Tabla de contenido

INTRODUCCIÓN

La gestión de seguridad de la información puede coordinar todos los esfuerzos encaminados para asegurar los activos de información, mediante la administración del recurso humano y tecnológico, sin un apropiado control se propicia un desordenado y confuso entorno inseguro para la entidad, para ello es necesario emplear actividades encaminadas para mitigar este riesgo. El documento que se presenta como políticas de seguridad, integra estos esfuerzos los cuales establecen las reglas, normas, controles que ayudan a prevenir, proteger los riesgos de seguridad.

En términos generales las políticas de seguridad informática, engloba los procedimientos más adecuados, tomando como lineamientos principales los criterios, que se detallan a continuación

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 elmanejo de equipos, transferencia de información y control de los accesos alas 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.

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.

Comité de Seguridad de la Información: Es un equipo integrado por representantes de las diferentes áreas de la organización, destinado a apoyar las iniciáticas de Seguridad de la Información.

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

Política: Son instrucciones mandatorias 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.

Usuarios Terceros: Todas aquellas personas naturales o jurídicas, que no son funcionarios del IDARTES, pero que por las actividades que realizan en la Entidad, deban tener acceso a Recursos Informáticos.

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 si misma, sea o no protegida por reserva legal.

GENERALIDADES

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. Construir un posicionamiento positivo del centro de Bogotá.
2. Promover y fomentar las prácticas artísticas y culturales como agente de cambio para la revitalización y transformación del centro de Bogotá.
3. Formular Y ejecutar proyectos de manera articulada con organizaciones públicas y privadas para revitalizar y transformar el centro de Bogotá.
4. Recuperar y transformar el antiguo Bronx mediante la creación del primer Distrito Creativo dé Bogotá.

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 de tecnología donde el comité de desempeño aprueba los documentos asociados al Modelo de Seguridad de la Información y las acciones que se derivan de ello. Para así en conjunto salvaguardar uno de sus activos más importantes.

Adicional al apoyo vinculado a la estrategia desde el proceso de Gestión Tecnológica, las políticas consignadas en este documento apoyan los objetivos estructurales de una forma transversal basándose principalmente en el objetivo asociado a (***Preservar la infraestructura física, técnica e informática de la entidad mediante su dotación, adecuación y mantenimiento, para acoger y servir a los grupos de valor***") donde a partir de las decisiones tomadas en el comité de desempeño la parte operativa genera las acciones que permitan cumplir los índices del modelo de gestión de seguridad y privacidad aprobado.

Con base a lo descrito anteriormente servicios, como correo electrónico, internet, intranet y 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.

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, tiene una serie de documentos publicados en su página web amparados en la resolución No 024 del 30 de Enero de 2019 expuestos para la ciudadanía en general y colaboradores, donde se describe 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. La entidad tiene publico los siguientes documentos donde da calidad sobre el tema:

Política de tratamiento de la información y protección de datos personales.
Políticas internas de Seguridad y tratamiento de datos.
Políticas web tratamiento de datos.
Manual recomendaciones de seguridad.
Protocolo de atención a titulares información.

Formatos Protección de Datos

Archivo Ejercicio del derecho de acceso o consulta
Archivo Ejercicio del reclamo por supresión
Archivo Ejercicio del reclamo por infracción
Archivo Ejercicio del reclamo de corrección
Archivo Revocatoria de la autorización

Se prohíbe la descarga de archivos, transmisión o almacenamiento que pudiera ser considerado pornográfico, difamatoria, racista, videos, música, etc. o que atente contra las buenas costumbres o principios, excepto que el trabajo lo amerite.

Todo usuario de la red institucional de la Fundación Gilberto Álzate gozará de privacidad limitada sobre su información o la información que provenga de sus acciones. La entidad podrá monitorear la actividad para evitar que ésta se vea involucrada en actos ilícitos o contraproducentes para la seguridad de la red institucional.

Los usuarios tendrán el acceso a Internet siempre y cuando se cumplan los requisitos mínimos de seguridad para acceder a este servicio y se acaten las disposiciones establecidas en la presente política de seguridad.

Los niveles de seguridad fueron organizados, desarrollando cada política con sumo cuidado sobre qué activo proteger, de qué protegerlo cómo protegerlo y por qué protegerlo; Los mismos se organizan siguiendo el esquema, normativo de seguridad, ISO 27002 y que a continuación se presenta:

Nivel de Seguridad Organizativo:

- Seguridad Organizacional
- Políticas de Seguridad
- Clasificación y Control de Activos:
- Responsabilidad por los Activos
- Clasificación de la Información
- Capacitación de Usuarios
- Respuestas a Incidentes y Anomalías de Seguridad

Nivel de Seguridad Física

- Seguridad Física
- Seguridad Física y Ambiental
- Seguridad de los Equipos
- Controles Generales

Nivel de Seguridad Lógico

- Control de Accesos
- Administración del Acceso de Usuarios
- Seguridad en Acceso de Terceros
- Control de Acceso a la Red
- Control de Acceso a las Aplicaciones
- Monitoreo del Acceso y Uso del Sistema

Nivel de Seguridad Legal

- Seguridad Legal
- Conformidad con la Legislación
- Cumplimiento de Requisitos Legales
- Revisión de Políticas de Seguridad y Cumplimiento Técnico

El funcionario o contratista debe cumplir todas las políticas pertinentes a su entorno de trabajo y utilización de los activos o recursos informáticos.

Objetivo:

Dotar de la información necesaria con un nivel de detalle a los funcionarios donde se establecen los estándares de seguridad informática que sirvan de base para la protección y aseguramiento de los activos de información.

Alcance:

Las políticas aquí definidas aplican a todos los funcionarios públicos de planta permanente, contratistas y proveedores.

1. POLÍTICA DE SEGURIDAD

La Fundación Gilberto Álzate Avendaño reconoce que la información es el activo más importante dentro de la entidad, por tanto gestiona y trabaja por la integridad, la disponibilidad y la confidencialidad de sus procesos, los sistemas, las redes de comunicación y el personal involucrado en su operación. En esesentido da prioridad a la protección de los activos de la informaciónen particular los servicios soportados por los Centros de Datos.

Se consideran activos de la información los siguientes elementos:

- La información en sus múltiples formatos (papel o digital, texto, imagen, audio o video).
- Los equipos e infraestructura tecnológica que soportan esta información.
- Los usuarios que utilizan la información y que tienen el conocimiento de los procesos institucionales a nivel misional o administrativo.

Todos los funcionarios, contratistas y proveedores son responsables del cumplimientode las políticas y procedimientos de seguridad establecidos en la entidad y de reportar las incidenciasque se detecten sobre los activos de información.

Las acciones señaladas deben ser continuamente mantenidas y mejoradas sobre la base metodológica de las normas ISO 27001:2013 e ISO 27002:2013, aplicable bajo los lineamientos de Gobierno en Línea.

2. CLASIFICACION Y CONTROL DE ACTIVOS

2.1. 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.

2.2. 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.

Los niveles de seguridad se detallan como nivel de seguridad bajo, nivel de seguridad medio y nivel de seguridad alto.

3. MANEJO Y SEGURIDAD DE INFORMACION EN MEDIOS EXTRAIBLES

Teniendo en cuenta que la información es el activo más importante de toda entidad, desde todas las áreas se debe velar por la seguridad del producto final, en la manipulación de dispositivos extraíbles y medios de almacenamiento masivo como discos duros y demás medios que permitan una copia no permitida de la información.

3.1. Manejo de memorias USB

Se recomienda no conectar a los computadores, dispositivos externos como USB, Discos Duros externos USB, Tarjetas SD, Celulares o cualquier otro dispositivo, ya que además del riesgo de contener virus o software malicioso que puede afectar la máquina, también puede extraer información no autorizada; por lo tanto, es responsabilidad de cada persona o usuario por la información o daños que esta cause. En caso de requerir compartir archivos entre dos o más equipos o usuarios, puede solicitar el ingreso ó creación de carpetas compartidas.

3.2. Manejo de discos duros

Los discos durosextraíbles al igual que las memorias USB deben permanecer sin información relevante, toda la información que requiera ser respaldada debe guardarse en las unidades de red correspondientes a cada uno de los usuarios que le son asignadas en la entrega y configuración del usuario de Red.

3.3. Manejo computadores portátiles

Los computadores portátiles de la Fundación Gilberto Álzate se han adquirido específicamente para facilitar el desarrollo de actividades laborales. Su uso debe estar relacionado con las actividades del área o proceso al cual ha sido asignado y el uso para propósitos personales debe ser ocasional, racional y no debe obstaculizar las actividades laborales habituales.

- En caso de licencia o vacaciones del funcionario, el equipo portátil debe quedar a disposición del área a la cual fue asignado.
- La instalación, configuración, modificación o eliminación de software sobre los equipos portátiles es responsabilidad exclusiva del área de Sistemas y no puede ser modificada bajo ninguna excusa directamente por el usuario.
- Si el usuario sospecha que hay infección por un virus, debe inmediatamente llamar informar mediante un caso GLPI al área de Tecnología y no utilizar el computador y desconectarlo de la red.
- El área de Tecnología tiene la potestad para remover, sin notificar al funcionario, cualquier software que no esté autorizado por la Subdirección Administrativa y Financiera.
- La configuración e instalación de hardware de los equipos portátiles de FUGA, debe ser solicitada y ejecutada exclusivamente por el área de Tecnología.
- Es responsabilidad de cada funcionario o contratista hacer copias de seguridad de la información almacenada en el equipo portátil. Si no está seguro del proceso debe comunicarse con el área de Tecnología.
- Es responsabilidad del funcionario o contratista reportar inmediatamente al área de Tecnología, cualquier daño, desconfiguraciónó pérdida del dispositivo que le ha sido asignado.
- Todo dispositivo personal que se requiera conectar a la red de FUGA, debe cumplir las normas de seguridad solicitadas por el área de Tecnología.

3.5. Manejo equipos de visitantes

Los computadores o cualquier otro dispositivo que permita conexión a la red a través de la tarjeta inalámbrica “Wifi” o tarjeta de red, sólo están autorizados a conectarse a la red de internet llamada “VISITANTES”, cuya clave será suministrada en el área de sistemas. En caso de requerir acceso a un servidor de la intranet, debe realizar la solicitud a través del Jefe de su dependencia o supervisor del contrato, por medio del GLPI.

4. SEGURIDAD EN LOS SERVIDORES Y SISTEMAS DE INFORMACIÓN

4.1. Seguridad en los equipos servidores

La seguridad de los equipos de administración de red y de infraestructura están protegidos de ataques externos desde la nube por el equipo utilizado para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas (firewall), en cual permite limitar, cifrar y descifrar el tráfico entre diferentes ámbitos sobre un conjunto de reglas. En la actualidad la Fundación cuenta con el software de firewall PfSense el cual es de licencia GPL.

- Cabe aclarar que un firewall correctamente configurado brinda la protección necesaria a la red, pero que en ningún caso debe considerarse suficiente toda vez que todos los días se crean nuevos códigos maliciosos con el fin de violar la seguridad.

- Sólo el personal de Tecnologíay administradores de los diferentes sistemas de información están autorizados para ingresar o conectarse al sistema operativo de los servidores, con un usuario diferente al administrador, con el fin de realizar tareas de administración y mantenimiento.

- En caso que una empresa externa requiera realizar alguna configuración en los servidores, sólo el personal de sistemas debe ingresar con el usuario y contraseña correspondiente, sin suministrar las claves a personal no autorizado.

- Se deben implementar herramientas en los servidores, que permitan su monitoreo, con el fin de conocer su rendimiento, capacidad de almacenamiento, registro de logs y consumo de red.

4.2. Seguridad en los sistemas de información

El área de sistemas deberá mantener actualizado el inventario de todos los sistemas de información existentes en la entidad.

Los sistemas de información alojados en los servidores físicos de la fundación, como Orfeo, GLPI, Pfsense y demás que hacen parte del inventario de sistemas de información, su administración está a cargo del personal asignado por la entidad.

A todos los sistemas de información se le debe actualizar sus paquetes, librerías y servicios a la última versión disponible. Si estas actualizaciones pueden provocar el fallo de alguna funcionalidad, se deben aplicar las actualizaciones en un ambiente alterno, donde se hagan las respectivas pruebas y ajustes al código fuente de ser necesario, para luego instalarlas en el ambiente de producción.

5. ADMINISTRACIÓN DE USUARIOS

Cada funcionario o contratista deber tener su correspondiente usuario de red, usuario de correo electrónico y usuario para las diferentes aplicaciones que requiera para el desarrollo de sus funciones o actividades contractuales.

Es responsabilidad de cada Jefe de área y Supervisor de Contrato, realizar la respectiva solicitud de creación y actualización de la cuenta de usuario a través del GLPI.

5.1. Desactivación temporal de la cuenta de red

En situaciones especiales como permisos, vacaciones, incapacidades o despidos del personal, podrá ser enviado un GLPI por parte del Jefe solicitando el bloqueo temporal de las cuentas del funcionario en cuestión, formalizando a la brevedad.

Ante situaciones de grave riesgo para la disponibilidad o continuidad del servicio, se podrá cambiar la contraseña de una cuenta de red. Esto podría impedir al usuario el acceso al resto de los servicios basados en las credenciales de la Intranet.

6. SEGURIDAD DE LAS CUENTAS DE CORREO ELECTRÓNICO

El correo electrónico institucional es una herramienta importante para la gestión y desarrollo de las funciones y actividades de los funcionarios y contratistas, por lo tanto se le debe dar un uso razonable y responsable, atendiendo las siguientes recomendaciones:

6.1. Tamaño de los buzones de correo electrónico

La capacidad máxima para los buzones de correo GMAIL es de 5 GB;cuando el sistema detecta que la ocupación del buzón de correo es superior al 90% automáticamente envía una notificación al usuario, con el fin de que pueda tomar las medidas pertinentes para no generar un bloqueo en su cuenta.

6.2. Suspensión de cuentas de correo electrónico

Se suspenderán aquellas cuentas de correo que no han sido consultadas durante un periodo continuado de tres meses, generando que el usuario no pueda acceder a los correos almacenados en dicha cuenta.

El uso inapropiado o el abuso en el servicio de correo electrónico pueden ocasionar la desactivación temporal o permanente de las cuentas. Las acciones en este sentido se pueden llevar a cabo en función de las posibles repercusiones en el buen funcionamiento del servicio. La desactivación de la cuenta implica la imposibilidad de enviar y recibir nuevos correos mientras no vuelva a ser activada.

Ante situaciones de grave riesgo para la disponibilidad o continuidad del servicio de correo, los administradores de la plataforma podrán cambiar la contraseña de una cuenta de correo. Esto podría impedir al usuario enviar o recibir correos en su cuenta corporativa hasta que se investigue el origen y mitigación del problema causado.

6.3. Envío de correos electrónicos masivos

El envío de correos masivos se canalizarán a través del funcionario de la Oficina de Comunicaciones, diligenciando el formato destinado para la publicación de información en masa. Solo esta Oficina tiene la facultad de la utilización del servidor PHPList para el envío de correos masivos. Al interior de la entidad, solo las personas autorizadas tienen permiso para el envío de correos a todo el dominio.

6.4. Cuentas de correo electrónico externas

Está prohibido el uso y realizar la vinculación o reenvío del correo institucional a otros servicios de correo como cuentas personales gmail, yahoo, outlook o cualquier otro servidor de correo que no corresponda al servicio de correo de la FUGA.

6.5. Problemas de seguridad en el correo electrónico

Son múltiples los problemas de seguridad que pueden afectar al correo electrónico, cabe destacar:

6.6. Robo de identidad. Phishing y scams:

Si se recibe un correo de origen desconocido consulten inmediatamente con el área de Sistemas, o levanten un ticket a través de la mesa de ayuda (Helpdesk). Bajo ningún aspecto se debe abrir o ejecutar archivos adjuntos a correos dudosos, ya que podrían contener códigos maliciosos (virus, troyanos, keyloogers, gusanos, etc). Si dicho archivo pide o contiene un formato para diligenciar con sus datos de usuario, claves y/o datos personales, no lo diligencie por ningún motivo. Puede ser víctima de robo de identidad a través de la técnica de captura de datos personales llamada phishing.

Cabe recordar que el área de Tecnología nunca requerirá este tipo de información a través del correo institucional.

6.7. Propagación de virus y spam

El correo electrónico es un vehículo ideal para la propagación de virus y sobre todo los gusanos que utilizan técnicas de spam para infectar un PC en combinación de virus y spam. Las últimas generaciones de virus se han creado para ayudar a los spammers que han incorporado código malicioso en su spam.

6.8. Ataques con direcciones falsificadas

Consiste en inundar el servidor de un dominio real con los errores generados por una máquina atacada al procesar spam para distribuirlo a miles destinatarios. El spammer coloca como dirección receptora de estos errores un dominio real y un usuario aleatorio. Esto provocará problemas de ancho banda, colapso del servidor (colas, disco etc.).

6.9 Generación innecesaria de tráfico SMTP

El envío y encaminamiento de un simple mensaje de correo electrónico implica el uso de varios recursos: conexiones SMTP, consultas DNS, procesamientos por MTA. Los propios errores de SMTP, el spam, los virus etc., generan informes a direcciones falsificadas provocando confusión en los usuarios y generando un exceso de tráfico.

Teniendo en cuenta lo anterior se especifican las siguientes recomendaciones generales para el manejo apropiado de la contraseña y uso general del correo:

- La contraseña de acceso al correo no debe ser cedida o facilitada a otros usuarios, siendo responsabilidad del propio usuario su custodia.
- Nunca se debe guardar las contraseñas, en ningún tipo de archivo digital ni físico como un papel, agenda, etc.
- Las contraseñas se deben mantener confidenciales en todo momento.
- Cambie su contraseña si se piensa que alguien más la conoce y si ha tratado de dar mal uso de ella.
- Seleccione contraseñas que no sean fáciles de adivinar.
- Cambia tus contraseñas regularmente.
- Nunca utilizar la opción de almacenar contraseñas en su navegador de Internet.
- No utilizar contraseña con números telefónicos, nombre de familia o similares ya que son fáciles de adivinar por terceros.
- No utilice el correo institucional para obtener información personal, comercial o de labores diferentes a las de su trabajo, para esto debe utilizar su correo personal.
- Utilizar el correo electrónico como una herramienta de trabajo y no como nuestra casilla personal de mensajes a amigos y familiares.

- No enviar archivos de gran tamaño a compañeros de oficina o área. Estos se deben transmitir a

través de carpetas compartidas, si no la tiene, se debe solicitar al área de sistemas.

- No utilizar para enviar cadenas de comentarios, chistes y demás material que no aporte en el proceso laboral.
- Los correos no deben contener información que pudiera ser interpretados como ámbito de ataque, discriminación o ilegalidad. Todo lo que escriba bajo el dominio de la organización, es en representación de la misma y las palabras podrían ser utilizadas de formas no previstas. Por eso, antes de enviar, relea el correo y proceda a corregir de ser necesario, tratando de aclarar cualquier frase ambigua o que se preste a suspicacias.
- El acceso a las cuentas personales debe ser el mínimo durante nuestra jornada laboral.

7. SEGURIDAD DE LA CONTRASEÑA

Se recomienda crear una contraseña de fácil recordación pero que cumpla con las siguientes sugerencias:

- Cree una contraseña fuerte que contienen números y letras.
- Utilice una contraseña que tenga por lo menos 8 caracteres.
- No socialice ni comparta su clave bajo ningún motivo.
- se debe cambiar periódicamente las claves.

8. MANEJO DE ACCESO A INTERNET

El acceso a internet se encuentra protegido por filtros para disminuir sitios peligros que contenga código malicioso o que se encuentren ajenos al servicio, permitiendo de esta manera aumentar la velocidad de acceso a los sitios necesarios y disminuir el riesgo de virus.

- No navegar por sitios no confiables o no autorizados por el área de Tecnología y las Directivas de la Fundación.
- No suministrar información institucional o personal en sitios desconocidos.
- Queda prohibido el uso de sitios de radios online debido al ancho de banda que consume este servicio.
- Queda prohibido el uso de intercambio de archivos (Ares, eMule, Torrents, Limewire, etc.).
- Queda prohibido el uso de sitios de chat (Messenger, chat, etc.).
- Queda prohibido el uso de internet para actividades ilícitas y/o fraudulentas que no solo exponen la seguridad corporativa sino también la imagen organizacional.
- Queda prohibida la descarga que no cumpla con la normativa vigente de copyright y similar.

- Se prohíbe el acceso a los sitios o páginas Web que contengan materiales amenazadores,

pornográficos, racistas, sexistas o cualquier otro que degrade la calidad del ser humano, salvo aquellas requeridas por la naturaleza de las funciones institucionales del usuario.

- No compartir sus claves para ingresar a sitios que lo requiera como bancos o correo personal.
- No permitir que el navegador de internet recuerde la contraseña automáticamente.
- Queda prohibido participar en juegos de entretenimiento en línea así como realizar compras online desde la red de la Fundación.
- Cualquier archivo que se reciba o descargue de internet deberá revisarse con el antivirus para asegurar que no tenga virus.
- El área de Tecnología tiene la facultad de suspender el servicio de navegación en internet bajo circunstancias que así lo requiera (Virus, mal uso de internet, trafico sospechoso, etc.).
- Si requiere navegar en algún sitio bloqueado el procedimiento es el de enviar la solicitud a través de la mesa de ayuda GLPI o por el correo electrónico al Subdirector Administrativo y Financiero, por parte del Jefe de área, justificando dicho acceso.

8.1. Manejo de redes sociales

El área bloquea todo tipo de sitio relacionado con redes sociales, permitiendo de esta manera aumentar la velocidad de acceso a los sitios necesarios y disminuir el riesgo de virus. Si algún funcionario por motivos de trabajo requiera acceder a ello, su Jefe de área o Gerencia debe enviar la solicitud formal al Subdirector Administrativo y Financiero por correo electrónico y al área de Tecnología a través de la mesa de ayuda GLPI, adjuntando el nombre del funcionario, área al que pertenece y motivo del acceso.

Cabe destacar que cualquier foto subida o comentario en facebook, twitter, Instagram o en alguna red social es responsabilidad exclusiva del que la emite y no compromete a la Fundación Gilberto Álzate, a no ser que la misionalidad de su cargo así lo exija.

9. CLAVES DE ACCESO

El cambio de claves de acceso inalámbrico de todas las sedes debe ser cambiadaperiódicamente, por parte del área de sistemas máximo cada seis (6) meses, de manera ordinaria ó de inmediato ante casos que de forma extraordinaria así lo ameriten.

Las claves de administrador de los equipos de escritorio y portátiles adscritos a FUGA, deben ser protegidas y conservadas únicamente por el área de Sistemas y deben ser cambiadas periódicamente cada seis (6) meses de manera ordinaria o en caso extraordinario cuando el personal adscrito al área cambie.

Las claves de servidores solo deben ser de uso privativo de los profesionales con rol de administrador de red y deben ser cambiadas con una periodicidad de un (1) año o cuando el personal con esos roles cambie.

10. SEGURIDAD FISICA

10.1. Ingreso al área de sistemas

El acceso al área de Sistemas esta verificado de manera inicial por el guarda de la recepción, quien permite o no el ingreso a dicha área. Para lograr ingresar a la zona en que está ubicada la infraestructura tecnológica se debe pasar por una puerta de vidrio templado. Sólo el área de Tecnología puede autorizar el ingreso a ésta área.

10.2. Bloqueo de estaciones de trabajos

Para generar una cultura de seguridad y prevenir hurto o acceso no permitido a la información y/o a su correo, se recomienda bloquear la sesión de usuario cada vez que se retire de su estación de trabajo, así sea por poco tiempo.

10.3. Escritorio limpio

Todos los escritorios o mesas de trabajo deben permanecer limpios, libre de objetos para proteger documentos en papel y dispositivos de almacenamiento como CDs, memorias USB y demás medios de almacenamiento, además de proteger los teclados y las estaciones de trabajo con fin de reducir los riesgos de pérdida y daño de la información accidental durante el horario normal de trabajo y fuera del mismo.

11. CAPACITACIÓN

Todos los funcionarios y contratistas de la FUGA y de ser necesario proveedores que desempeñen actividades en la entidad, deben ser capacitados y actualizados periódicamente en temas de seguridad, normas y procedimientos. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general.

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.	Deisy Estupiñan- Apoyo Equipo SIGD-MIPG, Oficina Asesora de Planeación

		(Pag 4-5 Generalidades).	

Elaboró:	Revisó:	Aprobó
Edwin Díaz Profesional Contratista - TIC	Licette Moros León Subdirectora Corporativa	Comité directivo del 26 de diciembre de 2019- soporte acta de comité.