Política de Seguridad de la Información

Corporación de Educación Tecnológica de Colsubsidio

https://cetcolsubsidio.edu.co/

Colsubsidio Educación Tecnológica

ACTA 11032021

Marzo 11 de 2021

Por el cual se establece la

Política de seguridad de la

Información

De la Corporación de Educación Tecnológica Colsubsidio

El Consejo Superior de la Corporación de Educación Tecnológica Colsubsidio en uso de sus atribuciones estatutarias,

Considerando

Propender a la comunidad educativa los recursos tecnológicos adecuados que faciliten el desarrollo de las funciones sustantivas de la educación superior tomando como base los principios orientadores de la ley 1341 del 30 de julio de 2009 en el que se menciona:

> *"la investigación, el fomento, la promoción y el desarrollo de las tecnologías de la información y las comunicaciones con una política de estado que involucra a todos los sectores y niveles de la administración pública y de la sociedad, para contribuir al desarrollo educativo, cultural, económico, social y político e incrementar la productividad, la competitividad, el respeto a los derechos humanos inherentes y la inclusión social".*

Que, el Decreto 1330 del 25 de julio de 2019 establece que la institución contará con: "Recursos suficientes para garantizar el cumplimiento de las metas. Se refiere a la existencia, 'gestión y dotación de los recursos tangibles e intangibles que le permiten desarrollar a la institución sus labores formativas, académicas, docentes, científicas, culturales y de extensión. Para tal fin, la institución deberá definir su misión, propósitos y objetivos institucionales, los cuales orientarán los requerimientos de: talento humano, recursos físicos, tecnológicos, y financieros, en coherencia con las modalidades (presencial, a distancia, virtual, dual u otros desarrollos que combinen e integren las anteriores modalidades), los niveles de formación, su naturaleza jurídica, tipología, identidad y misión institucional"

Que, en el mismo Decreto 1330 de 25 de julio de 2019, artículo 2.5.3.2.3.1.7, literal b) La institución deberá demostrar la disponibilidad, acceso y uso infraestructura y tecnológica coherente con los requerimientos de las labores formativas, académicas, docentes, científicas, culturales y de extensión, de bienestar y de apoyo a la comunidad académica, definidos por la institución y que sean comunes para todos los programas en sus niveles formación y modalidades (presencial, a distancia, virtual, dual u desarrollos que combinen e integren modalidades).

Por lo anterior, a continuación, se describe la política institucional que aplica para dar respuesta a las necesidades

enunciadas en materia de Tecnología.

Establece:

CAPÍTULO I:
DEFINICIONES

1. DEFINICIONES

Seguridad de La Información: La seguridad de la información significa la protección de la información y los sistemas de información del acceso no autorizado, la divulgación, la alteración, la modificación o destrucción. La gestión de la seguridad de la información se apoya en el cumplimiento de tres criterios: 1. La confidencialidad 2. La Integridad y 3. La Disponibilidad.

Confidencialidad de la Información: Se refiere a la preservación de las restricciones o limitantes que la Corporación, sus entes reguladores y sus obligaciones con los clientes han fijado para autorizar el acceso y la divulgación, así como los medios para la protección de la intimidad personal y propiedad de la información.

Integridad de la Información: La protección contra la modificación, exactitud o completitud de toda información que pertenezca a las actividades de la Corporación o sus transversales.

Disponibilidad de la información: Acceso oportuno y confiable del uso de la información de cada una de las unidades organizacionales de la Corporación.

Activo de información: Para la Corporación los activos corresponden a los objetos materiales o intangibles asociados con la información y que son requeridos para la operación de las actividades de los negocios.

BSIMM: Está diseñado para ayudar, comprender, medir y planificar una iniciativa de seguridad del software.

Cifrar: Es la codificación del contenido de un mensaje o archivo para que llegue solamente a la persona autorizada a recibirlo.

Código malicioso: Programas potencialmente peligrosos diseñados para dañar los sistemas y los datos, o modificarlos para que funcionen de manera incorrecta.

Correo electrónico: Es una herramienta de comunicación que permite intercambiar mensajes de texto y archivos adjuntos entre los equipos de la red de datos y entre estos e Internet.

Cuenta de usuario de una aplicación: Se asigna a un usuario para tener acceso a un sistema de aplicación (aplicativo). Tiene un nombre de usuario y una contraseña.

Cuenta de usuario de Windows: Se asigna a un usuario para tener acceso a un computador de la red de datos de la Corporación que tenga sistema operativo Windows. Tiene un nombre de usuario y una contraseña.

Fax: Es una herramienta de comunicación que permite intercambiar documentos físicos a través de un medio electrónico, entre las diferentes áreas de la organización o entre esta y el exterior.

File Server: Repositorio de información asignado a un área o proceso para guardar información, este sitio debe tener controles de ingreso de escritura, modificación o eliminación.

Internet: Es una red mundial de computadores en donde se publica información de todo tipo sin ningún control de contenido. Para consultar la información en mención se utiliza un navegador (browser) en leguaje html.

Intranet: Es una red de computadores limitada al interior de una organización o área específica la cual presta servicios similares a los de Internet. Para la Corporación, es un sistema de comunicación interactivo mediante el cual se puede emitir, recibir y compartir información de interés general para los funcionarios.

Medios de almacenamiento extraíbles: Medios para guardar y portar información de forma electrónica tales como disquetes, CD's, DVD's, discos ZIP, discos ópticos, discos duros externos, memoria digital USB, etc.

Microsoft SDL Security Development Lifecycle (SDL): Es un proceso de desarrollo de software que ayuda a los desarrolladores a crear software y los requisitos de cumplimiento de seguridad de direcciones más seguras al tiempo que reduce los costes de desarrollo.

OWASP: Es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro.

Periférico: Elemento o dispositivo del computador que no hace parte de la unidad central, tales como el monitor, mouse, teclado, parlantes, impresora, escáner, unidades de almacenamiento, etc.

Pruebas de Penetración: Tiene como principal propósito detectar vulnerabilidades que resultan de fallas en el software, configuraciones inapropiadas entre otras. Se puede realizar de forma remota o local y se ejecutan las pruebas tal y como lo intentaría un intruso con propósitos adversos para la organización.

Publicar: Es el acto mediante el cual se publica información, esta puede ser confidencial, sensible o privada.

Sistema operativo: Programa de computador que organiza y gestiona todas las actividades que sobre él se ejecutan. Algunos sistemas operativos son Windows, Unix y Linux.

Software Libre: Es software donde los usuarios tienen la libertad para ejecutar, copiar, distribuir, estudiar, modificar o mejorar el software. Este tipo de software debe ser autorizado por el centro de servicios compartidos. Se pueden encontrar diferentes distribuciones como shareware el cual cobra un monto de dinero para poder utilizar el software completamente y GNU que se caracteriza por ser compatible con UNIX.

Spam: Se denomina correo electrónico basura (en inglés también conocido como junk-mail o Spam) a una cierta forma de inundar la Internet con muchas copias (incluso millones) del mismo mensaje, en un intento por alcanzar a gente que de otra forma nunca accedería a recibirlo y menos a leerlo.

Teletrabajo: Una forma de organización laboral, consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y comunicación TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo.

USB (Universal Serial Bus): Puerto Serial Universal del computador al cual se pueden conectar los periféricos.

VPN: Es una tecnología que permite la extensión de una red privada en un espacio de red público, pero protegido por un canal virtual. Para los negocios es de vital

CAPÍTULO II
DECLARACIONES Y SEGURIDAD DE LOS RECURSOS

2. DECLARACIONES

1. La información es considerada por Corporación de Educación Tecnológica como un activo productivo y como tal, hace parte fundamental de la operación diaria, convirtiéndose en un componente esencial e imprescindible que debe

ser protegido para el cumplimiento de sus objetivos estratégicos de negocio. Este aspecto hace que todos aquellos a quienes se le haya autorizado el acceso a la información, sean responsables por el buen uso que se le dé a la misma.

2. La jefatura administrativa y financiera de la CET es responsable de requerir a los usuarios, empleados, contratistas y vinculados el cumplimiento de las medidas y mecanismos de seguridad de la información, lineamientos y procedimientos establecidos por la Corporación.

3. Todos los empleados, contratistas y vinculados que tengan relación contractual con Corporación de Educación Tecnológica Colsubsidio están obligados a conocer, entender, cumplir y hacer cumplir los lineamientos de seguridad y protección de la información y procedimientos establecidos por la Corporación.

4. Todo empleado, tercero o vinculado a Corporación de Educación Tecnológica Colsubsidio se compromete con la protección de la información y de la infraestructura tecnológica con el objetivo de asegurar su confidencialidad, integridad y disponibilidad.

5. El incumplimiento de los lineamientos aquí expresados, acarrearan acciones disciplinarias y sancionatorias a que haya lugar.

3. SEGURIDAD DE LOS RECURSOS HUMANOS

1. Todos los empleados deben cumplir con los procedimientos de verificación y contratación exigidos por parte de la Corporación.

2. Los empleados de la Corporación de Educación Tecnológica Colsubsidio deben recibir a su ingreso a la Corporación y durante su permanencia, inducciones en temas de seguridad de la información, así como dejar constancia del conocimiento respecto a las medidas y mecanismos de seguridad de la información, lineamientos y procedimientos establecidos por la Corporación que sean de su inherencia.

4. Ante cambios de cargo o terminación de contrato laboral, el empleado debe hacer entrega formal de los activos de información que le fueron asignados por la Corporación de Educación Tecnológica Colsubsidio para sus actividades laborales, tales como información física impresa y lógica que se encuentre en medios de almacenamiento externos como pendrive, discos duros, equipos de cómputo, servidores, bases de datos, entre otros.

4. GESTIÓN DE LOS ACTIVOS

1. Toda información debe estar identificada, clasificada y valorada acorde con el procedimiento de clasificación de información definido por la Corporación de Educación Tecnológica Colsubsidio el cual debe ser ejecutado con la periodicidad requerida en conjunto con el responsable designado por la Jefatura Administrativa y Financiera.

2. Los activos de información de la Corporación de Educación Tecnológica Colsubsidio deben contar con un custodio y un responsable de la información.

3. Todo activo de información debe contar con los controles asociados al valor que este posea para la Corporación de Educación Tecnológica Colsubsidio.

4. Ningún empleado o tercero vinculado a Colsubsidio puede divulgar información confidencial de la Corporación de Educación Tecnológica Colsubsidio, sus clientes y afiliados a personas no autorizadas.

5. El tratamiento y manejo que tendrá el activo de información en la corporación se definirá acorde a su nivel de clasificación.

6. Los activos de información que deban ser enviados y/o compartidos deberán estar etiquetados para este fin acorde con su nivel de confidencialidad.

7. La información física y los dispositivos de almacenamiento que contienen datos sensibles, deben destruirse físicamente o sobrescribir cuando ya no sean requeridos por el negocio, de tal forma que los datos no se puedan recuperar.

8. Los controles para la custodia de información sensible de la Corporación de Educación Tecnológica Colsubsidio deben estar acordes al nivel de su importancia para el negocio y el cumplimiento de dichos controles será una responsabilidad del Proceso Administrativo y Financiero.

CAPÍTULO III
CONTROL DE ACCESO LOGISTICO

5. CONTROL DE ACCESO LÓGICO

1. Las cuentas de usuario deben ser asignadas a las personas de acuerdo con el rol desempeñado en la Corporación

de Educación Tecnológica Colsubsidio y según las necesidades específicas del cargo.

2. Toda transacción y actividad realizada con la cuenta de usuario asignada a los sistemas de información de la Corporación de Educación Tecnológica Colsubsidio, será responsabilidad del propietario de dicha cuenta.

3. Las contraseñas o cualquier otro método de autenticación deben mantenerse bajo reserva y ser entregadas de forma personal o a través de un medio que asegure su confidencialidad.

4. Las cuentas de usuarios, contraseñas o cualquier otro mecanismo de autenticación a los sistemas de información, deben ser tratadas como información confidencial de la Corporación de Educación Tecnológica Colsubsidio, por lo cual no se deben divulgar, publicar ni compartir con ninguna persona.

5. Las cuentas creadas para los diferentes sistemas de procesamiento de información deben ser deshabilitadas una vez finalizadas o interrumpidas las funciones de los empleados o proveedores.

6. El aprovisionamiento de súper usuarios se hará con base en requerimientos de mantenimiento, falla de los sistemas y configuraciones.

7. Empleados, proveedores y contratistas no podrán en ejercicio de las actividades consignadas en un contrato firmado con Corporación de Educación Tecnológica, utilizar usuarios genéricos para ningún tipo de actividad.

8. Las cuentas administradoras deben ser totalmente independientes a las cuentas personales, únicamente se debe usar la cuenta administradora solo cuando sea estrictamente necesario, el uso de estos privilegios debe estar autorizado por la Dirección Administrativa y Financiera

9. Los perfiles estándar o aquellos que brinden todos los privilegios y accesos a los diferentes sistemas de información, no deben ser asignados en el ambiente productivo, sobre ningún usuario final y/o rol; exceptuando casos en los cuales que por razones propias de negocio se requiera su uso, por lo cual deben estar aprobados por la Jefatura Administrativa y Financiera y

10. Las carpetas creadas para almacenar información (file server) de los empleados, deben estar administradas teniendo en cuenta la siguiente información:

- No se deben otorgar permisos de control total.
- El acceso a las carpetas debe estar limitado al área o proceso al cual pertenece el usuario.
- Los permisos para crear, eliminar, ejecutar, leer y modificar se deben limitar de acuerdo con el cargo desempeñado.

11. Las cuentas de usuario deben ser asignadas a las personas que explícitamente lo han solicitado a través de los sistemas dispuestos para este fin través de procedimiento de Gestión de Accesos establecido.

12. Se debe informar al área encargada acerca de las novedades de terminación de contrato, vacaciones, licencias,

incapacidades o cambios de cargo de los empleados y terceros vinculados a la Corporación de Educación Tecnológica Colsubsidio.

CAPÍTULO IV
CORREO ELECTRONICO

6. CORREO ELECTRÓNICO

1. El acceso al correo electrónico está reservado para todos aquellos empleados que lo requieran de acuerdo con las necesidades del negocio y para el desempeño de las funciones propias del cargo.

2. Los mensajes por correo electrónico son considerados parte de los registros de los activos de información, por lo que están sujetos a directrices de monitoreo, auditoría e investigación de eventos.

3. No se permite el uso o envío del correo electrónico para actividades personales, comerciales, mensajes en cadena que contengan bromas, advertencias de software malicioso, mensajes con contenido religioso, juegos, racista, sexista, pornografía, publicitario no corporativo, político, mensajes mal intencionados o cualquier otro tipo de mensajes que no estén autorizados, atenten contra la dignidad de las personas o que comprometan de alguna forma los activos de información de la Corporación de Educación Tecnológica Colsubsidio.

4. La transmisión de mensajes en forma masiva utilizando el correo electrónico, debe ser autorizada por la Jefatura Administrativa y Financiera, cuyo contenido tratará únicamente asuntos relacionados con las operaciones de la Corporación de Educación Tecnológica Colsubsidio.

5. Todas las comunicaciones emitidas y/o recibidas por correo electrónico, deben preservar la conducta ética y profesional que el remitente y/o destinatario debe mantener como miembro de la Corporación de Educación Tecnológica Colsubsidio.

6. Todos los mensajes de correo electrónico deben ser considerados como información sensible. El correo electrónico debe ser manejado como una comunicación directa entre un remitente y un destinatario autorizado, en tal sentido, los empleados no deberán utilizar cuentas de correo electrónico asignadas a otra persona para enviar o recibir mensajes.

7. La Jefatura Administrativa y Financiera debe cumplir con los esquemas para el almacenamiento (respaldo), retención y destrucción de correos electrónicos. Adicionalmente, el sistema de correos electrónicos debe estar configurado de tal manera que todos los mensajes recibidos y/o enviados queden debidamente registrados en logs para ser revisados en caso de ser requeridos y borrado con una frecuencia establecida según el procedimiento de respaldo de plataforma tecnológica.

8. Si se reciben mensajes con archivos adjuntos o enlaces de dudosa procedencia no se deben abrir ya que pueden contener software malicioso como virus y troyanos que afecten los sistemas de información de la Corporación de Educación Tecnológica Colsubsidio. Estos casos se deben reportar a la mesa de ayuda y comunicados como un incidente a la Jefatura de Seguridad de la Información de Colsubsidio.

CAPÍTULO V
INSTALACIÓN Y USO DE PCs, PERIFERICOS Y MEDIOS DE ALMACENAMIENTO EXTRAIBLES

7. INSTALACIÓN Y USO DE PCs, PERIFERICOS Y MEDIOS DE ALMACENAMIENTO EXTRAIBLES

1. No se permite el uso de computadores, periféricos, medios de almacenamiento extraíbles de propiedad del empleado en cualquiera de las sedes de la Corporación de Educación Tecnológica Colsubsidio.

2. No se permite la activación de puertos y uso de dispositivos USB sin la autorización del Jefe Administrativo y Financiero. En caso de usar algún medio de almacenamiento extraíble autorizado, este debe ser verificado previamente por el software Antivirus.

3. Con el fin de proteger la información y el acceso a la red de la Corporación, los empleados deben guardar en un sitio seguro el equipo portátil asignado.

4. No está autorizado el uso de recursos informáticos (datos, hardware, software, redes, servicios, etc.) y de telecomunicaciones (teléfono, fax, etc.) para actividades que no estén autorizadas o relacionadas con la operación de la Corporación de Educación Tecnológica o diferentes a las funciones asignadas al cargo que desempeña el funcionario.

5. Toda instalación, configuración, mantenimiento y actualización de hardware y software que genere un impacto alto o medio sobre los negocios, debe cumplir con el procedimiento de control de cambios definido por la Corporación de Educación Tecnológica Colsubsidio y contar con las autorizaciones respectivas.

6. Ninguna aplicación, sistema, dispositivo de hardware, computadores o en general cualquier recurso que tenga que ver con Tecnología de Información podrá ser utilizado en el ambiente tecnológico de la Corporación de Educación Tecnológica Colsubsidio sin contar con los controles mínimos necesarios de seguridad establecidos en este documento y autorizados por la Jefatura Administrativa y Financiera.

CAPÍTULO VI
DISPOSITIVOS MOVILES Y TRABAJO EN CASA

8. DISPOSITIVOS MOVILES

1. Todo dispositivo móvil (iPad, teléfonos inteligentes, laptops, entre otros) con acceso a la red de la Corporación,

bien sean de propiedad de la Corporación de Educación Tecnológica Colsubsidio o personal, deberán sin excepción, ser configurados con los controles mínimos definidos para estos elementos.

2. Todo computador portátil (laptop) que contenga información confidencial debe contar con el cifrado de su disco duro.

3. Está prohibido el uso de funciones de equipos móviles como medio de almacenamiento, grabación y capturar información de la Corporación al que el usuario no esté autorizado por la Corporación de Educación Tecnológica Colsubsidio.

4. En caso de pérdida o hurto de un dispositivo móvil que se encuentre autorizado para acceder a las aplicaciones o información de la Corporación, se debe notificar de manera inmediata a la Jefatura Administrativa y financiera con el fin de deshabilitar las cuentas de usuario respectivas y evitar accesos no autorizados a la información.

5. Los empleados, contratistas o terceros que requieran el uso de dispositivos móviles con acceso a la red de Corporación de Educación Tecnológica, deben seguir los lineamientos establecidos para estos elementos.

9. TELETRABAJO / TRABAJO EN CASA

1. Los usuarios que por razones propias del negocio se encuentren autorizadas para realizar teletrabajo, serán responsables por la protección física del equipo asignado contra acceso, uso no autorizado, hurto, pérdida o daño.
2. Las conexiones que se realicen desde y hacia los equipos destinados para teletrabajo, se deben hacer a través de VPN con el fin de dar aseguramiento a los activos de información de la Corporación.

3. La Jefatura Administrativa y Financiera implementará los controles necesarios para el aseguramiento de los equipos de teletrabajo contra acceso lógico no autorizado, protección de la información y la red Corporativa.

CAPÍTULO VII
SISTEMAS DE INFORMACION Y SEGURIDAD FISICA

10. SISTEMA DE INFORMACIÓN

1. Los empleados que son administradores y usuarios de los sistemas de información de la Corporación de Educación Tecnológica son responsables del buen uso de la información que tienen a su cargo.
2. La Jefatura Administrativa y financiera es la única área autorizada para administrar los activos de información que se publica en la Intranet.
3. La Jefatura Administrativa y financiera es la única área autorizada para publicar información, crear usuarios en redes sociales, blogs, usar logos de la Corporación o cualquier otro tipo de contenido a nombre de la Corporación de Educación Tecnológica.

4. Se prohíbe almacenar usuarios y contraseñas de acceso a las aplicaciones de la Corporación en cualquier medio físico, magnético o electrónico.

5. Toda instalación, configuración, mantenimiento y actualización de hardware y software debe ser realizada por la Jefatura Administrativa y Financiera.

11. SEGURIDAD FÍSICA

1. Todo espacio físico donde resida la infraestructura tecnológica necesaria para la operación de la Corporación debe contar con mecanismos de acceso para la restricción de personal no autorizado como son los centros de cómputo, centros de cableado, entre otros.

2. Deben existir controles ambientales operando eficientemente en las sedes en las cuales se encuentre la infraestructura tecnológica necesaria para la operación de la Corporación como centros de cómputo, centros de cableado, entre otros.

3. Toda persona que visite las instalaciones de la Corporación debe cumplir con los controles de acceso físico dispuestos.

4. Todo equipo de cómputo de uso personal o de la corporación debe ser registrado por los responsables de seguridad física al ingreso y salida de las instalaciones de la Corporación de Educación Tecnológica.

5. El movimiento o traslado de equipos de cómputo, recursos informáticos y de comunicaciones, debe realizarse únicamente por la Jefatura Administrativa y Financiera con el fin de evitar pérdida, hurto o daño de los activos de información de la Corporación.

6. Todo ingreso de personas a los centros de cómputo de la Corporación de Educación Tecnológica debe quedar registrado en la bitácora de ingreso de visitantes.

7. El acceso físico a los centros de procesamiento de datos y cableado debe ser responsabilidad de la Jefatura Administrativa y Financiera.

8. Todos los empleados y contratistas deben portar en un lugar visible en todo momento el carné que los identifique como vinculados a la Corporación.

9. Todos los empleados y terceros vinculados a la Corporación deben tener acceso única y exclusivamente a las áreas de la Corporación de acuerdo con su rol y funciones. Cualquier excepción a los lineamientos dados en este documento, deberá contar con las autorizaciones respectivas.

10. La información física sensible de la empresa debe guardarse bajo llave (gabinete, archivador u otro medio físico seguro) cuando no está en uso, especialmente ante ausencias temporales o prolongadas y según el riesgo catalogado para el activo de información.

11. Los computadores, fotocopiadoras, oficinas administrativas y demás sedes de cualquiera de los negocios de la Corporación deben estar inventariados por el software de control de impresiones para evitar el uso no autorizado.

12. Cualquier alteración en la información que se haga por medio de los equipos de la Corporación, por descuido del usuario, será de su responsabilidad. Se deben tomar precauciones a través del bloqueo de sesión para evitar que el computador quede expuesto y se use de manera no autorizada.
13. No se deben tener accesos directos de información catalogada como sensible en el computador asignado, con el fin de evitar daño, hurto, modificación, eliminación o accesos no autorizados

CAPÍTULO VIII
SEGURIDAD DE LAS OPERACIONES Y SEGURIDAD EN LA RED

12. SEGURIDAD DE LAS OPERACIONES

Backups de la información

1. Toda la información sensible que se encuentra almacenada en las plataformas tecnológicas de la Corporación y de proveedores, debe contar con actividades periódicas de Backups para garantizar acciones de restauración confiables en casos de emergencia y según sea requerido y autorizado por el responsable del activo de la información.

Instalación y Uso de Software

1. No se permite el uso de software de distribución gratuita, shareware, GNU, entre otros; a menos que haya sido previamente revisado y aprobado por la Jefatura Administrativa y Financiera.
2. Todas las adquisiciones de software deben estar avaladas por la a Jefatura Administrativa y Financiera.
3. No se permite descargar, instalar y/o ejecutar software o archivos sin la debida revisión y autorización de la Jefatura Administrativa y Financiera.
4. Todo el software de la Corporación está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está prohibido hacer copias o usar este software para fines personales.

13. SEGURIDAD EN LA RED

Uso de Internet y de la Red Interna

1. El acceso a Internet estará reservado para todos aquellos empleados que lo requieran según sus funciones de trabajo, de acuerdo con las necesidades de la Corporación y para uso laboral exclusivamente.
2. La Corporación restringirá el acceso a sitios de internet que por alguna circunstancia vayan en contra de sus lineamientos institucionales, lineamientos de seguridad y buenas prácticas adoptadas por la Corporación tales como

consultar material ilegal, de acoso, difamatorio, abusivo, amenazador, nocivo, vulgar, obsceno o de cualquier otra manera censurable.

3. No está permitido hacer uso de los recursos de la Corporación tales como dispositivos, redes para acceder a redes sociales, servicios interactivos de almacenamiento masivo, streaming de videos, páginas de mensajería instantánea.

4. Está prohibido a los empleados y terceros que tengan acceso a red inalámbrica o cableada de la Corporación, menoscabar o eludir los controles establecidos por la Corporación para la protección de los activos de información.

5. Cualquier tipo de ataque, así como efectuar un escaneo, prueba o penetración de sistemas de computación, redes en Internet, o redes internas, está estrictamente prohibido, salvo en casos debidamente autorizados por la Jefatura Administrativa y Financiera y por requisitos propios del negocio.

6. Los sistemas de comunicación tales como modems, routers, switch, entre otros dispuestos por la Corporación, son los únicos autorizados para su uso en la red Corporativa.

7. Queda prohibido toda publicación o intercambio de información sensible de la Corporación a través de cualquier medio físico, magnético o electrónico sin el consentimiento y la respectiva autorización del responsable de la información y en cumplimiento de los controles establecidos para la protección de la información.

Conexiones Remotas

1. Toda conexión remota a la red de la Corporación debe ser a través de canales seguros como VPNs o canales dedicados. Éstas deben solicitar autenticación para establecer la conexión remota a la red con el fin de prevenir accesos no autorizados.

2. Se permite el uso de VPN para usuarios previamente autorizados a través de la Jefatura Administrativa y Financiera que por actividades propias de la Corporación requieran acceso a los sistemas de información.

3. El uso de la VPN es exclusivo de quienes no se encuentren dentro de la red LAN de la Corporación y deban hacer uso de sistemas de información de manera remota debido a las exigencias particulares de sus actividades.

4. Un empleado, contratista o tercero vinculado a la Corporación con autorización de acceso a los sistemas de información a través de VPNs, deberá hacer uso correcto de los activos de información tal como lo especifica el presente documento.

5. Toda autorización para conexiones remotas por parte de proveedores debe tener una vigencia, una contraseña de acceso y una cuenta de usuario que deberá ser bloqueada una vez finalizada las labores para las cuales se crea.

6. Toda conexión remota sea de empleados o proveedores de la Corporación, será monitoreada y podrá ser bloqueada en caso de identificar situaciones inusuales respecto al uso de la cuenta y el acceso a los activos de información.

CAPÍTULO IX
SEGURIDAD EN LOS DESARROLLOS, PROVEEDORES Y AFILIADOS

14. SEGURIDAD EN LOS DESARROLLOS

1. Se deben identificar los activos de información y los riesgos asociados para nuevos desarrollos o proyectos, con el fin de establecer los controles para el aseguramiento de la información.
2. Los datos de salida de los aplicativos que manejan información sensible deben contener los datos relevantes requeridos para el uso de acuerdo con el rol y se deberán enviar exclusivamente a los usuarios y/o terminales autorizadas.
3. Los aplicativos de la Corporación deben pasar por un proceso de pruebas y aceptación en un ambiente dedicado para tal fin antes de ser liberados a producción.
4. El acceso a la información contenida en las bases de datos sólo está permitido a través de las aplicaciones de los sistemas de la Corporación. Sólo tendrán acceso los usuarios autorizados que de acuerdo con su rol se identifican mediante usuario y contraseña.
5. Con el fin de preservar la confidencialidad de la información, a efectos de no vulnerar las condiciones de seguridad de acuerdo con su clasificación, la información que está en producción no debe ser utilizada para desarrollo o pruebas.
6. Para todo desarrollo se debe considerar la seguridad de la Información desde el inicio del proceso de diseño de los sistemas, pasando por cada una de las fases de desarrollo hasta su liberación a producción.
7. Los sistemas de procesamiento y almacenamiento de información de los sistemas operativos y aplicaciones deben contar con los últimos parches de seguridad provistos por el fabricante debidamente aprobado e instalado, con el fin de dar el aseguramiento adecuado.
8. No está permitido el acceso a personal no autorizado a editores, compiladores o cualquier otro tipo de utilitarios que estén asociados al ambiente productivo, cuando no sean indispensables para el funcionamiento de este.
9. Se debe contemplar en el mantenimiento y en la fase de los desarrollos, el establecimiento de buenas prácticas que provean el diseño, aseguramiento y ejecución para la protección de la información a través de buenas prácticas como OWASP, Microsoft SDL, BSIMM, entre otras.

15. PROVEEDORES Y AFILIADOS

Intercambio de Información

1. Los Proveedores, contratistas o terceros vinculados a la Corporación deben garantizar que el intercambio de información desde y hacia la Corporación cumple con las exigencias que éste defina con base en las leyes y regulaciones vigentes, así como también las medidas y lineamientos de seguridad y protección de la información

señaladas en este documento. Acuerdo de Niveles de Servicio.

2. Los Proveedores y Contratistas de la Corporación deben conocer y cumplir los acuerdos de niveles de servicio que se hayan definido en el marco del contrato celebrado entre las partes.

3. Los Proveedores o Contratistas deben informar inmediatamente al gestor de contrato cualquier incidente que afecte la confidencialidad, integridad y disponibilidad de los activos de información que ponga en riesgo la operación de la Corporación.

Acuerdos de Confidencialidad

Los Proveedores y Contratistas vinculados a la Corporación que tengan acceso a la información de la Corporación, deben firmar una cláusula de confidencialidad para su uso con el fin de proteger dicha información. Contratos

1. Los proveedores y contratistas deben contar con contratos vigentes de servicios, cumplir la legislación Colombia vigente, las medidas y lineamientos aquí establecidos y demás disposiciones dispuestas por la Corporación.

Uso de Portales Transaccionales

1. Los portales transaccionales deben tener publicado en su "home" las medidas y lineamientos de seguridad y protección de la información con alusión al uso de los activos de información de la Corporación, la cual debe ser de conocimiento de los usuarios y su aplicación es obligatoria.

2. Se debe por parte de los usuarios cambiar la contraseña por lo menos una vez al mes, con el fin de evitar accesos no autorizados

Uso de Sistemas de Información

1. Los usuarios que tengan acceso a sistemas de información de la Corporación deben conocer y aplicar las medidas y lineamientos de seguridad y protección de la información definida por la Corporación.

2. Los usuarios deben utilizar los sistemas de información y comunicación dispuestos por la Corporación solo para los fines de consulta que estos brindan y bajo ningún aspecto se debe tratar de ingresar a la red para consultar material ilegal, de acoso, difamatorio, abusivo, amenazador, nocivo, vulgar, intrusivo, obsceno o de cualquier otra manera censurable, o a la información de la Corporación para borrar, capturar, modificar o cualquier otra manifestación que esté en contra de las medidas y lineamiento de seguridad aquí definidas por la Corporación y la legislación Colombiana vigente.

3. Los usuarios deben mantener una solución confiable de antivirus en el computador desde el cual realizan sus

transacciones y que ésta se mantenga actualizada con las últimas firmas, con el fin de prevenir ataques provenientes por software malicioso.

4. Los usuarios deben realizar sus transacciones desde computadores seguros y confiables, para prevenir la captura de información por parte de usuarios no autorizados.

5. Los usuarios deben mantener actualizado los últimos parches de seguridad del sistema operativo y las diferentes aplicaciones, con el fin de evitar accesos no autorizados.

CAPÍTULO X
INCIDENTES DE SEGURIDAD Y CUMPLIMIENTO REGULATORIO

16. INCIDENTES DE SEGURIDAD

1. Todos los empleados y contratistas vinculados a la Corporación deben estar conscientes de los procedimientos y su importancia para reportar incidentes de seguridad.
2. Los empleados que utilicen servicios de información de la Corporación deben reportar cualquier sospecha de amenazas o debilidades en los sistemas o servicios de la Corporación. Dichos reportes deben ser comunicados a la Jefatura Administrativa y Financiera.
3. Se debe reportar a la Jefatura Administrativa y Financiera, cualquier incidente de seguridad que pueda comprometer la confidencialidad, integridad y/o disponibilidad de los activos de información de la Corporación, siguiendo el procedimiento de notificación de incidentes establecido.

17. CUMPLIMIENTO REGULATORIO

1. La Corporación velará por el cumplimiento de las medidas y lineamientos de seguridad de la información estipuladas por la Corporación y la legislación aplicable vigente por los entes de control.
2. Todos los empleados están obligados a ceder a la Corporación los derechos exclusivos de propiedad literaria, licencias, invenciones, u otra propiedad intelectual que ellos creen o desarrollen durante su periodo laboral con la Corporación. En el caso de aplicaciones de terceros, este aspecto se regirá por las condiciones y cláusulas establecidas en el contrato de adquisición de productos y/o servicios, con la finalidad de prevenir cualquier disputa respecto a la propiedad del software, licencias, entre otros, una vez que el proyecto sea completado.
3. La Corporación tiene propiedad legal de la información Corporativa almacenada, enviada y compartida en todos sus computadores, sistemas de información y comunicación que hayan sido transmitidos por medio de estos recursos, por lo cual se reserva el derecho de acceder a esta información sin autorización del autor o usuario del recurso, así como también se reserva el derecho de disponer de toda la información que cualquier empleado haya colocado en los medios de comunicación existentes en la Corporación.
4. La Corporación se reserva el derecho de monitorear los computadores que sean de su propiedad y estén

conectados o no a la red Corporativa en caso de presentarse incidentes que afecten la seguridad de la información de la Corporación

5. Los registros de información de la Corporación clasificados como confidencial deben estar adecuadamente protegidos por el responsable de la información contra pérdida, destrucción y falsificación. Aquellos documentos que estén bajo lineamientos legales o regulatorios deberán ser resguardados bajo las medidas de seguridad adecuadas para garantizar su integridad

6. La Dirección Administrativa y Financiera, deberá revisar periódicamente los acuerdos de licencias de hardware y software instalado a fin de verificar el cumplimiento de estos por parte de la Corporación.

7. Los contratistas y terceras partes deben cumplir con las disposiciones establecidas por la Legislación Colombiana vigente asociados a la de protección de datos personales, propiedad intelectual y seguridad de la información.

CAPÍTULO XI
CONSIDERACIÓN FINAL

1. La reglamentación y las situaciones no previstas en la presente política serán responsabilidad de la Jefatura administrativa y financiera

CAPÍTULO XII
VIGENCIA

2. La presente política rige desde su publicación y regula las situaciones que se realicen después de su vigencia.

Dado en Bogotá D.C. a los once (11) días del mes de marzo de dos mil veintiuno (2021).