PRODUCTO TIPO:

**MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN**

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

**OBJETIVO:**

Brindar a las entidades del orden nacional y territorial el alcance del manual para que los sujetos obligados a cumplir con la Política de Gobierno digital, en los términos del art. 2.2.9.1.1.2. del Decreto 1078 de 2015, que señala *"los sujetos obligados a las disposiciones contenidas en el presente capítulo serán las entidades que conforman la administración pública en los términos del Artículo* [39](https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=186#39) *de la Ley 489 de 1998 y los particulares que cumplen funciones administrativas"* , cuenten con un insumo base o plantilla, para la elaboración de su propio Manual de Políticas de Seguridad de la Información.

**¿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 que se incluyan lineamientos y políticas dentro de cada dominio que puedan cumplirse de manera realista.
2. La información y lineamientos de esta plantilla son los mínimos recomendados que todas las entidades deben tener, no se recomienda eliminar ninguno de los puntos, al contrario de ser posible añadir más lineamientos para reforzar la estructura del Sistema de Gestión de Seguridad de la Información.
3. Se debe 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. Teniendo en cuenta que este es un manual de políticas, es necesario crear manuales y procedimientos adicionales para varias temáticas aquí descritas.
5. Una vez diligenciada la plantilla con los lineamientos que la entidad quiere establecer, se debe realizar la FORMALIZACIÓN del manual a 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 DEL MANUAL 1](#_Toc81077449)

[2. ALCANCE DEL MANUAL 1](#_Toc81077450)

[3. DEFINICIONES 1](#_Toc81077451)

[4. POLÍTICAS 2](#_Toc81077452)

[POLÍTICAS DE SEGURIDAD DE LOS RECURSOS HUMANOS 2](#_Toc81077453)

[POLÍTICAS DE GESTIÓN DE ACTIVOS 2](#_Toc81077454)

[POLÍTICAS DE CONTROL DE ACCESO LÓGICO 2](#_Toc81077455)

[CRIPTOGRAFÍA 3](#_Toc81077456)

[POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO 3](#_Toc81077457)

[POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES 3](#_Toc81077458)

[POLÍTICAS DE SEGURIDAD DE LAS COMUNICACIONES 3](#_Toc81077459)

[POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS 4](#_Toc81077460)

[POLÍTICAS DE RELACIONES CON LOS PROVEEDORES 4](#_Toc81077461)

[POLÍTICAS DE GESTIÓN DE INCIDENTES 4](#_Toc81077462)

[POLÍTICAS DE CUMPLIMIENTO 5](#_Toc81077463)

[ESCRITORIO LIMPIO: 5](#_Toc81077464)

[USO ADECUADO DE INTERNET 5](#_Toc81077465)

[USO ADECUADO DE CORREO ELECTRÓNICO: 5](#_Toc81077466)

[USO DE USUARIOS Y CONTRASEÑAS: 6](#_Toc81077467)

[5. SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN 6](#_Toc81077468)

[SENSIBILIZACIÓN Y COMUNICACIÓN 6](#_Toc81077469)

[CAPACITACIONES EN SEGURIDAD 6](#_Toc81077470)

[6. APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS 7](#_Toc81077471)

[7. SANCIONES 7](#_Toc81077472)

**MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**

**(NOMBRE DE LA ENTIDAD)**

**2024**

## OBJETIVO DEL MANUAL

Establecer lineamientos relacionados con la seguridad de la información abordando temáticas específicas, como complemento a lo definido en la “***Política General de Seguridad de la Información de la Entidad****”* con el fin de preservar la confidencialidad, integridad, disponibilidad, autenticidad y privacidad de los activos de información **(NOMBRE DE LA ENTIDAD)**.

## ALCANCE DEL MANUAL

El presente manual de políticas aplica a funcionarios, contratistas, terceros que tengan acceso a información de la entidad, proveedores, usuarios y visitantes de **NOMBRE DE LA ENTIDAD** que, por alguna razón tengan cualquier tipo de interacción con los activos de información.

## DEFINICIONES

* **Activo de Información:** se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, documentos, soportes, edificios, personas...) que tenga valor para la organización.
* **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.
* **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 identificación, autenticación y autorización

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

## POLÍTICAS

**(NOMBRE DE LA ENTIDAD)**, establece a continuación, los siguientes lineamientos de seguridad de la información, los cuales deberán ser cumplidos por todos los funcionarios, contratistas, terceros, usuarios, proveedores y visitantes. Los lineamientos de seguridad están clasificados en diferentes temáticas, teniendo en cuenta como esta descrito en las funciones y objetivos del contexto interno y externo de la entidad: Para cada política definida se debe establecer el responsable correspondiente, por ejemplo, para la política de RH podría mencionarse La dirección de Talento humano o la dependencia que tenga a cargo sus funciones será la responsable del cumplimiento y seguimiento de la política.

(Para cada una de las políticas se debe definir las áreas responsables y especificar los roles y responsabilidades para cada una de estas políticas

**POLÍTICAS DE SEGURIDAD DE LOS RECURSOS HUMANOS**

* En el proceso de selección de personal de planta o contratistas, se verificarán antecedentes disciplinarios de los candidatos sin importar el cargo o posición al que se postulen.
* Todo el personal que labore en la entidad o preste servicios a la misma deberá firmar un acuerdo de confidencialidad, tratamiento de datos personales y un documento de conocimiento y aceptación de las políticas definidas para el sistema de seguridad de la información y buen uso de los activos de información mediante el cual se compromete a realizar un adecuado uso de estos.

### POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

* Toda información sea física o digital generada, almacenada o transformada por los funcionarios, contratistas o proveedores de la entidad, utilizando los recursos dispuestos por la entidad para tal fin o en desempeño de sus labores o servicio contratado, son activos de información propiedad de **(NOMBRE DE ENTIDAD)**.
* Los activos dispuestos por el **(NOMBRE DE ENTIDAD)** para el apoyo de las labores desempeñada por los funcionarios, contratistas o proveedores, únicamente se permitirá su utilización para ejecución de tareas establecidas en el ámbito laboral de **(NOMBRE DE ENTIDAD)**.
* **(NOMBRE DE ENTIDAD)** identificara, clasificara y gestionara su inventario de activos de información conforme a los manuales y procedimientos de Gestión de Activos formalizados.

### POLÍTICAS DE CONTROL DE ACCESO LÓGICO

* Para la protección de los activos de información, se establecerán procedimientos y políticas para el control de acceso a la red, sistemas de información e infraestructura física (Instalaciones). Para mitigar los riesgos asociados al acceso no autorizado a la información.
* Todos los usuarios deberán asumir la responsabilidad sobre la información física o digital que accedan y procesan dando un uso adecuado con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información.

### CRIPTOGRAFÍA

* **(NOMBRE DE ENTIDAD)** implementará herramientas de cifrado, con el fin de proteger la confidencialidad e integridad de la información. Así mismo, el Grupo/Oficina de Tecnológica de Información y las Comunicaciones determinara los equipos a los cuales se les deberán instalar controles criptográficos adicionales cuando así se requiera.

### POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO

* **(NOMBRE DE ENTIDAD)** adoptará medidas para el control de acceso físico a las instalaciones y áreas seguras con el fin de mitigar los riesgos asociados a la afectación de la confidencialidad, disponibilidad e integridad de la información.
* **(NOMBRE DE ENTIDAD)** definirá áreas seguras y los controles de acceso físico correspondientes como establece en el manual de políticas de seguridad y privacidad de la información (seguridad física y del entorno controles de monitoreo sobre esa área segura, como control de temperatura, humedad, alarma contra incendios, cámaras de vigilancia, entre otros.) para la protección de la información que allí se procese almacene.
* Todas las personas que ingresen a las instalaciones de **(NOMBRE DE ENTIDAD)** deben cumplir con los lineamientos establecidos para el control de acceso físico sin excepción.

### POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES

* Con el fin de asegurar las operaciones realizadas en los recursos tecnológicos que soportan la operación de la entidad. **(NOMBRE DE ENTIDAD)** planea, gestiona, respalda y monitorea la infraestructura tecnológica con el fin de establecer los controles de seguridad pertinentes que permitan proteger la confidencialidad, integridad y disponibilidad de la información siguiendo los lineamientos referenciados en los procedimientos establecidos para el SGSI.

### POLÍTICAS DE SEGURIDAD DE LAS COMUNICACIONES

* El Grupo de Tecnológica de la Información y las Comunicaciones, establecerá los controles para acceso lógico y protección de las redes del **(NOMBRE DE ENTIDAD)**, con el fin de asegurar y cumplir con los acuerdos de niveles de servicios que sean establecidos para los servicios tecnológicos y que deberán ser acordados con la alta dirección.
* El **(NOMBRE DE ENTIDAD)** definirá procedimientos y lineamientos para la transferencia segura de información interna o externamente, de tal forma que se garantice la integridad y confidencialidad de la información.

### POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

* El Grupo/Oficina de Tecnológica y Comunicaciones, velara que los sistemas de información que sean implementados en la entidad cumplan con los requerimientos de seguridad y buenas prácticas.
* Todos los procesos de la entidad que realicen desarrollos deberán cumplir con los procedimiento y metodologías de desarrollo al interior de la entidad por la oficina de tecnologías de la información TI, .
* Todos los procesos de la entidad deberán informar al área de tecnología sobre sus proyectos de adquisición de sistemas de información, con el fin de brindar las observaciones correspondientes y revisar los aspectos técnicos necesario para su desarrollo e implementación.

### POLÍTICAS DE RELACIONES CON LOS PROVEEDORES

* **(NOMBRE DE LA ENTIDAD)** establecerá políticas y requisitos de seguridad de la información para mitigar los riesgos asociados a cada proceso de contratación.
* Antes de Iniciar la ejecución de contratos con terceras partes, deberán suscribirse los respectivos acuerdos de confidencialidad que incluyan las cláusulas de confidencialidad y los aspectos de seguridad de la información necesario durante y después del contrato.

### SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIO

* **(NOMBRE DE LA ENTIDAD)** establecerá un plan de continuidad tecnológica donde se debe incluir la continuidad de la seguridad de la información y restauración oportuna de los servicios en un escenario de contingencia.
* Realizar un plan de pruebas del plan de continuidad de la operación y deberá ser ejecutado mínimo () n veces al año el objetivo de estas prueba es verificar la eficacia del plan y así comprobar que se esta cumpliendo con la tarea, aquí .enumero los tipos de pruebas que se pueden tener en cuenta a) prueba de lista de verificación, b) Prueba de simulacros.
* El Grupo/Oficina de TIC generará dicho plan de continuidad tecnológica con base a Planes de Recuperación de Desastres (DRP) y Análisis de Impacto al Negocio (BIA).

### POLÍTICAS DE GESTIÓN DE INCIDENTES

* Cada vez que se detecta un evento, incidente o debilidad relacionados con seguridad de la información por parte de un funcionario, contratista o terceras partes, se deberá reportar al Grupo/Proceso de TICS por cualquiera de los medios dispuestos para tal fin.
* Sera responsabilidad del Grupo de Tecnología y las Comunicaciones seguir los procedimientos establecidos para la gestión de los incidentes que puedan presentarse.
* El Grupo TIC, deberá documentar la documentación relacionada a los incidentes de seguridad en donde se puede evidenciar entre otras cosas, la clasificación del incidente de seguridad (categoría y prioridad), los tiempos de respuesta, responsables de atención según clasificación, las líneas de atención y los indicadores de medición.
* EL Grupo TIC deberá establecer la tipificación del incidente de seguridad de la información, así: Phishing, Malware, Fuga de Información, Defacement, entre otros

.

### POLÍTICAS DE CUMPLIMIENTO

* **(NOMBRE DE LA ENTIDAD)** velara por el cumplimiento de la legislación vigente respecto a los requisitos establecidos en la seguridad y privacidad de la información, derechos de propiedad intelectual, protección de datos personales, transparencia y del derecho de acceso a la información pública.

### ESCRITORIO LIMPIO:

* No deberán dejarse documentos con información clasificada o sensible en el “Escritorio” tanto físico como el Escritorio virtual (se denomina “Escritorio” al espacio digital en los equipos de cómputo).
* Cada vez que los funcionarios se retiren del lugar de trabajo, es importante que bloqueen los equipos de cómputo para garantizar la seguridad de la información. Una forma común de hacerlo es utilizando la combinación de teclas Win + L. Esta acción activa la función de bloqueo de pantalla y requiere una contraseña para desbloquear el equipo, evitando el acceso no autorizado.
* Es recomendable utilizar cajoneras o archivadores para almacenar de forma segura la información sensible o crítica

### USO ADECUADO DE INTERNET

El internet es un recurso valioso para el desempeño de las labores de todos los funcionarios y, por lo tanto, se definen los siguientes lineamientos para su uso adecuado.

* Estará limitado el acceso a portales de: Juegos, pornografía, drogas, terrorismo, segregación racial, hacking, malware, software gratuito o ilegal y/o cualquier otra página que vaya en contra de las leyes vigentes.
* Estará limitado el acceso a redes sociales como Facebook, WhatsApp, Instagram, Twitter entré otras
* Se restringirá el acceso a portales de nube e intercambio de información masiva (exceptuando a la nube corporativa o institucional).
* El grupo/oficina de TIC podrá verificar los logs o registros de navegación cuando así se solicite o se requiera para las investigaciones o requerimientos que puedan generarse.

### USO ADECUADO DE CORREO ELECTRÓNICO:

* Los buzones de correo asignados a los funcionarios, contratistas o terceros pertenecen a **NOMBRE DE LA ENTIDAD**, por lo tanto, su contenido también es propiedad de la Entidad.
* El correo electrónico solo deberá emplearse para uso institucional y el desempeño de las funciones correspondientes a cada cargo.
* La oficina/grupo de tecnología podrá verificar el contenido de los buzones de los correos telefónicos en los casos que se requiera acudir a información para continuar con la prestación del servicio o para investigaciones específicas.

### USO DE USUARIOS Y CONTRASEÑAS:

* Cada funcionario o contratista cuyas funciones requieran de acceso a sistemas de información o correo electrónico, deberá asignársele un usuario y contraseña.
* Las credenciales son personales e intransferibles.
* Deben utilizarse esquemas de seguridad para la creación de contraseñas (uso de Mayúsculas, Minúsculas, Caracteres, Números).

## SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN

### SENSIBILIZACIÓN Y COMUNICACIÓN

**(NOMBRE DE LA ENTIDAD),** definirá un “**Plan de Comunicación en Seguridad de la Información”** a través de su oficina de comunicación interna y externa y el Grupo/Oficina TIC (*ajustar a cada entidad*), donde se planificará ANUALMENTE la manera en que se comunicarán recomendaciones de seguridad de la información por diferentes medios a todos sus funcionarios y contratistas, con el fin de socializar las políticas institucionales en seguridad de la información o las buenas prácticas en seguridad que se desean socializar para aumentar las capacidades de todas las áreas y procesos de la entidad. La creación de los contenidos se hará con apoyo de la oficina TIC y/o el Oficial de Seguridad de la información.

### CULTURA DE LA SEGURIDAD DE LA INFORMACIÓN

**(NOMBRE DE LA ENTIDAD),** a través de sus áreas/procesos de Talento Humano y Contratos, incluirá dentro de sus capacitaciones e inducciones las temáticas de seguridad de la información, con el objetivo de que cualquier funcionario y/o contratista que se vincule a la entidad tenga pleno conocimiento de las políticas de seguridad de seguridad de la información, el grupo TIC y/o el Oficial de Seguridad de la Información apoyará en dichas inducciones. La entidad implementara las estrategias adecuadas para crear y fortalecer una cultura, cambio y apropiación de Seguridad de la información, lo cual implica un cambio en el comportamiento de los colaboradores en relación a las políticas y directrices que deben cumplir. Esto debe generar la identificación de perfiles de conocimiento, público objetivo, temáticas identificadas para el año, y finalmente la medición de esta gestión.

## APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS

Las políticas aquí definidas se harán efectivas a partir de su aprobación por la Alta Dirección y serán revisadas por lo menos anualmente, cuando existan incidentes de seguridad de la información o cuando se produzcan cambios estructurales considerables, esto con el fin de asegurar su vigencia y aplicabilidad dentro de **(NOMBRE DE LA ENTIDAD).**

## SANCIONES

 La política de Seguridad de la información que se adopte al interior de la entidad deberá estar sustentada por un acto administrativo Ej.: resolución

La falta de conocimiento de los presentes lineamientos no libera al personal de **(NOMBRE DE LA ENTIDAD)** de las responsabilidades establecidas en ellos por el mal uso que hagan de los recursos de TIC o por el incumplimiento de los lineamientos aquí descritos.

1. Se aplicarán sanciones de acuerdo con el Código Único Disciplinario.
2. Pueden aplicarse sanciones de tipo penal según sea el caso y la gravedad de este, si así lo consideran los entes investigativos y judiciales correspondientes.
3. El Grupo TIC será el encargado de recopilar y entregar a la Oficina de Control Disciplinario **(*ajustar según cada entidad*)** las evidencias de incumplimiento de los lineamientos, informes de impactos y consecuencias y cualquier otro insumo requerido para formalmente manejar la investigación inicialmente a nivel interno, así mismo, el grupo TIC será el encargado de registrar y gestionar el Incidente de seguridad derivado con el incumplimiento de las políticas.

|  |  |  |
| --- | --- | --- |
| **ELABORÓ** | **REVISÓ** | **APROBÓ** |
| Nombre:Cargo:Fecha: XX-XX-2021 | Nombre:Cargo:Fecha: XX-XX-2021 | Nombre:Cargo:Fecha: XX-XX-2021 |