


Código			Política			
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)			
Fecha de emisión						
29	08	2023				

Elaborado por: Vicepresidencia de Tecnología - Gerencia de Planeación de Tecnología – Profesional Especializado: Jhonatan Mauricio Riveros Casas	Revisado por: Vicepresidencia de Tecnología - Gerencia de Planeación de Tecnología – Coordinador: César Javier González Martínez	Aprobado por: Vicepresidencia de Tecnología - Gerencia de Planeación de Tecnología – Gerente: David Alberto Roldan Rojas
--	--	--

Nombre de proceso:

11.2 Gestión de la seguridad de la información

Nombre de Procedimiento:

11.2.1 Planeación de la gestión de la seguridad de la información

Objetivo:

Establecer los criterios y medidas básicas que deben aplicarse a toda la información de la Empresa de Telecomunicaciones de Bogotá ETB, para su correcto uso, 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.


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, practicantes, aprendices, proveedores, contratistas, aliados, clientes y asociados involucrados en la generación, almacenamiento, procesamiento, uso, transmisión y eventual eliminación de la información de ETB en los sistemas de información.

Segmento: N/A


Definiciones:

- Datos:** Los datos son las piezas individuales o recolección de hechos, cantidades, caracteres, símbolos, transacciones y en general elementos crudos de conocimiento; que pueden ser persistidos y relacionados de alguna manera por la institución, ya sea en medio físico o electrónico, y que no es necesario que hayan tenido un procesamiento, cálculos o estructuras elaboradas previas en su proceso de construcción, en este sentido los datos son componentes de la información y por tanto no constituyen activos de información.
- Datos personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables, como

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

puede ser información de tipo numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas e identificables

- **Información:** Conjunto de datos relacionados que le generan valor a la Organización siendo usada para la ejecución de actividades en cumplimiento de los objetivos de los procesos y, por tanto, debe ser protegida salvaguardando su confidencialidad, integridad y disponibilidad.
- **Activo primario de información:** Es un conjunto de informaciones vinculadas bajo el entendido que tienen los mismos niveles de confidencialidad, integridad y disponibilidad y que se encuentran contenidos en el mismo activo de soporte a la información de manera que comparten la misma necesidad de protección.
- **Activo de soporte a la información:** Corresponde básicamente al lugar dónde se almacena, consulta, procesa o transita la información. Tienen vulnerabilidades que sí son explotadas por las amenazas pueden deteriorar los activos primarios de información. En ETB pueden ser aplicaciones, sistemas de información, plataformas de servicios, computadores, servidores de archivos, archivos físicos, medios de almacenamiento extraíbles, entre otros.
- **Matriz de identificación y clasificación de activos de información:** Es el instrumento mediante el cual se hace el inventario de activos de información primarios o de soporte. Allí se identifican, entre otros, sus propietarios y custodios, y se clasifican en cuanto a confidencialidad, integridad y disponibilidad con lo cual se define su criticidad.
- **Activos de información críticos:** Son aquellos activos de información que cuentan con una criticidad MEDIA o ALTA en la matriz de identificación y clasificación de activos correspondiente.
- **Datos críticos:** Clasificación de datos que por su valor y sensibilidad pueden generar un alto impacto a un proceso o a la organización en general, sobre los cuales se enfocan las acciones de cuidado para su preservación entre estas la definición de procedimientos operativos estandarizados para que se asegure la calidad de estos. Los datos son críticos cuando, aún sin ser activos de información, son vitales para la ejecución de una actividad o requieren ser salvaguardados en cuanto a confidencialidad, como bien lo podrían ser las contraseñas o los datos personales.
- **Medios extraíbles:** Son aquellos soportes de almacenamiento diseñados para ser extraídos de la computadora sin tener que apagarla. Ciertos tipos de medios extraíbles están diseñados para ser leídos por lectoras y unidades también extraíbles.
- **Información física:** Corresponde a los activos primarios de información que están en medios físicos como lo son los documentos físicos.
- **Controles de seguridad de la información:** Es el conjunto de medidas preventivas, detectivas, disuasivas y correctivas implementadas en procesos, tecnología, infraestructura física y personas que permiten resguardar y


Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de los activos de información.

- **Información digital:** Corresponde a aquellos activos de información que están almacenados de forma electrónica
- **Clasificación de activos de información:** Es el nivel de protección que el propietario del activo de información considera deben tener sus activos, de acuerdo con las necesidades de seguridad requeridas desde el punto de vista del proceso de gestión bajo su cargo. El nivel de protección se basa en la confidencialidad, integridad y disponibilidad de la información.
- **Confidencialidad:** Se refiere a la preservación de las restricciones o limitantes que se deben fijar para autorizar el acceso y la divulgación de los activos de información, así como los medios para la protección de la intimidad personal y propiedad de la información. Las opciones son:
 - Pública (Valor 1): Cualquier información no clasificada se considera como pública. La información no catalogada y por tanto pública, será aquella cuya divulgación no afecte a la Empresa en términos de pérdida de imagen y/o económica
 - Uso interno (Valor 2): Información que, sin ser reservada ni restringida, debe mantenerse dentro de la Empresa y no debe estar disponible externamente, excepto para terceros involucrados en el tema. En el caso de terceros, deberán comprometerse a no divulgar dicha información.
 - Restringida (Valor 3): Información sensible, interna de áreas o proyectos a los que deben tener acceso controlado otros grupos, pero no toda la empresa debido a que se puede poner en riesgo la seguridad e intereses de la compañía, de sus clientes o asociados y empleados.
 - Reservada (Valor 4): Información de alta sensibilidad que debe ser protegida por su relevancia sobre decisiones estratégicas, impacto financiero, oportunidad de negocio, potencial de fraude o requisitos legales.


Los Datos Personales no públicos son considerados como mínimo como información restringida.

- **Integridad:** Se refiere a la protección contra la modificación no autorizada, exactitud o completitud de los activos de información. Los criterios de clasificación aplican dependiendo de lo que causan los datos inexactos, incompletos o modificados sin autorización y la facilidad con que se superan tales consecuencias. Las opciones son:
 - Sin consecuencias de fácil reparación (Valor 1)
 - Daño moderado subsanable (Valor 2)
 - Daño grave difícil de reparar (Valor 3)
 - Pérdidas económicas no reparables (Valor 4)
- **Disponibilidad:** Acceso oportuno y confiable del uso de los activos de información autorizados. Las siguientes opciones se dan teniendo en cuenta que se puede estar sin el activo en funcionamiento más de un determinado

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

tiempo al cabo del cual se comienzan a materializar riesgos financieros y operativos:

- Más de 72 horas (Valor 1)
 - De 24 a 72 horas (Valor 2)
 - De 6 a 24 horas (Valor 3)
 - De 0 a 6 horas (Valor 4)
- **Criticidad de los activos de información:** Es el principal insumo para definir si al activo de información debe realizársele gestión de riesgos o no. Las opciones son:
- ALTO: Activos de información en los cuales la clasificación de la información en dos o todos los principios de seguridad (confidencialidad, integridad, y disponibilidad) es de valor 4
 - MEDIO: Activos de información en los cuales la clasificación de la información es de valor 4 en uno de sus principios de seguridad o al menos uno de ellos es de valor 3
 - BAJO: Activos de información en los cuales la clasificación de la información en sus principios de seguridad sea máximo de valor 2
- **Sistemas de información:** Son los medios tecnológicos a través de los cuales se administra, recolecta, recupera procesa, almacena y distribuye información relevante para los procesos de ETB. En general están administrados por el área de tecnología de servicios internos en la organización.
- **Elementos de infraestructura TI:** Son los elementos interdependientes de software, hardware, redes e instalaciones necesarios para desarrollar, administrar, operar, controlar, monitorear y dar soporte a los entornos que permiten ofrecer servicios y soluciones de tecnología para la gestión de procesos y servicios de la organización. De manera general pueden ser: (i) las funcionalidades de procesamiento de servidores, entre los que se encuentran servidores de almacenamiento en red, servidores de carga de archivos, servidores web, servidores de aplicaciones y servidores de bases de datos, (ii) dispositivos de almacenamiento y respaldo de información, (iii) Estructura (árbol) de directorios y subdirectorios de sistemas operativos, base de datos y carpetas compartidas, (iv) Elementos de seguridad y (v) funcionalidades de red o comunicación para permitir que la información fluya a través de elementos como switches y routers.
- **Plataformas de servicios:** Para efectos de estas políticas se les denomina plataformas de servicios a los medios tecnológicos que administran los productos y servicios de ETB. En general están administrados por el área de tecnología de prestación de servicios de cara al cliente.
- **Tecnología que soporta los servicios:** En el presente documento hace referencia a la tecnología que es administrada por aquella(s) área(s) que tiene(n) bajo su cargo la administración de los servicios tecnológicos de cara a la prestación de productos y servicios como lo son aquellas plataformas core y no core que entrega los servicios de voz, internet, datos, tv, etc.

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		


- **Oficina Digital:** Es la ejecución de actividades laborales en un entorno exclusivamente digital pudiéndose desarrollar en dentro o fuera de las instalaciones de ETB.
- **SGSI:** El Sistema de Gestión de Seguridad de la Información es una herramienta de gestión que permite planear, hacer, verificar y actuar en un ciclo de mejora continua, las actividades necesarias para lograr proteger la información crítica de ETB. Este sistema hace parte de un modelo integrado de gestión empresarial (MIGE) que incluye una gestión procesos y la administración de otros sistemas de gestión.
- **PIGDP:** El Programa Integral de Gestión de Datos Personales es una herramienta de gestión que en ETB tiene como objetivo desarrollar la responsabilidad demostrada frente al régimen nacional de protección de datos personales con un enfoque de mejora continua.
- **Propietario de activos 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.

En atención a lo anterior es responsable de:

- Que los activos primarios de información a los cuales tienen acceso los usuarios bajo su cargo permanezcan identificados y valorados
- Determinar los derechos y restricciones de acceso a esos activos de información, para los usuarios bajo su cargo, y
- Velar porque esos accesos permanezcan actualizados en atención a las responsabilidades del personal bajo su cargo.


Así las cosas, un mismo activo primario de información puede tener más de un propietario. El rol de propietario de activos de información es ejecutado por quienes también fungen como dueños de proceso, establecido este último, en las responsabilidades del gobierno de procesos de ETB.

- **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 servicios, los sistemas de información o los lugares donde se almacena y procesa información, de acuerdo con su área de trabajo. En ese sentido administra los derechos de acceso a los activos de información.
- **Autorizador de Rol:** Es a quien el propietario de los activos de información delega su responsabilidad en cuanto al acceso a los activos de información que se encuentran en aplicaciones, plataformas o sistemas y por tanto tiene la facultad de autorizar los roles de acceso requeridos por los usuarios de su proceso o grupo funcional, según aplique, en virtud de sus responsabilidades. De acuerdo con lo anterior y teniendo en cuenta que una misma aplicación, plataforma o sistema puede requerir ser accedido por usuarios de diferentes procesos o grupos funcionales, un mismo rol puede ser autorizado por diferentes autorizadores de rol.
- **Líder Gestor de Acceso a Usuarios:** Administra los procedimientos establecidos para controlar la asignación de los derechos de acceso a las

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		


aplicaciones, plataformas y sistemas de manera que se asegure solo el acceso por usuarios autorizados. Estos procesos deben cubrir todas las etapas del ciclo de vida del acceso de los usuarios, desde el registro inicial de los nuevos hasta la baja del registro de los usuarios que ya no requieran dicho acceso. El Gestor de Acceso de usuarios atiende las políticas definidas por quienes administran la seguridad informática y de la información y da línea sobre la gestión de acceso a usuarios a la mesa de servicios de tecnología. Este rol es necesario para cumplir la necesidad planteada tanto para la tecnología que soporta los procesos como para la tecnología que soporta los servicios.

- **Comité de Seguridad de la Información:** Es la máxima instancia de decisión y seguimiento del Sistema de Gestión de Seguridad de la Información en ETB, como quiera que es el responsable de los deberes de la alta dirección para los temas específicos del SGSI.
- **Comité Gobierno de información:** Este comité tiene como objetivo ejecutar, monitorear y proponer acciones que estén encaminadas al mejoramiento de los componentes y/o necesidades requeridas para potenciar en la compañía su información como un recurso de valor empresarial, así como los niveles de calidad y satisfacción a alcanzar.
- **Líder gestor de consumo de información:** Administrar el repositorio del gobierno de información, los sitios y sub-sitios, identificar cambios o evolutivos dentro de la herramienta de gobierno de información, para remitir a las áreas correspondientes.
- **Usuario de activos de información:** Todo trabajador, contratista, practicante o aprendiz que requiere acceder, según sea pertinente con ocasión de sus responsabilidades, a las plataformas de servicios, los sistemas de información o los lugares donde se almacena, transita y/o procesa información, de acuerdo con su área de trabajo
- **Contraseñas:** son un mecanismo de autenticación secreta para verificar una identidad. Existen otros mecanismos adicionales de autenticación que pueden ser usados independientes o de manera complementaria como factor de autenticación adicional.
- **ID:** abreviación del término identificación el cual debe corresponder al *login* de red corporativa y de aplicaciones, plataformas y sistemas.
- **ID de usuario:** asignado a empleados o contratistas para acceder a los sistemas o plataformas y que permite identificarlos unívocamente
- **ID genérico:** es un identificador para acceso a una aplicación, plataforma o sistema que no identifica unívocamente a una persona (empleado o contratista)
- **ID de servicio:** es un ID genérico requerido para la interacción o integración entre los sistemas y no se encuentra asignado a un empleado o contratista el cual pueden ser:
 - Inherente al sistema, por defecto, que cuenta con los máximos privilegios.
 - Creado automáticamente por el sistema para habilitación de servicios para su funcionamiento y que no son usados por ningún ID de usuario

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

- Creado por un ID privilegiado.
- **ID compartido:** ID genérico requerido para el uso de varios empleados y contratistas con un ID único usuario y contraseña asignados.
- **ID privilegiado:** es un ID de usuario o genérico requeridos con perfil de altos privilegios el cual permite crear, modificar o eliminar cualquier tipo de información sobre el sistema o plataforma, incluyendo la gestión de los IDs.
- **Privilegio:** corresponde a un derecho o permiso para ejecutar una o más funciones sobre un sistema.
- **Rol de acceso:** O simplemente rol, es el conjunto de privilegios configurados como definiciones técnicas en aplicaciones, plataformas o sistemas a partir de unas definiciones funcionales requeridas para la ejecución de actividades por parte de los usuarios.

DESCRIPCIÓN DE LA POLÍTICA

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

Este documento contiene los lineamientos específicos en cuanto a seguridad de la información y ciberseguridad, abordando diferentes aspectos que complementan las diferentes políticas definidas en el SGSI.

1 Organización de la seguridad de la información


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.

2 Seguridad de 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 contar con acuerdos contractuales 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 soporte de la información que le fueron asignados por ETB para sus actividades laborales. Esta política deberá regirse por los lineamientos en cuanto a gestión de activos físicos vigente.

3 Gestión de activos

- a. Todo activo de información (primario y de soporte) debe estar identificado y valorado según los riesgos de seguridad asociados y acorde con los lineamientos establecidos en la metodología corporativa, bajo la


Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

responsabilidad de los propietarios de los activos con la periodicidad establecida.

- 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 y gestión correspondiente.
- c. Según su criticidad, los activos primarios y de soporte deben contar con los controles asociados a los riesgos de seguridad según corresponda.
- d. Ningún trabajador o tercero vinculado a ETB puede divulgar información valorada como de confidencialidad restringida o reservada de la empresa a sus clientes y asociados o a personas no autorizadas. Para lo anterior se debe definir y divulgar las sanciones correspondientes.
- e. El tratamiento que tendrá el activo de información en ETB, se definirá acorde al tipo de activo y su nivel de clasificación (primario o de soporte), siguiendo el Manual Operativo (Metodología gestión de activos de información, código 11-11.2-M-002, utilizando la última versión disponible y formalizada dentro de ETB).
- f. Los activos de información primarios que deban ser enviados y/o compartidos deberán estar etiquetados acorde al esquema de clasificación establecido, según el Manual Operativo (Metodología gestión de activos de información) en su última versión disponible y formalizada dentro de ETB.
- 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. Cuando sea necesario transmitir información magnética o electrónica valorada como de confidencial reservada, fuera de la red de ETB, deberá hacerse por un medio seguro alternativo, preferiblemente cifrado como VPN o FTPS. En caso de no ser posible porque no se tenga habilitada esta opción con el destinatario, los archivos a ser transmitidos deberán estar protegidos contra lectura y con el envío de claves de protección por un canal diferente.
- i. La información física y los dispositivos de almacenamiento que contienen datos críticos, deben destruirse físicamente o sobrescribir cuando ya no sean requeridos por el negocio, de tal forma que los datos no se puedan recuperar.

4 Control de acceso a la información

Los controles de acceso a los activos de información son tanto lógicos para los sistemas de información y plataformas de servicios, como físicos para los lugares donde se encuentra información física o digital alojada, por lo tanto, los aspectos

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

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 clasificación 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 tareas es decir que ningún usuario tenga la posibilidad de autorizarse a sí mismo los acceso físicos y lógicos a dónde se almacena, procesa o transita la información

4.1 Administración de acceso a los usuarios

- a. Los propietarios de los activos de información o los autorizadores de rol (estos últimos delegados por los primeros) son los responsables de la autorización de acceso a las plataformas, aplicaciones y elementos de infraestructura TI de ETB, particularmente para:
 - a. Procesos: Empleados, contratistas, practicantes y aprendices que se desempeñan en los procesos del negocio de los cuales estos propietarios son dueños
 - b. Tecnología: Empleados o contratistas que debido a su función realizan actividades de desarrollo, administración, soporte o mantenimiento de aplicaciones, infraestructura o plataformas.
- b. El acceso de las personas a las plataformas, aplicaciones y elementos de infraestructura TI se debe hacer a través de unos IDs a los cuales se les debe asociar unos roles que deben estar definidos en estas plataformas, aplicaciones y elementos de infraestructura TI.

4.1.1 Sobre los IDs

- a. Los ID son nombres de identificación necesarios para acceder a las plataformas, aplicaciones y elementos de infraestructura TI. Cada uno de ellos debe tener asignado una información de autenticación secreta. Los tipos de ID son: ID de usuario, ID compartido, ID de servicio y ID privilegiado.
- b. Los ID de usuarios son asignados a empleados, contratistas, practicantes o aprendices y permiten su identificación univoca en los sistemas y plataformas. Este es único e intransferible. En general los IDs de los usuarios deben ser responsabilidad de cada persona que lo solicita. Se deben establecer los controles necesarios por parte de las áreas pertinentes para lograr que, frente a la gestión de acceso, no existan personas con más de un

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

número de identificación ciudadana, ni números de identificación ciudadana con más de un ID de usuario.


En todo caso, el ID de usuario debe coincidir con el login asignado a las cuentas de usuario correspondientes en el Sistema de Directorio con el fin de poder tener un acceso integrado y general en todas las aplicaciones que así lo permitan. Con lo anterior, desde el mismo Sistema de Directorio debe definirse si las cuentas de usuario deben estar activas o inactivas. En el caso de las inactivas debe poder identificarse la razón de la inactividad, cómo mínimo por: vacaciones, sanción, licencia e incapacidad.

Para empleados es el área de Talento Humano quien establece los tipos de inactividad, según la situación pertinente a cada empleado, atendiendo a su alcance de conocimiento.

Para contratistas es el área de Seguridad Física, en general, o el área de Call Center, en particular, quienes establece los tipos de inactividad, según la situación pertinente a cada contratista, para lo cual deben asegurar el procedimiento necesario con los supervisores de contrato, quienes son lo que cuentan con el conocimiento de la situación laboral de estas personas.

En los casos donde se detecten o se evidencien prácticas con indicios de fraude o malas prácticas relacionadas con el uso indebido de los accesos, y toda vez que estas, afecten, lastimen, deterioren o corroan el ingreso de ETB, o en los casos donde dichas prácticas conlleven el favorecimiento a terceros, ya sea a través de pago de comisiones o de honorarios o valores que dependan de las cantidades, el área de Control Fraude cuenta con la potestad para requerir la inactivación preventiva de dichos usuarios y a su vez es la única área que tendrá la potestad para levantar esa inactivación. En todos los casos debe prevalecer la comunicación entre los Supervisores de Contrato con los contratistas en pro de evitar que las malas prácticas continúe y se conviertan en actividades comunes dentro de la operación. Para lo anterior el Líder Gestor de Acceso a Usuarios o quien haga sus veces gestionará esa inactivación haciendo uso de una tipología adicional para tal efecto. Las inactivaciones por cuanta de la tipología de fraude deben alimentar una base de datos custodiada por el área de Control Fraude de manera que la pueda poner en conocimiento del área de Seguridad Física para los asuntos pertinentes en cuanto a contratistas.

- c. Los ID compartidos son de nombres genéricos porque un solo ID está asociado a varias personas debido a actividades que requieren tal situación. Cuando sea requerido el uso de un ID compartido, éste se debe documentar y configurar con el mínimo de privilegios y definir su responsabilidad.
- d. Los ID de servicio son de nombres genéricos porque son requeridos para la interacción o integración entre las plataformas, aplicaciones y elementos de infraestructura TI. Un ID de servicio puede ser: (i) por defecto, inherente al sistema, (ii) creado automáticamente por el sistema para habilitación de


Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

servicios para su funcionamiento y, (iii) creado manualmente por un ID privilegiado. En cualquier caso, se debe asignar un responsable de este tipo de ID quien debe ser el administrador de la plataforma, aplicación y/o elemento de infraestructura TI. Todo ID de servicio creado de forma manual debería tener asignados los mínimos privilegios.

- e. Los ID privilegiados o comúnmente “superusuarios” son asignados a los administradores de las plataformas, aplicaciones y elementos de infraestructura TI debido a las características de su responsabilidad. Al igual que todos los ID, es importante resaltar que las actividades ejecutadas a través de ID privilegiados deben ser sujetas a seguimiento.
- f. Se debe asegurar que los derechos de acceso no estén activados sin que finalice el procedimiento de autorización de cualquier tipo de ID. Adicionalmente se debe mantener un registro centralizado del uso de los derechos de acceso otorgados a los diferentes ID para acceder a las plataformas, aplicaciones y elementos de infraestructura TI.


4.1.2 Sobre los roles

- a. La gestión de acceso a plataformas, aplicaciones y elementos de infraestructura TI debe estar basada en roles o perfiles con niveles de permisos claramente definidos. Un determinado conjunto de privilegios sobre una aplicación o plataforma en particular, que habilitan unas acciones específicas requeridas por los Procesos o por la Tecnología, constituye un rol de acceso.
- b. Con el fin de facilitar que la gestión de acceso a las plataformas, aplicaciones y elementos de infraestructura TI fluya más eficientemente, los propietarios de los activos de información deben delegar la responsabilidad de la autorización de acceso a unos autorizadores de rol, indicando para cada uno de ellos, sobre qué Procesos del mapa de procesos de ETB, se les concede tal facultad o sobre qué dominio o grupo funcional tecnológico. Para que no haya traumatismos en la operación, es necesario que los autorizadores de rol se aseguren de contar con las delegaciones correspondientes, desde el mismo momento en que son recibidos tanto los procesos como la tecnología bajo su cargo, según aplique, porque sin esta delegación no podrá autorizar ningún acceso.
- c. Los autorizadores de rol son definidos libremente por el propietario de los activos de información, considerando como criterio fundamental que el perfil de esas personas implique un conocimiento importante de las actividades que, sobre las plataformas, aplicaciones y elementos de infraestructura TI, harán los empleados, contratistas, practicantes o aprendices a quienes

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

autorizará los roles correspondientes y un conocimiento importante de los niveles de responsabilidad y autoridad que tienen esas personas frente a la gestión que van a realizar con esos roles. Así las cosas, los autorizadores de rol pueden ser, según aplique, líderes de equipos de trabajo en los procesos, supervisores de contrato, líderes funcionales, líderes de soporte de infraestructura TI, líderes de soporte de aplicaciones, etc.

- d. En general para la autorización de accesos requerida por los usuarios, es necesaria la aprobación de un solo autorizador de rol, salvo en los siguientes casos:
- En consideración a las particularidades establecidas por el Gobierno de Información de ETB, para el caso de los roles del Data Warehouse – DWH, es requerido un autorizador de rol adicional para las solicitudes realizadas por los procesos de la Organización, quien es la persona principal o suplente que funge como Líder Gestor de Consumo de ETB a quien se le delega esta responsabilidad por parte del Comité de Gobierno de Información de ETB.
 - Para los elementos de infraestructura de la tecnología que soporta los procesos de negocio, se requieren dos autorizadores de rol adicionales que son los líderes de soporte, tanto de la infraestructura TI, como de la aplicación, según corresponda. Y si se trata de autorizar un usuario con un rol especial (asociados a IDs privilegiados, compartidos o de servicio), también se requiere la aprobación del oficial de seguridad TI.
- e. La delegación realizada por el propietario de los activos de información debe documentarse de manera formal a través de un Acta de Rol (de la cual se dará mayor detalle en el numeral 5.1.2.g) el cual debe ser enviado, por el mismo propietario, a quien funge como Líder Gestor de Acceso a Usuarios o quien haga sus veces del área TI correspondiente. Teniendo en cuenta la excepción planteada en el literal anterior, la delegación para el Líder Gestor de Consumo o quien haga sus veces, en su calidad de autorizador adicional general de los roles del DWH, debe ser aprobada por el Comité de Gobierno de Información y enviada al señalado Líder Gestor de Acceso a Usuarios por quien se encarga de la secretaría técnica de este Comité.
- f. Particularmente para el área de tecnología que soporta los procesos de negocio, los roles en las aplicaciones pueden ser predefinidos o diseñados a medida, así:
- Los primeros corresponden a las aplicaciones propietarias en las cuales los roles están previamente definidos por el fabricante y por tanto son conocidos por el equipo de desarrollo de aplicaciones o por los equipos de soporte de infraestructura TI.
 - Los segundos corresponden a los desarrollos nuevos o cambios a aplicaciones existentes realizados por el equipo de desarrollo de aplicaciones, por requerimiento de las áreas de negocio, cuyos roles

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		


deben diseñarse teniendo en cuenta estos requerimientos y el concurso de la experiencia de los equipos de soporte de aplicaciones fundamentada en sus tareas de administración, de manera que se consideren aspectos tales como la segregación de funciones dentro de un mismo rol (en el numeral 5.1.4.b de esta política se describe una lista de chequeo guía para la segregación de funciones).

En cualquier caso, sea predefinido o diseñado, los equipos de infraestructura TI o el equipo de desarrollo de aplicaciones, según aplique, deben entregar las definiciones funcionales y técnicas de estos roles a los equipos de soporte de aplicaciones y al Líder Gestor de Acceso a Usuarios o quien haga sus veces.

- g. Considerando las delegaciones que hacen los propietarios de los activos a los autorizadores de rol y las definiciones funcionales y técnicas de los roles, el Líder Gestor de Acceso a Usuarios o quien haga sus veces debe coordinar lo pertinente para que los roles queden debidamente documentados en el formato Acta de Rol. En cada Acta de Rol pueden estar documentados uno o más roles, siempre que sean de un mismo proceso, de acuerdo con el mapa de procesos de ETB o de un mismo dominio o grupo funcional tecnológico. Cada Acta de Rol como mínimo debe contener la siguiente información:
- Código y nombre del proceso
 - Fecha del acta de rol
 - Nombre y firma del propietario de los activos a los cuales se va a acceder a través de los roles
 - Nombre de cada rol
 - Tipo de cada rol: Pueden ser roles corrientes o especiales. La diferencia consiste en que los roles especiales son más vulnerables en cuanto a seguridad de la información, como lo pueden ser los roles asociados a IDs privilegiados, IDs compartidos o IDs de servicio.
 - Aceptación del riesgo: Sólo para los roles asociados a IDs especiales. Aquí se deben identificar los riesgos a los cuales se expone la organización con la creación de un determinado rol, las acciones de definidas para mitigar la materialización de esos riesgos (si las hay) y la justificación para aceptar el riesgo residual.
 - Descripción funcional de cada rol
 - Descripción técnica de cada rol
 - Nombre y firma de los autorizadores de rol quien el propietario de los activos de información está delegando, mediante esta acta, la responsabilidad de autorizar los accesos.

La firma es el mecanismo de autenticación de la identidad de los propietarios de los activos y de los autorizadores de rol, no obstante, ese mecanismo de autenticación puede ser cambiado por algún otro dependiendo de los lineamientos que más se adecuen a la situación de ETB.

Estas Actas de Rol constituyen uno de los soportes documentales sin los cuales no se puede autorizar el acceso de los usuarios a las plataformas,


Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

aplicaciones y elementos de infraestructura TI y por tanto el Líder Gestor de Acceso a Usuarios o quien haga sus veces debe velar porque permanezcan actualizadas.

- h. El Líder Gestor de Acceso a Usuarios o quien haga sus veces debe velar porque la Mesa de Servicios, tenga para su tarea de validación, las Actas de Rol.

4.1.3 Sobre la solicitud de acceso

- a. Cuando un empleado, contratista, practicante o aprendiz requiera unos determinados privilegios de acceso a las plataformas, aplicaciones y elementos de infraestructura TI, deberá solicitarlo a la Mesa de Servicios de tecnología correspondiente a través del formato de solicitud de acceso que sea aplicable. El formato aplicable debe considerar como mínimo los siguientes aspectos:
- Los datos del usuario.
 - Las plataformas, aplicaciones y/o elementos de infraestructura TI a las cuales requiere acceder.
 - Los roles que requiere para cada una de las plataformas, aplicaciones y elementos de infraestructura TI.
 - Breve descripción funcional de los roles (se debe limitar esta descripción a una frase corta).
 - Se debe incluir la lista general de chequeo de segregación de funciones (en el numeral 5.1.4.b de esta política se describe esta lista) para que los autorizadores de rol puedan guiarse y así identificar si los roles que están autorizando presentan conflictos de segregación.
 - Casilla de identificación de conflictos de segregación de funciones.
 - Código y nombre del proceso del mapa de procesos de ETB o nombre del dominio o grupo funcional tecnológico para el cual se le hizo la delegación al autorizador de rol.
 - Nombre y firma de autorizador(es) de rol cuya facultad ha sido debidamente delegada (a través de acta de rol) por el propietario del activo de información (quien es el dueño del proceso a dónde se desempeña el usuario) o el Comité de Gobierno de Información (para el caso de DWH). En caso de que los usuarios sean contratistas, el autorizador de rol deberá ser el supervisor de contrato y en tal situación debe referirse el número del contrato.
 - Nombre y firma del propietario de los activos que van a ser accedidos por el rol. Solo será requerida la firma del propietario de los activos de información (o autorización del Comité de Gobierno de Información en el caso del DWH), si el rol a autorizar implica IDs privilegiados, compartidos o de servicio.
 - Nombre y firma del vicepresidente correspondiente. Sólo será requerida la firma del vicepresidente cuando se haya seleccionado la casilla que


Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

indica que con la autorización existe un conflicto de segregación de funciones. Se debe incluir una nota en la cual se resalte que, con su firma, el vicepresidente reconoce que fue informado de los riesgos que representa la autorización a un usuario de unos roles que implican conflictos de segregación de funciones, riesgo que deberá ser analizado y documentado por el autorizador de rol de acuerdo con uno de los puntos establecidos en 5.1.3.b

- La aceptación de responsabilidades frente al uso de ID o cuenta de usuario que se entregará mediante este formato. Estas responsabilidades deben ilustrarse de acuerdo con lo definido en las políticas de seguridad de la información.

Al igual que como sucede con el acta de rol, la firma es el mecanismo de autenticación de la identidad de los propietarios de los activos, los autorizadores de rol y vicepresidentes, no obstante, ese mecanismo de autenticación puede ser cambiado por algún otro dependiendo de los lineamientos que más se adecuen a la situación de ETB.

- b. Cuando el autorizador de rol está autorizando a través de su firma la generación de roles para los usuarios que están bajo su cargo, está aceptando lo siguiente:
- Que autoriza al área de tecnología que soporta los procesos o a la que soporta los servicios, según aplique, para que le genere al usuario los roles que solicita con base a su necesidad específica de uso y a los requisitos mínimos para sus funciones.
 - Que en caso de que, como consecuencia de tal solicitud el usuario quede con más de un rol en una o más las plataformas, aplicaciones y elementos de infraestructura TI, estos roles no tendrán conflictos de segregación de funciones de acuerdo con la lista de chequeo de segregación de funciones que se describe en el mismo formato.
 - Que realizó y documentó un análisis de riesgo, aprobado por el propietario de los activos de información, que le permitió tomar la decisión de autorizar que dos o más roles en una o más las plataformas, aplicaciones y elementos de infraestructura TI, para un mismo usuario, impliquen un conflicto en la segregación de funciones. En caso de tomar tal decisión deberá identificar esa situación marcando en el presente formato la casilla correspondiente para que quede constancia de que realizó tal autorización basada en la aceptación del riesgo.
 - Que está considerando que los privilegios que otorgará a través de los roles que está autorizando a los usuarios, corresponden con las competencias y con los niveles de responsabilidad y de autoridad de esos usuarios y por tanto debe considerar, también, la criticidad de los activos de información que van a acceder los usuarios, a través de esos roles, a las aplicaciones. La criticidad de los activos de información es identificada en las matrices de activos de información por proceso.

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

Es preciso destacar que para los roles del DWH que permiten consultar o modificar información detallada asociada a los activos de información cuya confidencialidad sea Restringida y Reservada, el autorizador de rol debe poder demostrar al Líder Gestor de Consumo o quien haga sus veces, que la persona que está autorizando no cuenta con puertos USB abiertos en el equipo de cómputo bajo su cargo. Adicionalmente y solo para los roles que permiten modificar en DWH, debe poderse evidenciar que a quien se autorice sea empleado directo de ETB. En caso de que el rol autorizador no pueda evidenciar alguno de los anteriores, debe justificarlo y contar con la firma del propietario de los activos de información en el formato correspondiente.

Para que el autorizador de rol tenga claro los alcances de su autorización es pertinente que estos ítems estén referidos en el formato en cuestión.


- c. Al recibir el formato, la Mesa de Servicios de tecnología correspondiente debe validar, como mínimo:
- Que el (los) autorizador(es) de rol cuente(n) con la debida delegación
 - Que los roles solicitados cuenten con su debida acta
 - Que, en caso de estar marcada la casilla de conflicto en la segregación de funciones, exista la firma del vicepresidente correspondiente.
 - En general, su correcto y completo diligenciamiento.

No cumplir con alguno de estos requisitos constituye causa de rechazo de la solicitud de acceso.

- d. Con el fin de mitigar posibles vulnerabilidades, los lineamientos aquí referidos frente a la solicitud de acceso son aplicables como mecanismo de formalización de los accesos que son creados en la etapa de desarrollo de aplicaciones, atendiendo lo dispuesto en las políticas de adquisición, mantenimiento y desarrollo, establecida en este mismo documento.

4.1.4 Sobre la segregación de accesos

- a. La segregación implica la restricción de tareas incompatibles que un mismo usuario pueda realizar en una plataforma, aplicación y elemento de infraestructura TI. Si llegare a ocurrir la señalada incompatibilidad, se estaría configurando un conflicto de segregación que facilitaría el incumplimiento de las políticas de seguridad de la información, la comisión de fraudes, la corrupción y en general el incumplimiento de la carta de valores de ETB. Si en alguna ocasión este conflicto se genera y por las características del


Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

negocio debe mantenerse, el conflicto deberá ser elevado como un nuevo riesgo a evaluar.

- b. Al momento de diseñar los roles y autorizar los accesos a las plataformas, aplicaciones y elementos de infraestructura TI, se deben considerar los siguientes aspectos:
- El acceso y modificación de activos debe tener autorización y detección.
 - Quien inicia un evento no debe ser el mismo que lo autoriza.
 - Quien realiza una requisición o solicitud no debe poder responderla.
 - Quien registra debe ser diferente a quien autoriza y diferente a quien aprueba.
 - Ninguna persona debe estar facultada para registrar, autorizar y conciliar una transacción.
 - Personas independientes deben realizar: aprobación, ejecución, registro y custodia.
 - Ninguna persona debe poder manejar todas las fases de una transacción.
 - Se deben segregar los siguientes roles: operadores, validadores, consultores y modificadores.
 - Un usuario no debe poder eliminar sus acciones, sin que un segundo o tercero intervengan a manera de control.
 - Un mismo usuario no debe poder registrar una orden de compra y liberarla
 - Quien define los accesos no debe ser el mismo que los otorgue
 - Se debe separar la solicitud de acceso, la autorización de acceso y la administración de acceso.
 - Los usuarios deben distinguir, dónde parten sus funciones y responsabilidades, y dónde comienzan las funciones de sus compañeros de grupo, área o proceso.


4.1.5 Sobre el seguimiento y control de accesos

- a. Los propietarios de los activos de información tienen la responsabilidad de velar porque las delegaciones a los autorizadores de rol se mantengan actualizadas y, por tanto, frente a cualquier cambio de autorizadores de rol, enviar inmediatamente al Líder Gestor de Acceso a Usuarios correspondiente o quien haga sus veces, las Actas de Rol debidamente actualizadas. Esta misma responsabilidad es aplicable para quien tiene la secretaría técnica del Comité de Gobierno de Información, respecto de la delegación del Líder Gestor de Acceso a Usuarios o quien haga sus veces, como autorizador de rol general de los roles del DWH.
- b. Particularmente para el área de tecnología que soporta los procesos de negocio, los grupos de infraestructura TI o el equipo de desarrollo de aplicaciones, según aplique, deben mantener actualizadas las definiciones funcionales y

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

técnicas de los roles a los equipos de soporte de aplicaciones y al Líder Gestor de Acceso a Usuarios o quien haga sus veces.

- c. El Líder Gestor de Acceso a Usuarios o quien haga sus veces tiene la responsabilidad de mantener actualizadas las Actas de Rol de las aplicaciones, plataformas y sistemas, conforme se van generando o actualizando las definiciones funcionales y técnicas de los roles y las delegaciones que los propietarios hacen a los autorizadores de rol.
- d. Los autorizadores de rol, sea líderes de equipos de trabajo en los procesos, supervisores de contrato, líderes funcionales, líderes de soporte de infraestructura TI, líderes de soporte de aplicaciones, etc., según aplique, deben gestionar inmediatamente con la Mesa de Servicios, la actualización de accesos frente a cambios de funciones, roles o responsabilidades de cara a los accesos a plataformas, aplicaciones y elementos de infraestructura TI. Sin perjuicio de lo anterior, ellos mismos deben revisar de manera periódica, los derechos de acceso de los usuarios y esta revisión se debería realizar a intervalos más frecuentes si los derechos de acceso cuentan con altos privilegios. En todo caso, aunque la responsabilidad es delegada a los autorizadores de rol, los propietarios de los activos deben hacer seguimiento a la ejecución de esta actividad.
- e. De la misma manera, el Líder Gestor de Acceso a Usuarios o quien haga sus veces debe informar periódicamente a los autorizadores de rol que aparezcan en las actas de rol (ya sean líderes de equipos de trabajo en los procesos, supervisores de contrato, líderes funcionales, líderes de soporte de infraestructura TI, líderes de soporte de aplicaciones, etc.), los usuarios activos junto con los roles asignados, con el fin de apoyar la revisión periódica que deben realizar.
- f. En el caso de los usuarios que se desvinculan de la organización, es responsabilidad del área de Talento Humano para los empleados de ETB y del área de Seguridad Física para los contratistas, la de informar, de acuerdo con los procesos definidos, al Líder Gestor de Acceso a Usuarios o quien haga sus veces para que se ejecute la debida cancelación del usuario pertinente en las plataformas, aplicaciones y elementos de infraestructura TI, incluyendo el acceso a ID compartidos. Respecto a los usuarios de los contratistas, y para cumplir con lo anterior, los supervisores de contratos pertinentes deben asegurar la gestión necesaria ante el área de Seguridad Física para informar el retiro de estas personas de los contratos que están supervisando. El área de Talento Humano, adicionalmente, deberá informar cuando tenga conocimiento de cualquier traslado de área o cambio de rol del personal de ETB para que así el Líder Gestor de Acceso a Usuarios o quien haga sus veces pueda gestionar lo necesario para ajustar los roles que estos


Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

usuarios tienen en las plataformas, aplicaciones y elementos de infraestructura TI.

- g. Los autorizadores de rol ya sean líderes de equipos de trabajo en los procesos, supervisores de contrato, líderes funcionales, líderes de soporte de infraestructura TI, líderes de soporte de aplicaciones, etc., según aplique, deben revisar de manera periódica, los privilegios autorizados a los usuarios que cuentan con más de un rol en una o más plataformas, aplicaciones y elementos de infraestructura TI, con el fin de verificar que no aparezcan conflictos de segregación de funciones y en caso de identificarlos, requerir los ajustes correspondientes a la Mesa de Servicios.
- h. De la misma manera, el Líder Gestor de Acceso a Usuarios o quien haga sus veces debe informar periódicamente a los autorizadores de rol que aparezcan en las actas de rol (ya sean líderes de equipos de trabajo en los procesos, supervisores de contrato, líderes funcionales, líderes de soporte de infraestructura TI, líderes de soporte de aplicaciones, etc.), los usuarios que cuentan con más de un rol en una o más plataformas, aplicaciones y elementos de infraestructura TI críticos, con el fin de apoyar la revisión periódica que deben realizar.

4.2 Administración de la información de autenticación secreta de los usuarios


- a. Se debe solicitar a los usuarios firmar una declaración en que mantengan la información de autenticación secreta de manera personal para los ID de usuario y que mantengan la información de autenticación secreta grupal para los ID compartidos.
- b. La información secreta de autenticación o contraseña debe cambiarse cada vez que un miembro de un grupo que gestiona un ID compartido cambia de rol, área o se retira de la empresa.
- 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.
- d. Se deben establecer mecanismos para verificar la identidad de un usuario antes de proporcionarle información de autenticación secreta nueva, de reemplazo o temporal.
- e. No se debe proporcionar información de autenticación secreta por ningún medio escrito sin cifrar.

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

- f. Se debe cambiar la información de autenticación secreta predeterminada del proveedor luego de la instalación de los sistemas o software.
- g. Se deben generar controles necesarios para la autenticación de los IDs de servicio creados manualmente que permiten el acceso automático a los sistemas de información y las plataformas de servicios para evitar que los sistemas sean vulnerables.
- h. Cuando se requiera un nivel alto de autenticación y verificación de identidad, lo cual sucede cuando la clasificación de la información es de confidencialidad reservada, se deben gestionar métodos alternativos o complementarios a las contraseñas. Definir la implementación de estos métodos dependerá de consideraciones estratégicas, financieras o de mercado, que tendrán que ser evaluadas en las instancias pertinentes

4.3 Responsabilidad de los usuarios frente a la información de autenticación secreta

- a. Los usuarios deben mantener la información de autenticación secreta como reservada asegurándose que no se divulgue a nadie, incluyendo a las personas con mayor autoridad. Toda transacción y actividad realizada sobre los sistemas de información de ETB con un ID de usuario, será responsabilidad del propietario de dicho ID.
- b. Las contraseñas o cualquier otro método de autenticación son de uso personal e intransferible. Todas las contraseñas deberán ser tratadas como datos críticos.
- c. Los usuarios no deben mantener registros de contraseñas en papel, en stickers, en archivos de software, en dispositivos de mano, ni en nada que se le parezca que no pueda ser cifrado, ni deben ser guardadas en línea usando las opciones de autocompletado, ni agentes de manejo de contraseñas que ofrecen el sistema operativo, bases de datos, aplicaciones o sistemas de información.
- d. Los usuarios son responsables de cambiar las contraseñas cuando exista alguna indicación de su posible compromiso.
- e. Adicional a las recomendaciones para definir contraseñas seguras que deberán socializarse, se deben implementar controles tecnológicos que aseguren unas limitaciones mínimas que mitiguen el riesgo de que personas no autorizadas consigan conocer, por medios automatizados o no, las contraseñas de acceso. Cuando los recursos informáticos tengan la

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		


posibilidad tecnológica de lograrlo, ya sea porque su autenticación se puede realizar a través del directorio activo o porque su autenticación local así lo permite, las limitaciones a aplicar deben ser:

- Estar compuesto por lo menos de 8 caracteres
- Un carácter no debe ser usado secuencialmente más de 2 veces.
- La contraseña se debe cambiar por lo menos cada 30 días
- La contraseña debe incluir por lo menos 2 caracteres numéricos y 2 caracteres alfabéticos.
- Contener caracteres alternados en mayúsculas y minúsculas.
- No se podrá reutilizar hasta 5 contraseñas ya empleadas anteriormente


Si alguna de las anteriores limitaciones no se puede ejecutar, ya sea porque no se cuenta con la posibilidad tecnológica o porque llegase a afectar la operación de algún proceso, se puede constituir en una excepción que debe ser documentada.

4.4 Control de acceso a los sistemas de información y plataformas de servicios

- a. Se deber verificar que las contraseñas de ID de sistema por defecto hayan sido modificadas cuando se establezca el inicio de entrada en operación de un sistema, plataforma o aplicación.
- b. No se debe mostrar identificadores del sistema o de la aplicación hasta que el proceso de inicio de sesión finalice correctamente.
- c. No se deben proporcionar mensajes de ayuda durante el procedimiento de inicio de sesión que pudieran facilitar el acceso a un usuario no autorizado.
- d. Se debe 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.
- e. Los sistemas y plataformas deben protegerse contra los intentos de inicio de sesión forzados y se deben registrar los intentos logrados y los fallidos.
- f. Al completar un inicio de sesión correcto se debe mostrar la fecha, hora y origen del último inicio de sesión.
- g. No se debe mostrar una contraseña que se ingresa.
- h. Para estaciones de trabajo, se debe mostrar una advertencia de aviso general que indique que solo deberían acceder usuarios autorizados.

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

- i. Se deben terminar las sesiones inactivas después de un periodo de inactividad.
- j. 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.
- k. Se debe permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación para permitir los errores de entrada.
- l. Se debe garantizar la selección de contraseñas de calidad en sintonía con las políticas específicas definidas en esa materia.
- m. Se debe garantizar que los usuarios cambien las contraseñas de sus IDs periódicamente según sea viable.
- n. Se debe garantizar que los sistemas, aplicaciones o plataformas no permitan el establecimiento de contraseñas utilizadas anteriormente.
- o. Se debe almacenar de manera segura la información de autenticación con algoritmos de cifrado o preferiblemente con función resumen, que sean reconocidos por la industria como idóneos en la actualidad.
- p. Todas las plataformas, aplicaciones y elementos de infraestructura TI deben integrarse con un sistema de directorio de manera que las credenciales de autenticación sean las mismas y se garantice la administración centralizada de accesos para mitigar riesgos de seguridad. Las excepciones deberán tratarse de acuerdo con el siguiente literal, pero en todo caso las plataformas, aplicaciones y elementos de infraestructura TI que se vayan a desarrollar o adquirir debe poder integrarse con el Sistema de Directorio.
- q. Si alguna de las anteriores definiciones no se puede implementar, ya sea porque no se cuenta con la posibilidad o capacidad tecnológica, o porque llegase a afectar la operación de algún proceso, se puede constituir en una excepción cuyos riesgos deben ser documentados, gestionados y aprobados por los dueños de procesos correspondientes.

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		


5 Correo electrónico

5.1 Sobre la asignación de cuentas de correo

- a. Todo empleado activo de ETB al momento de su ingreso tiene derecho a que se le asigne una cuenta individual de correo electrónico, para su desempeño laboral. Su derecho cesa con ocasión de su retiro definitivo de ETB. Cualquier otro individuo con vinculación indirecta que requiera una cuenta de correo electrónico, deberá seguir el procedimiento definido por la mesa de servicio de TI.
- b. La asignación de cuentas de correo electrónico de la empresa deberá ser autorizada y regulada en conformidad con los requisitos indicados en los lineamientos de la mesa de servicio TI
- c. Los propietarios de los activos pueden solicitar directamente cuentas de correo electrónico cuyo nombre no esté asociado a una persona individual sino a una función, grupo de trabajo o área. Estas cuentas tienen un objetivo definido durante un período determinado, luego del cual deberá ser solicitado por el propietario de los activos la respectiva desactivación.

5.2 Sobre el uso de las cuentas de correo individuales

- a. El contenido del correo electrónico no se deberá alterar sin el permiso del remitente. Si se altera el contenido para eliminar datos críticos, se deberá indicar claramente en el nuevo mensaje. Queda terminantemente prohibido alterar el contenido para cambiar la intención del autor. No olvidar que el incumplimiento de estas políticas puede ser susceptible de investigación disciplinaria
- b. Las direcciones electrónicas simuladas o falsificadas están terminantemente prohibidas.
- c. 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
- d. El contenido de un correo electrónico que documente una decisión, acción o transacción será considerado como un registro de la empresa y se deberá administrar y guardar de conformidad con la clasificación de activos de información asociados a ese contenido.

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

- e. 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.
- f. Las contraseñas de correo electrónico deben seguir los lineamientos de la información de autenticación secreta de usuarios en este mismo documento.


5.3 Sobre el uso de las cuentas de correo corporativas

El uso de las cuentas de correo electrónico cuyo nombre este asociado a una función, grupo de trabajo o área debe ser congruente con su temática, por lo que debe evitarse el envío de correos sobre temas o intereses diferentes al mismo. De esta manera está estrictamente prohibido enviar mensajes controversiales para generar respuestas. El propietario del activo del área solicitante, o quien él delegue, es responsable directo del contenido de los mensajes generados a través de esas cuentas.

5.4 Sobre el uso de cuentas personales, pública y/o gratuitas

Las cuentas de correo personales públicas y/o gratuitas como Yahoo, Hotmail, Outlook, Gmail, etc., no pueden garantizar que las comunicaciones electrónicas sean privadas y con acceso limitado solamente al destinatario (o a los destinatarios) previstos y que su contenido, incluidos los adjuntos, puede ser reenviado, interceptado, impreso y guardado por partes no autorizadas. A partir de lo anterior y teniendo en cuenta que el uso de estas cuentas no será restringido totalmente, es necesario atender las siguientes disposiciones:

- a. No se deben usar para hacer envíos de correo relacionados con asuntos de la empresa, salvo caso fortuito debidamente comprobado como lo puede ser una falla que inhabilite el correo corporativo de la organización, sólo si el asunto no da espera por necesidades del servicio o del negocio.
- b. No se deben reenviar a estas cuentas los mensajes que llegan al correo corporativo, a excepción de los que correspondan única y exclusivamente a información propia del funcionario y que requiera el reenvío. Los correos que hacen parte de la excepción son aquellos que contienen información de nómina, información tributaria, certificación laboral, certificaciones emitidas por la Gerencia de Talento Humano de ETB o certificaciones de formación académica personal.
- c. Los terceros, aliados, contratistas y socios de negocio no deben utilizar estas cuentas para gestión de información de ETB, sino que deben contar con

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		


dominios de correo debidamente constituidos y que identifiquen a su compañía o empresa.

5.5 Sobre los controles tecnológicos


- a. Cualquier correo enviado a múltiples usuarios con el propósito de hacer promociones comerciales o enviar información, sin que los usuarios hayan solicitado este servicio, es considerado como SPAM. Todos los correos SPAM y sus originadores podrán ser bloqueados automáticamente. Adicionalmente todo correo proveniente de esas cuentas podrá ser bloqueado, hasta que el interesado presente ante la cuenta mesadeservicioTI@etb.com.co justificación contraria al respecto. Una solicitud de bloquear una cuenta como SPAM tiene prelación sobre una de desbloquear la misma cuenta. Todo caso de conflicto en la clasificación de cuentas como SPAM será resuelto por el área de seguridad TI respectiva.
- b. El Administrador del correo electrónico no deberá revisar el contenido de las comunicaciones de un usuario individual por curiosidad personal o a petición de personas que no hayan tramitado la aprobación debida.
- c. El área de gestión de TIC pertinente debe cumplir con las tareas para el almacenamiento, respaldo y retención de correos electrónicos.

6 Instalación y uso de computadores portátiles y de escritorio, periféricos y medios de almacenamiento extraíbles

- a. El usuario que con ocasión de sus responsabilidades requiera que se habiliten los puertos USB y/o se le otorgue el permiso de ser administrador local de un equipo de cómputo bajo su cargo, deberá remitir debidamente diligenciado un formato a la Mesa de Servicios TI el cual deberá contemplar como mínimo los siguientes aspectos, no sin antes considerar que el privilegio de administrador no lo autoriza a instalar software y en concordancia con la política de Gobierno para la gestión de licenciamiento corporativo:
 - Nombre y firma del usuario al cual se le habilitarán o asignarán los privilegios. Con su firma el usuario está aceptando la responsabilidad por cualquier fuga o acceso no autorizado o fraudulento de la información que pueda suceder con ocasión del uso de puertos USB habilitados o cualquier baja de rendimiento del equipo, acceso de malware o incumplimiento de Ley sobre derechos de autor o instalación de software no autorizado que pueda ocurrir con ocasión de acciones ejecutadas por el privilegio de ser administrador local del equipo.
 - Serial y ubicación de la maquina al cual se le habilitará el servicio.

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		


- Tiempo para el cual se requiere que el servicio esté habilitado. En ningún caso podrá sobrepasar un año, tiempo luego del cual deberá ser suspendido el servicio. En caso de requerir que el servicio permanezca habilitado por más tiempo, deberá volver a diligenciar el formato correspondiente.
 - Justificación detallada o razón de negocio por la cual se requiere la habilitación del servicio.
 - Autorización del correspondiente propietario del activo de información quien es el dueño de proceso en el cual se desempeña el usuario. Con su firma el propietario del activo de información acepta y entiende los riesgos asociados a la fuga de información y uso inadecuado de recursos informáticos que conlleva la habilitación del servicio y, adicionalmente, reconoce que la persona cuya máquina se le está habilitando el servicio cuenta con las competencias y con los niveles de responsabilidad y de autoridad acorde con la criticidad de los activos de información que el usuario gestiona. Siempre es importante resaltar que la criticidad de los activos de información es identificada en las matrices de activos de información aprobadas por el mismo dueño de proceso.
- b. Con el fin de llevar un adecuado control de las máquinas a las cuales se les han habilitado el uso de puertos USB o la administración local por parte de algún usuario, deben tenerse los siguientes controles implementados:
- El equipo de seguridad informática correspondiente debe conservar un inventario, con actualización trimestral, dónde se identifique: (i) el tipo de permiso (USB o administración local), (ii) el usuario a cargo y si está activo o inactivo), (iii) la fecha de solicitud del permiso y si está vigente o no (no más de un año), (iv) Si tiene o no un formato de autorización en regla de acuerdo con lo definido en la presente política.
 - Se deben conservar los formatos de autorización de estos permisos ya sea en medio digital o físico con el fin de apoyar la actualización del mencionado inventario.
 - Se deben eliminar los permisos, previo aviso al usuario, en caso de que el formato de autorización haya perdido vigencia o no este en regla o el usuario esté inactivo.
 - El área correspondiente, debe realizar escaneos de seguridad a las maquinas que tengan estos permisos, con el doble de frecuencia que a los que se ejecutan en máquinas que no tienen estos permisos.
- c. En los discos de los computadores portátiles o de escritorio no deben reposar activos de información de criticidad restringida ni reservada. Para lo anterior la organización dispone de servidores de archivos con los controles de seguridad necesarios para su custodia y protección.
- d. En caso de usar algún medio de almacenamiento extraíble este debe ser verificado previamente por el software Antivirus.

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

- e. Con el fin de proteger la información y el acceso a la red de ETB, los trabajadores y contratistas deben conservar en condiciones de seguridad el equipo portátil asignado en donde quiera que este se encuentre, ya sea porque permanece atendido, está guardado en sitio seguro o este protegido mediante guaya de seguridad.
- f. Las áreas de TIC deben implementar controles con el fin evitar que los puertos lógicos y físicos que soporten los sistemas de información de las plataformas puedan ser usados por parte de personal no autorizado.
- g. 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.
- h. 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.
- i. 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.
- j. Cuando sea necesario almacenar o transportar en medios de almacenamiento extraíble, datos críticos o activos de información críticos, 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 otros controles se tienen: almacenamiento y transporte con las medidas medioambientales mínimas para su debida conservación, archivos guardados con contraseña o encriptados.

7 Dispositivos móviles


- a. Se debe adoptar medidas de soporte para gestionar los riesgos introducidos por el uso de dispositivos móviles.
- b. El acceso a la red de ETB a través de dispositivos móviles (teléfonos inteligentes, computadores portátiles, entre otros), bien sean de propiedad de ETB o de uso personal, deberá contar con controles de seguridad para mitigar el acceso no autorizado a la información de la organización.

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

- c. El computador portátil que contenga activos de información de confidencialidad valorada como reservada deberá contar con el cifrado de su disco duro.
- d. Está prohibida la captura de imágenes y videos a datos críticos o activos de información críticos.
- 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 de Seguridad Física con el fin de tomar las medidas respectivas y evitar accesos no autorizados a la información.

8 Usuarios de los sistemas de información y plataformas de servicios

- a. Los trabajadores y contratistas que son administradores y usuarios de los sistemas de información y las plataformas de servicios de ETB son responsables del buen uso de la información que tienen a su cargo, atendiendo estas políticas de seguridad y teniendo en cuenta el nivel de criticidad de los activos de información o los datos que allí se gestionen.
- b. 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 pertinente.
- c. Un tipo de sistema de información lo constituyen los portales que están bajo la administración de ETB y que son consultados por los grupos de interés internos y externos. Se deben identificar los roles responsables por la información publicada en estos portales. Los administradores de estos portales son los custodios de la información allí publicada y en tal sentido sólo deben publicar información de usuarios debidamente autorizados, para lo cual deben contar con un listado control de estos usuarios. Los dueños de los procesos que gestionan la información que se requiere publicar son los únicos responsables de autorizar ante los administradores de los portales, a los usuarios que podrán requerir una determinada publicación. Así mismo estos dueños de proceso son responsables de mantener vigente la información publicada de manera que deben informar a los administradores, a través de los usuarios autorizados, cualquier novedad de actualización o eliminación requerida.


Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

9 Criptografía

- a. Bajo consideraciones estratégicas, financieras o de mercado, que tendrán que ser evaluadas en las instancias pertinentes, se debe asegurar el uso adecuado y eficaz de cifrado para proteger la confidencialidad, la autenticidad y/o la integridad.
- b. Para la gestión de claves de cifrado, se deben desarrollar e implementar controles para el uso, protección y gestión del ciclo de vida de dichas claves de cifrado.


10 Seguridad física y ambiental

- a. Todo espacio físico donde resida la infraestructura TIC o la información física 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 datos críticos, 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

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

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, no considerando equipos de usuario interno, como portátiles y desktop, entre otros, 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 con activos de información críticos o con datos críticos 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.

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		


- 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 a activos de información críticos en el computador asignado, con el fin de evitar daño, hurto, modificación, eliminación o accesos no autorizados.

11 Seguridad en las operaciones

11.1 Respaldo de información

Las copias de respaldo de la información y los sistemas deben mantenerse y probarse regularmente para permitir la recuperación de datos o sistemas de manera que garanticen la integridad de la información en casos de emergencia y según sea requerido y autorizado, atendiendo a los siguientes lineamientos:


- a. Se deben realizar copias de respaldo, como mínimo, para los activos primarios de información con niveles de criticidad MEDIO y ALTO, activos primarios con niveles de criticidad ALTO y EXTREMO, aquellos definidos como críticos en el análisis de impacto en el negocio (BIA) y los acuerdos contractuales con los clientes.
- b. Los criterios para la configuración de las políticas específicas de respaldo y la periodicidad de las copias de respaldo dependerá de la valoración de disponibilidad de los activos de información inventariados en las matrices de activos correspondientes y de los puntos objetivos de recuperación (RPO) definidos en el análisis de impacto en el negocio (BIA), criterios que deberán ser avalados por los propietarios de los activos de información, atendiendo a la naturaleza de la información como lo son las consideraciones financieras, legales, regulatorias, operativas, de mercado y reputacionales.
- c. Se debe monitorear la ejecución de las copias de respaldo y atender las fallas de las copias programadas para garantizar su integridad.
- d. Se deben establecer criterios para los tiempos de retención de las copias de respaldo luego de lo cual se pueden eliminar, y deben estar alineadas con las definiciones establecidas en las tablas de retención documental (TRD), atendiendo a la naturaleza de los registros de información como lo son las consideraciones financieras, legales, regulatorias, operativas, de mercado y reputacionales.

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

- e. Se debe garantizar que el respaldo contenga las variaciones de la data través del tiempo.
- f. El lugar de dónde almacenan los respaldos debe tener controles que mitiguen violaciones a la confidencialidad, integridad y disponibilidad, por ejemplo, por fallas u obsolescencia y con un nivel adecuado de protección física y ambiental.
- g. Los arreglos de disco para almacenar las copias de respaldo deben permitir que se dé la cobertura en caso de falla de un disco. Se debe garantizar la disponibilidad en el diseño.
- h. Como mínimo los activos críticos, atendiendo a los criterios definidos para las matrices de activos de información, el BIA y los acuerdos contractuales con clientes, deben tener respaldo en un lugar remoto seguro y protegido.
- i. Los activos de información que están valorados con confidencialidad reservada deben contar con copias de seguridad cifradas.
- j. Se debe contar con controles para preservar la confidencialidad e integridad de las copias de respaldo en caso de que deban ser transportadas a una ubicación remota.
- k. Los procedimientos de copia de respaldo y de su restauración deben estar debidamente documentados.
- l. Se debe definir un plan de pruebas o verificación de copias de respaldo que incluya activos primarios de información con nivel de criticidad ALTA y activos de soporte de información con nivel de criticidad EXTREMO relacionados, atendiendo, como mínimo, los criterios definidos para el BIA y los acuerdos contractuales con clientes.
- m. Las pruebas o verificaciones que se realicen deben comprobar la capacidad de restaurar datos respaldados sin sobrescribir los medios de almacenamiento originales para evitar que se cause daños o pérdidas irreparables de datos. Adicionalmente deben considerar que se cumpla con los tiempos objetivos de recuperación (RTO) establecidos en el BIA en caso de que ello aplique.


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

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

necesarias para abordar el riesgo asociado. De acuerdo con 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 o por demanda cuando sean aplicables según el caso.
- c. Los escaneos planeados deben efectuarse sobre todos los sistemas de información prioritarios de acuerdo con 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 predefinido en los sistemas que se están escaneando.
- 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.

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

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. Las pruebas deberán realizarse a partir de un plan estructurado por cada área TIC el cual podrá incluir sistemas de información a los cuales se les haya identificado vulnerabilidades (ver 3.11.2) o aquellos prioritarios de acuerdo con 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.
- b. 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.
- c. Para cada sistema a probar se debe hacer un reconocimiento o exploración para la obtención de información, que podrá hacerse a través de herramientas o a través de datos que estén disponibles públicamente, con el fin de identificar lo que se va a hacer en la prueba.
- d. Se debe realizar un escaneo para determinar qué servicios y qué sistemas operativos corren en el sistema objetivo
- e. 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.
- f. 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.
- g. Se debe recolectar toda la evidencia posible con el fin de documentar debidamente el informe.
- h. 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


Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

- Análisis de resultados, incluyendo dirección IP y dominio del equipo probado, puertos TCP y UDP abiertos, descripción de los servicios, pruebas realizadas
- Recomendaciones

11.4 Uso de la red Interna e Internet

11.4.1 Red Interna

- a. El acceso a la red interna de ETB, será permitido para los funcionarios que lo requieran para el desarrollo de las funciones del cargo y necesidades del negocio, el equipo debe cumplir los requisitos de seguridad mínimos de conexión que incluye, antivirus instalado y actualizado, parches de seguridad al día y registro en el dominio.
- b. El acceso de terceros a la red interna de ETB se debe realizar a través de una red independiente con controles específicos de acceso, con el fin de proteger la infraestructura de la empresa.
- c. Al utilizar la red interna, los usuarios deben garantizar un uso responsable y seguro de los recursos sin sobrepasar controles, cumpliendo con los lineamientos de las políticas de seguridad de la información y ciberseguridad.
- d. Las conexiones entre servidores, aplicaciones y bases de datos se deben realizar a través de los canales autorizados, con el fin de garantizar la integridad y confidencialidad de los datos.
- e. El acceso a los diferentes segmentos de la red interna debe estar restringido con controles de acceso según corresponda, limitando únicamente a los funcionarios que lo requieran para el desarrollo de sus funciones.
- f. No se deben ejecutar actividades que puedan comprometer la infraestructura de la red interna incluyendo ataques cibernéticos, explotación de vulnerabilidades, pruebas de penetración o acciones similares que puedan vulnerar los activos, infraestructura, redes y/o servicios de ETB, cuando se requieran este tipo de pruebas, debe ser


Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

autorizado por los responsables de los activos, con el apoyo de ciberseguridad y deben ser efectuadas solo por personal calificado.

- g. El acceso remoto a la red interna debe realizarse a través de conexiones seguras y autenticadas como VPN y deben estar debidamente autorizadas y gestionadas.

11.4.2 Internet

- a. El acceso a Internet se encuentra autorizado para el desarrollo de las funciones de los empleados, de acuerdo con las necesidades del negocio y es controlado por ETB según el esquema del menor privilegio.
- b. Todas las conexiones desde y hacia Internet deben pasar a través del Sistema de Protección Corporativo y equipos de seguridad perimetral que correspondan. De acuerdo con lo anterior, no se debe hacer uso de conexiones directas a internet a través de módems u otros elementos, salvo aquellas autorizadas expresamente por un vicepresidente, como lo indica la directiva interna relacionada con la racionalización y consumo de servicios internos y con la justificación de negocio pertinente.
- c. Para todas las conexiones realizadas hacia Internet, es necesario que se evalúen las necesidades de la organización en cuanto a visitas a sitios web, de manera que se puedan definir unas categorías de navegación con el fin de implementar una gestión de acceso adecuada a esas necesidades y así desincentivar el uso de estas conexiones directas a internet.
- d. Todo tráfico que entre o salga de la red corporativa desde y hacia Internet debe ser revisado para buscar y eliminar código dañino tal como virus, gusanos, spyware, troyanos y cualquier software que atente contra la confidencialidad, integridad y disponibilidad de la información y los servicios tecnológicos de ETB. Los usuarios y propietarios que originan este tráfico asumen las consecuencias derivadas de las acciones que ETB emprenda para proteger su información y servicios.
- e. ETB se reserva el derecho de restringir la conectividad a páginas o servicios de Internet que considere dañinos para la infraestructura de comunicaciones o para la organización, lo que puede incluir (transmisión de audio o video, intercambio de archivos, sitios web maliciosos,


Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

propagación de mensajes no autorizados, etc.) dado su contenido, categoría y/o posible efecto perjudicial sobre la red.

- f. Queda prohibido toda publicación o intercambio de activos de información críticos o con datos críticos de la empresa a través de cualquier medio físico, magnético o electrónico hacia Internet o fuera de la red corporativa, sin el consentimiento y la respectiva autorización directa o delegada del propietario de la información y solo se debe realizar en función de las funciones del cargo cumpliendo los lineamientos establecidos para la protección de la información.
- g. El acceso a redes sociales se limita o restringe de acuerdo con los lineamientos establecidos en la Política Identidad pública – Redes sociales autorizadas por ETB, código 11-11.2-P-014, tomando como referencia la última versión disponible y publicada por ETB.


12 Transferencia de la información

- a. Se debe proteger la información transferida de la interceptación, la copia, la modificación, el ruteo incorrecto o su destrucción
- b. Cuando sea necesario comunicar de manera electrónica los activos de información valorados como de confidencialidad reservada deberán estar protegidos contra lectura y con el envío de claves de protección pertinentes a su destinatario por un canal diferente.
- c. Se prohíbe expresamente la transferencia 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.

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

13 Seguridad en la adquisición, desarrollo y mantenimiento de sistemas de información

- 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 activos críticos o con datos críticos deben contener los datos relevantes requeridos para el uso de acuerdo con el rol y se deberán enviar exclusivamente a los usuarios y/o terminales autorizadas.
- 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. Atendiendo a prioridades que deben ser documentadas, deben incluirse pruebas técnicas de seguridad y revisiones de seguridad de forma automatizada o manual que permitan identificar eventuales vulnerabilidades en el desarrollo.
- f. Los sistemas de procesamiento y almacenamiento de información de los sistemas operativos y aplicaciones deben contar con la última versión más estable emitida por el fabricante, con el fin de dar el aseguramiento adecuado. Si estos no pueden ser actualizados esta excepción deberá ser documentada.
- g. Si la información que está en producción es utilizada en los ambientes de desarrollo o prueba se deben aplicar controles de seguridad para evitar su fuga.
- h. 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.
- i. La generación de usuarios y privilegios de acceso durante la etapa de desarrollo debe considerar los lineamientos establecidos en la política de gestión de acceso, definida en este documento, para ambientes productivos.

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		


Con lo anterior ningún desarrollo puede pasar a producción sin que se haya realizado una depuración previa de usuarios creados, cuyo remanente debe ser justificado y oficializado a través de los formatos correspondientes. Las áreas que soportan las aplicaciones no deberán recibir a satisfacción estos desarrollos sin el cumplimiento previo de este requisito.

- j. Los usuarios de desarrollo no deben tener privilegios para poder acceder a los ambientes productivos.
- k. Debe supervisarse el desarrollo tercerizado de los sistemas y deben realizarse pruebas de funcionalidad de la seguridad
- l. 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.

14 Proveedores y contratistas

14.1 Relación con proveedores, contratistas y 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 con esa clasificación se debe establecer los tipos de acceso a la información que deberán tener los proveedores y si estos proveedores son críticos o no para la seguridad de la información
- b. 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.
- c. 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.
- d. Los Proveedores y Contratistas vinculados a ETB que tengan acceso a la información de la empresa, deben suscribir un documento firmado que contenga 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.


Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

- e. 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.
- f. 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.

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 propios 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 con los lineamientos de identificación y clasificación 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.

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

- f. Obligación del proveedor de establecer las contingencias necesarias para continuar con la gestión de información.
- 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. Implementar controles para que el personal contratado tenga los estudios de seguridad pertinentes a la clasificación 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.

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. Realizar auditorías de seguridad de la información a los proveedores críticos y hacer seguimiento a los problemas identificados.
- c. Validar junto con el proveedor los incidentes de seguridad de la información presentados.
- d. 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.

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

- e. Revisar que los cambios en los acuerdos contractuales en el servicio del proveedor realizados de manera unilateral o bilateral garanticen la continuidad de la adherencia de los requisitos de seguridad.

15 Incidentes de Seguridad de la información y Ciberseguridad

- a. Los empleados y contratistas vinculados a la empresa deben estar conscientes de los procedimientos y su importancia para reportar incidentes de seguridad.
- b. Los empleados, contratistas o terceros que utilicen los servicios de información de la empresa, deben reportar al área de Ciberseguridad y 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 y 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.
- d. El ciclo de vida incluyendo registro, categorización y documentación de los incidentes de ciberseguridad, debe gestionarse a través de la plataforma dispuesta por ETB para este propósito.
- e. Para el cierre del ticket asociado al incidente de ciberseguridad y de acuerdo con la tipología de este según su investigación, se debe documentar y asociar en alguno de los siguientes grupos de categorización:
- I. Abuso SPAM
 - II. Abuso/Ataque informático
 - III. Denegación de Servicio
 - IV. Malware
 - V. Fallas de escaneo o descarga de firmas
 - VI. Acceso no autorizado
 - VII. Cambio no autorizado
 - VIII. Phishing
 - IX. Contenido no bloqueado
- f. El registro de la información de los niveles 1,2 y 3 de la documentación del incidente en la plataforma de registro de incidentes, se debe realizar de acuerdo con lo descrito en el instructivo Incidentes o Eventos de seguridad (formato 05.1.5.-I-006) según la última versión disponible en ETB.


Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

16 Seguridad en la gestión 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 y servicios críticos.
 - Entender el impacto de las interrupciones o incidentes de seguridad en las actividades del negocio.
 - Formular y documentar planes 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 documentados deben ser probados y evaluados por lo menos una vez al año, para verificar su funcionamiento, de acuerdo con un plan establecido por las áreas responsables de los mismos.
- c. Los planes de continuidad del negocio deberán estar ubicados en un lugar seguro dentro de la empresa. Deberán ser de conocimiento de los empleados pertinentes a su ejecución y distribuidos según su inherencia a la estructura de la empresa.
- d. En general las políticas aquí establecidas deberán continuar siendo aplicables en caso de que un incidente de continuidad del negocio o una gestión de crisis esté en curso, salvo que por autorización de la dirección y atendiendo los intereses del negocio, sea necesario establecer excepciones.

17 Cumplimiento de los requisitos legales y contractuales

- a. Los trabajadores, contratistas y terceras partes deben velar por el cumplimiento de las políticas de seguridad de la información y deben cumplir con las disposiciones establecidas por la Legislación Colombiana vigente asociados a la de protección de datos personales y seguridad de la información.
- b. Todos los requisitos relevantes a nivel legislativo, estatutario, regulatorio y contractual, así como el enfoque de la organización para cumplir con tales requisitos debe estar explícitamente identificado, documentado y actualizado para la organización.
- c. Las áreas de gestión de seguridad de la información y/o las áreas de gestión regulatoria a partir de la identificación de requisitos de seguridad de la


Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

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 proteger los activos de información.

- d. Aquellos documentos que estén bajo lineamientos legales o regulatorios deberán ser resguardados bajo las medidas de seguridad adecuadas para garantizar su integridad.
- e. 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.
- f. Los activos de información y los datos críticos de la empresa deben estar adecuadamente protegidos por los propietarios o responsables contra su pérdida, destrucción, falsificación, acceso no autorizado y liberación o divulgación no autorizada de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio.
- g. Los sistemas de información deben ser revisados regularmente en cuanto a su cumplimiento frente a las políticas de seguridad de la información de la organización y estándares.


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 especial seguimiento.
- b. Deben existir controles para que sólo personal debidamente autorizado, 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 de que se tenga información personal en medios de almacenamiento

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		


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.
- g. Se pueden usar, transmitir o transferir datos personales para finalidades diferentes a las establecidas en las relaciones contractuales con los titulares o cuando medie una orden judicial o un mandato legal, sólo si se verifica que efectivamente el titular de la información lo autorizó expresamente. Para lograr lo anterior es necesario que los datos personales a tratar estén contenidos en bases de datos vigentes que sean suministradas por aquellas áreas que tiene la misión de realizar tal verificación, en atención a protocolos que se deben documentar.
- h. Queda prohibido el uso de las bases de datos personales de los proveedores o contratistas para fines comerciales a menos que se haya obtenido autorización previa, expresa e informada sobre esta finalidad, por parte de ellos.
- i. Siendo posible compartir información personal, sea porque los titulares de la información dieron autorización, o sea porque medie una razón legal, judicial o contractual, sólo se pueden circular al interior y fuera de ETB aquellos datos que sean estrictamente necesarios para los fines de su uso.

Código			Política			
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)			
Fecha de emisión						
29	08	2023				

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	Actualizaciones políticas de gestión de acceso y de proveedores.	10/04/2018
5.0	Actualizaciones generales de las políticas a partir de una revisión detallada entre el SGSI y TI teniendo en cuenta la situación actual de ETB. Actualización de política de protección de datos personales.	22/05/2020
6.0	Actualización administración IDs y conexiones seguras ente servidores, aplicaciones y bases de datos.	16/10/2020
7.0	Actualización de alcance, definiciones, numeral 5.1 administración de acceso a los usuarios, numeral 7 instalación y uso de portátiles, periféricos y medios de almacenamiento extraíbles	29/10/2021
8.0	Actualización de la política de gestión de acceso en cuanto a la integración con el sistema de directorio. Actualización de la política de adquisición, mantenimiento y desarrollo, incluyendo los lineamientos frente a la creación de usuarios en la etapa de desarrollo de aplicaciones y las pruebas técnicas de seguridad. Actualización de la política de Instalación y uso de computadores portátiles y de escritorio, periféricos y medios de almacenamiento extraíbles, incluyendo los lineamientos relativos a la gestión de la administración local de computadores portátiles y de escritorio.	27/05/2022
9.0	Actualización de la política de adquisición, mantenimiento y desarrollo, incluyendo el lineamiento que restringe el acceso de los	31/10/2022

Código			Política	
11-11.2-Pol-002-v.12			Seguridad de la Información (Específicas)	
Fecha de emisión				
29	08	2023		

	usuarios de desarrollo a los ambientes productivos.	
10	Actualización política de respaldo de información. Eliminación de las políticas de trabajo remoto y de derechos de autor y propiedad intelectual las cuales fueron definidas en documentos independientes.	09/02/2023
11	Actualización política de Instalación y uso de computadores portátiles y de escritorio, periféricos y medios de almacenamiento extraíbles acotando la responsabilidad respecto a la instalación de software cuando se soliciten privilegios de administrador.	23/06/2023
12	Actualización de las políticas 3 Gestión de activos, 5.4 Sobre el uso de cuentas personales, pública y/o gratuitas, 11.4 Uso de la red Interna e Internet y 15. Incidentes de seguridad de la información.	29/08/2023