Contenido

1. POLITICAS DE SEGURIDAD INFORMATICA

Las políticas de seguridad tienen como objeto establecer las medidas de índole técnico y de organización que son necesarias para garantizar la seguridad de las tecnologías de la información que comprenden equipos de cómputo, bases de datos, infraestructura de voz y datos y del personal que interactúa directamente u ocasionalmente con estas áreas de la información en la Corporación Tecnológica de Bogotá.

2. DISPOCIONES GENERALES

2.1 Definiciones

2.1.1 Administrador de base de datos

Es el responsable de los aspectos técnicos, tecnológicos, científicos, la inteligencia de los negocios y legales de la base de datos.

2.1.2 Administrador de la tecnología y la información

Administrador de tecnológica y la información, es el responsable de administrar todos los equipos de cómputos, sistemas de información y redes de cómputo, está en cargado en vigilar el buen funcionamiento de todos los procesos informáticos, redes de cómputo y de comunicación.

El proceso de TIC en la Corporación Tecnológica de Bogotá está conformado por 3 personas las cuales tienen diferentes funciones a su cargo como soporte y mantenimiento de los equipos de cómputo, administración de bases de datos, administración de redes de computo, gestión de los recursos tecnológicos, administración de las plataformas tecnológicas. Por esta razones es necesario establecer políticas de uso de esta infraestructura para la seguridad de los recursos he información perteneciente a la Corporación.

El departamento de TIC está conformado por el director del departamento, líder funcional de SIA y el auxiliar de mantenimiento con las siguientes responsabilidades.

a) Mantener en buen funcionamiento todos los equipos de cómputo que se utilizan en las 2 sedes de la Corporación.

b) Definir estrategias de mejoramiento de los equipos de cómputo, comunicaciones y redes de computo acorto mediano y largo plazo.

c) Ejercer control sobre el servicio prestado en cuanto a calidad en las soluciones y los tiempos de respuesta.

d) Mantener el inventario actualizado de los equipos tecnológicos de la Corporación

e) Divulgar y hacer respetar las políticas de seguridad informática establecidas, la divulgación de las políticas está sometida a los espacios de trabajo de cada funcionario o a las reuniones que sean de conveniencia asignadas por la Corporación para hacer este tipo de divulgaciones.

2.1.3 Comité

Equipo integrado por la Rectoría y los jefes de los procesos y algunos casos el personal administrativo cuando son convocados donde se puede tratar temas como:

a) Establecer el uso de los medios tecnológicos
b) Adquisición de hardware y software.
c) establecer la arquitectura tecnológica necesaria para el funcionamiento de las actividades institucionales
d) capacitaciones para los empleados en el manejo de los equipos de cómputo dándoles a conocer las políticas de seguridad informática.

2.1.4 Contraseña

Palabra o frese o señal que solo conoce el usuario del equipo de cómputo, la cual le permite el ingreso al sistema.

2.1.5 Datacenter

Cuarto con los diferentes equipos de cómputo (servidores) y de comunicaciones con las condiciones ambientales adecuadas para prestar servicios de comunicación y de redes y plataformas tecnológicas a las diferentes áreas de trabajo.

2.1.6 Rectoría

Persona que marca, dirige y lidera la Corporación Tecnológica de Bogotá conforma diferentes comités bajo administración y seguimiento.

2.1.7 Gestor de seguridad

Es la persona preparada con los conocimientos para prestar seguridad de la información de una forma adecuada, realizando diferentes actividades de seguridad como auditorias de seguridad, llevar un control de los servicios de seguridad de cada equipo.

2.1.8 Red

Sistema debidamente organizado de equipos de cómputo que cumple una función previamente asignada en cuanto a comunicación con diferentes dispositivos para efectos de traslado de información y de seguridad.

2.1.9 Responsable de los activos.

Personal del proceso de Administrativo que es responsable por el funcionamiento de los diferentes activos teniendo actualizado el inventario en los diferentes Procesos y es responsable de mantener al día las diferentes pólizas de protección para los activos tanto informáticos como de las diferentes áreas.

2.1.10 Usuario

Cualquier Colaborador de la Corporación Tecnológica de Bogotá que haga uso de los equipos de cómputo o de comunicación de las diferentes dependencias.

2.1.11 Virus informático

Código malicioso con habilidades de ejecutarse y reproducirse, esta como archivo oculto en documentos del usuario para no causar sospechas, algunas de sus funciones es dañar archivos he infectar el sistema operativo causando daños permanentes en la información o están dedicados al robo de información importante como bancaria, claves de correos etc.

3. ALCANCE

Este manual esta creado pensado en las diferentes necesidades de seguridad que tiene la Corporación Tecnológica de Bogotá identificando los diferentes puntos débiles del eslabón para evitar filtraciones de agentes externos perjudicando el buen funcionamiento de los equipos de cómputo y las funciones de los diferentes procesos.

Las políticas de seguridad son aplicables a todos los funcionarios de la corporación tecnológica de Bogotá, personal externo, personal contratado

eventualmente y empleados de otras instituciones o Empresas que requieran conectar un equipo de cómputo a la Red.

Esta política también cubre a todo equipo arrendado que deba de alguna manera utilizar red local o aceda a ella remotamente y a todo recursos tecnológico de la Corporación Tecnológica de Bogotá que haga uso e intercambio de archivos y programas.

Estas normas están analizadas con el fin de proteger los diferentes equipos de cómputo, comunicaciones y redes sin afectar las diferentes funciones que ejercen los usuarios en los procesos garantizándoles las diferentes actividades básicas para el buen desarrollo, no es una camisa de fuerza más bien se pretende que los usuarios tenga un modelo adecuado que les garantice el buen funcionamiento de los recursos con seguridad y efectividad, respetando todo el tiempo los estatutos y reglamentos institucionales.

4. OBJETIVOS

1. Informar todos los usuarios de la Corporación Tecnológica de Bogotá de las de las políticas de seguridad que deben cumplir para proteger el hardware y software de la red así como la información que se almacena en ellos.

2. Ejecutar las diferentes actividades de mantenimiento de los equipos con el fin de garantizar el buen funcionamiento y la protección de la información que está contenida en los diferentes dispositivos.

Los objetivos para alcanzar una vez establecida las normas de política de seguridad:

1. Implantar el esquema de seguridad que nos determine las funciones que se deben de seguir para mantener los equipos en perfecta funcionalidad y la integridad de la información.

2. Establecer compromisos por parte de todos los funcionarios de la Corporación Tecnológica de Bogotá frente a los procesos de seguridad agilizando la aplicación de los controles.

3. Ganar calidad en los servicios de seguridad.

4. Convertir a todos los usuarios en promotores de seguridad.

5. VIGENCIA

Con los actuales avances de la tecnología las amenazas en la red son cada vez más efectivas y difíciles de detectar, lo cual hace que ningún sistema de seguridad sea 100% seguro por el contrario cada día se hace más vulnerable a cualquier ataque, por esto es de suma importancia mantener una gestión adecuada de todos los dispositivos donde todo colaborador de la Corporación de comprometerse al seguimiento y cumplimiento de unos estándares de seguridad para el acceso de información o modificación de la misma también de cumplir con informar a su jefe inmediato en caso que detecte alguna norma que no le permita desempeñar sus funciones en el sistema y el motivo por el cual no es posible hacer sus tareas.

Las políticas de seguridad estarán en vigencia en el momento que sean aprobadas por Rectoría, esta normativa será revisada y aprobada de acuerdo con el reglamento y estatutos de la Corporación y así mismo actualizada conforme a las exigencias de la Corporación o en el momento que se requiera cambios sustanciales en la infraestructura tecnológica de la Corporación.

6. REPORTE DE NOVEDADES DE VIOLACION DE LA SEGURIDAD.

Es una obligatorio de todos los empleados de la Corporación Tecnológica de Bogotá, notificar de manera inmediata de cualquier problema o violación a la seguridad, del cual fuere testigo, esta notificación debe realizarse por escrito vía correo electrónico al director del departamento de TIC con copia al correo electrónico del auxiliar de mantenimiento quienes están capacitados y obligados a gestionar los procedimientos necesarios para certificar si la sospecha es real y tomar las medidas necesarias para solventar la trasgresión al sistema.

Es obligación de todo empleado que maneje datos o información a través de accesos debidamente autorizados, el cumplimiento de las políticas de control de acceso, ya que el desconocimiento de estas reglas acarrea responsabilidades donde se incurra en alguna violación como pueden ser sanciones dependiendo de la gravedad de la falta, es por esto que las personas que tengan cualquier manejo de tecnología deben ser conscientes y asumir las responsabilidades del manejo de la información por tanto se debe conocer y respetar las políticas de seguridad.

Es de suma importancia que todo el personal de la Corporación Tecnológica de Bogotá conozca sus responsabilidades, sanciones y medidas que se tomaran en caso de que incurran en alguna violación o falta, escrita en las políticas de seguridad firmado por el empleador o proveedor. Solo una adecuada política de seguridad obligara al empleador a concientizarse de la importancia que es el

manejo de la información y la seguridad con la que se debe tratar, igualmente con el hardware de la Corporación y a entender los problemas que le puede acarrear el incumplimiento de las políticas de seguridad.

7. AQUICISION DE BIENES INFORMATICOS

La adquisición de bienes informáticos de la Corporación Tecnológica de Bogotá se hace mediante comité, los administradores de la tecnología de información deben plantar las operaciones para las cuales se necesita la adquisición de los bienes teniendo en cuenta lo siguiente:

1. Precio
   Se deberá tener al menos 3 cotizaciones diferentes de diferente proveedor teniendo en cuenta las garantías y la disponibilidad de la mercancía.

2. Calidad
   El personal del departamento de TIC deberá tener en cuenta la calidad de los recursos que se quieren adquirir medirlos con referencia a las diferentes marcas del mercado.

3. Experiencia
   Se deberá analizar el mercado, la estructura y confianza de las diferentes empresas que ofrecen la mercancía con el fin de determinar calidad precio competitividad de las máquinas y confiabilidad del producto.

4. Desarrollo tecnológica.
   Se deberá analizar el tiempo que lleva en el mercado, su nivel tecnológico frente con respeto a la oferta existente y su permanencia en el mercado.

5. Estándares
   Toda adquisición de los equipos tecnológicos se hace basados en las necesidades de la corporación definidas en comité siguiendo los lineamientos software tecnológico que con los que debe trabajar la corporación.

6. Capacidades

Los equipos de la corporación serán seleccionados pensando en las necesidades de la Corporación, sus funcionarios y estudiantes para el buen desarrollo de las actividades tanto administrativas como educativas. Siempre pensado el crecimiento por lo cual se adquieren con cualidades de crecimiento en hardware, se debe tener en cuenta lo siguiente para hacer la adquisición

a) Los equipo que se van adquirir deben de estar dentro de las listas vigentes de los proveedores de hardware.
b) Los equipos deben tener mínimo un año de garantía por el proveedor y contar con el servicio técnico que se requiera dentro del país.
c) Deberán ser equipos de fábrica o integrados con piezas debidamente evaluadas y aprobadas en comité.
d) Las marcas de los equipos deberá contar con presencia en el país y permanencia en el mercado nacional, así como con una asistencia técnica en el país y cambio de repuestos, se debe tener en cuenta que tratándose de computadoras debemos pensar en que hay que hacer constantemente actualización de repuestos y se debe tener acceso a los recursos tecnológicos de una manera eficaz y rápida.
e) Los dispositivos de almacenamiento como las entradas de periféricos deben de estar acorde con las nuevas tecnologías del mercado tanto en velocidad como en procesamiento de datos.
f) En lo que se refiere a los servidores, equipos de comunicaciones, switches y otros equipos que se justifiquen por ser de operación crítica y/o de alto costo, deben de contar con un programa de mantenimiento preventivo y correctivo que incluya el suministro de repuestos al vencer su período de garantía.

8. SOFTWARE

Todo equipo adquirido deberá tener el software adecuado para el funcionamiento ya preinstalado con su licencia correspondiente.

Para las de más adquisiciones de software como bases de datos y utilitarios, se tiene contratación anual de licenciamiento de software con MIcrosfot y una licencia perpetua de base de datos con Oracle.

8.1 Sistemas operativos.

a) Linux
b) Windows 8.1, 10, 7 profesional
c) Windows XP
d) Vmware

e) Macintosh

8.2 bases de datos.

a) MySQL
b) Postgres
c) Oracle

8.3 Leguajes de programación

d) C#
e) PHP
f) Visual Base
g) .Net
h) Unity
i) Construct

8.4 Utilidades de oficina.

Microsoft Ofice 2013.
Open Ofice.

8.5 Correo electrónico

Google APP

8.6 Navegadores de internet

Internet explore

Mozilla

Chrome

Safari

8.7 DISEÑO

Adobe CC 2015 Full

9. LICENCIAMIENTO

Todos los productos de software deberán contar con su debida factura y licencia de uso.

El departamento de Tic debe liderar y promover el uso de software libre de sitios seguros.

10. BASES DE DATOS.

Para la operación del software de red se deberá tener en consideración lo siguiente:

a) Toda la información de Las Corporación Tecnológica de Bogotá deberá ser operada a través de un mismo tipo de sistema manejador de base de datos para beneficiarse de los mecanismos de integridad, seguridad y recuperación de información en caso de presentarse alguna falla.

b) El acceso a los sistemas de información, deberá contar con los privilegios o niveles de seguridad de acceso suficientes para garantizar la seguridad total de la información de Las Empresas. Los niveles de seguridad de acceso deberán controlarse por un administrador único y poder ser manipulado por software.

c) Se deben delimitar las responsabilidades en cuanto a quién está autorizado a consultar y/o modificar en cada caso la información, tomando las medidas de seguridad pertinentes.

d) Los datos de los sistemas de información, deben ser respaldados de acuerdo a la frecuencia de actualización de sus datos, guardando respaldos históricos periódicamente. Es indispensable llevar una bitácora oficial de los respaldos realizados, asimismo, en cuanto a la información de los equipos de cómputo personales, se recomienda a los usuarios que realicen sus propios respaldos en los servidores de respaldo externo (Google Drive) o en medios de almacenamiento alternos.

e) Todos los sistemas de información que se tengan en operación, deben contar con sus respectivos manuales actualizados. Un técnico que describa la estructura interna del sistema así como los programas, catálogos y archivos que lo conforman y otro que describa a los usuarios del sistema y los procedimientos para su utilización.

f) Los sistemas de información, deben contemplar el registro histórico de las transacciones sobre datos relevantes, así como la clave del usuario y fecha en que se realizó (Normas Básicas de Auditoria y Control).

g) Se deben implantar rutinas periódicas de auditoria a la integridad de los datos y de los programas de cómputo, para garantizar su confiabilidad.

a) TIEMPO DE EVALUACION DE LAS POLITAS.

Se evaluara las policías de seguridad registradas en este documento con una prioridad de un año.

b) POLITICAS DE SEGURIDAD FISICAS.

2.1 Acceso físico

La corporación cuenta con un data center donde están ubicados los dispositivos de comunicación y servidores.

Todos estos dispositivos están protegidos donde no tienen acceso físico ni lógico ningún usuario ni a los servidores ni a los equipos de comunicaciones.

El acceso de personal de otras empresas debe ser autorizado previamente por el director de Tic el personal debe estar plenamente identificado, controlado y vigilado durante el acceso al data center, este personal debe estar identificado por un rotulo que les será asignado por el área de seguridad de acceso al edificio y a las oficinas de Las institución.

Toda visita a las instalaciones de la Corporación tecnológica de Bogotá podrá acceder a las áreas restringidas siempre y cuando se encuentren acompañadas con al menos un responsable del área a la cual se le otorgo acceso.

Las visitas a las instalaciones físicas del data center harán en el horario establecido.

El personal autorizado para mover, cambiar o extraer equipo de cómputo es el poseedor del mismo o el superior responsable o los ATI, a través de formatos de autorización de Entrada/Salida, los cuales notificarán a las personas delegadas del Área Administrativa y al personal de seguridad del edificio.

2.2 Protección física

2.2.1 Data center

El data center deberá estar dotado de:

a) Tener una puerta de acceso de vidrio templado transparente, para favorecer el control del uso de los recursos de cómputo.

b) Ser un área restringida. Tener un sistema de control de acceso que garantice la entrada solo al personal autorizado por el director de Tic.

c) Recibir limpieza al menos una vez por semana, que permita mantenerse libre de polvo.

d) Estar libre de contactos e instalaciones eléctricas en mal estado

e) Aire acondicionado. Mantener la temperatura a 21 grados centígrados.

f) Respaldo de energía redundante.

g) Seguir los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores.

h) Los sistemas de polo a tierra, sistemas de protección e instalaciones eléctricas deberán recibir mantenimiento anual con el fin de determinar la efectividad del sistema.

i) Contar con algún esquema que asegure la continuidad del servicio.

j) Prevención y/o detección de incendios extintores

k) Contar por lo menos con dos extintores de incendio adecuado y cercano al Data Center.

2.3 Infraestructura

Se deberá contar con el cableado estructurado actualizado a las últimas referencias del mercado en los casos de nuevos proyectos para facilitar el funcionamiento de los mismos.

La infraestructura de servidores y comunicaciones deberá estar ubicada en la oficina del el Director de Tic con todas las restricciones de seguridad contra personal no autorizado, en alguna eventualidad de requerir acceso debe ser autorizado solo por el director del departamento de Tic, la visita será supervisada por el auxiliar de mantenimiento.

2.4 Instalación de equipos de cómputo

Cualquier instalación de equipo de cómputo estará sujeta a las siguientes condiciones:

a) Los equipos que sean para uso de los funcionarios se instalarán en lugares adecuados, para el buen funcionamiento de los mismos y contando con todas las normas de corriente y de transmisión de datos.

b) El Área de Tic, así como las áreas operativas deberán contar con un plano actualizado de las instalaciones eléctricas y de comunicaciones del equipo de cómputo en red.

c) Las instalaciones eléctricas y de comunicaciones, estarán fijas y resguardadas del paso de personas o materiales.

d) Las instalaciones se apegarán estrictamente a los requerimientos de los equipos, cuidando las especificaciones del cableado y de los circuitos de protección necesarios.

e) No es permitido hacer instalaciones hechizas o tener multitomas recargadas o hacer uso de las tomas reguladas para otra función más que la de alimentar la corriente del computador.

2.5 Controles

a) Los ATI deben llevar un control total y sistematizado de los recursos de cómputo y licenciamiento.

b) Los encargados del área de tecnología son los responsables de organizar al personal encargado del mantenimiento preventivo y correctivo de los equipos de cómputo.

c) El Área de desarrollo Humano deberá reportar a los administradores de tecnología de la información cuando un usuario deje de laborar o de tener una relación con Las Corporación Tecnológica de Bogotá.

d) Contraseñas de ingreso a los recursos y supervisar la correcta devolución de los equipos y recursos asignados al usuario.

e) El usuario, en caso de retiro, deberá tramitar ante el Área de Tecnología el paz y salvo correspondiente.

2.6 Backup

a) Todas las bases deben tener respaldos automáticos o en su defecto manuales según sea la necesidad.

b) Los respaldos deben ser alojados en más de un dispositivo debidamente reguardados.

c) Todo el sistema deberá estar debidamente resguardado por claves y niveles de acceso protegiendo la integridad de información.

d) Se asignó dispositivo FREENAS para el Backup's de la parte administrativa, se recomienda que se haga todos los días, (no es una obligación pero es lo que hace la recomendación)

- Se asigna unidad de red que está vinculada con el servidor
- La información es totalmente privada
- Cada funcionario e autónomo de elegir la información que es de importancia para ellos
- No es responsabilidad del departamento de tic que esta información no sea la pertinente para cada proceso.

2.7 Recursos de los usuarios

2.7.1 Uso

a) Los usuarios deberán hacer uso de los recursos tecnológicos de una manera adecuada, cuidando la integridad física y lógica del mismo.

b) Los usuarios deberán informar al departamento de Tic en el caso que tenga alguna duda en el manejo de los recursos que se le autorizaron.

c) En ningún caso los usuarios están autorizados a desinstalar programas ya preinstalados ni instalar nuevos que no sean autorizados previamente por el departamento de Tic.

d) El manejo del correo institucional para los funcionarios de la corporación está sujeto a las siguientes condiciones:

- El usuario se responsabiliza de mantener la confidencialidad de su contraseña y cuenta, y de todas las actividades que se efectúen bajo éstas.
- no se permite el uso del correo electrónico suministrado por la Corporación tecnológica de Bogotá con fines comerciales ni su uso para el envío de correos masivos que atenten con el buen funcionamiento de los servicios en Internet.
- el usuario se obliga a cumplir las normas sobre protección de la información y de los datos.
- Los usuarios del correo electrónico institucional no deben enviar mensajes personales u ofensivos, injuriosos, cadenas de mensajes o mensajes que se relacionen con actividades ilegales y no éticas o que atenten contra el buen nombre de la Institución.
- El servicio de correo electrónico de la Institución no debe ser utilizado para enviar correo basura (Spam).
- El servicio de correo debe ser utilizado para materias relacionadas con la función desempeñada.

2.8 Protección derechos de autor

Queda estrictamente prohibido bajar, almacenar, ejecutar software que no esté autorizado por el departamento de tic y que violen los derechos de autor, para tal efecto todos los usuario deberán firmar el documento normas y restricciones para el uso de computadores e infraestructura de comunicaciones.

Para la seguridad de no incurrir en la violación de la norma de derechos de autor, el director del departamento de Tic a establecido normas de seguridad donde el usuario no puede instalar software ni hacer cambios no autorizados previamente por el departamento, pero para conocimiento de los usuarios se debe tener en cuenta los siguientes parámetros:

a) No está autorizada la descarga de Internet de software que no esté previamente informada al director de Tic o en su defecto al auxiliar de mantenimiento.

b) Es de suma gravedad que un funcionario realice copias no autorizadas de programas.

c) Es de suma gravedad que algún funcionario descargue o actualice programas peer-to-peer (P2P – Ej. Kazaa) que pueden utilizarse para comercializar trabajos protegidos por los derechos de autor.

d) No es permitido que los usuarios realice intercambios o descargas de archivos digitales de música (MP3, WAV, etc) de los cuales no es el autor o bien no posee los derechos de distribución del mismo.

e) Si se descubre que un funcionario ha copiado software o música en forma ilegal, este puede ser sancionado, suspendido o despedido según la gravedad de la acción.

f) Si un funcionario es descubierto con copia software en forma ilegal para dárselos a un tercero, también puede ser sancionado, suspendido o despedido.

g) Si un usuario desea utilizar software autorizados por Las Corporación tecnológica de Bogotá en su hogar, debe consultar director del departamento de Tic para asegurarse de que ese uso esté permitido por la licencia del distribuidor del software.

h) El auxiliar de mantenimiento del departamento de Tic ara revisiones periódicas de los equipos de cómputo para revisar el inventario de software y determinar que son los autorizados por el departamento de Tic.

i) Si se encuentran software no autorizado o copias de software no licenciado estas serán eliminadas y de ser software muy necesario para el desarrollo de las actividades se remplazara por software autorizado y licenciado.

j) Solo se autoriza el software que este en virtud de los acuerdos de licencia y no instalarán copias no autorizadas de software no comerciales.

k) Los usuarios no descargarán ni cargarán programas informáticos no autorizados a través de Internet.

l) Los usuarios no realizarán intercambios o descargas de archivos digitales de música (MP3, WAV, etc) de los cuales no es el autor o bien no posee los derechos de distribución del mismo.

m) Es deber de los usuario que se enteren de un mal uso del software o de los demás recursos informáticos deberá informar al director del departamento de Tic de la incidencia o enviar un correo explicando detalladamente el caso.

n) Según las leyes vigentes de derechos de autor, las personas involucradas en la reproducción ilegal de programas informáticos pueden estar sujetas a sanciones civiles y penales, incluidas multas y prisión. No se permite la duplicación ilegal de programas informáticos.

c) SEGURIDAD LÓGICA

3.1 Red

El propósito de la red en la corporación es de transmitir información y compartir archivos entre los diferentes usuarios para a cual debemos tener en cuenta las siguientes condiciones:

a) El departamento de Tic no se hace responsable por el tráfico de datos dentro o fuera de la corporación, la responsabilidad recae sobre los usuarios que la soliciten y la trasmitan.

b) Es de suma gravedad que un usuario vea, modifique, copie o elimine información de un equipo de cómputo sin previo aviso del usuario del equipo.

c) No se debe utilizar los servicios de la red para asuntos que no sean servicios de la Corporación Tecnológica de Bogotá.

d) Las contraseñas son de uso exclusivo e intransferible los usuarios, es responsabilidad del usuario el manejo que le dé a su contraseña y de lo que con ella puedan hacer otro usuario.

e) El software analizador de red es uso exclusivo del departamento de Tic, no se permite que los usuarios de usen este tipo de software.

f) En caso de detectar un uso indebido de la red, se suspenderá de manera inmediata la clave de acceso a los diferentes dispositivos hasta dar claridad del caso y tomar las correcciones que sean viables.

3.2 SERVIDORES

3.2.1 Configuración e instalación

1. La instalación, conexión y configuración (seguridad de la red) de los servidores son una responsabilidad de los administradores del departamento de Tic; durante la configuración de los servidores los administradores de la red deben tener planes de contingencia para seguir prestando el servicio con efectividad.

2. Los servidores que preste servicio en la red y Internet deberán estar conectados 24 horas 365 días al año.

3. Recibir mantenimiento preventivo mínimo 2 veces al año.

4. La información de los servidores deberá ser respaldada de acuerdo con los siguientes criterios, como mínimo:

   - ✓ Diariamente, información crítica.
   - ✓ Semanalmente, los documentos web.
   - ✓ Mensualmente, configuración del servidor y logs.

13.3 Correo Electrónico

El Web Master se encargara de asignar las cuentas a los usuarios para el uso de correo electrónico para este efecto se debe cumplir con los siguientes lineamientos:

1. Para asignarle su cuenta de correo al usuario, el área de Desarrollo Humano deberá llenar una solicitud en formato establecido para tal fin y entregarlo al área de Tic para la creación de la cuenta y su respectiva asignación de clave de seguridad.

2. La cuenta será activada en el momento en que el usuario ingrese por primera vez a su correo y será obligatorio el cambio de la contraseña de acceso inicialmente asignada.

3. La cuenta se crea para los admirativos de la siguiente forma:

   - ✓ Nombre del cargo.
   - ✓ Como opcional el nombre de la dependencia.

4. La cuenta de correo de los estudiantes se crea de la siguiente forma:

   - ✓ La primera letra del primer nombre
   - ✓ Primer apellido completo (si el apellido tiene algún carácter de habla hispana se remplaza).
   - ✓ Últimos 2 dígitos del documento de identidad (si el correo a crear ya existe se agrega 3 últimos dígitos del documento)

5. La longitud mínima de las contraseñas será igual o superior a ocho caracteres debe tener al menos una mayúscula y un carácter.

3.3 Bases de Datos

1. El administrador de la base de datos no deberá eliminas información del sistema, exceptuando si esta información pone en peligro la demás información del sistema o la misma está dañada.

2. El administrador de la base de datos es el encargado de asignar perfiles de uso de la base en las cuentas que crea para el acceso a la información.

3. En caso que la contraseña de acceso a la bases de datos el usuario deberá acudir al administrador para que sea restaurada su contraseña.

4. La longitud de la contraseña será mínimo de 6 caracteres alfanumérica.

3.4 Recursos de cómputo

3.4.1 Seguridad de cómputo

El departamento de TIC es el encargado de brindar toda la seguridad necesaria en los equipos de cómputo, para evitar la instrucción de agente externos que puedan dañar información o de cualquier Software de la Corporación; hay que tener en

cuenta que con los nuevos avances en la tecnología cada vez hay más mecanismos para romper la seguridad de los sistemas por lo que no hay sistema 100% seguro.

El departamento de tic debe suministrar la forma de atacar posibles ingresos no autorizados por software malicioso, para lo cual los usuarios deben reportar cualquier cambio o presunción de ataque a sus equipos de cómputo.

El auxiliar del departamento de Tic es el único autorizado para hacer la respectiva revisión en búsqueda de agentes maliciosos; el director del departamento es el único que podrá monitorear constante la red en busca de accesos indebidos que provoquen fallas en el sistema o en los diferentes equipos de cómputo.

13.5 Auxiliar de soporte

El auxiliar de soporte tiene las siguientes obligaciones:

a) Tendrá permiso para analizar los equipos de cómputo en búsqueda de software malicioso.
b) Deberá realizar respaldos cuando tenga que hacer cambios que signifique posible pérdida de la información
c) Deberá registrar los equipos en el inventario de computo
d) Deberá auditar periódicamente los equipos de cómputo y evaluar sus condiciones de uso por el usuario y verificar los documentos en búsqueda de archivos no autorizados por la Corporación (tomar evidencia del caso).
e) El auxiliar debe reportar ante el jefe inmediato en caso que encuentre información o software no autorizado en los equipos de cómputo.

13.6 Renovación de equipos

a) El auxiliar de Tic debe determinar el tiempo de vida útil de los equipos de cómputo, para poder anticipar las posibles renovaciones.

b) Cuando de algún proceso institucional soliciten la renovación o cambio de equipo, deben contar con la autorización del departamento de Tic para que se le asigne el equipo adecuado a las funciones del departamento, esto con el fin que los procesos no sigan su continuidad con igual o mejor efectividad.

14 SERVICIOS RED

a) El departamento de tic definirá que servicios de internet ofrecerá a los diferentes administrativos y usuarios regulares.

b) El departamento de Tic Definirá a que personas externas le brindara acceso a internet.

c) El director del departamento de tic es el único que puede dar acceso al servidor para asignación de claves de seguridad, las cuales son solo de conocimiento del usuario.

d) El director del departamento de tic deberá hace respaldos de las bases de datos.

e) Revisar constantemente el cumplimiento de las normas de las políticas de seguridad

f) Reportar si es necesario a los usuarios que están incumpliendo con las normas

g) Monitorear los servicios de red en búsqueda de posibles intrusos que puedan dañar el sistema

h) Monitorear y supervisar al personal de mantenimiento para que se esté cumpliendo con los requerimientos necesarios para el buen funcionamiento de los equipos.

i) El auxiliar puede instalar cualquier servidor de red, previamente notificado al director del departamento de Tic, cumpliendo las siguientes condiciones.

- ✓ Que los servicios adicionales implique un mejor servicio.
- ✓ Que sirvan para detectar posibles ingresos no autorizados
- ✓ Para detectar programas no autorizados
- ✓ Que detecte violación a las políticas de seguridad
- ✓ Que la instalación de incumpla ningún protocolo establecido por las políticas de seguridad.
- ✓ Que reporten tráfico no autorizado y que violen algún tipo de seguridad.
- ✓

15 USUARIOS

15.1 Identificación de usuarios y contraseñas.

a) Todos los usuarios con accesos a la red o al servicio de internet debe contar con una contraseña que se le asignara desde el departamento de tic con los perfiles que sean necesarios para el desempeño del funcionario, recordar que esta contraseña solo es de conocimiento del usuario.
b) Ningún usuario recibirá contraseñas de ningún equipo de cómputo hasta que no lea y acepte el documento normas y restricciones para el uso de computadores e infraestructura de comunicaciones.

c) El usuario definirá su contraseña con un mínimo de ocho caracteres y un máximo de 10 debe ser alfanumérica y con al menos una letra en mayúscula.

d) El usuario deberá renovar su contraseña al menos 1 vez en el año, cuando sienta que fue copiada por otro usuario y si su calve es muy débil y de fácil acceso por otra persona.

e) El usuario deberá notificar al departamento de Tic en caso que:

- ✓ En caso que detecte anomalías en mensajes extraños, lentitud en el computador o en el servicio de red (internet).
- ✓ Si tiene algún problema a los servicios proporcionados por el servidor.

f) Si un usuario viola las políticas de no uso de los servidores, el departamento de tic lo bloqueara de inmediato en todos los servicios que el departamento le asigno y será notificado ante rectoría para tomar las medidas pertinentes al caso.

16 RESPOSABILIDAES PERSONALES

a) Los usuarios son responsables de todas las actividades echas con su usuario y contraseña

b) Los usuarios no deben revelar bajo ningún concepto su usuario y contraseña y tenerla por escrito en ningún documento.

c) Los usuarios no deben autorizar ningún acceso a los equipos que están a cargo de ellos ni ingresar a ningún equipo a si tenga autorización por el usuario del equipo.

d) Si algún usuario tiene sospechas que algún usuario esta utilizado su equipo por favor notificar de inmediato al departamento de Tic para hace las revisiones respectivas del caso, aplica lo mismo en caso de que se tenga sospecha que está siendo usado su usuario y contraseña en otro equipo o en el mismo sin autorización.

e) El usuario no debe tener información de índole personal en los computadores que les asigno

f) El usuario que de manejo a información de índole personal de los usuarios de la corporación o de personal externo a ella debe garantizar la integridad de esos datos.

g) El usuario solo deberá crear archivos que sean necesarios para el orden de los documentos y para el buen desempeño de las funciones de su cargo.

17 USO APROPIADO DE LOS RECUSOS.

Los servicios de red, internet, sistemas de cómputo, servicios de plataformas, de comunicaciones y software son exclusivamente para el cumplimiento de las actividades asignadas por la Corporación tecnológica de Bogotá y totalmente confidencial toda la información que está contenida en los discos duros internos como externos asignados.

18 SEGURIDAD PERIMETRAL

La seguridad perimetral es uno de los métodos que se han implementado en la corporación con el fin de proteger nuestros recursos de red y de hardware, está basado en los recursos disponibles de la corporación, donde definimos diferentes niveles de seguridad que permiten ciertos ingresos a diferentes usuarios según su actividad dentro de la corporación

El departamento de Tic implementara soluciones lógicas y físicas que garanticen la protección de la información de posibles ataques internos o externos.

- ✓ Rechazar conexiones servidores que se detecten como comprometidos o a información infectada.

- ✓ Permitir sólo ciertos tipos de tráfico (como el correo electrónico, http, https).
- ✓ Proporcionar un único punto de interconexión con el exterior.
- ✓ Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet
- ✓ Auditar el tráfico entre el exterior y el interior.
- ✓ Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red cuentas de usuarios internos.

18.1 Firewall

La Corporación cuenta con un firewall físico (PFsense) debidamente actualizado a la última versión, el cual nos controla los puertos y conexiones no permite las conexiones no autorizadas a otros servidores ni que otros servidores nos acedan

- ✓ Este equipo deberá estar cubierto con un sistema de alta disponibilidad que permita la continuidad de los servicios en caso de fallo.
- ✓ El director de Tic establecerán las reglas en el Firewall necesarias bloquear, permitir o ignorar el flujo de datos entrante y saliente de la Red.
- ✓ El firewall debe bloquear las “conexiones extrañas” y no dejarlas pasar para que no causen problemas.
- ✓ El firewall debe controlar los ataques de “Denegación de Servicio” y controlar también el número de conexiones que se están produciendo, y en cuanto detectan que se establecen más de las normales desde un mismo punto bloquearlas y mantener el servicio a salvo.

18.2 Redes Privadas Virtuales (VPN)

Solo hay una conexión la cual solo podrá ser ingresada por el director del departamento de Tic y por los administradores de bases de datos.

18.3 Conectividad a Internet

La red de internet solo es habilitada para las funciones que son asignadas en la Corporación todos los usuarios tienen las mismas responsabilidades:

- ✓ El acceso a Internet se restringe exclusivamente a través de la Red establecida para ello, es decir, por medio del sistema de seguridad con Firewall incorporado en la misma.

- ✓ Internet es una herramienta de trabajo. Todas las actividades en Internet deben estar en relación con tareas y actividades del trabajo desempeñado.

- ✓ Sólo puede haber transferencia de datos de o a Internet en conexión con actividades propias del trabajo desempeñado.

18.3.1 WIFI

El Wifi es un servicio que está dedicado más que todo a los estudiantes de la corporación pero es de libre acceso a para todos los funcionarios de la Corporación donde halla cubertura del servicio.

- ✓ El servicio de Internet está definido de manera controlada.

- ✓ Las condiciones de uso del servicio de red son aspectos importantes que deben tenerse en cuenta para la utilización del servicio, estas condiciones aplican para cualquier dispositivo que tengan la facultada de conectarse a la red Wifi.

- ✓ Los administradores del departamento de Tic, son los encargados de la administración, habilitación y/o bajas de usuarios en la red inalámbrica.

18.3.2 Identificación y activación

Para hacer uso de la red Wifi, el solicitante necesariamente deberá ser miembro de la Corporación o ser autorizado por el departamento de Tic.

- ✓ El primer paso es que los usuarios que deseen utilizar el servicio debe pedir autorización al departamento de Tic.

- ✓ La activación de la cuenta se realizará por un periodo semestral como máximo,

- ✓ Para conectarse a la red inalámbrica se deberá emplear autenticación tipo WPA2-AUTO-PSK para lo cual se usara nombre de usuario y contraseña.

- ✓ A pesar de que se han establecido sistemas de encriptación de datos mediante el uso de seguridad WPA2-AUTO-PSK, NO SE RECOMIENDA hacer uso de tarjetas de crédito para compras.

- ✓ Se determinarán las medidas pertinentes de seguridad para usar las redes

- ✓ No se debe hacer uso de programas que recolectan paquetes de datos de la red inalámbrica. Esta práctica es una violación a la privacidad y constituye un robo de los datos de usuario, y puede ser sancionado.

- ✓ Con la finalidad de evitar responsabilidades, en caso de que algún usuario haga cambio de cualquiera de los equipos previamente dado de alta, este necesariamente deberá comunicar al departamento de Tic para su respectiva baja del equipo de la red inalámbrica.

18.4 Restricciones/prohibiciones de acceso a Internet

Para el buen funcionamiento de los equipos de red se debe cumplir con las siguientes restricciones:

- ✓ El uso de programas para compartir archivos (Peer to Peer).

- ✓ El acceso a páginas con cualquier tipo de contenido explícito de pornografía.

- ✓ El uso de sitios de videos en línea o en tiempo real.

- ✓ Debido a las limitaciones de ancho de banda existentes NO se permite la conexión a estaciones de radio por Internet.

- ✓ Uso de JUEGOS "on line" en la red.

18.5 Excepciones

a) La corporación ha restringido sitios de internet que parecen ser inofensivos pero por la calidad de información de ventanas emergentes serán bloqueados, en caso de que sean de uso necesario para el funcionario debe pasar el requerimiento al departamento de Tic.

b) En caso de eventos, cursos, talleres, conferencias, etc, se podrán habilitar equipos con acceso a la red inalámbrica de manera temporal por el tiempo necesario previa solicitud de los interesados con una anticipación de por lo menos un día hábil.
c) En el caso de estos eventos las restricciones para acceder podrán ser “anuladas” temporalmente previa solicitud expresa por parte de la parte interesada y con anticipación de por lo menos un día hábil.

18.6 Acceso a Invitados:

La red inalámbrica también cumple el servicio de conexión a personas externas a la corporación que son debidamente autorizados limitados a las zonas de cobertura asignadas por la Corporación y que están restringida por las siguientes condiciones:

- ✓ Estos usuarios no tendrán acceso a la Red de Las Corporación ni a ningún recurso de uso privado.
- ✓ La red inalámbrica solo tiene restricción de usuario y contraseña por lo cual no tienen restricciones de tiempo.

19 PLAN DE CONTIGENCIA

El departamento de tic deberá crear un plan para los departamentos que cumpla las siguientes condiciones:

- ✓ Continuar con la operación del área con procedimientos informáticos alternos.
- ✓ Tener los respaldos de información en un lugar seguro, fuera del lugar en el que se encuentran los equipos.
- ✓ Tener el apoyo por medios magnéticos o en forma documental, de las operaciones necesarias para reconstruir los archivos dañados.
- ✓ Contar con un instructivo de operación para la detección de posibles fallas, para que toda acción correctiva se efectúe con la mínima degradación posible de los datos.
- ✓ Ejecutar pruebas de la funcionalidad del plan.
- ✓ Mantener revisiones del plan a fin de efectuar las actualizaciones respectivas.

20. ACTUALIZACIONES DE LA POLÍTICA DE SEGURIDAD

Con las actualizaciones en la tecnología cada vez es más las infracciones a la seguridad de las Corporaciones por lo cual la Corporación Tecnológica de Bogotá modificara las políticas de seguridad cada vez que así lo determine el departamento de Tic.

Es de responsabilidad de cada uno de los usuarios la lectura del manual de seguridad de la información y sus cambios

21 Disposiciones

- ✓ Las disposiciones aquí enmarcadas, entrarán en vigor a partir del día de su difusión.

- ✓ Las normas y políticas objeto de este documento podrán ser modificadas o adecuadas conforme a las necesidades que se vayan presentando, mediante acuerdo del Comité; una vez aprobadas dichas modificaciones o adecuaciones, se establecerá su vigencia.

- ✓ La falta de conocimiento de las normas aquí descritas por parte de los usuarios no los libera de la aplicación de sanciones y/o penalidades por el incumplimiento de las mismas.