de la presente Ley, todas las entidades del Estado a más tardar el 31 de enero de cada año, deben publicar en su respectiva página web el Plan de Acción para el año siguiente".

Con base en lo anterior se establece el Plan de Seguridad y Privacidad de la Información de la Gobernación de Nariño.

2. OBJETIVOS.

2.1. OBJETIVO GENERAL

Establecer acciones que apoye el establecimiento, operación, mejora continua y sostenibilidad del Sistema de Gestión de Seguridad y Privacidad de la Información de la Gobernación de Nariño, acorde con los requerimientos de la entidad y en cumplimiento a las disposiciones legales vigentes emitidas por el Gobierno Nacional.

2.2. OBJETIVOS ESPECIFICOS

- Coordinar las acciones a realizar para la Implementación del Sistema de Gestión de Seguridad y Privacidad de la Información de la Entidad.
- Gestionar los recursos disponibles para lograr una efectiva implementación de las actividades planeadas.
- Adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad y privacidad de la información digital.
- Planear acciones enfocadas a salvaguardar los activos de la información de la Entidad, la seguridad de los datos personales y el cumplimiento de las expectativas de seguridad de los diferentes grupos de interés de la entidad.

- Construir acciones orientadas en los lineamientos de MINTIC, la Norma ISO 27001 e ISO 31000 y COSO (análisis y gestión de riesgos) y demás normas relacionadas.

3. ALCANCE.

El alcance del Plan de seguridad y privacidad de la información abarca el diagnóstico, la planificación, implementación, evaluación y mejora continua el sistema, aplicado a todas las áreas, procesos y procedimientos de la entidad respaldados por la infraestructura tecnológica clasificada y administrada por la Secretaría TIC, Innovación y Gobierno Abierto, y que conforman el Modelo Integrado de Planeación y Gestión MIPG de la Gobernación de Nariño.

4. MARCO NORMATIVO.

- Ley 1581 de 2012, Protección de datos personales.
- Ley 1712 de 2014, Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria
- Decreto Presidencial 1083 de 2015: “Por medio del cual se expide el Decreto único Reglamentario del Sector de Función Pública”, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.
- Decreto Presidencial 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”.
- Resolución número 00500 de marzo 10 de 2021, Arts. 2 y 3 “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”.
- Resolución Ministerial 00500 de 2021: “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”.
- Decreto Presidencial 767 de 2022: “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.
- ISO/IEC 27001:2013: Tecnología de la información-Técnicas de seguridad-Sistemas de Gestión de la Seguridad de la Información (SGSI).

5. DEFINICIONES.

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.

AMENAZA: Es la causa potencial de un daño a un activo de información.

ANEXO SL: Nuevo esquema definido por International Organization for Standarization - ISO para todos los Sistemas de Gestión acorde al nuevo formato llamado “Anexo SL”, que proporciona una estructura uniforme como el marco de un sistema de gestión genérico.

ANÁLISIS DE RIESGOS: Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

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).

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: Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de FINDETER. [CE 007 de 2018 SFC].

CONFIDENCIALIDAD: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

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 BIOMÉTRICOS: parámetros físicos únicos de cada persona que comprueban su identidad y se evidencian cuando la persona o una parte de ella interacciona con el sistema (huella digital o voz).

DATOS PERSONALES: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

DATOS PERSONALES PÚBLICOS: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión

u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

DATOS PERSONALES 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)

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).

DISPONIBILIDAD: propiedad de ser accesible y utilizable por los usuarios autorizados de la entidad autorizados.

ESTÁNDAR: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas.

GESTIÓN DEL RIESGO: proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

IMPACTO: el coste para la empresa de un incidente “de la escala que sea”, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Resultado de intentos intencionales o accidentales de romper las medidas de seguridad de la información impactando en la confidencialidad, integridad o disponibilidad de la información.

INFORMACIÓN PÚBLICA: Es aquella información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.

INFORMACIÓN: Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla.

INTEGRIDAD: propiedad de exactitud y completitud de la información.

INVENTARIO DE ACTIVOS: lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. (ISO 27000.es,2012).

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.

RESPONSABLES DEL ACTIVO: Personas responsables del activo de información.

RIESGO: Es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o de los procesos. Se expresa en términos de probabilidad y consecuencias.

RIESGO DE SEGURIDAD Y PRIVACIDAD: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. Se mide en términos de probabilidad y consecuencias.

SEGURIDAD DE LA INFORMACIÓN: preservación de la confidencialidad, integridad y disponibilidad de la información.

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).

SISTEMA DE INFORMACIÓN: se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales

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).

6. DIAGNÓSTICO.

El estado actual de la Gestión de Seguridad y Privacidad de la Información en la Gobernación de Nariño, de acuerdo a la valoración realizada con respecto al nivel de madurez, es **ESTADO INICIAL**, con un nivel de cumplimiento **INTERMEDIO**.

		NIVEL DE CUMPLIMIENTO
NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Inicial	INTERMEDIO
	Repetible	CRÍTICO
	Definido	CRÍTICO
	Administrado	CRÍTICO
	Optimizado	CRÍTICO

Nivel de madurez de los controles de seguridad de la información aplicados actualmente en la entidad es **INICIAL**

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	10	100	INICIAL
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	16	100	INICIAL
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	27	100	REPETIBLE
A.8	GESTIÓN DE ACTIVOS	19	100	INICIAL
A.9	CONTROL DE ACCESO	26	100	REPETIBLE
A.10	CRIPTOGRAFÍA	0	100	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	22	100	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	29	100	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	46	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	8	100	INICIAL
A.15	RELACIONES CON LOS PROVEEDORES	10	100	INICIAL
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0	100	INEXISTENTE
A.18	CUMPLIMIENTO	15	100	INICIAL
	PROMEDIO EVALUACIÓN DE CONTROLES	16	100	INICIAL

7. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La Gobernación de Nariño, comprometida con sus usuarios, la familia, la comunidad, proveedores, clientes y de más partes interesadas, establece la necesidad de implementar un Sistema de Gestión de Seguridad y Privacidad de la Información encaminado a proteger los activos de la información a través de la generación de Políticas específicas, procedimientos, lineamientos, apoyo en la implementación de herramientas tecnológicas de prevención y forjar una cultura de concientización de seguridad de la información en todos los funcionarios y contratistas de la organización, todo esto con el objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la información, garantizando la continuidad del negocio y minimizar el impacto causado por los riesgos identificados, logrando así mantener la confianza y responder frente a las necesidades de sus diferentes grupos de interés.

8. ROLES Y RESPONSABILIDADES.

Se elaboró la Matriz de Responsabilidad, Aprobación, Consulta e Información RACI donde se encuentran definidos los roles y responsabilidades de seguridad y privacidad de la información, teniendo en cuenta los cargos Directivos, De procesos y Operativos, que permitan la correcta toma de decisiones y una adecuada gestión para el cumplimiento de los objetivos de la Entidad.

Matriz RACI

PROCESO	CARGOS / ACTIVIDADES	Secretario TIC	Sub Secretario de Innovación	Profesionales Universitarios	Responsable Recursos Humanos	Responsable Compras y Logística	Responsable Financiero	Responsable Infraestructura IT	Responsable Soporte Tecnico	Profesional de Apoyo	Proveedores y Terceros
GESTIÓN ESTRATEGICA	Determinar politicas de la organización	A-R-E-C-I	A-R-E-C-I	E-C-I	E-C-I	E-C-I	E-C-I	E-C-I	E-C-I	E-C-I	C-I
	Autoriza la toma de Decisiones frente a los Sistema de Gestión de la Organización	A-R-E-C-I	A-R-E-C-I	E-C-I	E-C-I	E-C-I	E-C-I	E-C-I	E-C-I	E-C-I	C-I
	Determina asignacion de recursos	A-R-E-C-I	A-R-E-C-I	A-R-E-C-I	R-E-C-I	R-E-C-I	E-C-I	R-E-C-I	E-C-I	E-C-I	E-I
	Delega nuevos cargos criticos	A-R-E-C-I	A-R-E-C-I	C-I	C-I	C-I	C-I	C-I	C-I	C-I	I
	Establecer objetivos y metas	A-R-E-C-I	A-R-E-C-I	R-E-C-I	R-E-C-I	R-E-C-I	R-E-C-I	R-E-C-I	E-C-I	E-C-I	E-I
	Comunicar directrices establecidas y asegurar su entendimiento	A-R-E-C-I	A-R-E-C-I	A-R-E-C-I	A-R-E-C-I	R-E-C-I	R-E-C-I	E-C-I	E-C-I	E-C-I	C-I
	Realizar revisión por parte de la dirección	A-R-E-C-I	A-R-E-C-I	R-E-C-I	R-E-C-I	R-E-C-I	R-E-C-I	R-E-C-I	R-E-C-I	R-E-C-I	C-I
	Verificar ejecución del presupuesto	A-R-E-C-I	A-R-E-C-I	R-I	R-I	R-E-C-I	A-R-E-C-I	C-I	I	R-E-C-I	I
	Verificar atención de quejas y reclamos	A-R-E-C-I	A-R-E-C-I	A-R-E-C-I	A-R-E-C-I	R-E-C-I	R-E-C-I	C-I	C-I	R-E-C-I	C-I
	Delegar Autoridad sobre toma de decisión de presupuesto	A-R-E-C-I	A-R-E-C-I	R-E-C-I	R-E-C-I	R-E-C-I	A-R-E-C-I	C-I	C-I	R-E-C-I	C-I
	Tomar acciones correctivas, preventivas y/o de mejora	A-R-E-C-I	A-R-E-C-I	A-R-E-C-I	A-R-E-C-I	R-E-C-I	R-E-C-I	E-C-I	E-C-I	R-E-C-I	C-I

En la matriz las acciones asignadas para cada Cargo y Proceso, se encuentra determinadas por las siguientes siglas:

A: Autoriza

R: Responde

E: Ejecuta

C: Comunica – Participa

I: Debe ser Informado – Informar

9. PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN.

Para la gestión de la seguridad en la entidad se crearon los procedimientos alineados a la guía MinTIC No. 3 Procedimientos de seguridad de la información., que a continuación se numeran:

- Control de acceso
- Gestión del Cambio
- Gestión de la Capacidad
- Adquisición desarrollo y mantenimiento de sistemas de información
- Gestión de incidentes de seguridad de la información
- Aspectos de seguridad de la información de la gestión de continuidad de negocio

10. METODOLOGÍA DE GESTIÓN DE ACTIVOS DE INFORMACIÓN.

Estructuración de la metodología del inventario de activos de la información en el cual se dan las pautas para la construcción de la matriz y la metodología para la identificación de los activos de la información por cada proceso.
Se crea e identifica el inventario de activos de la información de la infraestructura tecnológica de la entidad.

Matriz de Inventario de Activos de información

IDENTIFICACIÓN DEL ACTIVO						MEDIOS DE CONSERVACIÓN			
ID ACTIVO	TIPO DE MACROPROCESO	PROCESO	DEPENDENCIA	NOMBRE DEL ACTIVO	Tipo de Activo	FISICO	ELECTRÓNICO	Placa Equipo	IDIOMA
29	Apoyo	Transformación Digital	Secretaría TIC, Innovación y Gobierno Abierto	raulortiz@narino.gov.co	Servicio	N/A	servidor de dominio narino.gov.co	N/A	Español
30	Apoyo	Transformación Digital	Secretaría TIC, Innovación y Gobierno Abierto	Drive de Google cuenta raulortiz@narino.gov.co	Servicio	N/A	servidor de dominio narino.gov.co	N/A	Español
51	Apoyo	Transformación Digital	Secretaría TIC, Innovación y Gobierno Abierto	brendarivas@narino.gov.co	Servicio	N/A	servidor de dominio narino.gov.co	N/A	Español
71	Apoyo	Transformación Digital	Secretaría TIC, Innovación y Gobierno Abierto	bases de datos de los sistemas de información de las dependencias	Información	Servidor máquinas virtuales	N/A	N/A	Español
79	Apoyo	Transformación Digital	Secretaría TIC, Innovación y Gobierno Abierto	Archivo de inventario servidores y switches	Información	Equipo a cargo del contratista de apoyo a la gestión de la secretaría TIC	N/A	11515	Español
80	Apoyo	Transformación Digital	Secretaría TIC, Innovación y Gobierno Abierto	Equipo de cómputo 11515	Hardware	Oficina de la dependencia secretaría Tic	N/A	11515	NA

11. METODOLOGÍA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

Estructuración de la metodología de la identificación y valoración de riesgos de seguridad y privacidad de la información, en la cual se definen los Criterios de probabilidad e impacto y el nivel de criticidad del riesgo identificado, todo esto alineado al Modelo nacional de gestión de riesgos de seguridad de la información en entidades públicas del MinTIC.
Se crea, identifica y valora los riesgos de seguridad y privacidad de la información de los activos de la infraestructura tecnológica de la entidad.

Matriz de Identificación, Valoración y tratamiento de Riesgos

ACTIVO DE INFORMACION	IDENTIFICACION DEL RIESGO				VALORACIÓN DEL RIESGO INHERENTE			
	No.	DESCRIPCIÓN DEL RIESGO	POSIBLES CAUSAS	POSIBLES CONSECUENCIAS	PROBABILIDAD	IMPACTO	VALORACIÓN	
	R1				5	4	20	MUY ALTO

12. DECLARACIÓN DE APLICABILIDAD.

La aplicabilidad del Sistema de Gestión de Seguridad y Privacidad de la Información, se definió en una matriz que contempla:

1. Todos los controles del anexo A de la norma ISO 27001
2. La determinación de que controles aplican en la entidad y cuáles de ellos están implementados en la entidad y en operación.
3. La justificación de los controles que no aplican para ser implementados.

Estado y Aplicabilidad de controles de Seguridad de la Información

Sección	Controles de Seguridad de la Información	Estado	Recurso	Preguntas	Comentarios
A5	**Políticas de seguridad de la información**				
A5.1	Directrices de gestión de la seguridad de la información				
A5.1.1	Políticas para la seguridad de la información	Inicial	Repetible	¿Existe una clara evidencia de un marco / estructura / jerarquía global razonablemente diseñada y administrada? ¿Las políticas son razonablemente completas y cubren todos los riesgos de información y áreas de control relevantes? ¿Cómo se autorizan, comunican, comprenden y aceptan las políticas? ¿Están formalmente obligados a cumplir todos los trabajadores y, en su caso, sus empleadores? ¿Hay acuerdos adecuados de cumplimiento y refuerzo? ¿Hay referencias cruzadas a buenas prácticas (como ISO27k, NIST SP800, CSC20 y otras normas y directrices	Documento Política General de seguridad de la información version 1.3 - 2014

13. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

Para el tratamiento de los riesgos de seguridad de la información, se construyó una matriz para identificación de riesgos donde se plasman los controles que aplican para la mitigación de riesgos tomados de la declaración de aplicabilidad, se definen responsables y fechas de implementación.

Para hacer el seguimiento de efectividad de controles se registrarán indicadores.

Matriz de Identificación, Valoración y tratamiento de Riesgos

PLAN DE TRATAMIENTO DE RIESGOS			RESPONSABLE	SEGUIMIENTO			
ACCIONES O TAREAS	CONTROL DEL ANEXO A Y DE LA NORMA ISO 27001	TIEMPO		PERIODO	FECHA DE SEGUIMIENTO	INDICADORES	

14. PLAN DE CAPACITACIÓN, SENSIBILIZACIÓN Y COMUNICACIÓN.

Actividad	Detalle
Buenas prácticas	- Protectores y fondos de pantalla: con recomendaciones de buenas prácticas en seguridad de la información y ciberseguridad. - Videos Tutoriales: instructivos de procedimientos relacionados con seguridad como la elaboración del inventario de activos de la información, buenas prácticas en seguridad de la información, identificación de riesgos. - Boletines Informativos: Envío al correo electrónico institucional, boletines con novedades y recomendaciones de seguridad de la

	información y ciberseguridad. - Infografías: plasmar procedimientos de seguridad de la información implementados en la entidad, que deben ser aplicados por todos los funcionarios y contratistas
Retroalimentación	Micrositio en Intranet sobre Seguridad de la Información donde se alojará: - La Política general de Seguridad de la Información - Las políticas específicas que se generen - Tips de Seguridad - Videos de las charlas de sensibilización que se hayan presentado. - Videos tutoriales institucionales relacionados con el tema - Videos de las capacitaciones brindadas - Publicación del ciclo de charlas de manera oportuna para su asistencia. - Publicación del ciclo de capacitaciones de manera oportuna para su asistencia. La información contenida en el sitio servirá para la inducción a funcionarios y contratistas nuevos y de retroalimentación para reforzar al resto de personal.
Charlas	Charlas de sensibilización presenciales y/o virtuales sobre temas relacionados con seguridad de la información y ciberseguridad. Ciclo de charlas: Trimestrales Duración: máximo 2 horas en las cuales se dicta la charla, se da un espacio para preguntas y se evalúa. Temas para las Charlas: (Primer Ciclo) - Acceso seguro, permisos y contraseñas - Ingeniería social - Ransomware – Secuestro de datos - Ataques de phishing
Socialización de políticas	Toda política que se genere una vez aprobada será socializada ya sea de manera presencial o virtual a todos los funcionarios y contratistas de la entidad, esto se hará de manera general e independiente, teniendo en cuenta los siguientes aspectos: 1. Difusión general: Cuando se aprueba por primera vez una política se socializará en un solo evento para todos los funcionarios y contratistas. 2. Difusión individual: Cuando ingresa un nuevo contratista o funcionario se le dará a conocer las políticas de seguridad de la información implementadas en la entidad. Para dar a conocer la Política General de Seguridad de la Información se

	utilizarán las siguientes estrategias: - Pendón de la política de seguridad, - Volante que contiene la política para entregarse de manera personalizada a funcionarios, contratistas y demás partes interesadas, - Video institucional de La Política de Seguridad General de Seguridad de la Información. - Presentación de política a través de la intranet y pagina web institucional. - Socialización por comunicación interna - Presentación de la política de seguridad en la inducción y reinducción - Presentación de política General de Seguridad de la Información y programa a través de comunicado de prensa desde la Dirección general.
Capacitación	Las capacitaciones se darán en 2 niveles ya sea de manera presencial o virtual. A nivel de usuarios finales A nivel de usuarios de TI y otros procesos involucrados. Temas para las capacitaciones: - Identificación y Reporte de incidentes de Seguridad de la información y ciberseguridad, dirigido a funcionarios y contratistas - Respuesta a incidentes de seguridad de la información, dirigido a equipo de respuesta a incidentes de la Secretaría Tic. - Capacitación en el tratamiento de datos personales, datos sensibles, ley 1581 2012, dirigido a todos los funcionarios y contratistas de la entidad. Frecuencia: la frecuencia de las charlas será cuatrimestral
Programación	Cada estrategia se programará de manera periódica y distribuida en un año para mantener la continuidad y la atención del público objetivo.
Evaluación	Evaluación: Las actividades de Charlas, Socialización y capacitación serán evaluadas con el fin de medir el nivel de comprensión de los asistentes sobre los temas presentados. Las evaluaciones serán de tipo selección múltiple y de 5 a 6 preguntas. Encuestas: se realizarán encuestas para medir el grado de satisfacción de los asistentes a las charlas y capacitaciones.

15. CRONOGRAMA PLAN DE SEGURIDAD DE LA INFORMACIÓN 2025.

El plan de seguridad y privacidad de la información para la vigencia 2025 será ejecutado con recursos propios de la Secretaría TIC.

ACTIVIDADES	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Set	Oct	Nov	Dic
Aprobación del Plan de seguridad y privacidad de la información y Plan de tratamiento de Riesgos de Seguridad.												
Socialización de la Política de seguridad y privacidad de la información a los funcionarios y contratistas de la entidad												
Creación del equipo de Seguridad y Privacidad de la Información, según manual de Roles y responsabilidades.												
Planificación de la implementación de la Política de Tratamiento de datos personales (ley 1581) con base en las recomendaciones del diagnóstico.												
Implementar la Política de seguridad de la información en la relación con proveedores.												
Implementación del procedimiento de gestión de incidentes de seguridad digital.												
Actualización del inventario de activos de información de la Secretaría TIC y presentar para aprobación al comité institucional.												
Actualización de la Matriz de análisis, evaluación y valoración de riesgos sobre inventario de activos de información de la Secretaría TIC.												
Actualización e implementación del Plan de tratamiento de riesgos de seguridad de la información de los activos de la Secretaría TIC.												

Implementación parcial del Plan de Capacitación y sensibilización en Seguridad de la Información.												
Gestionar la contratación de la adquisición o renovación de licencias antivirus y soporte técnico. Implementación de funcionamiento en la totalidad de computadores de la entidad.												
Gestionar y monitorear de manera permanente los dispositivos firewall de seguridad interna y perimetral implementados en la Secretaría TIC..												
Monitorear de manera permanente la consola de administración del sistema antivirus implementado en la entidad y aplicar los controles de seguridad pertinentes.												
Elaboración del Plan de Recuperación de Desastres de Infraestructura TI.												
Realizar una autoevaluación interna en la secretaría TIC sobre seguridad de la información en la entidad.												

16. DOCUMENTOS Y REGISTROS RELACIONADOS

Matriz RACI – Roles y responsabilidades.

17. ANEXOS.

Anexo 1. Matriz RACI.

Anexo 2. Matriz Inventario de Activos de Información

Anexo 3. Matriz de Identificación y Valoración de Riesgos - Plan tratamiento de riesgos 2025

18. CONTROL DE CAMBIOS.

Versión	Fecha de versión	Descripción del cambio	Responsable
01	14/01/2025	Creación del Documento	Secretaría TIC, Innovación y Gobierno Abierto

19. RESPONSABLE.

El responsable de este documento es la Secretaría TIC, Innovación y Gobierno Abierto, quien debe revisarlo, y si es necesario actualizarlo.

20. REVISIÓN, VALIDACIÓN Y APROBACIÓN.

Revisión:	Aprobación:	Verificación:
Jonnathan Huertas	Jonnathan Huertas	Lizeth López Erazo
Secretario TIC, Innovación y Gobierno Abierto	Secretario TIC, Innovación y Gobierno Abierto	Secretaria de Planeación