

| | |
|---------------------------------|---------------------------------|
| Código: GTI-002-P | Versión: 9 |
| Fecha: Noviembre/2021 | Página Página 1 de 15 |

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

Bogotá D.C., Noviembre de 2021

| | |
|---------------------------------|---------------------------------|
| Código: GTI-002-P | Versión: 9 |
| Fecha: Noviembre/2021 | Página Página 2 de 15 |

JAVIER ALEJANDRO CASTRO GUTIÉRREZ

Subdirector de TI

LINA MARCELA GALLEGO RUIZ

Jefe Oficina de Planeación

Grupo de trabajo del Proceso Gestión de Tecnologías de la Información

Ana Marcela Peña Nieto
Claudia Mónica Peña Rubiano
Cristian David Home Acosta
Juan Sebastián Carreño Peñaloza
Luis Felipe Noreña López

| CONTROL DE CAMBIOS | | |
|---------------------------|--------------------|--|
| VERSIÓN | FECHA | DESCRIPCIÓN DEL CAMBIO |
| 1 | Julio de 2008 | Elaboración inicial del documento |
| 2 | Noviembre de 2008 | Ajustes en la estructura del documento y codificación |
| 3 | Agosto 2009 | Cambio de código |
| 4 | Septiembre de 2010 | Se agregaron las especificaciones y operatividad del servidor de backup para la información de los servidores de la Dirección Nacional, el cual se encuentra ubicado en el CIEN |
| 5 | Agosto de 2011 | Se indicó el nuevo tamaño máximo de buzón asignado al correo electrónico Se actualizaron las políticas sobre el Backup de servidores Se eliminaron las consideraciones referentes al CIEN |
| 6 | Octubre de 2013 | Se actualizan las políticas de backup y las responsabilidades de los usuarios en el manejo de la información. |
| 7 | Agosto de 2016 | Se realizó una revisión de la política, teniendo en cuenta la nueva modernización de la planta y la nueva infraestructura contratada. |
| 8 | Septiembre de 2019 | Se actualiza la política general de seguridad y privacidad de la información, se adicionan políticas específicas: Política de uso Adecuado de recursos tecnológicos, de control de acceso y gestión de comunicaciones y política Privacidad y Confidencialidad. |
| 9 | Noviembre de 2021 | Se modifica la introducción del documento, así como la Política general de seguridad y la Política de Control De Acceso y gestión de comunicaciones. Se elimina la sección "Comité de Seguridad de la Información" y se adiciona "Organización de la Seguridad de la Información" Se elimina la sección "Políticas de Privacidad y Confidencialidad" y se adiciona "Políticas de recursos humanos" |

POLITICA DE SEGURIDAD DE LA INFORMACIÓN

| | |
|---------------------------------|---------------------------------|
| Código: GTI-002-P | Versión: 9 |
| Fecha: Noviembre/2021 | Página Página 4 de 15 |

| | | |
|--|--|---|
| | | Se modifica la sección “Gestión de la plataforma tecnológica “, cambiando el nombre a “Política de la Operación de la Plataforma Tecnológica” y se modificando parte del contenido. |
|--|--|---|

| | |
|---------------------------------|---------------------------------|
| Código: GTI-002-P | Versión: 9 |
| Fecha: Noviembre/2021 | Página Página 5 de 15 |

TABLA DE CONTENIDO

| | |
|--|-----------|
| Definiciones | 5 |
| Introducción | 6 |
| Política General de Seguridad de la Información | 7 |
| Alcance / Aplicabilidad | 7 |
| Conocimiento y cumplimiento de las Políticas de Seguridad de la Información | 8 |
| Organización de la Seguridad de la Información | 8 |
| Políticas específicas para la implementación de controles de seguridad de la información..... | 9 |
| Política de Uso Adecuado de recursos tecnológicos | 9 |
| Política de Control De Acceso y gestión de comunicaciones..... | 10 |
| Políticas de recursos humanos | 11 |
| Políticas de Plataforma Tecnológica | 12 |

| | |
|--------------------------|--------------------------|
| Código: GTI-002-P | Versión: 9 |
| Fecha: Noviembre/2021 | Página Página 6 de 15 |

DEFINICIONES

Acuerdo de Niveles de Servicio: Documento mediante el cual se establecen los tiempos y compromisos sobre procesos y/o tareas y/o acciones correctivas. Su definición y cumplimiento son importantes en toda una cadena de otorgamiento de producto o servicio.

Almacenamiento de la Información: Procedimiento mediante el cual se utiliza cualquier dispositivo físico o tecnológico con el fin de guardar archivos y/o datos en forma ordenada. Para el caso de los dispositivos electrónicos se tienen desde unidades pequeñas de almacenamiento (ej: pen drive o disco duro portátil), hasta grandes equipos en centros de datos que almacenan millones de registros de información.

Confidencialidad: Es la propiedad y dominio de la información con el fin de garantizar que es accesible únicamente al personal autorizado para consultarla.

Control: Conjunto de medidas para el manejo del riesgo, incluyendo políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas que pueden ser de carácter administrativo, técnico o legal.

Derechos de Autor: Conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

Disponibilidad: Consiste en garantizar que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Evento de Seguridad de la Información: Se considera un Evento de Seguridad de la Información a cualquier situación identificada que indique una posible brecha en las Políticas de Seguridad o falla en los controles y/o protecciones establecidas.

Habeas Data: Es un derecho que tiene toda persona de conocer, actualizar y rectificar la información que se encuentre almacenada sobre ella en archivos y bancos de datos de naturaleza pública o privada.

Incidente de Seguridad de la Información: Se considera un Incidente de Seguridad de la Información a cualquier evento que haya vulnerado la seguridad de esta o que intente vulnerarla, sin importar el tipo de información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

Integridad: Es la protección de la exactitud y estado completo de los activos.

Plataforma Tecnológica: Conjunto de elementos tecnológicos (hardware y software), que operan e interactúan para entregar servicios informáticos. Una plataforma está conformada por equipos de comunicación, equipos de almacenamiento de información, equipos servidores de aplicaciones, computadores de escritorio, programas de computador, programas de ofimática y centros de datos entre otros.

| | |
|--------------------------|--------------------------|
| Código: GTI-002-P | Versión: 9 |
| Fecha: Noviembre/2021 | Página Página 7 de 15 |

Respaldo: Es la garantía sobre un bien tangible o intangible. En tecnología el respaldo hace referencia a las copias de seguridad de la información, su almacenamiento en sitios seguros para poder disponer de los datos en eventos críticos donde se requiera restaurar la información.

Riesgo: Es la posibilidad de sufrir daños o pérdidas.

Usuario: Persona que hace uso de utiliza cualquiera de los recursos informáticos o de la red de CPE.

Trabajador: El personal vinculado a CPE a través de contrato laboral

Proveedor: Persona o empresa que provee bienes o servicios informáticos a CPE.

Tercero: Persona que, sin contar con un vínculo laboral o contrato con la entidad, tiene acceso en las instalaciones de CPE.

| | |
|--------------------------|--------------------------|
| Código: GTI-002-P | Versión: 9 |
| Fecha: Noviembre/2021 | Página Página 8 de 15 |

1. INTRODUCCIÓN

Computadores Para Educar (CPE), entendiendo la importancia de sus activos de información para el cumplimiento de su misión institucional, es consciente del valor de la información independiente de cuál sea su forma u origen, por tal razón vela por la protección y el cuidado de la misma mediante el establecimiento de directrices en seguridad de la información, que permiten mitigar los factores que pueden afectar la confidencialidad, integridad o disponibilidad de información. La presente política se encuentra alineada con el modelo de seguridad de la Información, las políticas de gobierno digital conforme a lo dispuesto en el Decreto 1078 de 2015, modificado por el artículo 2.2.9.1.1.3 del Decreto 1008 de 2018¹ y demás requisitos de ley.

La seguridad de la información en CPE, tiene como objetivo proteger la información de las distintas amenazas a las que hoy se ve expuesta, con el fin de asegurar la continuidad del negocio, minimizar el riesgo, reducir los impactos por incidentes de seguridad, generar oportunidades de mejora y dar cumplimiento legal, contractual y regulatorio; el debido cuidado en el manejo de la información, permitirá mitigar los factores que pueden afectar la confidencialidad, integridad o disponibilidad de la información y garantiza relaciones de confianza con sus grupos de interés en el marco de las buenas prácticas de seguridad.

2. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Computadores para Educar reconoce la información como un activo fundamental para el cumplimiento de sus objetivos misionales y para la toma de decisiones eficientes, por lo que existe el compromiso expreso de gestionar de forma responsable la Información de la entidad y de sus interesados estratégicos, estableciendo un marco de confianza en el ejercicio de su misión para preservar los principios de confidencialidad, integridad y disponibilidad de la información, todo enmarcado en el estricto cumplimiento de los requisitos normativos, legales y contractuales aplicables.

Computadores para Educar en su propósito de dar cumplimiento con la política de seguridad y privacidad de la información, establece los siguientes objetivos:

OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Objetivo 1. Fortalecer la cultura de seguridad de la información en los colaboradores, así como en contratistas o tercero involucrado en manejo de información de CPE.

Objetivo 2. Minimizar el riesgo de todos los procesos de Computadores para Educar.

Objetivo 3. Implementar los controles tecnológicos necesarios para la protección de los activos de la entidad y para la reducción de los riesgos.

¹"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".

| | |
|---------------------------------|---------------------------------|
| Código: GTI-002-P | Versión: 9 |
| Fecha: Noviembre/2021 | Página Página 9 de 15 |

3. ALCANCE / APLICABILIDAD

Esta política aplica para toda la entidad y debe ser cumplida por los trabajadores de CPE de todos los niveles, así como por los contratistas en el desarrollo de los procesos en los que se involucren activos de Información y el personal externo que acceda a las instalaciones de la Entidad.

El incumplimiento de las políticas, normas y procedimientos dará lugar a iniciar las acciones que sean pertinentes conforme a lo establecido en el Reglamento Interno de Trabajo de CPE, y las disposiciones legales aplicables a la materia, según se trate de trabajadores, contratistas y/o terceros.

4. CONOCIMIENTO Y CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

La Dirección Ejecutiva de Computadores para Educar – CPE, apoyará la definición, implementación, divulgación, seguimiento y cumplimiento de la Política de Seguridad de la Información al interior de la Entidad; promoverá activamente una cultura de seguridad de la información, y definirá y establecerá los roles y responsabilidades relacionados con la seguridad de la información en todos los niveles jerárquicos.

5. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

De acuerdo con la “Guía de Conformación y Funciones del Comité Institucional de Gestión y Desempeño”, en su numeral 6, el comité deberá asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información y aprobar y hacer seguimiento a la implementación de la Estrategia de Gobierno Digital y Seguridad de la Información en la Entidad.

El Comité Institucional de Gestión y Desempeño coordina la implementación del Modelo de Seguridad y privacidad de la Información al interior de la entidad y deberá recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.

El proceso de Gestión de TI velará por mantener un Sistema de Gestión de Seguridad de la Información que preserve la Confidencialidad, Disponibilidad e Integridad de la información de sus partes interesadas, controlando y mitigando riesgos.

El proceso de Gestión de TI y los demás procesos de CPE, están obligados a identificar y controlar los riesgos para realizar un manejo efectivo de sus activos de información.

| | |
|---------------------------------|----------------------------------|
| Código: GTI-002-P | Versión: 9 |
| Fecha: Noviembre/2021 | Página Página 10 de 15 |

Los propietarios, usuarios y custodios de la información de CPE deben:

- Aceptar y cumplir las políticas de seguridad de la información que se establezcan
- Entender claramente sus responsabilidades frente al acceso a los sistemas de información.
- Los colaboradores deben utilizar la información de la entidad exclusivamente para fines laborales, quedando prohibido explícitamente cualquier uso comercial y/o privado no autorizado.
- Los terceros (contratistas y proveedores) que interactúan con la entidad no deben hacer copias del software suministrado, ni podrán transferirlo a otro equipo a través de la red, sin la autorización escrita de la entidad.
- Debe existir un propietario para cada uno de los recursos de tecnología y activos de información importantes en la entidad. Las responsabilidades deben estar delimitadas de tal manera que no existan varios propietarios y responsables de un mismo recurso.

Todos los colaboradores deben actuar de acuerdo con las políticas de seguridad de la información y participar en las revisiones de seguridad que se lleven a cabo, adicionalmente participar en las distintas capacitaciones y/o jornadas de sensibilización lideradas por el proceso Gestión de TI.

6. POLITICAS ESPECÍFICAS PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN.

6.1 Política de Uso Adecuado de Recursos Tecnológicos

El uso adecuado de los recursos tecnológicos asignados por COMPUTADORES PARA EDUCAR a sus trabajadores y contratistas debe ajustarse a los siguientes lineamientos:

- La instalación de cualquier tipo de software o hardware en los equipos de cómputo de Computadores para Educar, está sujeta al análisis previo de viabilidad por parte de la Subdirección de TI y, por tanto, son los trabajadores de esta subdirección los únicos autorizados para aprobar dicha instalación.
- Los usuarios no deben utilizar software diferente al establecido por Computadores para Educar para el desarrollo de sus actividades laborales. En caso de requerirse la instalación de un software adicional, se deberá solicitar autorización por escrito a la Subdirección de TI, al correo soporteti@cpe.gov.co. La subdirección procederá a validar las condiciones de licenciamiento, seguridad y pertinencia para la instalación y uso del software solicitado.

| | |
|---------------------------------|----------------------------------|
| Código: GTI-002-P | Versión: 9 |
| Fecha: Noviembre/2021 | Página Página 11 de 15 |

- Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, protector de pantalla corporativo, entre otros.

6.2 Política de Control de Acceso y Gestión de Comunicaciones

Esta política hace referencia a las directrices para el acceso a la información de Computadores para Educar, esto es, determina los límites y mecanismos de protección relacionados con el acceso a la información de la Entidad, en los siguientes términos:

- La Subdirección de TI es responsable del control de acceso a redes, aplicaciones, y/o sistemas de información de la Entidad. Los trabajadores de esta subdirección son los únicos autorizados a realizar las labores de creación, modificación, suspensión o eliminación de usuarios (ID) y contraseñas.
- Todos los usuarios de la plataforma tecnológica de Computadores para Educar deben tener una identificación y una contraseña única e intransferible para hacer uso de la información y de los recursos tecnológicos contenidos en dicha plataforma. Cada usuario es responsable de sus credenciales de acceso y del uso que se haga de las mismas. Los trabajadores y contratistas de Computadores para Educar deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. Los proveedores o terceros que requieran acceso a la red de CPE, deben solicitar autorización a la Subdirección de TI, la cual deberá estar debidamente justificada. El acceso a la red se limitará al período requerido para llevar a cabo las actividades previamente establecidas.
- La conexión remota a la red de área local del Ministerio debe establecerse a través de una conexión VPN, la cual debe ser aprobada, registrada y monitoreada por la Oficina de Tecnologías y Sistemas de Información.
- La configuración de enrutadores, switches, firewall, sistemas de detección de intrusos y otros dispositivos de seguridad de red, será realizada por la Subdirección de TI que se encargará de adoptar las medidas necesarias para garantizar la seguridad de los activos de información. Con este fin, los trabajadores de CPE y terceros autorizados deberán tener en cuenta las siguientes medidas:
 - a. Las redes de comunicaciones institucionales deben ser utilizadas exclusivamente con fines laborales.
 - b. Se prohíbe la conexión de dispositivos de comunicación no autorizados por la Subdirección de TI que puedan alterar el funcionamiento normal de la red o comprometer la seguridad, tales como switches, routers, unidades de almacenamiento externas, equipos portátiles o teléfonos celulares.

| | |
|---------------------------------|----------------------------------|
| Código: GTI-002-P | Versión: 9 |
| Fecha: Noviembre/2021 | Página Página 12 de 15 |

- La cuenta de correo electrónico institucional debe ser usada para el desempeño de las funciones asignadas en la Entidad y será responsabilidad de cada uno de los usuarios su utilización conforme a los lineamientos establecidos por CPE en concordancia con sus deberes misionales.
- Los mensajes y la información contenida en los buzones de correo son propiedad de Computadores para Educar, por lo tanto, cada usuario como responsable de su buzón, deberá procurar por conservar únicamente los mensajes relacionados con el desarrollo de sus funciones.
- No se permite el uso de la dirección de correo electrónico institucional de Computadores para Educar como medio de acceso a comunidades interactivas de contacto social², para fines diferentes a las funciones y actividades asignadas.
- Se prohíbe el envío de archivos con cualquier tipo de contenido malicioso, potencialmente peligroso y/o ajeno a las funciones propias del rol asignado como trabajador y/o contratista de CPE.
- El envío de información corporativa debe ser realizado, exclusivamente, desde la cuenta de correo que Computadores para Educar proporciona a cada uno de los usuarios. De igual manera, las cuentas de correo institucionales genéricas no se deben emplear para uso personal.

6.3 Políticas de seguridad de los recursos humanos

El objetivo de esta política es asegurar que los colaboradores, contratistas y/o proveedores de CPE comprendan su rol y sus responsabilidades en el cumplimiento de las Políticas de Seguridad de la Información, así como garantizar la apropiación de los controles implementados con el fin de mitigar los riesgos asociados a la pérdida o afectación de los principios de seguridad de la información.

- El proceso de Gestión de TI deberá sensibilizar e impulsar a los colaboradores de CPE hacia una correcta adopción y apropiación en las mejores prácticas de seguridad y privacidad de la información.
- La Oficina de Talento Humano en los eventos que corresponda, gestionará la suscripción de acuerdos de confidencialidad con los trabajadores de CPE que requieran conocer, publicar o intercambiar información de la Entidad. De igual forma la Oficina de Contratación, incluirá en las minutas de los contratos y convenios, independientemente de su modalidad, cláusulas y obligaciones relacionadas con el cumplimiento de las políticas de Seguridad y Privacidad de la Información.

² Es decir, sitios web de contacto personal o de ocio, en los que se involucren temas personales con la cuenta corporativa.

| | |
|--------------------------|---------------------------|
| Código: GTI-002-P | Versión: 9 |
| Fecha: Noviembre/2021 | Página Página 13 de 15 |

- Cuando se realiza la desvinculación o cambio de cargo de algún colaborador, la responsabilidad de custodia de cualquier información producida en razón del cumplimiento de sus funciones recae en el jefe inmediato, líder de proceso o supervisor del contrato según sea el caso.
- El incumplimiento de las políticas de seguridad de la información por parte de los colaboradores, contratistas y/o proveedores podrá incurrir en sanciones disciplinarias o legales según corresponda.
- Los trabajadores y los contratistas de Computadores para Educar están obligados a dar cumplimiento de la Ley 1581 de 2012, “*Por la cual se dictan disposiciones generales para la protección de datos personales*” y el Decreto 1377 de 2013, “*por el cual se reglamenta parcialmente la Ley 1581 de 2012*”, así como lo establecido en los Principios del Tratamiento de Datos personales:

Principios del tratamiento de datos personales:

- *Principio de legalidad: El tratamiento de datos personales debe estar sujeto a lo establecido en la normatividad vigente.*
- *Principio de finalidad: La finalidad del tratamiento de datos personales, debe ser informada a su titular.*
- *Principio de libertad: El tratamiento de datos personales sólo puede llevarse a cabo con el consentimiento previo, expreso e informado del titular de los mismos.*
- *Principio de veracidad o calidad: La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.*
- *Principio de transparencia: Garantizar al titular de los datos el derecho a obtener, por parte del encargado del tratamiento de estos, la información que le concierne.*
- *Principio de acceso y circulación restringida: El tratamiento sólo podrá hacerse por personas autorizadas por el titular o por las personas establecidas en la normatividad vigente sobre la materia.*
- *Principio de seguridad: La información sujeta a tratamiento se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.*
- *Principio de confidencialidad: Todas las personas que participen en el tratamiento de datos personales deben garantizar la reserva de dicha información.*

| | |
|---------------------------------|----------------------------------|
| Código: GTI-002-P | Versión: 9 |
| Fecha: Noviembre/2021 | Página Página 14 de 15 |

Los lineamientos generales en esta materia se pueden consultar en el documento **GTI-001-Po POLÍTICA DE TRATAMIENTO INFORMACIÓN PERSONAL**.

6.4 Política de la Operación de la Plataforma Tecnológica

La plataforma tecnológica de Computadores para Educar - CPE, será actualizada, modificada, operada, controlada y respaldada siguiendo prácticas que garanticen las características de seguridad, confidencialidad, control de acceso, integridad, disponibilidad y el no repudio de la información y las operaciones que se realicen sobre la misma.

- El proceso Gestión de TI, mantendrá un proceso continuo de monitoreo, análisis y evaluación del rendimiento y capacidad de su infraestructura tecnológica de procesamiento de información, con el fin de identificar y controlar el consumo de sus recursos y prever su crecimiento de forma planificada.

Separación de los ambientes de desarrollo, pruebas, y producción

- El proceso Gestión de TI, tiene definido el ambiente pruebas y ambiente de producción para la ejecución de actividades de pruebas y puesta en producción de sus aplicaciones de negocio, con el fin de garantizar la integridad de la información procesada y evitar interferencias en el desempeño y seguridad de cada uno de los ambientes.
- Los cambios a los distintos aplicativos, sistemas de información y medios se deberán poner en ambiente de pruebas antes de ser aplicados en el ambiente de producción.
- La información considerada como sensible o crítica para la entidad, no debe ser llevada a un ambiente de pruebas, salvo donde se requiera, deberá tener los controles necesarios que impidan la pérdida de su confidencialidad, integridad y disponibilidad.
- A través de la política de control de acceso de la entidad, se controla el acceso a cada uno de los ambientes.
- El área propietaria de la información debe aprobar las migraciones entre los ambientes de pruebas y producción de sistemas de información nuevos y/o de cambios.

Control de software operacional

- El proceso Gestión de TI, realizará seguimiento y control al software operacional instalado en los diferentes equipos de la entidad.

| | |
|---------------------------------|----------------------------------|
| Código: GTI-002-P | Versión: 9 |
| Fecha: Noviembre/2021 | Página Página 15 de 15 |

- La instalación de cualquier tipo de software en los equipos de cómputo de Computadores para Educar está sujeta al análisis previo de viabilidad por parte del proceso de Gestión de TI y, por tanto, son los trabajadores de esta área los únicos autorizados para aprobar dicha instalación.
- Los usuarios deben utilizar únicamente software licenciado y autorizado por el proceso de Gestión de TI. En caso de requerir la instalación de software adicional, el líder de proceso debe realizar la solicitud a la Subdirección de TI, con la debida justificación para revisión y a probación. La subdirección procederá a validar las condiciones de licenciamiento, seguridad y pertinencia para la instalación y uso del software solicitado.
- Por ningún motivo se autorizará la instalación de software que viole las leyes de propiedad intelectual y derechos de autor en especial la ley 23 de 1982 y relacionadas.

Protección contra software malicioso

- La entidad cuenta con herramientas de seguridad como Firewall, antivirus, AntiSpam, antispyware y otras aplicaciones las cuales brindan protección contra código malicioso, con el fin de evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso.
- El proceso Gestión de TI, debe proporcionar los mecanismos para generar cultura de seguridad entre los colaboradores, contratistas y proveedores frente a los ataques de software malicioso.
- Asegurar que el software del Firewall, antivirus, AntiSpam, antispyware y otras aplicaciones cuente con las licencias de uso requeridas, posean las últimas actualizaciones y parches de seguridad certificando así su autenticidad.
- Los colaboradores, contratistas y proveedores, que sospechen o detecten alguna infección por software malicioso deben notificar al proceso Gestión de TI, mediante los canales destinados para tal fin.
- Así mismo, la entidad define los siguientes lineamientos que no están permitidos:
 - La desinstalación y/o desactivación de software y herramientas de seguridad avaladas previamente por la entidad
 - Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.
 - Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo.