Tabla de contenido

INTRODUCCIÓN.

GENERALIDADES.

1. INTRODUCCIÓN 4

2. OBJETIVOS: 5

3. ALCANCE 5

4. MARCO LEGAL Y/O NORMATIVO 5

4.1 Documentos de referencia 6

4.2 Definiciones 6

5. RESPONSABILIDADES 8

5.1 Compromiso de la Dirección General 8

5.2 Compromiso Comité Institucional de Gestión y Desempeño 8

5.3 Compromiso de Control Interno 8

5.4 Compromiso proceso Gestión TIC 8

5.5 Responsabilidades de los propietarios de los activos de información 9

5.6 Responsabilidades de los funcionarios, contratistas y terceros usuarios de la información 9

5.7 Responsabilidades generales referente al MSPI – Política de seguridad de la información 9

5.8 Organización interna 9

6. GESTIÓN DE ACTIVOS 10

6.1 Responsabilidad por los activos 10

6.2 Inventario de activos 10

6.3 Propiedad de los activos 10

6.4 Uso aceptable de los activos 10

6.5 Clasificación de la información 11

6.6 Etiquetado y manejo de información 11

6.7 Responsabilidad por los Activos 11

6.8 Clasificación de la Información 12

7. SEGURIDAD DE LOS RECURSOS HUMANOS 12

7.1 Roles y responsabilidades 12
7.2 Selección 12
7.3 Términos y condiciones laborales 13
7.4 Durante la vigencia de la contratación 13
7.5 Responsabilidades de la dirección 13
7.6 Concientización sobre la seguridad de la información 13
7.7 Proceso disciplinario 13
7.8 Terminación o cambio en la contratación 14
7.8.1 Devolución de activos informáticos 14
8. SEGURIDAD FÍSICA Y DEL ENTORNO 15
8.1 Áreas seguras 15
8.2 Controles de acceso físico 15
8.3 Seguridad de oficinas, recintos e instalaciones 15
8.4 Protección contra amenazas externas y ambientales. 15
8.5 Seguridad de los equipos 15
8.6 Servicios de suministro 16
8.7 Mantenimiento de los equipos 16
8.7.1 Seguridad de los equipos fuera de las instalaciones 16
8.7.2 Seguridad en la reutilización o eliminación de los equipos. 17
9. GESTIÓN DE COMUNICACIONES Y OPERACIONES 17
9.1 Procedimientos operacionales y responsabilidades 17
9.2 Gestión del cambio. 17
9.3 Distribución de funciones 17
9.4 Separación de las instalaciones de desarrollo, pruebas y producción 19
9.5 Protección contra códigos maliciosos y móviles 19
9.6 Respaldo 19
9.7 Gestión de la seguridad de las redes 20
9.8 Manejo de los medios 20
9.8.1 Gestión de los medios removibles 20
9.8.2 Eliminación de los medios 20
9.8.3 Mensajería electrónica 20

9.8.4 Transacciones en línea 21

10. CONTROL DE ACCESO 21

10.1 Uso de contraseñas 21

10.2 Lineamientos de escritorio despejado y de pantalla despejada 21

10.3 Uso de los servicios de red. 22

10.4 Autenticación de usuarios para conexiones externas 22

10.5 Control de conexión a las redes 22

10.6 Controles criptográficos 22

11. GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN 22

11. 1 Responsabilidades incidencias seguridad de la información 23

12. Control de cambios 24

1. INTRODUCCIÓN

La gestión de la seguridad de la información coordina esfuerzos para asegurar y preservar los activos de información de la Fundación Gilberto Alzate Avendaño, basado en la adopción de lineamientos técnicos y legales con el objetivo de fortalecer la confidencialidad, integridad disponibilidad y no repudio de la información, mediante una adecuada administración del recurso humano y tecnológico, esta política debe ser aplicada por todos los (as) funcionarios (as), contratistas, proveedores, consultores y todo personal externo que utilice los servicios informáticos que ofrece la entidad, deben conocer y aceptar el reglamento vigente sobre su uso, el desconocimiento del mismo, no exonera de responsabilidad al usuario.

La presente política busca el fortalecimiento de la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, en la entidad y está determinado por la adopción objetiva, de los requisitos de seguridad de acuerdo a los procesos, tamaño y estructura de la Fundación, cabe resaltar, que sin un apropiado control se propicia un desordenado y confuso entorno, generando inseguridad, para ello es necesario emplear actividades encaminadas a mitigar el riesgo.

Los servicios de la red institucional son de uso exclusivo operativo, misional y para gestiones administrativas relacionados con la actividad de la Fundación Gilberto Álzate, donde sus objetivos estratégicos promueven:

1. Mejorar la calidad de vida de la ciudadanía al ampliar el acceso a la práctica y disfrute del arte y la cultura como parte de su cotidianidad en condiciones de equidad.
2. Potenciar a los creadores del Centro que quieran expresarse y ver en el arte, la cultura y la creatividad una forma de vida.
3. Impulsar la reactivación física, económica y social del sector del antiguo Bronx y articularlo con las comunidades y territorios del centro de la ciudad a partir del arte, la cultura y la creatividad.
4. Aumentar la apropiación del Centro de la ciudad como un territorio diverso, de convivencia pacífica, encuentro y desarrollo desde la transformación cultural.
5. Consolidar modelos de gestión, desarrollando capacidades del talento humano y optimizando los recursos tecnológicos, físicos y financieros para dar respuesta eficaz a las necesidades de la ciudadanía y grupos de valor.

Siendo así, la información se convierte en un activo de suma importancia para lograr cumplir los objetivos mencionados con anterioridad, cabe resaltar que la alta dirección trabaja constantemente para velar por su protección a través de acciones promovidas desde el proceso de Gestión TIC donde el comité de gestión y desempeño aprueba los documentos asociados al Modelo de Seguridad de la Información y las acciones que se derivan de ello. Con base a lo descrito anteriormente servicios, como correo electrónico, internet, intranet, aplicaciones y sistemas de información son de uso exclusivo en el desarrollo de las funciones y actividades de la entidad, por lo tanto, queda restringido el uso para otros fines como los comerciales o personales, resaltando que a través de las acciones de no repudio, si se logra identificar a través de las diferentes transacciones que el emisor y/o receptor hizo una actividad no convencional, no se podrá negar la acción dado que las evidencias de su actividad quedan alojados en los diferentes servicios TIC, de igual forma que la posesión de un documento y su firma electrónica asociada será prueba efectiva del contenido y del autor del documento.

Dicho lo anterior y en concordancia a La ley 1581 de 2012 y el Decreto 1377 de 2013, implementa el Régimen General de Protección de Datos Personales, el cual desarrolla el derecho constitucional que tienen todas las

personas a conocer, actualizar y rectificar todo tipo de información recogida o que haya sido objeto de tratamiento de datos personales en bancos o bases de datos y en general en archivos de entidades públicas y/o privadas.

Para dar cumplimiento a lo previsto en esta normatividad, La Fundación Gilberto Álzate Avendaño, tiene una serie de documentos publicados en su página web en link de transparencia (https://fuga.gov.co/transparencia-y-acceso-a-la-informacion-publica/normativa/politicas-de-seguridad-de-la-informacion-del-sitio) para la ciudadanía en general y colaboradores, donde se describen principalmente las actividades que realiza la entidad para proteger, manejar y mantener la información personal, la cual es recopilada en diferentes bases de datos, para el desarrollo de sus funciones o actividades. Dicha información puede ser conocida, actualizada y rectificada por cada persona en el momento que lo requiera.

2. OBJETIVOS:

Garantizar las acciones operativas, técnicas y administrativas necesarias para la protección de los activos de información de la Fundación Gilberto Alzate, así como el cumplimiento de los requisitos legales, contractuales y normativos aplicables a la Entidad.

Implementar y mejorar continuamente el Modelo de Seguridad y Privacidad de la Información – MSPI, liderado por MINTIC.

Integrar la seguridad de la información a la estrategia general de entidad, gestionar los riesgos y fortalecer los componentes asociados a la integridad, disponibilidad, confidencialidad y no repudio de la información.

Cumplir con los controles de seguridad para el cumplimiento normativo y regulatorio de la Entidad.

3. ALCANCE

Las políticas aquí definidas aplican a todos los funcionarios de planta permanente, provisionales, contratistas y proveedores que tienen acceso o interactúan con los activos de información de la organización, así como a todos los sistemas, redes y dispositivos utilizados para procesar, almacenar o transmitir información. El alcance de esta política incluye tanto los entornos físicos como virtuales de la entidad, tanto en las instalaciones de la empresa como en ubicaciones remotas o fuera de las instalaciones. Además, la política de seguridad se aplica a todos los datos confidenciales, personales y comerciales propiedad de la organización, así como a la infraestructura tecnológica utilizada para su gestión y protección
.

4. MARCO LEGAL Y/O NORMATIVO

El marco legar y normativo que cobija la presente política se encuentra en el normograma institucional él es actualizado por el proceso Gestión TIC y verificado por la oficina Jurídica periódicamente y se encuentra publicado para consulta en la página web de la FUGA: (https://www.fuga.gov.co/transparencia-y-acceso-a-la-informacionpublica/normativa/normograma?field_calificacion_de_la_norma_target_id=90&field_fecha_de_emision_value=All) la entidad se acoge las normas vigentes de seguridad de información, protección de datos

personales y directrices de ciberseguridad a nivel nacional y territorial aplicando las prácticas y estándares recomendados para su cumplimiento.

4.1 Documentos de referencia

Documento	Contenido del documento	Código
Decreto Distrital	Por medio del cual se adopta el Modelo Integrado de Planeación y Gestión Nacional y se dictan otras disposiciones	591 de 2018
Norma Técnica Internacional ISO 27001, 27002, 27005	Norma internacional emitida por la Organización Internacional de Normalización (ISO) para gestionar la seguridad de la información en una organización pública o privada	ISO/IEC 27001, 27002, 27005
Norma Técnica Internacional ISO 31000: 2018	Es el estándar para la gestión de riesgos y describe cuatro pasos básicos – Identificación de riesgos, análisis de riesgos, valoración de riesgos y tratamiento de riesgos– para llevar a cabo un proceso de evaluación de riesgos exitoso; esto con el fin de identificar aquellas amenazas que pueden ser un obstáculo para que la organización logre sus metas.	ISO/IEC 31000
Manual de Gobierno Digital	Para la Implementación de la Política de Gobierno Digital, entidades del orden nacional; Modelo de Seguridad y Privacidad de la Información-MSPI; Formato Política SGSI – MSPI para la Política de Gobierno Digital.	Versión 7
Documento Maestro del Modelo de Seguridad y Privacidad de la Información marzo 2021	Actualización del documento para la implementación del modelo MSPI en las entidades del estado	Versión 4

4.2 Definiciones

Procedimiento: Detalle de cursos de acción y tareas que deben realizar los usuarios para hacer cumplir las definiciones de las normas.

Estándares técnicos: Conjunto de parámetros específicos de seguridad para cada una de las tecnologías informáticas utilizadas.

Confidencialidad: La información solo puede ser conocida por las personas definidas.

Integridad: La información solo puede ser creada y/o modificada por las personas autorizadas.

Disponibilidad: La información esté disponible cuando lo necesite el usuario.

Incidentes de Seguridad: Es cualquier evento que comprometa la confidencialidad, integridad y disponibilidad de la información de la organización

Política: Son instrucciones mandatorios que indican la intención de la alta gerencia respecto a la operación de la organización.

Recurso Informático: Elementos informáticos (base de datos, sistemas operacionales, redes, sistemas de información y comunicaciones) que facilitan servicios informáticos.

Información: Puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

Ataque cibernético: intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado a accederlo, por lo general con intenciones insanas y perjudiciales.

Brecha de seguridad: deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en sí misma, sea o no protegida por reserva legal.

Seguridad organizacional: Debe sustentar servicios o contrataciones externas a la infraestructura de seguridad, Integrando el recurso humano con la tecnología, denotando responsabilidades y actividades complementarias como respuesta ante situaciones anómalas a la seguridad.

Seguridad lógica: Establecer mecanismos y procedimientos, que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades, perfiles de seguridad, control de acceso a las aplicaciones y documentación sobre la gestión de soporte en sistemas, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, selección y aceptación de sistemas, hasta el control de software malicioso.

Seguridad Física: Cumplir en cuanto a perímetros de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas con base en la importancia de los activos.

Seguridad Legal: Integra los requerimientos de seguridad que deben cumplir todos los funcionarios y usuarios de la red institucional bajo la reglamentación de la normativa interna de políticas y manuales de procedimientos.

Firewall: Es una parte de un sistema diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

5. RESPONSABILIDADES

5.1 Compromiso de la Dirección General

La Dirección General debe acreditar su compromiso con el establecimiento, implementación, operación, seguimiento y revisión del Modelo de seguridad y privacidad de la información

A través del Comité Institucional de Gestión y Desempeño el cual es responsable de la aprobación y de realizar el seguimiento a la estrategia de implementación de la presente política, así mismo de la aprobación de controles técnicos asociados a la normatividad especifica emitidos por Gestión TIC.

5.2 Compromiso Comité Institucional de Gestión y Desempeño

- Analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario de acuerdo al procedimiento almacenado en Gestión TIC.
- Verificar el cumplimiento de las políticas de seguridad de la información aquí mencionadas.
- Aprobar controles restrictivos que impacten a la comunidad institucional.

5.3 Compromiso de Control Interno

Las auditorías y seguimientos a la gestión de tecnologías de la información se realizarán conforme a los lineamientos definidos por el jefe de la oficina.

5.4 Compromiso proceso Gestión TIC

- El proceso es responsable de la elaboración y/o modificación y/o actualización y/o eliminación e implementación, monitoreo y seguimiento de la Política de Seguridad de la Información, asegurando así los recursos adecuados.
- Informar de los eventos que estén en contra de la seguridad de la información y de la infraestructura tecnológica.
- Proporcionar medidas de seguridad físicas, lógicas y procedimentales para la protección de la información digital de la Entidad.
- Brindar el soporte necesario a los usuarios a través de los canales de mesa de ayuda actualmente implementados en la entidad.
- Implementar los mecanismos de controles necesarios y pertinentes para verificar el cumplimiento de la presente política.

5.5 Responsabilidades de los propietarios de los activos de información

Son propietarios de la información cada uno de los líderes de las oficinas donde se genera, procesa y mantiene información, en cualquier medio.

Valorar y clasificar la información que está bajo su administración y/o generación, aplicando los formatos y guías correspondientes que abarcan procesos como gestión documental y Gestión TIC en el tratamiento de la información.

5.6 Responsabilidades de los funcionarios, contratistas y terceros usuarios de la información

Los(as) funcionarios(as), contratistas y terceros que realicen labores en o para la Fundación, tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información.

Usar software autorizado que haya sido adquirido legalmente por la entidad, no está permitido la instalación ni uso de software diferente al Institucional sin el consentimiento de sus superiores y visto bueno Gestión TIC.

Evitar la divulgación no autorizada o el uso indebido de la información.

La Dirección General y la oficina de Control Interno de la entidad puede solicitar una inspección de la información a su cargo sin importar su ubicación o medio de almacenamiento, por lo cual los los(as) funcionarios(as), contratistas y terceros deberán responder ante dichas solicitudes.

5.7 Responsabilidades generales referente al MSPI – Política de seguridad de la información

La aplicación de la gestión de la política de seguridad de la información, busca brindar asesoría a la dirección para la protección adecuada de los activos de información.

El presente documento se debe publicar y comunicar a todas las partes interesadas del mismo modo se debe revisar una vez al año su aplicabilidad con relación a su eficacia y eficiencia. El link donde se realizará la publicación una vez aprobada la política corresponderá a su sitio web (https://fuga.gov.co/transparencia-y-acceso-a-la-informacion-publica/normativa/politicas-de-seguridad-de-la-informacion-del-sitio)

5.8 Organización interna

Compromiso: Con relación a este criterio La Dirección General debe apoyar activamente la seguridad, demostrando el compromiso existente con los criterios de su implementación aplicando las directrices y controles que el proceso de Gestión TIC solicite en conjunto con las directrices emitidas por la subdirección de gestión corporativa.

Coordinación de la seguridad de la información: Se deben involucrar las partes relacionadas en la presente política y que cada una asuma el rol que le compete de acuerdo a la necesidad que se tenga en el momento de realizar la solicitud.

Acuerdos sobre confidencialidad: Se deben realizar las validaciones correspondientes con el apoyo de los procesos de talento humano y la oficina jurídica lo cual permita identificar las posibles actualizaciones de los documentos relacionados con funcionarios de planta y contratistas respectivamente, siempre velando por la protección de la información.

Identificación de riesgos: Se realizarán las mesas de trabajo aplicando la metodología de riesgos gestionada por la oficina de planeación de la entidad en concordancia con los diferentes procesos, teniendo como prioridad la identificación referenciada a la protección de activos de información.

6. GESTIÓN DE ACTIVOS

6.1 Responsabilidad por los activos

Mantener la protección adecuada de los activos de la entidad mediante la aplicación de procedimientos políticas guías y/o sensibilizaciones emitidas por el proceso de recursos físicos perteneciente a la subdirección de gestión corporativa.

6.2 Inventario de activos

Aplicar los procedimientos referenciados en los procesos de apoyo de recursos físicos y tecnología de la Fundación, referenciando la gestión de activos tangibles (consumo y devolutivos), intangibles (licencias) y lógicos digitales (bases de datos y activos de información) con roles y responsabilidades para acceso a la información sobre los cuales se aplicarán regulaciones internas para el uso controlado y seguro de la misma.

6.3 Propiedad de los activos

Toda la información y los activos asociados con los servicios de procesamiento de información son propiedad específica del emisor, lo cual indica que es responsabilidad el tratamiento y custodia, se deben articular con Gestión TIC para el backup cuando esta información se encuentre en medio digital sea base de datos o cliente servidor, dicha comunicación se hará a través de los medios oficiales para tal fin y de acuerdo a la política expresa en el procedimiento definido.

6.4 Uso aceptable de los activos

La Fundación implementa las directrices para lograr y mantener la protección y uso de los activos de información, mediante la asignación a los usuarios responsables desde varios aspectos, uno de ellos corresponde a la firma de inventarios y/o recepción de solicitudes relacionadas con inventarios el otro aspecto es a través de correo referentes a la publicación de información de los activos de información definidos por las diferentes

dependencias en un formatos especifico definido y aplicado en una guía que se encuentra en el proceso de Gestión TIC.

6.5 Clasificación de la información

La información se debe clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la entidad. Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de vídeo, música, y fotos y cualquier tipo de archivo que no sean de carácter institucional.

Las reglas específicas definidas en la presente política y en políticas asociadas se dictamina que el proceso encargado de clasificar y tipificar la información es Gestión Documental de la entidad bajo las directrices especificas aprobadas por las tablas de retención documental (TRD).

6.6 Etiquetado y manejo de información

Se desarrollan bajo los procedimientos establecidos en el proceso Gestión documental de acuerdo al esquema de clasificación adoptado por la entidad**.**

Se deben desarrollar e implementar acciones para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por la entidad.

Gestionar el activo de información como un elemento definible e identificable que almacena registros, datos o información en cualquier tipo de medio, cabe resaltar que en la entidad se consideraron las siguientes características:

- El activo de información es reconocido como valioso para la Fundación.
- No es fácilmente reemplazable sin incurrir en costos, habilidades especiales, tiempo, recursos o la combinación de los anteriores.
- Los niveles de clasificación de la información valiosa que se ha establecido son Información pública reservada, Información pública clasificada (privada y semi-privada), Información pública, de acuerdo Guía metodológica de gestión de activos de información GT-GU-01 y el GT-FT-10.

6.7 Responsabilidad por los Activos

- La Dirección debe nombrar un responsable de activos en cada una de las áreas de la Fundación Gilberto Álzate.

- Los líderes de proceso de la FUGA, son responsables de mantener o proteger los activos de mayor importancia.

6.8 Clasificación de la Información

- Cada líder de proceso dará importancia a la información en base al nivel de clasificación que demande el activo.
- La información pública puede ser visualizada por cualquier persona dentro o fuera de la entidad.
- La información interna, es propiedad de la Fundación Gilberto Álzate, en ningún momento intervendrán personas ajenas a su proceso o manipulación.
- La información confidencial es propiedad absoluta de la entidad, el acceso a ésta es permitido únicamente al personal administrativo autorizado para ello, teniendo en cuenta la naturaleza de sus funciones u obligaciones.
- Los niveles de seguridad se detallan como nivel de seguridad bajo, nivel de seguridad medio y nivel de seguridad alto.
- Los permisos asignados para el acceso a la información, en el software que apoya la gestión documental al interior de la entidad, en principio se centra en una restricción sobre los expedientes de historias laborales y procesos disciplinarios, dicho lo anterior mientras no se realice una solicitud aprobada por gestión documental y la subdirección corporativa no se generan cambios para restringir otros expedientes, por tal motivo se cataloga el resto de información como pública.

7. SEGURIDAD DE LOS RECURSOS HUMANOS

Informar al personal desde su ingreso y en forma continua, cualquiera sea su situación laboral con la entidad, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad, esto deberá realizarse en el marco de los procesos de inducción, reinducción o a través de las distintas herramientas de comunicación que la entidad tiene dispuesto para socializar la información institucional.

7.1 Roles y responsabilidades

Cuando un individuo es contratado para un rol de seguridad de la información específico, debe asegurar q ue el candidato tenga la competencia necesaria para desempeñar el rol de seguridad; validando idoneidad para desempeñar el rol, especialmente si es crítico para la organización.

7.2 Selección

Se deben realizar revisiones para la verificación de antecedentes de los candidatos a ser empleados, contratistas o usuarios de terceras partes, de acuerdo con los reglamentos, la ética y las leyes pertinentes, y deben ser proporcionales a los requisitos del negocio, la clasificación de la información a la cual se va a tener acceso y los

riesgos percibidos. La entidad realizará los controles previos de verificación del personal en el momento en que se solicita el cargo/contratista. Estos controles incluyen antecedentes disciplinarios, procuraduría, personería y judiciales y todos los aspectos que a tal efecto requiera la entidad.

7.3 Términos y condiciones laborales

Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes deben estar de acuerdo y firmar los términos y condiciones de su contrato laboral, el cual debe establecer sus responsabilidades y las de la organización con relación a la seguridad de la información.

7.4 Durante la vigencia de la contratación

Asegurar que todos los empleados, contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respecto a la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, al igual que reducir el riesgo de error humano.

7.5 Responsabilidades de la dirección

La Dirección debe exigir que los empleados, contratistas y usuarios de terceras partes apliquen la seguridad según las políticas y los procedimientos establecidos por la entidad.

Todos los usuarios de la infraestructura interna y externa de la Fuga cuando sea pertinente recibirán una adecuada capacitación y/o inducción y reinducción en materia de normas que permitan comprender los requerimientos de seguridad y las responsabilidades legales.

7.6 Concientización sobre la seguridad de la información

Se habilitarán los medios técnicos necesarios para comunicar y socializar a todo el personal, eventuales modificaciones o novedades en materia de seguridad, puede ser por el boletín de comunicaciones enviado por correo electrónico por parte de la oficina de comunicaciones o inclusive por los grupos establecidos vía WhatsApp.

7.7 Proceso disciplinario

El proceso de Gestión TIC publicará en la web el documento Política de Seguridad de la Información, donde se socializa su contenido. (https://www.fuga.gov.co/transparencia-y-acceso-a-la-informacion-publica/normativa/politicas-de-seguridad-de-la-informacion-del-sitio)El desconocimiento de la política de seguridad de la información de la Fundación, por parte de funcionarios, contratistas y terceros puede generar acciones disciplinarias. Las investigaciones disciplinarias y las respectivas sanciones les corresponden a las instancias autorizadas por la entidad.

Actuaciones que conllevan a la violación de la seguridad de la información:

- No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.
- No realizar la debida custodia de la información y de los activos de información a su cargo.
- Hacer uso de la red de datos de la institución, para obtener, mantener o difundir en los equipos de sistemas, material pornográfico u ofensivo, cadenas de correos para fines no institucionales y correos masivos no autorizados.
- Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de la plataforma tecnológica institucional.
- Enviar información pública reservada o información pública clasificada (privada o semiprivada) por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación.
- Los equipos, dispositivos portátiles o móviles entregados para actividades no están bien protegidos y mantenidos en buen estado.
- Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizado por el proceso de Gestión TIC.

7.8 Terminación o cambio en la contratación

- Todos los colaboradores al finalizar su relación contractual con la Fuga deberán tramitar el formato Paz y salvo retiro de personal y/o contratista TH-FT-04.
- La gestión del paz y salvo, que deberá realizarse por Orfeo e iniciará por el proceso Talento Humano.
- El paz y salvo será diligenciado y verificado por cada responsable en el orden establecido en la correspondiente tabla relacionada en el formato correspondiente.
- Si quien se desvincula es contratista, SÓLO debe diligenciarse la tabla para “CONTRATISTA”.
- Cada paz y salvo deberá estar en Orfeo asociado al expediente contractual o historia laboral de la persona que se desvincula, según sea el caso
- La firma de este documento por parte de los responsables de la entidad, encargados de verificar cada actividad, da cuenta de si quien se desvincula cumplió o no con cada una de dichas actividades. El paz y salvo no requiere la firma de quien se desvincula, el proceso de Gestión TIC, será el último en firmar el paz y salvo y finalizar.
- Si se quiere realizar algún comentario o precisión sobre las actividades y su cumplimiento, en especial cuando se establezca que quien se desvincula NO CUMPLIÓ con alguna actividad, debe efectuarse en el recuadro de OBSERVACIONES ubicado al final de este documento, identificando la actividad a la que se hace referencia.

7.8.1 Devolución de activos informáticos

Todos los colaboradores que tengan asignados este tipo de elementos deben devolver todos los activos pertenecientes a la organización que estén en su poder al finalizar su contratación, en las mismas condiciones entregadas, Gestión TIC realizara un diagnóstico visual y físico e informará al proceso de recursos físicos el estado del equipo.

- Así mismo Gestión TIC validará antes de la firma del paz y salvo que los administradores de los diferentes sistemas de información desactiven las cuentas de usuario y aplicará el procedimiento GT-PD-04 Asignación de cuentas.
- El administrador del dominio deberá verificar el vencimiento de la cuenta e inactivar las credenciales, con el fin de asegurar, que el usuario no pueda iniciar una sesión con las credenciales que en su momento le fueron otorgadas.
- El administrador de la plataforma del correo electrónico, procederá a generar una copia del contenido del buzón del correo y de la información que tenga almacenada en la unidad de drive.

8. SEGURIDAD FÍSICA Y DEL ENTORNO

8.1 Áreas seguras

Evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información. El centro de cómputo, los cuartos de distribución del cableado lógico y eléctrico y el cuarto de ubicación de las UPS en el sótano deben ser lugares de acceso restringido y cualquier persona que ingrese a ellos deberá estar acompañada permanentemente por el personal profesional de Gestión TIC.

8.2 Controles de acceso físico

- Aplicar gestión de ingresos con un área de recepción con vigilancia u otro medio para controlar el acceso físico al sitio o edificación, esto se realiza básicamente con la intervención del equipo de vigilancia de la entidad, quienes realizan los controles asociados al numeral correspondiente.
- Está prohibido prestar el carné de identificación, se considera como suplantación de identidad por parte de la persona que lo usa sin ser la persona autorizada.

8.3 Seguridad de oficinas, recintos e instalaciones

- El ingreso de computadores debe ser registrado en la minuta de vigilancia al ingreso de cada persona.
- Tener un registro de la fecha y hora de entrada y salida de colaboradores y visitantes.
- Establecer que el acceso a las áreas en las que se procesa o almacena información confidencial o financiera debe ser restringido a los individuos autorizados.

8.4 Protección contra amenazas externas y ambientales.

Contar con sistema de alarmas y monitoreo de cámaras, y así mismo, estar probadas, para establecer el nivel requerido de acuerdo con normas y deben funcionar de manera segura de acuerdo a los lineamientos, dicha actividad liderada por el equipo de recursos físicos de la entidad y en operación por parte del proveedor de vigilancia de la entidad.

8.5 Seguridad de los equipos

Los equipos de cómputo (computadores, servidores, equipos de comunicaciones, entre otros) no deben moverse o reubicarse sin la aprobación previa del proceso Gestión TIC y el correspondiente acompañamiento técnico.

8.6 Servicios de suministro

Los equipos tecnológicos de la Fuga están protegidos contra posibles fallas en el suministro de energía u otras anomalías eléctricas. De esta forma se asegura la continuidad del suministro de energía:

- Múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.
- Suministro de energía interrumpida mediante UPS para asegurar el apagado regulado.
- Equipos de UPS inspeccionados y probados periódicamente para asegurar que funcionan correctamente.

8.7 Mantenimiento de los equipos

Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad. Se realizará el mantenimiento periódico de los equipos informáticos para asegurar su disponibilidad e integridad permanentes, para ello el proceso de Gestión TIC en el marco del PETI realiza la vinculación de un cronograma de actividades de mantenimiento.

- Únicamente el personal calificado y autorizado puede realizar actividades de mantenimiento y llevar a cabo reparaciones o modificaciones en los equipos tecnológicos.
- Se registrarán todos los mantenimientos preventivos y las acciones correctivas que se realicen en los equipos tecnológicos.
- Establecer que solo el personal de mantenimiento autorizado debería llevar a cabo las reparaciones y el servicio a los equipos activos y servidores.
- Establecer que antes de volver a poner el equipo en operación después de mantenimiento, se debería inspeccionar por el grupo de tecnología para asegurarse de que no ha sido alterado y que su funcionamiento es adecuado.

8.7.1 Seguridad de los equipos fuera de las instalaciones

Se debe suministrar seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización. Los activos retirados de las instalaciones de la FUGA deben ser reportadas en las minutas correspondientes del equipo de vigilancia, si se requiere de autorización especial esta deberá ser diligenciada, autorizada y enviada al proceso de recursos físicos, de igual forma la responsabilidad del cuidado y del salvamiento del activo le corresponde a la persona que figura en el inventario.

- Identificar a los empleados y usuarios de partes externas que tienen autoridad para permitir el retiro de activos del sitio.
- Definir cuando sea necesario y apropiado, registrar los activos se retiran del sitio y cuando se hace su devolución, para ello hay un formato de retiro de elementos en el proceso de recursos físicos denominado Control de entrada y salida de bienes RF-FT-05.

8.7.2 Seguridad en la reutilización o eliminación de los equipos.

Se deben verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos sensibles o asegurar que se hayan sobrescrito de forma segura, antes de una posible baja de elementos informáticos.

- Se eliminará toda la información que contenga cualquier equipo informático que se requiera retirar, realizando previamente las respectivas copias de resguardo.
- Mantener los equipos de acuerdo con la vida útil y especificaciones de servicio recomendados por el proveedor.

9. GESTIÓN DE COMUNICACIONES Y OPERACIONES

9.1 Procedimientos operacionales y responsabilidades

La Fuga asegura la operación correcta y segura de los servicios de procesamiento de información, mediante la actualización constante de los procedimientos vinculados al proceso de Gestión TIC

- Operaciones del centro de datos GT-PD-07
- Gestión de incidentes, amenazas y debilidades de seguridad GT-PD-09
- Seguridad de redes GT-PD-10

9.2 Gestión del cambio.

Se deben controlar los cambios en los servicios y los sistemas de procesamiento de información, el responsable del desarrollo e implementación de los sistemas de Información controlará y dará seguimiento a que los cambios en los ambientes productivos no afecten la seguridad de estos ni de la información que soportan, procedimiento (s) vinculados al proceso de Gestión TIC.

- Gestión de soluciones y servicios de tecnologías y MTO GT-PD-03.
- Implementación de soluciones y servicios de Tecnología GT-PD-06.

9.3 Distribución de funciones

Las funciones y las áreas de responsabilidad en operaciones sobre la plataforma tecnológica se deben distribuir para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de la organización el proceso de Gestión TIC realiza controles como monitoreo de las actividades, registros de control y seguimiento se realiza mediante la documentación relacionada:

Se debe asegurar la independencia de las funciones de auditoría de seguridad, tomando precauciones para que ninguna persona pueda realizar actividades en áreas de responsabilidad

A continuación, se presenta el equipo de TI de la Entidad. Es importante indicar que, dado que no hay un área en la entidad, las personas dedicadas a TI son de la Subdirección de Gestión Corporativa y de la Oficina Asesora de Planeación. El equipo humano trabajando en TI con sus áreas, roles y perfiles se presenta en el cuadro siguiente:

Personas TI -Rol	Responsabilidad	Tipo de contratación	Perfil
1 profesional Infraestructura y seguridad TI - Subdirección de Gestión Corporativa	Prestar los servicios profesionales a la Fundación Gilberto Alzate Avendaño en el diseño y ejecución del plan estratégico de tecnologías de la información 2022	Contratista	Ingeniero Senior
1 profesional. Mesa de ayuda de TI - Subdirección de Gestión Corporativa	Prestar los servicios profesionales a la Fundación Gilberto Alzate Avendaño en los temas inherentes al Proceso de Gestión de TIC.	Contratista	Ingeniero
1 profesional. Desarrollador Sistema Gestión Documental Orfeo - Subdirección de Gestión Corporativa	Prestar los servicios profesionales a la Fundación Gilberto Alzate Avendaño en la implementación de soluciones y mejoras tecnológicas sobre la herramienta informática del Sistema de Gestión de Documentos Electrónicos de Archivos - SGDEA.	Contratista	Ingeniero Senior
1 profesional Implementador Sistema información Pandora - Oficina Asesora de Planeación	Prestar los servicios profesionales a la Oficina Asesora de Planeación de la Fundación Gilberto Alzate Avendaño, en la implementación y puesta en producción del Sistema de Información de Planeación y Gestión Pandora	Contratista	Ingeniero desarrollador Senior

Con relación a las necesidades de personal el proceso deberá ser fortalecido con ingenieros que desarrollen software a la medida de las necesidades y que ayuden la implementación de los diferentes planes a cargo.

9.4 Separación de las instalaciones de desarrollo, pruebas y producción

Los ambientes de desarrollo, pruebas y producción deben estar separados para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.

- Establecer que el software de desarrollo y de producción debe funcionar en diferentes máquinas virtuales y/o físicas.
- Los cambios en los sistemas operativos y aplicaciones se deben probar en un entorno de pruebas antes de aplicarlos a los sistemas operacionales.
- Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión.

En cumplimiento de lo anterior, la Fuga vela por la creación de las máquinas para los servicios en espacios virtuales de su infraestructura local interna, los servicios se separan en ambientes de prueba y producción, para dar continuidad a los aspectos nombrados en el numeral correspondiente.

9.5 Protección contra códigos maliciosos y móviles

La fuga a través del proceso Gestión TIC Protege la integridad del software y de la información con la configuración del antivirus para los equipos controlados y la validación del firewall aplicando las reglas correspondientes para la protección de los activos.

- Controles contra códigos maliciosos.

Se implementan controles de detección, prevención y recuperación para proteger contra códigos maliciosos en los dispositivos para tal fin.

- Los controles aplicados a la seguridad de la información para protección de malware y virus tienen en cuenta lo siguiente:
  - Prohibir el uso de software no autorizado por la entidad se bloquea mediante reglas generales.
  - Instalar y actualizar periódicamente software de detección y reparación de virus, con la finalidad de examinar computadoras y medios informáticos, como medida.

9.6 Respaldo

Mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información, por esto, con el propósito de mantener la integridad y disponibilidad de la información, así como los medios tecnológicos para el procesamiento de información, se debe cumplir con el procedimiento definido de copias y respaldos para implementar los controles de respaldo acorde a la estrategia para tomar backup de los datos definida por el administrador de cada sistema, mediante la actualización constante de los procedimientos vinculados al proceso de Gestión TIC

- Respaldo de la información GT-PD-05.

9.7 Gestión de la seguridad de las redes

La Fuga aplica la tecnología a la seguridad de servicios de red, tales como autenticación, encriptación y controles de conexión de red; Identifica las redes y los servicios de red a los cuales se permite el acceso. El proceso Gestión Tic define lineamientos de autorización para determinar las personas, las redes y los servicios de red a los cuales se les otorgará el acceso y establece controles y procedimientos de gestión para proteger el acceso a las conexiones y los servicios de red.

- Seguridad de redes GT-PD-10
- Asignación de cuentas GT-PD-04

9.8 Manejo de los medios

Evitar la divulgación, modificación, retiro o destrucción de activos no autorizada, y la interrupción en las actividades de la Fundación Gilberto Alzate.

9.8.1 Gestión de los medios removibles

Es responsabilidad de cada funcionario o Contratista que utilice medios removibles, tomar las medidas de resguardo necesarias sobre estos activos, con el fin de evitar accesos no autorizados, daños, perdida de información o del activo mismo.

Ante la pérdida, extravío o robo de un medio removible, el funcionario o contratista debe informar oportunamente a través del correo mesadeayuda@fuga.gov.co al personal de Gestión TIC de acuerdo a lo indicado en el procedimiento de Gestión de Incidentes de Seguridad de la Información.

9.8.2 Eliminación de los medios

Cuando ya no se requieran estos medios, su eliminación se debe hacer de forma segura y sin riesgo.

Al recibir un computador los miembros del grupo de Soporte deben respaldar la información contenida en este y luego eliminar toda información que el computador contenga para, posteriormente actualizar los programas y sistema operativo y finalmente, almacenarlo o entregarlo.

9.8.3 Mensajería electrónica

Los correos electrónicos institucionales contaran con niveles altos de controles de autenticación para los accesos desde las redes accesibles**.**

La Entidad en cualquier momento podrá implementar las medidas necesarias en la plataforma del correo institucional, en aras de incrementar los niveles de seguridad y/o de brindar calidad en un mejor servicio.

Las cuentas de correo institucional son de uso personal e intransferible, por lo tanto, es responsabilidad del usuario salvaguardar la contraseña, cambiarla periódicamente, y no prestarla bajo ninguna circunstancia, a excepción de aquellas que sean creadas para fines colaborativos de las unidades de gestión con la respectiva justificación y autorización.

Se recomienda hacer caso omiso a los links que vengan agregados en el cuerpo del correo de cuentas externas; por lo tanto, se aconseja digitar directamente la página que deseen consultar en el navegador del equipo.

El uso no adecuado o incumplimiento de las medidas definidas en el uso del correo institucional, da lugar a la aplicación de las medidas administrativas, disciplinarias o legales a que haya lugar.

9.8.4 Transacciones en línea

La información involucrada en las transacciones en línea debe estar protegida para evitar transmisión incompleta, enrutamiento inadecuado, alteración, divulgación, duplicación o repetición no autorizada del mensaje.

- Para las transacciones en línea se dispondrá de medios de validación de seguridad digital para las firmas de autorizaciones y aprobaciones.

10. CONTROL DE ACCESO

El objetivo de este numeral corresponde a controlar el acceso a la información y abarca las siguientes acciones:

- Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo y/o de acuerdo con sus obligaciones contractuales para ello se aplicará procedimiento Asignación de cuentas GT-PD-04
- La conexión remota a la red de área local de la FUGA debe ser establecida a través de una conexión VPN segura aprovisionada por la entidad, la cual debe ser autorizada por Gestión TIC que cuenta con el monitoreo y registro de las actividades necesarias.

10.1 Uso de contraseñas

Se debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas.

- Se debe identificar y autenticar a cualquier usuario que, de manera local o remota, requiera utilizar los recursos tecnológicos.
- Una vez se han identificado y autenticado, los usuarios sólo podrán acceder a los recursos sobre los cuales están autorizados.

10.2 Lineamientos de escritorio despejado y de pantalla despejada

Todo el personal de la FUGA debe conservar su escritorio libre de información propia de la entidad, que pueda ser copiada, utilizada o estar al alcance de terceros o por personal que no tenga autorización para su uso o conocimiento.

10.3 Uso de los servicios de red.

Los usuarios sólo deben tener acceso a los servicios para cuyo uso están específicamente autorizados. El servicio institucional de Internet se constituye en una herramienta tecnológica que facilita el cumplimiento de las funciones y responsabilidades de los servidores de la Institución, funcionarios, contratistas, terceros y/o pasantes autorizados, dentro de los procesos institucionales.

10.4 Autenticación de usuarios para conexiones externas

- La autenticación es una manera de restringir el acceso a usuarios específicos cuando acceden a un sistema remoto. La autenticación se puede configurar en el nivel del sistema y en el nivel de red , la fuga tiene un equipo de red denominado firewall donde se configuran los parámetros.
- Se crearán políticas de firewall para dar acceso a recursos específicos de red a usuarios y grupos en los ambientes de red donde varios usuarios comparten direccionamiento IP.

10.5 Control de conexión a las redes

- El acceso remoto a los servidores críticos y bases de datos, se realiza para los administradores del sistema y se otorgan los permisos de acuerdo a las necesidades que se tengan sobre el servicio.

10.6 Controles criptográficos

La entidad y el proceso de gestión TIC protege la información, por medios criptográficos, con el uso de técnicas que permiten proteger la confidencialidad, integridad y la autenticidad de la información, para unidades de gestión o procesos establecidos, entiéndase, para ello se adquiere token que respalda firmas digitales, a nivel de software concretamente sistema operativos se crean llaves virtuales para la comunicación entre servidores.

11. GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN

En caso que se materialice un incidente referente a la seguridad en la infraestructura de la fuga se debe tener en cuenta lo siguiente, además de aplicar Gestión de incidentes, amenazas y debilidades de seguridad GT-PD-09.

- Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible.
- Aplicar un modelo técnico de gestión de incidentes de seguridad de la información se involucran las siguientes fases de manera cíclica:

- Preparación, reporte y registro de eventos e incidentes
- Detección y análisis.
- Contención, erradicación, recuperación y respuesta.
- Actividades Post-Incidentes.

Todos los incidentes de seguridad deberán estar registrados en la herramienta de gestión de mesa de ayuda con los canales que sean establecidos por la FUGA y adaptando el procedimiento mencionado anteriormente.

El equipo de soporte y mesa de ayuda debe realizar el registro de los eventos tecnológicos o incidentes de seguridad de la información que reporte los funcionarios, en la herramienta de mesa de ayuda de la Entidad, teniendo en cuenta que el o los administradores de la herramienta definida deben mantenerla activa y configurada para el registro de los eventos tecnológicos o incidentes de seguridad de la información, y para la emisión de los informes que se requieran.

11. 1 Responsabilidades incidencias seguridad de la información

Una vez se reciba el reporte del posible Incidente de seguridad, la mesa de servicio debe realizar la primera categorización en la herramienta que se maneja para iniciar con la atención de este, allí se generará un ticket de servicio para la atención del caso.

Clasificar el incidente de seguridad de acuerdo con su impacto y urgencia en la herramienta de gestión con la que cuenta la FUGA con el fin de permitir una atención adecuada a los incidentes.

Realizar el análisis, contención y erradicación, determinando el nivel de prioridad de este, y de esta manera atenderlos adecuadamente según la necesidad.

De acuerdo a la criticidad del incidente se conformarán equipos gestión que podrán solicitar información o la participación de otros colaboradores, procesos, especialistas y/o operadores estratégicos requeridos para la atención del incidente de seguridad.

En caso de que se presente un incidente de seguridad relacionados con base de datos que contenga información sensible, deberá ser revisado con el apoyo del oficial de datos personales

Si la FUGA no cuenta con los recursos necesarios y personal capacitado se debe recurrir a entidades externas como CSIRT o ColCERT notificando la incidencia.

12. Control de cambios

Fecha	Versión	Razón del cambio	Verificación SIG
13/02/2017	1	Versión inicial	NA
20/02/2020	2	Adopción plataforma estrategia, vinculación de la resolución de tratamiento de datos personales. (Pag 4-5 Generalidades).	Deisy Estupiñan- Apoyo Equipo SIGD-MIPG, Oficina Asesora de Planeación
20/11/2023	3	Se integra al SIG con los Ajustes aprobados en el comité directivo del mes de Octubre: introducción - integración criterio generalidades Actualización de objetivos, Actualización Alcance, Actualización marco normativo, Actualización definiciones y adopción numerales de la norma ISO 27001.	Tatiana López - Profesional de apoyo SIG OAP

Elaboró:	Revisó:	Aprobó
Edwin Díaz Profesional Contratista - TIC	Luis Fernando Mejía Castro Subdirector Gestión Corporativa	Comité directivo del 30 de octubre de 2023 Soporte acta de comité.