**PRODUCTO TIPO:**

**POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN**

**MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES**

**OBJETIVO:**

Brindar a las entidades del Orden Nacional y Territorial, un insumo base o plantilla, para la elaboración de su propia Política General de Seguridad y Privacidad de la Información.

\*. Establecer los lineamientos para la adecuada gestión de la seguridad y privacidad de la información en la entidad, enmarcados en la implementación de un Sistema de Gestión de Seguridad de la Información, basado en la identificación y valoración de los riesgos asociados a ella, propendiendo por la protección de su confidencialidad, integridad, disponibilidad, privacidad, continuidad, autenticidad y no repudio y por el cumplimiento de la normatividad vigente aplicable.

**¿COMO USAR LA PLANTILLA?:**

1. Antes de empezar a utilizar la plantilla, se recomienda que la entidad revise su contexto interno y externo, su tamaño y capacidades para ajustarla a su realidad.
2. La información y lineamientos que se encuentran dentro de esta plantilla son los mínimos recomendados que todas las entidades deben tener, no se recomienda eliminar ninguno de los puntos (a menos que la entidad así lo decida), sino que por el contrario, de ser posible se añadan lineamientos adicionales para reforzar la estructura del Sistema de Gestión de Seguridad de la Información.
3. Revisar cada una de las secciones y completar la plantilla con base a lo identificado en el punto 1, es decir, el contexto de la entidad, tamaño y capacidades.
4. Esta plantilla se diseñó para generar la Política General de Seguridad, se deben indicar cosas puntuales, notará que a partir de aquí es necesario crear manuales y procedimientos para complementar lo que se describe en la política general.
5. Una vez diligenciada la plantilla con los lineamientos que la entidad quiere establecer, se debe realizar la FORMALIZACIÓN de la Política General de Seguridad de la Información través de los procedimientos/mecanismos definidos por la entidad (firma de representante legal, subcomités, comités, la oficina asesora de planeación entre otros) para empezarse a aplicar lo más pronto posible.

**TABLA DE CONTENIDO**

[1. OBJETIVO 4](#_Toc76056685)

[2. DEFINICIONES/GLOSARIO 4](#_Toc76056686)

[3. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN 4](#_Toc76056687)

[4. COMPROMISO DE LA ALTA DIRECCIÓN 5](#_Toc76056688)

[5. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN 6](#_Toc76056689)

[6. APLICABILIDAD 6](#_Toc76056690)

[7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ROLES Y RESPONSABILIDADES) 6](#_Toc76056691)

[8. SANCIONES 8](#_Toc76056692)

[9. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL SGSI 8](#_Toc76056693)

[10. APROBACIÓN Y REVISIONES A LA POLÍTICA 9](#_Toc76056694)

**POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN**

**(NOMBRE DE LA ENTIDAD)**

**2024**

## OBJETIVO

Establecer los lineamientos definidos por la Alta Dirección de (**NOMBRE DE LA ENTIDAD***)* para la seguridad de la información, teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información, las políticas de Seguridad Digital y Gobierno Digital y demás requisitos de ley y las necesidades de las partes interesadas.

## DEFINICIONES/GLOSARIO

* **Confidencialidad:** Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.
* **Integridad:** Propiedad de la información que busca preservar su exactitud y completitud.
* **Disponibilidad:** Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
* **Sistema de Gestión de Seguridad de la Información:** Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.
* **Controles:** Medida que permite reducir o mitigar un riesgo.
* **Activo De Información:** conocimiento o información que tiene valor para la organización.
* **Activo Crítico:** Son aquellos elementos o componentes que hacen parte de la infraestructura critica.
* **Alta Dirección:** Persona o grupo de personas que dirigen y controlan al más alto nivel una entidad. Es la máxima autoridad en el sistema.
* **Sistema de Gestión de seguridad de la información (SGSI):** Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.
* **Amenaza:** causa potencial de un incidente no deseado que puede resultar en perjuicio de un sistema o la organización.
* **Autenticación:** Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.
* **Autenticidad**: Busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
* **Ciberseguridad:** Es el proceso de proteger los activos de información por medio del tratamiento de las amenazas a la información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.
* **Cifrado:** Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.
* **Criptografía:** Práctica que consiste en proteger información mediante el uso de algoritmos codificados, hashes y firmas.
* **Acceso Lógico:** restricción de acceso a los datos. Esto se logra mediante técnicas de ciberseguridad como id
* Resolución número 00500 de marzo 10 de 2021

***(Se pueden añadir tantas definiciones como se requiera para el adecuado entendimiento del documento para cualquier parte interesada de la entidad).***

## POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La **(NOMBRE DE LA ENTIDAD)**, entendiendo la importancia de sus activos de información para el cumplimiento de su misión institucional, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) buscando proteger la confidencialidad, integridad y disponibilidad de los activos de información y además establecer un marco de confianza en el ejercicio de su misión con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes aplicables.

La **(NOMBRE DE LA ENTIDAD)** en su propósito de dar cumplimiento con la política de seguridad y privacidad de la información, establece los siguientes objetivos: (*recordar que los objetivos que se definan deben CUMPLIRSE y deben ser medibles de alguna forma, para que permitan determinar si en efecto son eficientes, efectivos o eficaces*)

**OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN:**

* (Objetivo 1). Fortalecer la cultura de seguridad de la información en los funcionarios, proveedores, aprendices, practicantes y clientes de la (ENTIDAD).
* (Objetivo 2). Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
* (Objetivo 3). Minimizar los riesgos de seguridad y privacidad de la información de todos los procesos de la entidad.
* (Objetivo 4). Mejorar continuamente el sistema de gestión de seguridad de la información.
* (Objetivo 5). Implementar los controles tecnológicos necesarios para la protección de los activos de información de la entidad y para la reducción de los riesgos.

***La entidad puede manejar los objetivos de seguridad que considere pertinentes.***

## COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección de **NOMBRE DE ENTIDAD** se compromete a apoyar y liderar el establecimiento, implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información (SGSI); así mismo, se compromete a revisar el avance de la implementación del SGSI de manera periódica y también garantizará los recursos suficientes (tecnológicos y talento humano calificado) para implementar y mantener el sistema, así mismo, incluirá dentro de las decisiones estratégicas, la seguridad de la información. Como consta en el “ARTÍCULO 5. La estrategia de seguridad digital. De la RESOLUCIÓN NÚMERO 00500 DE MARZO 10 DE 2021”. “Y el ARTÍCULO 2. Ámbito de aplicación. Serán sujetos obligados de la presente resolución los señalados en el artículo 2.2.9.1.1.2. del Decreto 1078 de 2015 (DUR-TIC), "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones" “Artículo 2.2.9.1.2.3. Responsable de coordinar la implementación de la Estrategia de Gobierno en línea en los sujetos obligados. El representante legal de cada sujeto obligado será el responsable de coordinar, hacer seguimiento y verificación de la implementación y desarrollo de la Estrategia de Gobierno en línea.

## ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La implementación del Modelo de Seguridad y Privacidad de la Información conforme a los requisitos normativos comprende a todos los procesos de la entidad.

Nos permite conocer la aplicabilidad y los límites para la protección de la información y otros activos, ahí la importancia de su declaración en la implementación de las medidas de seguridad

## APLICABILIDAD

La presente política, sus objetivos, además de los manuales, procedimientos o documentos derivados o complementarios para establecer mucho más la aplicabilidad de la política de seguridad de la entidad se sugiere cambiar a: funcionarios, contratistas, terceros, proveedores, así: como aquellas personas que en razón del cumplimiento de sus funciones y las de la ENTIDAD, compartan, utilicen, recolecten, procesen, intercambien o consulten su información, al igual que a las entidades de control y demás entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información" **(NOMBRE DE LA ENTIDAD)**.

El incumplimiento a la Política de Seguridad y Privacidad de la Información o de sus lineamientos derivados, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad.

En el ARTÍCULO 4 de la resolución 500. “Sistema de gestión de seguridad de la información y seguridad digital. Los sujetos obligados deben aplicar los modelos, guías, y demás documentos técnicos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones a través del habilitador de seguridad y privacidad de la información en el marco de la Política de Gobierno Digital y propenderán por la incorporación de estándares internacionales y sus respectivas actualizaciones o modificaciones, al igual que otros marcos de trabajo que defina mejores prácticas en la materia”.

## ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ROLES Y RESPONSABILIDADES)

**(NOMBRE DE LA ENTIDAD)**, define los roles y responsabilidades para la implementación del MSPI y el cumplimiento de los lineamientos de seguridad descritos en esta política y los demás documentos derivados (Manuales, Procedimientos, Formatos etc.…):

| **ROL / INSTANCIA / DEPENDENCIA** | **RESPONSABILIDADES (Definir los deberes respecto a la SEGURIDAD DE LA INFORMACIÓN)** |
| --- | --- |
| **Alta Dirección** | * Proporcionar los recursos necesarios para la implementación y mantenimiento del sistema de gestión de seguridad de la información (Recursos económicos, formación y recursos tecnológicos). |
| **Comité de Gestión y Desempeño** | * Aprobar los recursos correspondientes para la implementación y el mantenimiento del sistema de gestión de seguridad de la información. |
| **Grupo TIC** | * Implementar los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información. |
| **Oficial de Seguridad Digital** | * Analizar, definir, documentar y gestionar el plan estratégico de seguridad de la información y proponer las decisiones que permitan gestionar la seguridad de la información en el marco del cumplimiento de la política y los lineamientos definidas y aprobados por la entidad. * Apoyar en la generación de los lineamientos (Manuales, procedimientos y formatos) que permitan el establecimiento y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información en la Entidad. |
| **Talento Humano** | * Asegurar que los empleados y contratistas tomen conciencia de sus responsabilidades en seguridad de la información y las cumplan, además de dar aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos. |
| **Control Interno** | * Incluir la seguridad de la información, dentro de los planes de auditoría institucionales. * Apoyar en situaciones de posibles violaciones a las políticas de seguridad de la información. |
| **Prensa / Comunicación Interna** | * Apoyar en las labores de comunicación y sensibilización en seguridad de la información, para difundir la información en todos los niveles de la entidad. |
| **Oficina de Contratación** | * Verificar e implementar las medidas de seguridad de la información en la gestión con los proveedores y contratistas de la entidad. * Procurar la protección de la seguridad de la información de todos los activos de la información que puedan verse involucrados en procesos o contratos. |
| **Área/Proceso 1** | * Añadir los procesos y responsabilidades que la Entidad considere pertinentes. |
| **Área/Proceso 2** | * Añadir los procesos y responsabilidades que la Entidad considere pertinentes. |
| **Líderes de Proceso** | * Implementar las políticas y procedimientos de seguridad de la información que se definan como parte del SGSI (Por ejemplo: gestión de activos, gestión de riesgos, entre otros). |
| **Todos los funcionarios y contratistas** | * Apoyar a los líderes de proceso en el desarrollo de tareas como gestión de activos y gestión de riesgos. * Cumplir a cabalidad con las políticas y procedimientos de seguridad de la información definidos y aprobados. |

## SANCIONES

**a**. Cualquier violación a las políticas de seguridad de la información de **(NOMBRE DE LA ENTIDAD)** debe ser sancionada de acuerdo con el Reglamento Interno de Trabajo, a las normas, leyes y estatutos de la ley colombiana, así como la normativa atinente y supletoria, y apoyados en las leyes regulatorias de delitos informáticos de Colombia.

**b**. Las sanciones podrán variar dependiendo de la gravedad y consecuencias generadas de la falta cometida o de la intencionalidad de la misma.

**c.** ***(Si la entidad considera agregar más factores en este punto, puede hacerlo con base a las normas, leyes y estatutos vigentes).***

## SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL SGSI

**(NOMBRE DE LA ENTIDAD)** indica querealizará revisiones periódicas al SGSI. Dichas revisiones estarán enfocadas en los siguientes aspectos:

* Revisión de indicadores definidos para el Sistema de Gestión de Seguridad de la Información.
* Revisión de avance en la implementación del Modelo de Seguridad y Privacidad de la Información del Ministerio TIC.
* Revisión de avance de la Política de Seguridad Digital de acuerdo con lo solicitado por FURAG o la herramienta definida para tal fin.

## APROBACIÓN Y REVISIONES A LA POLÍTICA

Esta política será efectiva desde su aprobación por la (Alta Dirección/Instancia). La revisión de esta política se hará en las siguientes condiciones:

1. De forma anual, donde se deberá revisar la efectividad de la política y sus objetivos.
2. Si se dan cambios estructurales en la entidad (restructuración de áreas o procesos).
3. Incidentes de seguridad de la información que requieran que la política requiera cambios.
4. ***(La entidad puede adicionar más condiciones si así lo considera).***

|  |  |  |
| --- | --- | --- |
| **ELABORÓ** | **REVISÓ** | **APROBÓ** |
| Nombre:  Cargo:  Fecha: XX-XX-2023 | Nombre:  Cargo:  Fecha: XX-XX-2023 | Nombre:  Cargo:  Fecha: XX-XX-2023 |