PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La alcaldía distrital de santa marta se compromete a proteger la información y garantizar su disponibilidad, integridad y confidencialidad, alineándose con los lineamientos del plan de uso y apropiación de MINTIC y el modelo integrado de planeación y gestión (MIPG).

Esta política establece las directrices para la gestión de la seguridad y privacidad de la información en la entidad.

2. OBJETIVOS

- **Gestionar riesgos de seguridad digital:** Implementar controles para mantener niveles de riesgo aceptables.
- **Prevenir y gestionar incidentes:** Establecer procedimientos para la gestión de incidentes de seguridad de la información.
- **Identificar, evaluar y clasificar activos de información:** Implementar un mecanismo robusto de gestión de activos.
- **Fortalecer la cultura de seguridad**: Promover la sensibilización y formación en seguridad de la información.
- **Alinear con MIPG:** Integrar las directrices de seguridad y privacidad de la información dentro de los componentes del MIPG.

3. ALCANCE

- Cubre todos los aspectos de la información, incluyendo datos electrónicos, físicos y cualquier forma de comunicación.
- Se aplica a todos los empleados, contratistas, proveedores y cualquier entidad que interactúe con la información de la organización.
- Incluye todos los sistemas de TI, redes, dispositivos y cualquier infraestructura relacionada que maneje datos.
- Se enfoca en la protección de datos sensibles y críticos para la organización, tales como información personal, financiera, propiedad intelectual, entre otros.
- Considera las normativas y leyes aplicables a la industria y región específica de la organización.

4. TÉRMINOS Y DEFINICIONES

Acceso remoto: capacidad de acceder a datos, correo, información y aplicaciones desde fuera del entorno de la entidad.

Activos: cualquier cosa que tenga valor para la entidad es considerada un activo en este caso la información es un activo.

Activo de información: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de la Alcaldía Distrital de Santa Marta y, en consecuencia, debe ser protegido.

Amenaza: causa potencial de un incidente no deseado, que puede producir un daño a un sistema

Análisis de riesgos de seguridad de la información: proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Centros de cableado: son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Centro de cómputo: Es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

Ciberseguridad: es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes.

Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados; se encuentra resguardada o salvaguardada en nuestros centros de datos con control de acceso a los usuarios a cada información.

Control: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Disponibilidad: es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Dispositivo móvil: tipo de computadora que presenta las siguientes características:

- Movilidad: puede ser transportado con frecuencia y facilidad.
- Tamaño pequeño: esta característica está ligada a la anterior, para que sea fácil de transportar, su tamaño es pequeño.
- Comunicación inalámbrica: tiene la capacidad de enviar y recibir datos sin ningún tipo de cableado.
- Capacidad de interacción con las personas mediante pantalla y/o teclado.

Equipo de cómputo: dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

Incidente de Seguridad: es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerar, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

Licencia de software: es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Política: su objetivo es establecer, a partir de la observación de hechos de la realidad política, principios generales acerca de su funcionamiento.

Recursos tecnológicos: son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la Alcaldía Distrital de Santa Marta.

Riesgo: riesgo es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

Seguridad de la Información: se entiende el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información. Dicho de otro modo, son todas aquellas políticas de uso y medidas que afectan al tratamiento de los datos que se utilizan en una organización.

Sistema de Gestión de Seguridad de la Información SGSI: Es el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Sistema de información: Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por la Alcaldía Distrital de Santa Marta, o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.

Teletrabajo: trabajo que se realiza desde fuera de las oficinas de la entidad, mediante sistemas de telecomunicación.

Terceros: persona o entidad que se reconoce como independiente.

Usuario: Es aquella persona que usa una cosa o servicio habitualmente. Un usuario es un conjunto de permisos y de recursos a los cuales se tiene acceso.

5. RESPONSABLES

Los responsables del cumplimiento del plan de tratamiento de seguridad y privacidad de la información son de todos, los directivos, funcionarios y terceros que laboren o tengan relación con la Alcaldía Distrital de Santa Marta, con el acompañamiento de La Dirección de TIC.

6. MARCO NORMATIVO

- MINTIC: Seguridad y Privacidad de la Información - Guía No. 2
- Ley 1581 de 2012: Protección de datos personales.
- Ley 1712 de 2014: Transparencia y acceso a la información pública.
- MIPG: Modelo Integrado de Planeación y Gestión

7. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Prevenir y mitigar riesgos para avanzar en el cumplimiento de la política de seguridad y privacidad de la información, garantizando la disponibilidad de los activos críticos de información.

El plan de seguridad y privacidad de la información busca concientizar la importancia de proteger la información en la era digital. Con el propósito de recordar la importancia de proteger los sistemas, programas e información para mejorar la seguridad de la información se tendrá en cuenta que se debe:

- Mantener un inventario actualizado.
- Utilizar contraseñas seguras, instalar antivirus y firewalls, mantener sistemas operativos y software actualizados.
- Monitorear la red y realizar seguimiento de cambios en los sistemas.
- Tener un plan de contingencia y un equipo de respuesta capacitado.
- Mantener copias de seguridad actualizadas y un plan de contingencia para la recuperación de datos.

7.1. Componentes del Plan de Seguridad y Privacidad de la Información

8. POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Formalizar, documentar y difundir las políticas y procedimientos a todos los funcionarios, aprendices, practicantes, contratistas y proveedores que trabajen directa e indirectamente con la entidad es el primer paso para poder implementar una adecuada seguridad de la información.

La Alcaldía Distrital de Santa Marta reconoce la importancia de identificar y proteger los activos de información de la entidad. Para ello, evitará la destrucción, divulgación, modificación, acceso y utilización no autorizada de toda la información que produce y/o utiliza, independientemente de su soporte, comprometiéndose a implantar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, mediante el cual se desarrollarán los controles necesarios que permiten salvaguardar los principios de:

- **Confidencialidad:** asegurar que sólo quienes estén autorizados puedan acceder a la información.
- **Integridad**: asegurar que la información y sus métodos de proceso sean exactos y completos.
- **Disponibilidad:** asegurar que los usuarios autorizados tengan acceso a la información cuando lo requieran.

La Alcaldía Distrital de Santa Marta declara el cumplimiento con la normativa y legislación vigente en relación con aspectos de seguridad de la información.

Para gestionar la seguridad de la información, la alcaldía conformará un comité de seguridad de la información que tendrá como principal objetivo promover, difundir y apoyar la seguridad de la información, garantizando que la misma sea parte del proceso de planificación, definiendo las estrategias, así como aprobar los planes, políticas y todo aquello que incremente y mejore la seguridad de la información.

Además, designará un responsable de la seguridad de la información, quien se encargará de la guía, implementación, mantenimiento y revisión del sistema de gestión de seguridad de la información.

Es política de la entidad:

- Establecer objetivos con relación a la seguridad de la información, elaborar y actualizar el plan de acción para la obtención de dichos objetivos.
- Desarrollar un proceso de evaluación y tratamiento de riesgos de seguridad, e implementar las acciones correctivas y preventivas adecuadas de acuerdo con su resultado.
- Clasificar y proteger la información de acuerdo con la normativa vigente y a los criterios de valoración en relación con la importancia que posee para la entidad.
- Sensibilizar a todo el personal en materia de seguridad de la información.
- Contar con una política de gestión de incidentes de seguridad de la información de acuerdo con los lineamientos establecidos.
- Establecer que todo el personal es responsable de reportar las violaciones a la seguridad, confirmadas o sospechadas de acuerdo con los procedimientos correspondientes.
- Establecer los medios necesarios para garantizar la continuidad de las operaciones.

Esta política de seguridad de la información se integrará a la normativa de la institución.

Responsabilidades

- La Dirección de TIC será responsable de presentar ante el comité institucional de gestión y desempeño, la documentación, estrategia y propuestas para el mantenimiento y fortalecimiento del SGSI.
- Las secretarías son responsables de apoyar la difusión de la política de seguridad de la información toda vez que el responsable de seguridad de la información así lo solicite y brindar los recursos necesarios para el cumplimiento de esta.
- Todas las dependencias son responsables de la implementación de la política de seguridad de la información y de la adhesión del personal a su cargo.
- El personal, sin importar su relación contractual, es responsable por la adhesión a la política de seguridad de la información de la entidad.

8.1. ACCESO REMOTO

La Alcaldía Distrital de Santa Marta debe garantizar la seguridad de la información cuando se accede remotamente a los sistemas de información de la entidad, tanto por el personal interno (funcionarios, practicantes, contratistas) como proveedores autorizados a trabajar en esta modalidad, y definir las condiciones y restricciones del teletrabajo.

- Definir servicios y sistemas accesibles remotamente.
- Mantener un inventario de accesos remotos autorizados.
- Utilizar comunicaciones seguras y protección contra software malicioso.
- Revisar periódicamente los accesos remotos y sus condiciones de uso.

8.2. SEGURIDAD FISICA Y ACCESO A LAS ÁREAS SEGURAS

La Alcaldía Distrital de Santa Marta establecerá lineamientos generales para controlar el acceso físico a las áreas seguras de la entidad, con el objetivo de minimizar el riesgo de accesos no autorizados.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, tales como, centros de datos (MDF e IDFs) se consideran áreas de acceso restringido.

- Controlar el acceso físico a áreas sensibles.
- Implementar medidas de seguridad física en centros de datos y áreas de procesamiento de información sensible.

8.3. GESTION DE ACTIVOS

La Alcaldía Distrital de Santa Marta debe establecer los criterios de clasificación de la información que esté en poder del organismo sin importar el medio que la soporte.

- Clasificar y proteger activos de información según su criticidad y valor.
- Implementar controles para proteger los equipos institucionales.

La clasificación de los activos de información en la Alcaldía Distrital de Santa Marta se establece de acuerdo con la Ley 1712 de 2014 de transparencia y del derecho de acceso a la Información pública, la cual determina que la información producida por las entidades del estado es de naturaleza pública y en sus artículos 18 y 19, establece su clasificación en pública clasificada y pública reservada.

El nivel de clasificación se determina basado en la confidencialidad como principio rector en la selección, estableciendo un nivel de bajo para la información pública, nivel medio para la información pública clasificada y alto para la información pública reservada.

Los lineamientos para la clasificación de la información en la Alcaldía Distrital de Santa Marta se establecen en el Manual Gestión de Activos de Información (codificación).

Los líderes de proceso son los responsables de clasificar los activos pertenecientes a su proceso. La Dirección de TIC apoya a los líderes de proceso en la clasificación de sus activos dándoles a conocer la metodología de clasificación y aplicación de esta.

Dicha información, permanecerá con tal carácter hasta un período determinado desde su clasificación. Además, su carácter pasará a ser público cuando se extingan las causas

que dieron lugar a su clasificación. Sólo se ampliará el periodo de reserva sobre cierta documentación cuando permanezcan y se justifiquen las causas que le dieron origen.

El organismo debe implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad requeridos, en el marco de lo establecido en la presente política.

8.4. SEGURIDAD PARA LOS EQUIPOS INSTITUCIONALES.

Los equipos que conforman la infraestructura tecnológica de la Alcaldía Distrital de Santa Marta, tales como, servidores, estaciones de trabajo, equipos de redes y telecomunicaciones, central telefónica virtual, dispositivos de almacenamiento, que procesen información, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado, adoptando los controles necesarios para mantener estos equipos alejados de sitios que puedan tener riesgo de amenazas físicas y/o ambientales.

Las medidas tomadas deberán ser proporcionales a los riesgos identificados.

En caso de pérdida o robo de un equipo, el responsable del activo se deberá comunicar con la Dirección de TIC para que esta pueda informar inmediatamente a la autoridad correspondiente, y al responsable de seguridad de la información para que lo registre como incidente de seguridad de la información y realice el tratamiento que corresponda.

Alcance

Afecta a toda la infraestructura tecnológica de la entidad, en especial a los centros de datos y áreas relacionadas.

Responsabilidades

- Las secretarías deben velar por el cumplimiento de la presente política y realizar las revisiones oportunas.
- Los directores, coordinadores, jefes de oficinas, líderes de procesos son responsables de disponer de los recursos necesarios para la implementación de la presente política.
- Todos los funcionarios, aprendices, practicantes, contratistas y proveedores son responsables por cumplir con los procedimientos y políticas que estén orientados a la protección y aseguramiento del equipamiento en su poder.

Descripción

Todos los trabajadores son responsables de velar por la seguridad de los equipos propiedad de la entidad, que se encuentren fuera de las instalaciones, siguiendo las siguientes directrices:

- No dejar los equipos de cómputo desatendidos en lugares públicos o a la vista.
- Los equipos de infraestructura deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.
- Los equipos portátiles siempre deben ser llevados como equipaje de mano.
- El retiro de equipamiento propiedad de la entidad fuera de las instalaciones, debe seguir los procedimientos establecidos, contemplando cláusulas de confidencialidad e integridad de la información sensible que esté contenida en este.

Eliminación o reutilización segura de equipos y medios: La entidad debe identificar los riesgos potenciales que puede generar destruir, reparar o eliminar equipos y medios de almacenamiento. Para ello, debe definir e implementar los mecanismos y controles adecuados para que la información sensible contenida en ellos sea eliminada de manera segura, alineados a la política de destrucción de información.

Cuando un equipo sea reasignado o dado de baja, se deberá asegurar la información para luego eliminarla, con el fin de evitar pérdida y/o recuperación no autorizada de la misma.

8.5. CONTINUIDAD OPERATIVA Y RECUPERACIÓN ANTE DESASTRES

La Alcaldía Distrital de Santa Marta deberá planificar y gestionar la continuidad operativa de los procesos críticos de la entidad ante la eventualidad de ocurrencia de eventos anormales que afecten personas, oficinas y edificios, tecnología, información y proveedores, provocando la disrupción de las operaciones.

Esta política aplica a todos los procesos críticos de la entidad, los recursos que se utilizan para su ejecución, la información que éstos generan o usan, y las instalaciones donde se desarrollan.

Responsabilidades

- Las secretarías son responsables por generar las condiciones adecuadas para la ejecución y comunicación de la presente política, así como de establecer el alcance para su aplicación. Así mismo, de la aprobación de los planes de respuesta, de la designación de un vocero para las comunicaciones externas e internas en ocasión de un incidente disruptivo, y de aprobar el contenido de dichas comunicaciones.
- Los directores, coordinadores, jefes de oficinas y líderes de programas son responsables por la identificación de los procesos críticos, los activos y sistemas que los soportan. Así mismo, de la realización de un análisis de impacto en caso de que los procesos críticos de sus áreas se vieren afectados.
- El comité de seguridad de la información es responsable de revisar el plan de contingencia y de recuperación ante desastres, coordinar formalmente a los diferentes actores para la realización de las pruebas y revisar los informes de las pruebas para establecer el plan de mejora.
- La Dirección de TIC debe participar en la planificación técnica del plan de contingencia y recuperación en caso de desastres, en coordinación con el responsable de la oficina de gestión del riesgo
- Los funcionarios de la entidad deben cumplir con lo establecido en la presente política y deben participar, previa coordinación con las secretarías, en las pruebas que se realicen al plan de contingencia y recuperación ante desastres.

Descripción

La Alcaldía Distrital de Santa Marta comprende que es necesario contar con un plan formal de continuidad operativa y un plan de recuperación en caso de desastres ante eventos anormales, teniendo como premisas fundamentales la seguridad y protección de las personas, los recursos y la información.

- Desarrollar y mantener un plan de continuidad operativa.
- Realizar pruebas periódicas del plan de recuperación ante desastres.

El plan de continuidad operativa deberá considerar el riesgo de interrupción de actividades por eventos tecnológicos, humanos y naturales, originados por causas internas o externas, los que estarán debidamente documentados siguiendo lo establecido en la política de gestión de riesgos. El plan deberá definir la contingencia para los procesos críticos incluyendo ventanas de tolerancia, así como un plan de recuperación para el retorno a la operativa normal de la entidad.

El comité realizará la coordinación formal de las pruebas a los planes con todas las partes involucradas, facilitando la coordinación que deba realizar para la seguridad de la información. Éste será el encargado, en conjunto con las secretarías que sea necesario para la ejecución de las pruebas al plan de contingencia y recuperación en caso de desastres, informar al alcalde y al comité el resultado de estas, registrar las lecciones aprendidas y confeccionar el plan de acción para la mejora.

8.6. CICLO DE VIDA DE LA INFORMACIÓN

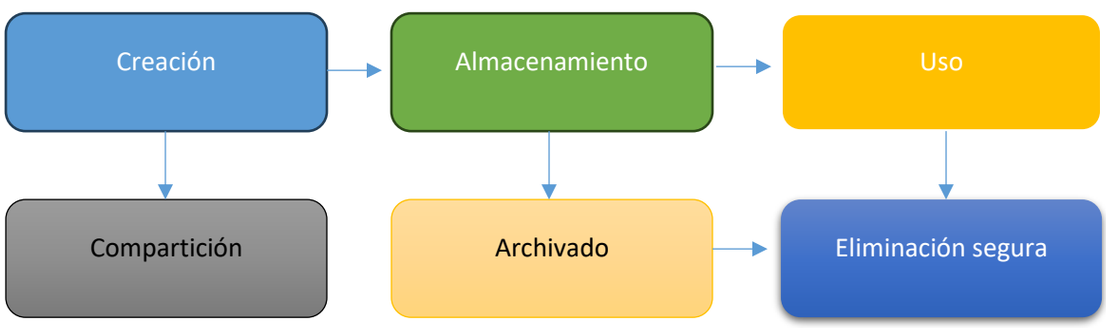
La Dirección de TIC debe garantizar que toda información de la entidad, o en poder de esta, cualquiera que sea su medio de almacenamiento y de acuerdo con su ciclo de vida, sea eliminada de forma segura.

Alcance

Esta política aplica a toda la información de propiedad de la entidad o en poder de esta, según su ciclo de vida.

Responsabilidades

- La Dirección de TIC debe proporcionar los recursos necesarios a fin de contribuir con una adecuada gestión de la información.
- Las secretarías son responsables de velar por el cumplimiento de la presente política y las revisiones que correspondan.
- El propietario del activo de información, o quien este designe, deberá asegurar el adecuado registro del proceso realizado, dejando evidencia del método utilizado e indicando si la operación resultó satisfactoria. Deberá también, informar a La Dirección de TIC para mantener actualizado el inventario de activos indicando la información que fue eliminada.



Descripción

Para completar el ciclo de vida de la información es necesario pasar por el proceso de destrucción de esta. Por lo tanto, se deben definir métodos formales de eliminación segura de la información, de acuerdo con su medio de almacenamiento.

- Gestionar la información desde su creación hasta su eliminación segura.

Se deberán utilizar métodos de borrado seguro de forma que garantice que la información y/o los medios que la contienen no se puedan recuperar. Posibles métodos de borrado seguro son: trituración, desintegración, pulverización, fusión e incineración, des magnetización, sobre escritura, entre otras. Otros métodos, como la utilización de comandos de borrado del sistema operativo algunos tipos de formateo podrían ser métodos no seguros de destrucción de información y permitirían su recuperación.

Durante la destrucción de la información, se debe velar por el cumplimiento del conjunto de políticas que afecten a la información, especialmente las vinculadas a divulgación y acceso.

Registro de las operaciones de borrado

- Deberá existir una solicitud formal, dirigida al propietario del activo de información, indicando en forma unívoca, el medio o la información que requiere destrucción.
- El propietario del activo, o quien éste designe, deberá evaluar si corresponde la destrucción de dicha información tomando en cuenta en los decretos, leyes y otra normativa vigente.
- En cada proceso de destrucción se debe generar un reporte que identifique al personal actuante, la metodología empleada para la destrucción de la información y toda observación que se considere pertinente. Se deberá identificar claramente que el proceso se ha efectuado.
- Aquellas situaciones donde la destrucción de la información no se pueda realizar correctamente, deberán ser documentadas.
- En caso de traslados de soportes físicos, lógicos y/o información almacenada externa a la entidad, hay que asegurar que se cumple la cadena de custodia de estos, para evitar fugas de información, y las demás políticas vinculadas.

8.7. DISPOSITIVOS MÓVILES

La Alcaldía Distrital de Santa Marta deberá proteger la información de la entidad, o en poder de ésta, almacenada o accesible desde los dispositivos móviles.

Evitar que los dispositivos móviles sean foco de infección y distribución de código malicioso dentro de la entidad y prevenir que éstos sean el origen de accesos no autorizados a las redes o recursos privados.

Alcance

Esta política aplica a todos los dispositivos móviles que manejen o accedan a información de la entidad.

Responsabilidades

- Las secretarías son responsables de velar por el cumplimiento de la presente política, así como de establecer los mecanismos de revisión apropiados.
- Los directores, coordinadores, jefes de oficinas, líderes de procesos son responsables de planificar acciones de sensibilización a su personal y proveedores autorizados respecto a la importancia de esta política.
- La Dirección de TIC es responsable por proveer los medios técnicos para el cumplimiento de la presente política.
- El personal y proveedores autorizados para utilizar dispositivos móviles son responsables por cumplir con lo establecido en la presente política.

8.8. FINALIZACIÓN O CAMBIO EN LA RELACION LABORAL

Los servidores públicos y contratistas de la Alcaldía Distrital de Santa Marta deben cumplir con las responsabilidades y deberes de seguridad de la información.

Alcance

Todo el personal, independientemente de su rol funcional o su relación contractual.

Responsabilidades

- Las secretarías son responsables por difundir la presente política a todo el personal, independientemente del cargo que desempeñen.
- El responsable de seguridad de la información debe velar por la difusión y cumplimiento de la política, siendo el Director, el responsable principal y último sobre dicho cumplimiento.
- La Dirección de Capital Humano será responsable de comunicar en tiempo y forma las finalizaciones o cambios en los vínculos a la unidad de sistemas de información y al servicio de seguridad del edificio, para que se deshabiliten los accesos lógicos y físicos que correspondan.

Descripción

Deberán retirarse los permisos de accesos lógicos y físicos, y niveles de autorización a toda persona que finalice o cambie su relación funcional o contractual. Todo usuario de servicios que posean claves de acceso o niveles de autorización y que finalizan su relación laboral ya sea en forma definitiva o transitoria (ej. destitución, renuncia, licencia sin goce de sueldo por períodos prolongados, finalización de contrato); así como aquellos que cambien su relación funcional (ej. pase en comisión, comisión de servicio “permanente”, traslados.) se le deberán retirar los permisos y niveles de autorización que ostenten hasta ese momento.

Este retiro deberá incluir:

- Correo Institucional: se dará de baja la cuenta de correo electrónico que para los fines institucionales se le otorgó oportunamente.
- Se eliminará el usuario de las listas de distribución de correo electrónico y grupos de trabajo.
- Otras aplicaciones: el usuario será dado de baja de todos los accesos a las diferentes aplicaciones en las que se encuentre activo
- Acceso a la red institucional: se bloqueará el acceso la nube institucional, y toda otra forma de acceso a archivos, carpetas y otra información compartida.
- Ingreso Físico: se le retirara a la persona el acceso a las diferentes áreas físicas de la entidad a las que estaba autorizado a acceder.

La inhabilitación (ya sea temporal o definitiva) debe realizarse inmediatamente al momento del cese, por lo cual las comunicaciones deberán efectuarse oportunamente, siendo responsables las áreas intervinientes.
Se debe definir un procedimiento específico que garantice el cumplimiento de la presente política.

8.9. PROTECCIÓN CONTRA SOFTWARE MALICIOSO

La Dirección de TIC se asegurará que la información y los sistemas informáticos que la procesan se encuentren protegidos contra software malicioso (por ejemplo: virus, gusanos, troyanos, spyware, adware intrusivo, crimeware, entre otros).

Alcance

Todos los sistemas informáticos que soportan los procesos de la entidad.

Responsabilidades

- Las secretarías son responsables de velar por el cumplimiento de la presente política y realizar las revisiones oportunas.
- La Dirección de TIC es responsable de la gestión técnica relacionada con la presente política.
- Los funcionarios, aprendices, practicantes, contratistas y proveedores deben cumplir con lo establecido en la presente política.

Descripción

Se debe utilizar una solución de antivirus corporativo que cumpla con los siguientes:

- Incluir dispositivos móviles como parte de la solución.
- Implementar la seguridad en la navegación por la web y el correo electrónico.
- Que cuente con un firewall como escudo de seguridad.
- Implementar y actualizar medidas de protección contra software malicioso.

La entidad debe:

- Definir procedimientos y responsabilidades de gestión para la protección de los sistemas ante software malicioso.
- Brindar capacitación al personal afectado en la operación y uso de la solución antivirus, así como cualquier otro mecanismo utilizado para la detección de software malicioso.
- Concientizar a los usuarios finales sobre las formas en las que se puede adquirir el software malicioso, los riesgos y problemas que acarrea, así como sobre el procedimiento que se debe seguir en caso de sospechar o constatar estar afectado (tanto en los equipos informáticos a los cuales accede regularmente como otros en los que haya detectado su presencia). Este procedimiento debe estar formalizado y difundido a nivel de todo el organismo.
- Contar con controles que prevengan y detecten el uso de software no autorizado (por ejemplo, lista blanca de aplicaciones), ya que estos pueden abrir la puerta a software malicioso.
- Contar con controles que eviten el acceso a sitios web maliciosos y/o no autorizados (por ejemplo, listas negras).
- Analizar periódicamente los sistemas informáticos en búsqueda de software malicioso.
- Analizar periódicamente los logs de los sistemas en búsqueda de actividades inusuales.

Todo equipo informático, tanto de escritorio, portátil, estaciones de trabajo y/o servidores, debe estar protegido por una solución técnica residente en el equipo contra software malicioso, gestionado de forma centralizada. Esta solución técnica, así como la base de

datos y registro de las amenazas a detectar, deben estar actualizadas y acompañarse de un procedimiento que coadyuve hacia un comportamiento preventivo de los usuarios, así como del personal especializado de TI.

8.10. GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Alcaldía Distrital de Santa Marta debe establecer lineamientos generales para la gestión de incidentes de seguridad de la información, con el fin de prevenir y mitigar el impacto de estos; basándose en el contexto de la entidad, concientización, reducción en tiempos de respuesta, estrategias para la recuperación y la generación de una base de conocimientos con lecciones aprendidas de eventos e incidentes.

Alcance

Toda persona que tenga legítimo acceso a los activos de información de la entidad, incluso aquellos gestionados mediante contratos con terceros y lugares relacionados.

Responsabilidades

- Todas las secretarías de la entidad son responsables por difundir la presente política a todo el personal, independientemente del cargo que desempeñe o su relación contractual y de brindar los recursos necesarios para el cumplimiento de esta.
- Los directores, coordinadores, jefe de oficinas son responsables de la seguridad de la información, la ejecución de los planes y demás actividades vinculadas a la gestión de incidentes y debe velar por el cumplimiento de esta política y realizar las revisiones periódicas y oportunas.
- Los funcionarios, aprendices, practicantes, contratistas y proveedores son responsables por dar cumplimiento a la presente política y reportar los eventos de seguridad que detecten, siguiendo los procedimientos operativos establecidos para tal fin.

Descripción

Es responsabilidad de cada uno de los funcionarios, contratistas, aprendices y practicantes de la entidad reportar de forma inmediata los eventos, incidentes o debilidades en cuanto a la seguridad de la información por medio de la mesa de ayuda.

- Establecer un proceso claro para la gestión de incidentes de seguridad.

8.11. CORREO ELECTRÓNICO

La Alcaldía Distrital de Santa Marta, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre los funcionarios y terceras partes. Por lo anterior proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

- Definir políticas de uso seguro del correo electrónico e internet.

Alcance

Todo funcionario y/o contratista que tenga legítimo acceso al uso del correo electrónico institucional.

Responsabilidades

La Dirección de TIC debe establecer e implantar controles o filtros que permitan detectar y proteger la plataforma de correo electrónico contra contenido o código malicioso que pudiera ser adherido y/o transmitido a través de los mensajes.

Descripción

Los mensajes y la información contenida en los correos electrónicos que sean emitidos desde la Alcaldía Distrital de Santa Marta a su entidad adscrita, dirigidos a direcciones de correo electrónico externas, que contengan información confidencial con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional de la Alcaldía Distrital de Santa Marta, deben incluir una nota (Disclaimer) como: *La información contenida en este mensaje es confidencial y tiene como único destinatario la persona a quien está dirigida* y en su defecto: *El sistema para el control de virus implementado, no asume ninguna responsabilidad por virus que pueda llevar este mensaje o sus anexos*. El correo institucional no debe ser utilizado para actividades personales.

Los mensajes y la información contenida en los buzones de correo son propiedad de la Alcaldía Distrital de Santa Marta y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

Los usuarios de correo electrónico institucional tienen prohibido el envío de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los funcionarios de la institución y el personal provisto por terceras partes.

No es permitido el envío de archivos que contengan extensiones ejecutables, en ninguna circunstancia; a excepción de los que, por su importancia, envíen los proveedores y/o contratistas que brindan soporte a los sistemas de información bajo contrato vigente.

Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por la Alcaldía Distrital de Santa Marta y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

8.12. INTERNET

La Alcaldía Distrital de Santa Marta debe regular el uso de Internet en la entidad.
Se considera Internet como una herramienta valiosa para la entidad, por lo que su uso está permitido y se promueve en tanto es compatible y contribuye al cumplimiento de las metas y objetivos estratégicos. Sin embargo, su uso indebido representa un riesgo por el impacto negativo que puede tener. Por tanto, deberán monitorearse y controlarse las conexiones que se realicen.

Alcance

Esta política aplica a todas las personas (ej.: personal, proveedor, organismos públicos, organismos internacionales, etc.) con acceso al servicio de Internet de la entidad.

Trazabilidad de registros

Toda actividad que se realice a través de Internet será monitoreada y se generarán registros con la trazabilidad de las conexiones, los cuales podrán ser revisados y analizados en oportunidad de un incidente o para análisis estadístico.
Estos registros serán entregados al responsable de seguridad de la información o al secretario que los solicite, bajo petición escrita y fundada, y su contenido será de conocimiento de los referidos y del personal técnico responsable de extraerlos de los sistemas de información.
Dichos informes no podrán ser divulgados y se tomarán las previsiones pertinentes respecto a su archivo y custodia.

Disponibilidad de servicios

Se proporcionará acceso a Internet con una serie de servicios básicos que incluyen:

- Libre navegación por los sitios cuyo contenido no esté comprendido dentro de las prohibiciones o limitaciones dadas por una norma legal aplicable o por esta política.
- Acceso a servicio de Correo Electrónico.
- Acceso a Servicio de Mensajería Instantánea.

La ampliación de servicios asignados a las personas alcanzadas por esta política debe gestionarse por escrito por el jefe o supervisor donde se desempeña y deberá obtener el aval técnico del área que corresponda.

La ampliación o reducción de servicios de internet, es revocable en cualquier momento por disposición del jefe de oficina y a petición fundada de los supervisores o el responsable de seguridad de la información.

Uso aceptable

El uso de Internet:

- Debe estar acorde con el marco legal vigente, respetando pautas establecidas.
- Debe tener como principal utilidad servir como herramienta para cumplir las tareas asignadas. El uso fuera de esta situación no debe interferir con el desarrollo de la actividad laboral.
- Debe estar regido por los principios de buenas prácticas, la moral y ética, así como en procura de un mejor desempeño y productividad de quien lo haga.

Uso inaceptable

El uso de Internet considerado inaceptable puede comprender la pérdida del acceso, dar lugar a la revocación de permisos sobre internet, una investigación administrativa y/o las sanciones legales aplicables.

Sin ser una lista taxativa, se considera uso inaceptable del servicio de internet los siguientes:

- Descargar material con expresa y manifiesta propiedad intelectual u otros derechos necesarios para dicha descarga o uso, sin los permisos necesarios, las licencias que correspondan o cualquier otro formalismo que deba cumplirse y se omite intencionalmente.
- Utilizar Internet para almacenamiento, divulgación o transmisión de cualquier información, archivos, documentos, imágenes, sonidos u obras que puedan infringir el marco normativo vigente referido a propiedad intelectual, marcas o patentes.
- Involucrarse o participar de cualquier manera en actividades ilícitas en cualquier sitio y desde cualquier dispositivo conectado a la red desde el servicio de Internet.
- Divulgación de información deliberadamente falsa, sensible o difamatoria sobre personas o instituciones en cualquier sitio o herramienta disponible en línea (correo electrónico, webs, wiki, redes sociales, chat, foros, etc.).
- Hacer uso del servicio de internet sin contar con herramientas básicas de resguardo y seguridad, instaladas en el computador o dispositivo a emplear, a saber: antivirus y las actualizaciones del sistema operativo que posea el computador o dispositivo. La validación de estas condiciones será determinada y pueden consultarse en el área técnica.
- Hacer uso de herramientas de software instaladas que habiliten servicios potencialmente riesgosos para la entidad. La validación de estas condiciones debe consultarse con el área técnica.
- El uso del servicio de internet en situaciones que afecten la dignidad humana tenga carácter discriminatorio u ofensivo, sean usados para amenazar y generar persecuciones a personas o empresas, generen situaciones de acoso laboral, sexual, contrarias a la moral, pornografía o similares.

Recursos institucionales de conectividad

La Alcaldía Distrital de Santa Marta se reserva el derecho de establecer la prioridad para la prestación del servicio de acceso a Internet y sus servicios en función de necesidades propias. Los usuarios del servicio aceptan tácitamente esta pauta de prestación de este.

8.13. USO INSTITUCIONAL DE REDES SOCIALES

La Alcaldía Distrital de Santa Marta debe gestionar de manera segura los perfiles de redes sociales utilizados por la entidad.

- Regular el uso de redes sociales para proteger la imagen y la información de la entidad.

Alcance

Todos los perfiles de carácter institucional utilizados por la entidad en las redes sociales.

La Alcaldía Distrital de Santa Marta, puede crear su perfil oficial en las redes sociales (por ejemplo: Instagram, Facebook, Twitter, YouTube) para dar a conocer sus

programas, actividades y otros temas de interés, y para tener un contacto directo con la ciudadanía o clientes, y de esta manera poder conocer sus necesidades y requerimientos. No obstante, se debe cumplir con los lineamientos expresados a continuación.

- La entidad no se hace responsable de los sitios web no propios a los que se puede acceder mediante vínculos (links) desde nuestros perfiles o de cualquier contenido puesto a su disposición por terceros, que incluyan fotos, documentos, vídeos y otros contenidos.
- Si se detecta un contenido potencialmente inseguro, se debe reportar al responsable de seguridad de la información, y eliminar si corresponde.
- Se debe tener claramente identificadas las personas (y sus correspondientes usuarios) con acceso a los perfiles en redes sociales, debiendo estos corresponder con cuentas institucionales y no personales.
- Las cuentas utilizadas para recuperación de los datos de acceso deben ser institucionales.
- Se deberá seguir las pautas y procedimientos definidos por la entidad, para el traspaso de usuarios en casos de cambio o desvinculación de los administradores de los perfiles.
- Siempre que la red social lo permita, se debe verificar la cuenta, de manera de garantizar a los ciudadanos o clientes que es la cuenta oficial de la entidad.
- La contraseña utilizada en cada cuenta de red social debe ser diferente; la misma deberá ser una contraseña segura conforme a las pautas establecidas en las políticas vigentes.

Responsabilidades

- Las secretarías son responsables por difundir la presente política a todo el personal, independientemente del cargo que desempeñe o de su relación contractual.
- El responsable de seguridad de la información debe velar por el cumplimiento de la presente política. Deberá identificar y promover los controles de seguridad de la información para habilitar el acceso a un proveedor a los activos de información.
- La Oficina de Comunicaciones Estratégicas debe velar por el contenido de lo que se publica en las redes sociales de carácter institucional.

8.14. COPIAS DE RESPALDO

Esta política define la estrategia para gestionar las copias de respaldo de información y de las aplicaciones de la Alcaldía Distrital de Santa Marta y tiene como objetivo asegurarse de obtener un respaldo de la información contenida en los servidores a fin de que, en caso de una eventualidad, se pueda continuar con la operación de la entidad.

La información de los servidores y demás sistemas serán respaldados mediante un método de copia de seguridad adecuado, igualmente, se debe utilizar un medio de almacenamiento apropiado o cualquier otro medio reconocido.

- Realizar y mantener copias de respaldo de la información crítica.

Alcance

Toda la información generada y/o procesada por la entidad de carácter institucional, con previa autorización del propietario o custodio del activo.

Responsabilidades

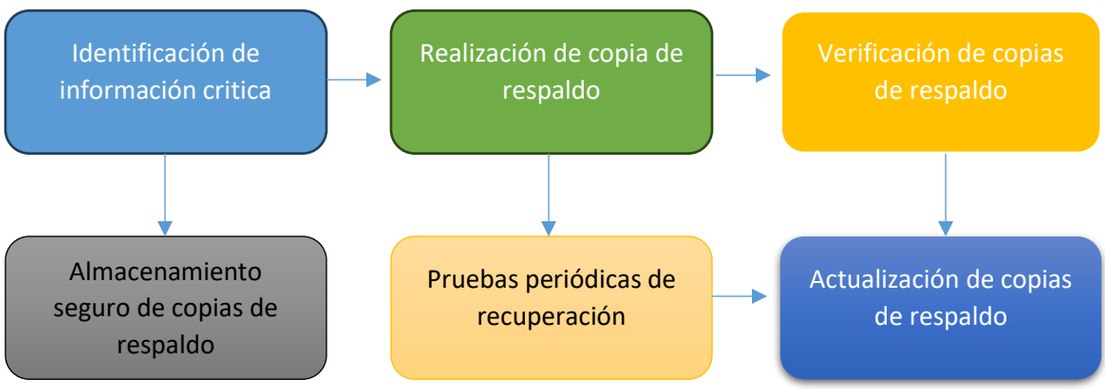
- Las secretarías son responsables por difundir la presente política a todo el personal, independientemente del cargo que desempeñe o de su relación contractual.
- Los funcionarios y contratistas de la Alcaldia Distrital de Santa Marta son responsables del respaldo de su información y de verificar que los respaldos de información se ejecuten correctamente, estos deben ser realizados en medios de almacenamiento digitales y entregados al custodio o jefe de cada área de la entidad.
- La Dirección de TIC es responsable de mantener custodiadas copias idénticas de respaldo de sistemas operativos que respondan a eventos de contingencia y disminuyan el impacto en caso de una falla, así como las copias de seguridad de los correos electrónicos que generan alto volumen de almacenamiento.

Respaldo de la información

La data de cada sistema de información debe ser respaldado regularmente sobre un medio de almacenamiento, tales como, nube de respaldo, cinta, CD, DVD, de acuerdo con lo definido con el propietario del activo. Los medios de almacenamiento deben ser custodiados con mecanismos de protección ambiental como detección de humo, incendio, humedad y mecanismos de control de acceso físico, de acuerdo con los procedimientos establecidos.

Se deben realizar pruebas periódicas de verificación de la información almacenada en los medios con el fin de verificar su integridad y disponibilidad, de acuerdo con los establecido en los procedimientos.

Todas las solicitudes de restauración de copia de seguridad y respaldos, así como la restauración las debe realizar el propietario o custodio de los activos a través de la Mesa de Ayuda colocando el respectivo Ticket o por correo electrónico. Las copias de respaldo y restauraciones realizadas deben ser registradas en los formatos elaborados para el control y ejecución de citado proceso.



La Dirección de TIC debe realizar las copias de seguridad de:

- Correos electrónicos con el límite de almacenamiento en la nube lleno.
- Bases de datos en producción.
- Software de aplicaciones.
- Sistemas operativos de los servidores.
- Software base de la Alcaldia Distrital de Santa Marta.

8.15. TELEFONIA IP

La Alcaldia Distrital de Santa Marta cuenta con un sistema de Telefonía IP conformado por una planta telefónica virtualizada bajo sistema operativo Linux lo cual permite tener capacidad para 150 extensiones telefónicas.

Alcance

Aplica a toda la infraestructura de Telefonía IP instalada en todas las dependencias de la entidad.

Responsabilidades

La Dirección de TIC es responsable de monitorear la plataforma de telefonía IP virtualizada, realizando el respectivo seguimiento y Up Time a la operación de la planta y las extensiones.

Las tareas de configuración, tales como, cambios de nombre, número, asignación de cuentas SIP, traslados, configuración de privilegios de todas las extensiones son realizadas por el operador privado que administra el servicio bajo contrato vigente.

9. DIRECTRIZ DE SUPERVISIÓN DE CONTRATOS CON TERCEROS

Los supervisores de contratos con terceros deben divulgar las políticas, normas y procedimientos de seguridad de la información de la Alcaldía Distrital de Santa Marta a dichos terceros, así como velar porque el acceso a la información y a los recursos de almacenamiento o procesamiento de ésta, por parte de los terceros se realice de manera segura, de acuerdo con las políticas, normas y procedimientos de seguridad de la información.

10. ARTICULACION CON MIPG

Para asegurar una gestión integrada y articulada dentro del MIPG, la política de seguridad y privacidad de la información bebe:

- Alinear los objetivos de seguridad y privacidad con los objetivos estratégicos de la Alcaldía.
- Incorporar indicadores de desempeño en seguridad y privacidad en el sistema de monitoreo y evaluación del MIPG.
- Establecer mecanismos de retroalimentación para mejorar continuamente los procesos de seguridad y privacidad.
- Integrar la formación en seguridad y privacidad de la información dentro de los programas de desarrollo de competencias del MIPG.

11. POLÍTICA DE CUMPLIMIENTO

La Alcaldía Distrital de Santa Marta deberá lograr que todas las obligaciones legales, reglamentarias y contractuales que afectan a la entidad estén debidamente identificadas, documentadas y actualizadas. Todas las operaciones de la entidad.

Responsabilidades

- La Alta Dirección es responsable por identificar toda la normativa aplicable con el fin de cumplir con los requisitos de acuerdo con el contexto en el que cumple sus funciones, teniendo en cuenta aspectos legales y regulatorios, contratos, etc.

- Todas las dependencias son responsables de velar por el cumplimiento de la presente política.

12. MONITOREO

Se realiza una revisión periódica de todos los elementos como son los equipos de red, servidores y firewall para verificar su funcionamiento, en caso de detectar una falla o anomalía se toman los correctivos del caso. Estos eventos son recopilados en una bitácora para llevar un registro de las incidencias.

13. REVISIÓN

La presente Política estará a cargo de La Dirección de TIC de la Alcaldía Distrital de Santa Marta y esta se revisará cuando sea considerado necesario.

14. VALIDEZ DE LA POLITICA

La presente política es aplicable a partir de su aprobación.

Se destaca que el incumplimiento de la presente política aumenta la exposición de la información y el riesgo de tener un incidente de seguridad de la información. Ante la verificación de un incumplimiento la Alta Dirección podrá tomar las medidas que se considere pertinentes, a efectos de darle el debido cumplimiento

15. REFERENCIAS

- Función Pública. (2022). Guía para la Administración del Riesgo y el diseño de controles en entidades públicas - Versión 6. https://www.funcionpublica.gov.co/documents/28587410/34299967/Guia_administracion_riesgos_capitulo_riesgo_fiscal.pdf

- Función Pública. (2014). Ley 1712 de 2014 - Transparencia y del derecho de acceso a la información pública. https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=56882

- Función Pública. (2012). Ley 1581 de 2012 - Protección de datos personales. https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981

- Función Pública. (s.f.). MIPG https://www1.funcionpublica.gov.co/web/mipg

- MinTIC. (2016). Seguridad y Privacidad de la Información - Elaboración de la política general de seguridad y privacidad de la información. Guia No. 2 https://mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

- NQA. (2013) ISO 27001:2013 Guía de Implantación para la seguridad de la información https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

- NTC-ISO 9001:2015 - Sistemas de Gestión de la Calidad. Fundamentos y Vocabulario.

- NTC-ISO 9001:2015 - Sistemas de gestión de la calidad. Requisitos. https://www.guadalupanolasalle.edu.co/sgc/ISO9001-2015-Requisitos.pdf

- Villamizar, Carlos. (2023). Global Suite. Los principales cambios de la actualización de la norma ISO 27002:2022 https://www.globalsuitesolutions.com/es/cambios-norma-iso-27002-2022/

16. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS	
Versión	**Descripción de la modificación**
1	Creación del documento
2	Ajustes año 2024 acuerdo con la articulación MIPG y normas de MINTC

ELABORO	REVISO	APROBO
Nombre: **Jorge González** Cargo: **Profesional Universitario** Fecha: **mayo 31 2024** **Firma:**	Nombre: **Jhon Fredy Velázquez** Cargo: Profesional Especializado Fecha: 16-07-2024 **Firma:**	**COMITÉ GESTION DE DESEMPEÑO**
Nombre: **Jackelines Granados** Cargo: **Técnico administrativo - SIG** Fecha: 28-06-2024 **Firma:**	**Nombre: Rigoberto García Guillot** **Cargo: Director TIC** **Fecha:** 18-07-2024 **Firma:**	