Código			Política	
11-11.2-P-002-v.4			Políticas específicas de Seguridad de la Información	
Fecha de emisión				
10	04	2018		

Elaborado por:	Revisado por:	Aprobado por:
Yezid Ospina Piñeros – Líder Sistema de Gestión de Seguridad de la Información – Gerencia Procesos y Proyectos	Jenny Elizabeth Caipe Balcazar – Oficial de Seguridad de la Información– Vicepresidencia de Infraestructura Juan Manuel Corredor García – Oficial de Seguridad de la Información – Vicepresidencia de Informática Sergio Vargas –Oficial de Seguridad de la Información - Coordinación Seguridad y Vigilancia	Natalia Gutiérrez Leal – Gerente Procesos y Proyectos Yezid Ospina Piñeros – Líder Sistema de Gestión de Seguridad de la Información – Gerencia Procesos y Proyectos Jenny Elizabeth Caipe Balcazar – Oficial de Seguridad – Vicepresidencia de Infraestructura Juan Manuel Corredor García – Oficial de Seguridad – Vicepresidencia de Informática Sergio Vargas – Oficial de Seguridad - Coordinación Seguridad y Vigilancia

TABLA DE CONTENIDO

1. OBJETIVO

Establecer los criterios y medidas básicas que deben aplicarse a toda la información de la Empresa de Telecomunicaciones de Bogotá ETB para su uso correcto, con el fin de establecer y mantener un ambiente controlado de riesgos, definiendo las intenciones globales y orientación de ETB relativas a la seguridad de la información, tal y como se expresan formalmente por la alta dirección.

2. ALCANCE

Este documento contiene las políticas de seguridad de la información específicas que respaldan la política de seguridad de nivel superior y que estipula la implementación de controles de seguridad de la información en atención a la declaración de aplicabilidad de ETB. Está dirigido a trabajadores, terceros (proveedores y contratistas) clientes y asociados involucrados en la generación, almacenamiento, procesamiento, uso, transmisión y eventual eliminación de la información de ETB. Por tal motivo el incumplimiento de las políticas aquí expresadas, acarrearán sanciones disciplinarias de acuerdo a la magnitud y característica de la situación ocurrida

3. DESCRIPCION DE POLITICAS ESPECÍFICAS DE LA SEGURIDAD DE LA INFORMACIÓN

3.1 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION

Como parte integral para el cumplimiento continuo de la política, ETB establece el Comité de Seguridad de la Información, como la máxima instancia de decisión y seguimiento del Sistema de Gestión de Seguridad de la Información – SGSI y del Programa Integral de Gestión de Datos Personales - PIGDP, como quiera que por medio de la directiva interna 00664 del 2017 se le delega de manera expresa los deberes de la alta dirección para los temas específicos del SGSI y se define su conformación y responsabilidades entre las que se encuentra la de diseñar, fijar, expedir y actualizar las políticas y directrices de la seguridad de la información y de tratamiento de datos personales y velar por su mejora continua. En ese sentido, deben implementarse los mecanismos para generar y hacer

seguimiento periódico a las directrices que en materia de seguridad de la información se generen incluyendo los canales de comunicación para tal fin.

3.2 SEGURIDAD EN LOS RECURSOS HUMANOS

a. Los trabajadores deben cumplir con los procedimientos de verificación y contratación exigidos por parte de la Gerencia de Gestión del Talento Humano.

b. Los trabajadores y terceros vinculados a ETB deben firmar una cláusula de confidencialidad para la protección de los activos de información.

c. Los trabajadores de ETB deben recibir a su ingreso a la Empresa y durante su permanencia, inducciones en temas de seguridad de la información, así como dejar constancia del conocimiento respecto a las políticas y procedimientos de seguridad de la información que sean de su inherencia.

d. Ante cambios de cargo o terminación de contrato laboral, el trabajador debe hacer entrega formal de los activos de información que le fueron asignados por ETB para sus actividades laborales. Esta política deberá regirse por el procedimiento de gestión de activos físicos.

3.3 GESTION DE LOS ACTIVOS

a. Toda información debe estar identificada, clasificada y valorada acorde con el documento de clasificación de activos de la información definido por ETB, el cual debe ser ejecutado con la periodicidad requerida en conjunto con el responsable de la información y el área donde se encuentra el liderazgo del Sistema de Gestión de Seguridad de la Información.

b. Los activos de información de ETB deben contar con un propietario quien tendrá la responsabilidad de velar por la administración correcta de los activos durante su ciclo de vida.

c. Los activos críticos de información deben contar con los controles asociados al valor que este posea para la Empresa.

d. Ningún trabajador o tercero vinculado a ETB puede divulgar información confidencial de la empresa, sus clientes y asociados a personas no

autorizadas. Para lo anterior se debe definir y divulgar las sanciones correspondientes.

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

f. Los activos de información que deban ser enviados y/o compartidos deberán estar etiquetados acorde al esquema de clasificación establecido.

g. Al finalizar la vinculación con la Empresa, los empleados y contratistas deben devolver los activos de la organización que estén en su posesión.

h. La información magnética o electrónica clasificada como confidencial, debe guardarse y transmitirse de manera cifrada a través de los medios establecidos por las áreas de Gestión de TIC y deben considerarse los respaldos necesarios para protegerla con los debidos controles de seguridad.

i. 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.

3.4 CONTROL DE ACCESO A LA INFORMCIÓN

Los controles de acceso a los activos de información, son tanto lógicos para los sistemas de información y plataforma de gestión, como físicos para los lugares donde se encuentra información física o digital alojada, por lo tanto, los aspectos referenciados en esta política deben considerar su pertinencia a ambos tipos de acceso.

La fortaleza de los controles de acceso debe corresponder con la clasificación de la información a la que se accederá. En consecuencia, se debe contemplar la criticidad de los activos de información al momento de definir los controles requeridos para su protección en cuanto a la posibilidad de accederlos.

Se debe garantizar la segregación de los roles de control de acceso. Estos roles son:

Usuario: Todo trabajador o contratista que requiere acceder, según sea pertinente, a las plataformas de gestión, los sistemas de información o los

lugares donde se almacena y procesa información, de acuerdo a su área de trabajo.

Propietario del activo de información: Se encarga de asegurar la administración correcta de los activos de información durante todo su ciclo de vida, con el fin de proteger la información crítica del negocio que se encuentra bajo su cargo. Entre las diferentes actividades que realiza, está la de determinar los derechos y restricciones de acceso para los usuarios específicos de sus activos.

Custodio de activos de Información: Se encarga de asegurar que los controles de seguridad de la información permanezcan eficaces según sea pertinente en las plataformas de gestión, los sistemas de información o los lugares donde se almacena y procesa información, de acuerdo a su área de trabajo. En ese sentido administra los derechos de acceso a los activos de información.

3.4.1 ADMINISTRACIÓN DE ACCESO A LOS USUARIOS

a. Para usar sistemas o plataformas se debe obtener autorización del propietario de la información que se pretende gestionar en el sistema de información o plataformas de gestión.

b. Los privilegios de los usuarios deben ser autorizados por el propietario de la información que los usuarios bajo su cargo pretenden gestionar, con base a su necesidad específica de uso y a los requisitos mínimos para sus roles o funciones.

c. En general los IDs de los usuarios deben ser únicos para hacerlos responsables de sus acciones. Cuando sean requeridos IDs compartidos deben ser autorizados por una jerarquía superior a la que autoriza los usuarios únicos. No debe estar permitida la creación de IDs de usuario redundante.

d. Al proporcionar derechos de acceso a un determinado ID de usuario, los administradores de los sistemas y plataformas deben verificar que el nivel de acceso otorgado es adecuado para las políticas de acceso del presente documento y que es coherente con la segregación de los roles señalados.

e. Se debe asegurar que los derechos de acceso no estén activados sin que finalice el procedimiento de autorización.

f. Se debe mantener un registro centralizado de los derechos de acceso otorgados a los diferentes usuarios para acceder a los sistemas de información y plataformas de gestión.

g. Es responsabilidad de los propietarios de la información que gestionan los usuarios bajo su cargo la de requerir la actualización de los derechos de acceso cuando dichos usuarios han cambiado de roles o trabajo frente a dicha información. En el caso de los usuarios que se desvinculan de la organización, es responsabilidad del área de Talento Humano la de informar a los administradores de los sistemas y plataformas para que se ejecute la debida cancelación del usuario pertinente en los sistemas o servicios de información, incluyendo el acceso a cuentas de usuario de grupos de personas. Lo anterior sin perjuicio de la responsabilidad que tienen los administradores de los sistemas y plataformas de revisar periódicamente los usuarios que deben estar activos de acuerdo a su base de datos de solicitud, actualización o revocación de acceso a los sistemas o servicios de información (esta revisión podría ser reemplazada por el envío periódico de los usuarios activos a los diferentes propietarios, con el fin de que ellos actualicen la información).

h. Se deben establecer derechos de acceso en perfiles típicos de acceso de usuario de acuerdo a las condiciones específicas de las áreas que custodian tanto los sistemas de información como las plataformas de gestión, con el fin de facilitar la gestión y control de tales accesos.

i. Se deben incluir cláusulas en los contratos de los trabajadores de ETB y contratistas donde se especifiquen advertencias y/o sanciones en el caso de que intenten accesos no autorizados.

j. Se debe identificar los derechos de acceso privilegiado (súper-usuarios) asociados con cada sistema o plataforma, junto con cada aplicación y los usuarios a los que se deberían asignar y se deberían definir los requisitos para el vencimiento de los derechos de acceso privilegiado.

k. Los propietarios de la información que gestionan los usuarios privilegiados son responsables de tales usuarios cuenten con las competencias necesarias para el uso responsable de tales privilegios.

l. Los usuarios grupales deben tener un autorizador adicional al propietario de la información que se pretende gestionar (con una jerarquía superior) y debe contar con controles adicionales de protección, para evitar su uso no autorizado, como lo es la obligatoriedad de cambio más frecuente de contraseñas.

3.4.2 ADMINISTRACIÓN DE LA INFORMACIÓN DE AUTENTICACIÓN SECRETA DE LOS USUARIOS

a. Las contraseñas son un tipo de información de autenticación secreta de uso común y son una forma común de verificar la identidad de un usuario. Otros tipos de información de autenticación secreta son claves criptográficas y otros datos almacenados en tokens de hardware (es decir, tarjetas inteligentes) que producen códigos de autenticación.

b. Se debe solicitar a los usuarios firmar una declaración en que mantengan la información de autenticación secreta de manera personal y que mantengan la información de autenticación secreta grupal (es decir, compartida) solo dentro de los miembros del grupo.

c. Cuando se vaya a proporcionar a un usuario información de autenticación secreta, se debe suministrar tal información de manera temporal, única para una persona y no se debería poder adivinar. El usuario debe cambiar obligatoriamente tal información en el primer uso.

d. Se deben establecer mecanismos para verificar la identidad de un usuario antes de proporcionarle información de autenticación secreta nueva, reemplazo o temporal.

e. No se debe proporcionar información de autenticación secreta por ningún medio escrito sin cifrar.

f. Se debe alterar la información de autenticación secreta predeterminada del proveedor luego de la instalación de los sistemas o software.

g. Los propietarios de la información que gestionan los usuarios bajo su cargo, deben revisar de manera periódica, los derechos de acceso de esos usuarios y después de cada cambio de rol, traslado o desvinculación con la empresa. La revisión se debería realizar a intervalos más frecuentes si los derechos de acceso son privilegiados.

h. Los usuarios que inician automáticamente los sistemas de información y las plataformas de gestión deben contar con los controles necesarios para evitar que los sistemas sean vulnerables. Por ejemplo: Información de autenticación secreta segura.

3.4.3 RESPONSABILIDADES DE LOS USUARIOS FRENTE A LA INFORMACIÓN DE AUTENTICACIÓN SECRETA

a. Los usuarios deben mantener la información de autenticación secreta como confidencial asegurándose de que no se divulgue a nadie, incluyendo a las personas con mayor autoridad. Toda transacción y actividad realizada con la cuenta de usuario asignada a los sistemas de información de ETB, será responsabilidad del propietario de dicha cuenta.

b. 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. Los usuarios no deben mantener registros de contraseñas, ni en papel, ni en archivos de software, ni en dispositivos de mano, ni en nada que se le parezca. Los usuarios son responsables de cambiar las contraseñas cuando exista alguna indicación de su posible compromiso.

c. Las áreas de tecnología deben definir, publicar y divulgar políticas específicas sobre la definición de contraseñas seguras, relacionadas por ejemplo con la extensión, contenido y no repetición de las contraseñas

3.4.4 CONTROL DE ACCESO DE LOS SISTEMAS DE INFORMACIÓN Y PLATAFORMAS DE GESTIÓN

a. Controlar los datos a los que un usuario en particular puede acceder y los derechos de acceso de lectura, escritura, eliminación y ejecución.
b. Se debe seleccionar una técnica de autenticación adecuada para corroborar la identidad que un usuario afirma tener. Cuando se requiera un nivel alto de autenticación y verificación de identidad, lo cual sucede cuando la clasificación de la información es reservada, se deben utilizar métodos alternativos a las contraseñas, como medios criptográficos, tarjetas inteligentes, tokens, o medios biométricos. Definir la implementación de estos métodos dependerá de consideraciones estratégicas, financieras o de mercado, que tendrán que ser evaluadas en las instancias pertinentes.

c. No se debe mostrar identificadores del sistema o de la aplicación hasta que el proceso de inicio de sesión finalice correctamente.

d. Se debe mostrar una advertencia de aviso general que indique que solo deberían acceder usuarios autorizados a las estaciones de trabajo.

e. No proporcionar mensajes de ayuda durante el procedimiento de inicio de sesión que pudieran servir de ayuda a un usuario no autorizado.

f. Validar la información de inicio de sesión solo al completar todos los datos de entrada. Si surge una condición de error, el sistema no debe indicar qué parte de los datos son correctos o incorrectos.

g. Los sistemas y plataformas deben proteger contra los intentos de inicio de sesión forzados y registrar los intentos logrados y los fallidos.

h. Al completar un inicio de sesión correcto se debe mostrar la fecha y hora del inicio de sesión correcto anterior y detalles de cualquier intento de inicio de sesión fallido desde el último intento de inicio de sesión correcto.

i. No se debe mostrar una contraseña que se ingresa.

j. No se debe transmitir contraseñas en texto sin cifrar en la red.

k. Se deben terminar las sesiones inactivas después de un periodo de inactividad.

l. Se deben restringir los tiempos de conexión para los sistemas de información críticos con el fin de reducir la ventana de oportunidad para el acceso no autorizado.

m. Se debe forzar el uso de usuarios y contraseñas individuales para mantener la responsabilidad.

n. Se debe permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación para permitir los errores de entrada.

o. Se debe imponer la selección de contraseñas de calidad y en sintonía con las políticas específicas definidas en esa materia.

p. Se debe obligar a los usuarios a cambiar sus contraseñas al primer inicio de sesión e imponer cambios regulares de contraseñas según sea necesario.

q. Se debe mantener un registro de las contraseñas utilizadas anteriormente y evitar su nuevo uso.

r. Se debe almacenar archivos de contraseñas de manera separada de los datos del sistema de aplicación.

3.5 CORREO ELECTRONICO

a. Los mensajes por correo electrónico son considerados parte de los registros de los activos de información, por lo que están sujetos a políticas de monitoreo, auditoría, revisión e investigación de eventos. Debe evitarse su uso para actividades personales.
b. El área de gestión TIC pertinente deben definir el uso correcto y los requisitos de seguridad y control para los sistemas de correo electrónico.

c. El área de gestión TIC pertinente debe cumplir con los esquemas para el almacenamiento, respaldo, retención y destrucción de correos electrónicos.

d. 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 ETB.

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

3.6 INSTALACION Y USO DE PORTATILES, PERIFERICOS Y MEDIOS DE ALMACENAMIENTO EXTRAIBLES

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

b. Con el fin de proteger la información y el acceso a la red de la ETB, los trabajadores y contratistas deben guardar en un sitio seguro el equipo portátil asignado.

c. Las áreas de TIC deben garantizar que los puertos lógicos y físicos que soporten los sistemas de información de las plataformas, se encuentren restringidos con el fin de evitar el acceso por parte de personal no autorizado.

d. 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 el negocio de ETB o diferentes a las funciones asignadas al cargo que desempeña el trabajador.

e. 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 ETB y contar con las autorizaciones respectivas.

f. 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 ETB sin contar con los controles mínimos necesarios de seguridad establecidos en los procedimientos de línea base tecnológica y sin previa autorización de las áreas de Tecnología.

g. Cuando sea necesario almacenar o transportar en medios de almacenamiento extraíble, información importante del negocio incluyendo los datos personales que trata ETB, ellos y su información contenida deben contar con los controles de seguridad necesarios para evitar la pérdida de su integridad y el acceso o uso no autorizado o fraudulento. Sin limitarse a ellos, entre estos controles se tienen: almacenamiento y transporte con las medidas medioambientales mínimas para su debida conservación, archivos guardados con contraseña o encriptados.

3.7 DISPOSITIVOS MÓVILES

a. Se debe adoptar medidas de soporte para gestionar los riesgos introducidos por el uso de dispositivos móviles.

b. Todo dispositivo móvil (iPad, teléfonos inteligentes, laptops, entre otros) con acceso a la red de ETB, bien sean de propiedad de ETB o personal, deberán sin excepción, ser configurados con los controles mínimos definidos en el procedimiento de uso de dispositivos móviles.

c. El computador portátil (laptop) que contenga información confidencial deberá contar con el cifrado de su disco duro.

d. Está prohibido el uso de funciones de equipos móviles como medio de almacenamiento, grabación y capturar información de la empresa al que el usuario no esté autorizado por ETB.

e. En caso de pérdida o hurto de un dispositivo móvil que se encuentre autorizado para acceder a las aplicaciones o información de ETB, se debe notificar de manera inmediata al área respectiva TIC con el fin de tomar las medidas respectivas y evitar accesos no autorizados a la información.

3.8 SISTEMAS DE INFORMACION

a. Los trabajadores que son administradores y usuarios de los sistemas de información de ETB son responsables del buen uso de la información que tienen a su cargo.

b. Comunicaciones y Marca es el área autorizada para administrar los activos de información que se publican en la Intranet y Mercadeo y Publicidad es el área autorizada para administrar los activos de información que se publican en las páginas web de ETB.

c. Mercadeo y Canales es la única área autorizada para publicar información de los negocios, crear usuarios en redes sociales, blogs, usar logos de la empresa o cualquier otro tipo de contenido a nombre de ETB.

d. Toda instalación, configuración, mantenimiento y actualización de hardware y software debe ser realizada por administrador responsable cumpliendo con el procedimiento de cambios o de transición.

3.9 CRIPTOGRAFIA

a. Se debe asegurar el uso adecuado y eficaz de cifrado para proteger la confidencialidad, la autenticidad y/o la integridad de la Información.

b. Se deben desarrollar e implementar controles criptográficos para la protección de la información.

c. Para la gestión de claves se deben desarrollar e implementar controles para el uso, protección y gestión del ciclo de vida de las claves de cifrado, a lo largo de su ciclo de vida.

3.10 SEGURIDAD FISICA Y AMBIENTAL

a. Todo espacio físico donde resida la infraestructura TIC necesaria para la operación de los negocios de ETB, debe contar con mecanismos de acceso para la restricción de personal no autorizado, como son los centros de procesamiento de datos, bodegas, centros documentales, entre otros.

b. Deben tomarse las precauciones necesarias para que no quede desatendida información crítica del negocio en documentos y medios de almacenamiento

removibles, que se encuentre en puestos de trabajo o cualquier otro lugar al que pueda tener acceso personas no autorizadas.

c. Siempre que un trabajador o contratista se ausente de su lugar de trabajo, debe bloquear su estación de trabajo, computador de escritorio o portátil de manera que se proteja el acceso a sistemas, aplicaciones, servicios y en general cualquier información de la Empresa.

d. No obstante, el anterior literal, se debe tener implementado un protector de pantalla en todas las estaciones de trabajo, computadores portátiles y de escritorio, de manera que se active ante un tiempo sin uso.

e. Deben tomarse las precauciones necesarias para que ningún tipo de información escrita quede desatendida en ventanas, vidrios y tableros, para lo cual será necesario que al ausentarse de salas de reuniones o lugares de trabajo en general, la eventual información escrita, sea eliminada.

f. Deben tomarse las medidas necesarias para que no esté disponible para su uso, papel reciclable con información sensible, entre los que se incluyen los datos personales que trata ETB.

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

h. Toda persona que visite las instalaciones de las diferentes sedes de ETB debe cumplir con los controles de acceso físico dispuestos por la empresa. De igual manera el ingreso de personas a los centros de cómputo de la empresa, debe quedar registrado en la bitácora de ingreso de visitantes.

i. Todo equipo de cómputo debe ser registrado por los responsables de seguridad física al ingreso y salida de las instalaciones de ETB.

j. El movimiento o traslado de equipos de cómputo, recursos informáticos y de comunicaciones, debe realizarse únicamente por el área de TIC con el fin de evitar pérdida, hurto o daño de los activos de información de la empresa.

k. La autorización de ingreso a los centros de procesamiento de datos, salones de comunicaciones y cableado debe ser responsabilidad de las áreas de Gestión de TIC.

l. Los trabajadores y contratistas deben portar en un lugar visible en todo momento el carné que los identifique como vinculados a la empresa.

m. Los trabajadores y terceros vinculados a la empresa deben tener acceso única y exclusivamente a las áreas de ETB de acuerdo con su rol y funciones.

n. Los componentes, equipos de procesamiento de información, comunicaciones y archivos importantes para el negocio, deben estar ubicados en áreas de acceso restringido a personal no autorizado, deben ser monitoreadas y permitir la identificación inmediata y posterior de quienes ingresan y salen de dichos espacios.

o. La información física y los medios extraíbles de información sensible de la empresa, entre los que se incluyen los datos personales que trata ETB, 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.

p. Los computadores y fotocopiadoras de centrales, colegios, oficinas administrativas y demás sedes de la empresa deben estar inventariados por el software de control de impresiones para evitar el uso no autorizado.

q. Cualquier alteración en la información que se haga por medio de los equipos de ETB, 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.

r. 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.

3.11 SEGURIDAD EN LAS OPERACIONES

3.11.1 RESPALDO DE LA INFORMACION

La información sensible que se encuentra almacenada en las plataformas tecnológicas de ETB y de proveedores, debe contar con acciones de restauración que garanticen la integridad de la información en casos de emergencia y según sea requerido y autorizado por el responsable del activo de la información.

3.11.2 VULNERABILIDADES TÉCNICAS

Se debe obtener la información sobre las vulnerabilidades técnicas de los sistemas de información de manera oportuna y la exposición de la organización a dichas vulnerabilidades se debe evaluar y se deben tomar las medidas necesarias para abordar el riesgo asociado. De acuerdo a lo anterior, las siguientes son las acciones que se deben ejecutar por parte de las áreas de gestión TIC:

a. Se deben establecer roles y responsabilidades asociados a la administración de vulnerabilidades técnicas.

b. Se deben definir procedimientos específicos para escaneos planeados y por demanda.

c. Los escaneos planeados deben efectuarse sobre todos los sistemas de información prioritarios de acuerdo a un plan estructurado por cada área, siempre y cuando cada sistema prioritario se escanee al menos una vez por año. Esa prioridad debe basarse en unos criterios previamente definidos los cuales deben ser aprobados por el dueño del proceso que tiene a su cargo las actividades de vulnerabilidades técnicas. Estas prioridades deben ser divulgadas a los roles pertinentes.

d. Las vulnerabilidades identificadas deberán ser priorizadas para su tratamiento de acuerdo con el nivel de riesgo.

e. Como mínimo se deben tratar las vulnerabilidades de los activos críticos.

f. Debe fijarse un plazo máximo de tratamiento de las vulnerabilidades de cuatro (4) meses. En los casos en que no se logre la remediación deberá contarse con justificación y alinearse con la gestión de riesgos.

g. Debe considerarse si las acciones para remediar las vulnerabilidades son viables frente al riesgo de su implementación

h. Las acciones para las remediaciones pertinentes deben considerar los procedimientos de gestión de cambios o transición y/o migración a nuevas secciones de red según aplique.

i. Se debe realizar de manera periódica seguimiento a la ejecución de las acciones de remediación.

j. Trimestralmente deberá realizarse y presentarse un informe ejecutivo que debe contener como mínimo: tendencia de la mejora, métricas de gestión de vulnerabilidades y necesidades de escalamiento.

3.11.3 PRUEBAS DE PENETRACIÓN

Se deben realizar pruebas de penetración en los sistemas de información para intentar comprometerlos con el propósito de evaluar su seguridad, de manera que se pueda verificar el daño potencial que un atacante puede provocar al ganar acceso, destruir datos o dañar los valores de la compañía.

a. Se deben realizar estas pruebas al menos dos veces al año

b. Las pruebas deberán realizarse a partir de un plan estructurado por cada área el cual podrá incluir sistemas de información a los cuales se les haya identificado vulnerabilidades (ver 3.11.2) o aquellos prioritarios de acuerdo a criterios previamente definidos, en todo caso este plan deberá ser aprobado por el dueño del proceso que tiene a su cargo las pruebas de penetración.

c. El plan debe contemplar el ámbito en el que se llevará a cabo cada prueba, es decir si son de caja negra, blanca o gris, horarios, si los administradores serán conscientes de las pruebas, y en general si se permiten denegaciones de servicio, instalación de troyanos, ataques a sitios web, ingeniería social etc.

d. Para cada sistema a probar se debe hacer un reconocimiento para la obtención de información que podrá hacerse a través de herramientas o a través de información que está disponible públicamente.

e. Se debe realizar un escaneo para determinar qué servicios y qué sistemas operativos corren en el sistema objetivo

f. A partir de la información obtenida en los puntos anteriores y de los resultados de los escaneos de vulnerabilidades, se procede a explotar tales fallas.

g. Se deben eliminar las evidencias de los ataques perpetrados con el fin de evaluar cuáles de ellos pueden ser exitosos al cubrir los rastros dejados

h. Se debe recolectar toda la evidencia posible con el fin de documentar debidamente el informe

i. Semestralmente deberá realizarse y presentarse un informe ejecutivo que debe contener como mínimo:
   - El rango de direcciones IP probadas
   - Factores como si se utilizó la ingeniería social, si se utilizaron troyanos o backdoors, por mencionar algunos
   - Análisis de resultados, incluyendo dirección IP y dominio del equipo probado, puertos TCP y UDP abiertos, descripción de los servicios, pruebas realizadas
   - Recomendaciones

3.11.4 INSTALACION Y USO DE SOFTWARE

Solamente se permite el uso de software de distribución gratuita, shareware, GNU, entre otros; que haya sido previamente revisado y aprobado por el administrador responsable.

a. Las adquisiciones de software deben estar avaladas por el área responsable de Tecnología y por el líder del negocio o proceso corporativo.

b. No se permite descargar, instalar y/o ejecutar software o archivos sin la debida revisión y autorización del área de TIC.

c. El software de la empresa está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está prohibido hacer copias, descargar o usar este software para fines personales.

3.11.5 USO DE INTERNET Y DE LA RED INTERNA

a. El acceso a Internet estará reservado para todos aquellos empleados que lo requieran según sus funciones de trabajo, de acuerdo a las necesidades del negocio y para uso laboral exclusivamente.

b. La empresa restringirá el acceso a sitios de internet que por alguna circunstancia vayan en contra de sus políticas institucionales y del negocio, políticas de seguridad y buenas prácticas adoptadas por ETB tales como

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

c. No está permitido hacer uso de los recursos de ETB, tales como dispositivos para acceder a redes sociales, servicios interactivos de almacenamiento masivo, streaming de videos, páginas de mensajería instantánea. Todo lo anterior salvo que se implemente alguno de estos recursos como de uso estrictamente corporativo.

d. Está prohibido a los trabajadores, contratistas y terceros que tengan acceso a red inalámbrica o cableada de ETB, menoscabar o eludir los controles establecidos por la empresa para la protección de los activos.

e. 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 las áreas responsables de la administración de los activos y por requisitos propios del negocio.

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

g. Queda prohibido toda publicación o intercambio de información sensible de la empresa 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.

3.11.6 CONEXIONES REMOTAS

a. Toda conexión remota a la red de ETB debe ser a través de canales seguros y prevenir accesos no autorizados.
.

b. Se permite el uso de VPN para usuarios previamente autorizados a través de la Mesa de Servicios TIC que por actividades propias de la empresa requieran acceso a los sistemas de información, de acuerdo a lo establecido en el procedimiento de control de accesos.

c. El uso de la VPN es exclusivo de quienes no se encuentren dentro de la red LAN de ETB y deban hacer uso de sistemas de información de manera remota debido a las exigencias particulares del negocio.

d. Un empleado, contratista o tercero vinculado a la empresa 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 la presente política de seguridad de la información y el procedimiento de control de accesos.

e. Toda conexión remota sea de empleados o proveedores de ETB, 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.

3.12 TRANSFERENCIA DE LA INFORMÁCIÓN

a. Se debe proteger la información transferida de la intercepción, la copia, la modificación, el ruteo incorrecto y la destrucción

b. Proteger la información electrónica sensible comunicada en forma de elemento adjunto

c. Se prohíbe expresamente la trasferencia de información que incluya la difamación, el acoso, el reenvío de cartas de cadena y las, compras no autorizadas

d. No dejar mensajes que contienen información confidencial en máquinas contestadores debido a que personas no autorizadas pueden volver a reproducir los mensajes, se pueden almacenar en sistemas comunales o almacenar incorrectamente como consecuencia de una mala manipulación

e. Se debe concienciar al personal que no deberían sostener conversaciones confidenciales en lugares públicos o a través de canales de comunicación, oficinas abiertas y lugares de encuentro inseguros

3.13 SEGURIDAD EN LA ADQUISION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACION

a. 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.

b. Las transacciones deben estar protegidas para prevenir la transmisión incompleta, errores de enrutamiento y alteraciones no autorizadas de los mensajes o su reenvío

c. Debe protegerse la información involucrada en los cambios a los sistemas en el ciclo de vida de desarrollo y a las plataformas de producción y aplicaciones críticas, mediante procesos formales de control de cambios.

d. Los datos de salida de los aplicativos que manejan información sensible deben contener los datos relevantes requeridos para el uso de acuerdo al rol y se deberán enviar exclusivamente a los usuarios y/o terminales autorizadas.

e. Los aplicativos de la empresa deben pasar por un proceso de pruebas y aceptación en un ambiente dedicado para tal fin antes de ser liberados a producción.

f. El acceso a la información contenida en las bases de datos sólo está permitido a través de las aplicaciones de los sistemas de la empresa. Sólo tendrán acceso los usuarios autorizados que de acuerdo a su rol se identifican mediante usuario y contraseña.

g. 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.

h. 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.

i. 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.

j. Debe supervisarse el desarrollo tercerizado de los sistemas e independientemente de quien adelante el desarrollo, deben realizarse pruebas de funcionalidad de la seguridad

k. 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.

3.14 PROVEEDORES Y CONTRATISTAS

3.14.1 RELACIÓN CON PROVEEDORES, CONTRATISTAS Y/O TERCEROS

a. Se debe identificar cual es la información a la que tendrán acceso los proveedores, la cual debe estar valorada a partir de las necesidades de integridad, disponibilidad y confidencialidad requeridas por ETB. De acuerdo a esa valoración se deben establecer los requisitos mínimos de seguridad de la información y los tipos de acceso a la información que deberán tener los proveedores.

b. Con los requisitos del ítem anterior se debe establecer un perfil de seguridad de cada proveedor que maneje información sensible.

c. Se debe establecer cuáles son los tipos de obligaciones legales, regulatorias y contractuales que les son aplicables a los proveedores en materia de protección de la información y velar por su cumplimiento.

d. Los proveedores y contratistas deben ser incluidos en las disposiciones establecidas en las políticas de este documento, principalmente en las de control de acceso a los sistemas de información y a las instalaciones físicas, en la gestión de incidentes de seguridad de la información y en las disposiciones de recuperación y/o contingencia que procuren la protección de la información.

e. Los Proveedores y Contratistas vinculados a ETB que tengan acceso a la información de la empresa, deben firmar una cláusula de confidencialidad para su uso con el fin de proteger dicha información y se deben definir las reglas para compartir la información y cualquier posible problema y compromiso.

f. Cualquier movimiento, cambio o transición que involucre activos de información en la operación de los proveedores, debe administrarse de manera que se conserven los controles y requisitos de seguridad de la información establecidos.

g. Deben establecerse mecanismos de capacitación y concienciación en materia de seguridad de la información a los proveedores y a todo aquel personal de ETB que interactúe con ellos en atención al perfil de seguridad identificado.

3.14.2 SOBRE LOS ACUERDOS CONTRACTUALES

Para todos aquellos proveedores que puedan acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura TI para la información de ETB, se debe incluir en los acuerdos contractuales, lo siguiente:

a. Cumplimiento de las políticas de seguridad de la información pertinente al objeto contractual y obligación del proveedor de realizar los acuerdos necesarios con sus sub-proveedores, para cumplir las políticas de seguridad de la información pertinentes.

b. En los contratos con los proveedores se debe establecer la obligación del proveedor de colaborar con la gestión de los riesgos de seguridad de la información de acuerdo a la metodología de clasificación y valoración de activos de la información y de gestión de riesgos de ETB y por tanto la obligación de cumplir con las reglas de uso aceptable de la información, incluido el uso inaceptable, en caso de ser necesario.

c. Para los contratos relacionados con adquisición de tecnología, se deben gestionar los riesgos de los componentes de tecnología que ya no estén disponibles por obsolescencia o porque los proveedores ya no estén en el negocio.

d. Obligación del proveedor de ejecutar las acciones necesarias para cumplir con los controles de seguridad de la información considerados en la declaración de aplicabilidad (SOA, por sus siglas en inglés) vigente de ETB. Incluye la obligación del proveedor a entregar periódicamente un informe independiente sobre la efectividad de los controles y un acuerdo sobre la corrección oportuna de los asuntos pertinentes indicados en el informe.

e. Obligación del proveedor de informar oportunamente a ETB sobre la ocurrencia de incidentes de seguridad de la información y de la colaboración durante su remediación.

f. Obligación del proveedor de establecer las contingencias necesarias para continuar con el procesamiento de información en caso de que no pueda suministrar sus productos y servicios.

g. Obligación del proveedor de capacitar y sensibilizar al personal contratado sobre los procedimientos específicos y requisitos de seguridad de la información de ETB.

h. Obligación del proveedor de informar a ETB las personas que deben tener acceso a los sistemas de información de ETB y así mismo, la obligatoriedad de informar a ETB sobre las personas que deben perder ese derecho en virtud de la desvinculación de la empresa contratista.

i. Garantizar que el personal contratado tenga los estudios de seguridad pertinentes a la sensibilidad de la información a acceder.

j. Los requisitos de seguridad de la información deberán ser replicados si los proveedores realizan subcontrataciones incluyendo si hay componentes comprados a otros proveedores.

k. En los contratos con los proveedores se debe establecer la obligación del proveedor de cumplir con los requisitos legales y normativos, incluida la protección de datos personales, los derechos de propiedad intelectual y derechos de autor.

l. Derecho a auditar los procesos y los controles del proveedor relacionados al acuerdo.

3.14.3 MONITOREO Y REVISIÓN DE LOS SERVICIOS CON EL PROVEEDOR

a. Monitorear los niveles de desempeño del servicio con el fin de verificar la adherencia a los acuerdos.

b. Se debe monitorear la adherencia a las políticas de seguridad de la información y al cumplimiento de los requisitos de seguridad de la información por parte de los proveedores.

c. Realizar auditorías a los proveedores y seguimiento a los problemas identificados.

d. Revisar los incidentes de seguridad de la información.

e. Revisar los aspectos de seguridad de la relación que tiene el proveedor con sus propios proveedores y monitorear la replicación de los requisitos de seguridad a los subcontratistas.

f. Revisar que los cambios en el servicio del proveedor realizados de manera unilateral o bilateral, garanticen la continuidad de la adherencia de los requisitos de seguridad.

3.15 INCIDENTES DE SEGURIDAD DE LA INFORMACION

a. Los trabajadores y contratistas vinculados a la empresa deben estar conscientes de los procedimientos y su importancia para reportar incidentes de seguridad.

b. Los trabajadores, contratistas o terceros que utilicen los servicios de información de la empresa, deben reportar al área de TIC o propietario del riesgo, cualquier incidente de seguridad que pueda comprometer la confidencialidad, integridad y/o disponibilidad de los activos de información de la empresa, siguiendo la documentación de notificación de incidentes establecida. Dichos reportes deben ser comunicados a las áreas de TIC o propietarios de riesgos.

c. Los incidentes de seguridad que afecten los activos de información, deben ser manejados con la participación de la mesa de ayuda TIC, por lo cual, queda expresamente prohibido divulgarlos a personal no autorizado, a menos que haya sido formalmente autorizado.

3.16 SEGURIDAD EN LA GESTION DE CONTINUIDAD DEL NEGOCIO

a. Se debe mantener un proceso para la continuidad del negocio basado en los siguientes aspectos:

- Entender los riesgos que enfrenta la empresa y su impacto, incluyendo la identificación y sensibilidad de sus procesos críticos.
- Entender el impacto de las interrupciones o incidentes de seguridad en las actividades del negocio.
- Formular y documentar planes estratégicos de continuidad del negocio acorde con los objetivos y prioridades de la empresa.
- Asegurar que la administración de la continuidad del negocio sea incorporada en los procesos y la estructura de la empresa.
- Asignar responsabilidades para la coordinación y administración del plan de continuidad del negocio.

b. Los planes de continuidad del negocio deben ser documentados, probados y evaluados por lo menos una vez al año, según un cronograma establecido por el área donde se encuentra el liderazgo del Sistema de Gestión de Continuidad del Negocio y el centro de servicios de tecnología para verificar su funcionamiento adecuado.

c. Los planes de contingencia deberán estar ubicados en un lugar seguro dentro de la empresa. Deberán ser de conocimiento de los empleados y distribuido según su inherencia a la estructura de la empresa.

d. Los terceros contratados deben contar con planes de continuidad debidamente documentados y probados, con el fin de dar continuidad a las operaciones críticas del negocio.

3.17 CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES

a. ETB velará por el cumplimiento de las políticas seguridad de la información estipulada por la empresa y la legislación aplicable vigente por los entes de control.

b. Aquellos documentos que estén bajo lineamientos legales o regulatorios deberán ser resguardados bajo las medidas de seguridad adecuadas para garantizar su integridad.

c. Las áreas de seguridad de la información en conjunto con el Área Jurídica mediante el proceso de identificación de requisitos de seguridad de la

información que sean de cumplimiento obligatorio y emitidos por entes gubernamentales o privados y cualquier disposición colombiana vigente, impartirán directrices y harán seguimiento a la implementación de los controles necesarios por parte de las áreas pertinentes de la organización, para dar cumplimiento y protección a los activos de información.

d. Los trabajadores están obligados a ceder a la empresa los derechos exclusivos de propiedad literaria, licencias, invenciones, u otra propiedad intelectual que ellos creen o desarrollen durante su periodo laboral con la empresa. 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.

e. La empresa tiene propiedad legal de la información almacenada, enviada y compartida en 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 trabajador haya colocado en los medios de comunicación existentes en la empresa.

f. La empresa 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 empresa. Los registros de información de la empresa clasificados como confidencial deben estar adecuadamente protegidos por el responsable de la información contra pérdida, destrucción y falsificación.

g. Las áreas de servicios de tecnología, deberá revisar periódicamente los acuerdos de licencias de hardware y software instalado a fin de verificar el cumplimiento de los mismos por parte de la empresa.

h. 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.

3.18 PROTECCIÓN DE DATOS PERSONALES

a. El acceso a la información personal sensible, es decir aquella cuyo uso inadecuado puede generar discriminación, debe hacerse únicamente por el personal que trata esa información con ocasión exclusiva de la finalidad para la cual se tiene recolectada y con la debida autorización del titular, salvo en los casos que por ley no sea requerida dicha autorización. Los controles de acceso a esta información, tanto a nivel tecnológico como físico, deben tener un especial seguimiento a su eficacia.

b. Se debe garantizar que sólo personal debidamente autorizado y con la debida autorización, tenga acceso a copiar o transferir masivamente información de datos personales

c. Las bases de datos personales no deben estar almacenadas en computadores personales, ellos deben reposar en los sistemas informáticos o en los repositorios de archivos administrados por el área TIC pertinente y con los privilegios de acceso debidamente gestionados y justificados. En caso que se tenga información personal en medios de almacenamiento extraíble debe atenderse lo definido en la política de seguridad pertinente a estos medios.

d. Los trabajadores y contratistas deben mantener la información personal íntegra cada vez que sea tratada por ellos. Los dueños de los procesos deben velar porque la gestión de sus procesos apoye sistemáticamente esta misión.

e. Se entiende que los controles de seguridad de la información que se implementan a partir de los lineamientos establecidos en las políticas de este documento, aplican para los activos de información entre los que se encuentran las bases de datos de información personal.

f. Deben ejecutarse auditorias periódicas que permitan identificar oportunidades de mejora en el tratamiento de datos personales que contribuyan a su protección eficaz y al cumplimiento de la ley particularmente a lo establecido en el régimen de protección de datos personales.

Control de Cambios:

Versión	Descripción del Cambio	Fecha del Cambio
1.0	Documento inicial	17/07/2015

2.0	Inclusión política pruebas de penetración	16/12/2015
3.0	Actualización de políticas de vulnerabilidades, correo electrónico, seguridad física y del entorno, medios de almacenamiento extraíbles y datos personales.	16/08/2017
4.0	Actualización políticas de gestión de acceso y de proveedores	10/04/2018