<table>
<tr><td colspan="3">Código</td><td>POLÍTICA</td><td rowspan="4">  </td></tr>
<tr><td colspan="3">1 1-11.2-P-001-v.4</td><td rowspan="3">Política de
Seguridad de la Información y
Ciberseguridad</td></tr>
<tr><td colspan="3">Fecha de emisión</td></tr>
<tr><td>14</td><td>09</td><td>2022</td></tr>
</table>

Elaborado por:	**Revisado por:**	**Aprobado por:**
Líder de Seguridad de la Información.	Oficial de Seguridad de la Información.	Oficial de Seguridad de la Información.

Objetivo:

Establecer y regular los principios de confidencialidad, integridad, disponibilidad, compromiso y transparencia de ETB, guiada por los estándares y regulaciones nacionales e internacionales en la materia, que permitan y orienten las disposiciones generales y los principios rectores de la Seguridad de la Información y Ciberseguridad a las que hace referencia esta política y que resultan aplicables a toda la empresa, filiales y terceros.

Alcance y aplicabilidad:

La política de Seguridad de la Información y Ciberseguridad debe ser comunicada, entendida, aplicada y de obligatorio cumplimiento de la Alta Dirección, Vicepresidencias, Gerencias, Direcciones y en general los colaboradores vinculados, filiales, aliados, terceros y demás grupos de interés de ETB que tengan contacto con los activos de información, sistemas de información.

DEFINICIONES:

Activo de información: Algo de valor tangible o intangible que vale la pena proteger, incluidas las personas, la información, infraestructura de T.I, finanzas y reputación para ETB, con los activos corresponden a los objetos materiales o intangibles asociados con la información y que son requeridos para la operación de las actividades de los negocios.

Aliados: Cualquier ente o empresa que apoya, fortalece o respalda a otra compañía o genera algún tipo de beneficio.

Ciso: Es el miembro de la organización que se encarga de la Seguridad de la Información y Ciberseguridad dentro de la Compañía.

Ciberseguridad: La práctica de proteger y recuperar redes, dispositivos, programas y activos de información de cualquier tipo de ciberataque malicioso.

Comité: Es un Órgano Directivo que representa y defiende los intereses de la compañía**.**

Confidencialidad: Se refiere a la preservación de las restricciones o limitantes que La Empresa de Telecomunicaciones de Bogotá (ETB), sus entes reguladores y sus obligaciones con los clientes han fijado para autorizar el acceso y la divulgación, así como los medios para la protección de la intimidad y propiedad de la información.

Controles: Medios para administrar Políticas, procedimientos y actividades definidas para gestionar los riesgos y aumentar la probabilidad de alcanzar los objetivos y metas establecidos.

Cumplimiento: Adhesión a las políticas, planes, procedimientos, leyes, regulaciones, manuales, contratos y otros mecanismos que la compañía adopte para impartir directrices en desarrollo de su operación.

Dato: Es un término que se refiere a hechos, eventos, transacciones que han sido registrados, que pueden ser cuantitativos o cualitativos y son la entrada sin procesar de la cual se produce la información.

Disponibilidad: Asegurar el acceso oportuno y confiable del uso de la información de cada una de las unidades organizacionales de La Empresa de Telecomunicaciones (ETB) autorizadas.

Estándar: Es un requisito obligatorio, código de práctica o especificación aprobada por un organismo externo reconocido como la ISO, que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir y promover la implementación de las políticas de alto nivel en La Empresa de Telecomunicaciones de Bogotá (ETB).

Grupos de Interés: Son personas naturales, organizaciones o grupos que pueden estar vinculados o relacionados de manera directa o indirecta, se pueden ver afectados de manera significativa por las actividades, productos o servicios de la empresa, sus acciones o decisiones afectan o influyen en la capacidad de la organización para implementar con éxito sus estrategias y alcanzar los objetivos.

Input: Conjunto de datos que se introducen en un sistema, proceso, procedimiento o un programa informáticos.

Integridad: La protección contra la modificación no autorizada, exactitud o completitud de toda información que pertenezca a los negocios de La Empresa de Telecomunicaciones de Bogotá (ETB) y sus filiales**.**

IEC: Comisión Electrotécnica Internacional.

ISO: Organización de estándares Internacionales.

Output: son los productos o salidas resultantes del proceso o procedimiento**.**

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Procedimientos: Son las guías de ejecución de un proceso completo o de sus etapas. Deben incluir las descripciones de las actividades a realizar, así como los responsables de realizarlas, las evidencias o registros de su ejecución y la descripción del producto intermedio o final.

Procesos: Son las formas de organizar el trabajo dentro de la empresa. En general tienen una entrada (Input) y un producto o entregable (Output) que debe cumplir con unos requisitos de calidad y oportunidad. Para lograr estos objetivos del producto, generalmente se incluyen en las actividades de Control.

Seguridad de la Información: hace alusión a la protección de la información y los sistemas de información del acceso, la divulgación, la alteración y la modificación o destrucción no autorizados. La gestión de la seguridad de la información y Ciberseguridad se apoya en el cumplimiento de tres criterios de confidencialidad, integridad y disponibilidad.

Sistema de Información: Un sistema de información es un conjunto de datos, que interactúan entre sí con un fin común. En informática, los sistemas de información ayudan a administrar, recolectar, usar, recuperar, procesar, almacenar y distribuir información de gran valor e importancia para los procesos fundamentales y las particularidades de cada organización.

SGSI: Sistema de Gestión de Seguridad de la Información.

Terceros: Es cualquier persona natural o jurídica ajena a la organización pero que interactúa con ella, como lo es un cliente, proveedor, filiales, compañía, o ente gubernamental.

T.I: Tecnologías de la Información.

Transparencia: La cualidad de un gobierno, empresa, organización o persona natural, que tiene la obligación de actuar de manera visible, predecible y comprensible en la promoción de la participación y la rendición de cuentas sobre la divulgación de información, Políticas, normas, planes, procesos, procedimientos y acciones.

La Política de Seguridad de la Información y Ciberseguridad

Busca la disminución del impacto generado sobre sus activos de información e infraestructura de T.I, en particular a la de los servicios de Data Center, negocios especiales, datos, televisión, voz e Internet fijo y móvil; por los riesgos identificados de manera sistemática con el objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de las diferentes áreas, sedes, empresas, filiales, terceros, aliados, proveedores y demás grupos de interés.

Esta política reconoce la importancia de identificar y proteger los activos de información e infraestructura de T.I de la organización, evitando la destrucción, la divulgación, la modificación indebida o el uso no autorizado de cualquier información relacionada con sus clientes, colaboradores, precios, estrategia, datos personales, datos comerciales, gestión u otros conceptos relacionados con el manejo adecuado de la información en la entrega de los servicios; así como el comportamiento personal y profesional de los colaboradores, áreas, sedes empresas, filiales, terceros, aliados, proveedores y demás grupos de interés, sobre la información obtenida, generada o procesada por ETB.

Adicionalmente permitirá que las áreas trabajen bajo las mejores prácticas de Seguridad de la Información y Ciberseguridad de acuerdo con la normatividad y estándares internacionales que cumplan con los requisitos legales a los cuales este obligada a cumplir dentro ETB.

Lineamientos generales:

Esta política aplica para ETB, se basa en el desarrollo de las acciones o toma de decisiones alrededor del Sistema de Gestión de Seguridad de la Información (SGSI) y Ciberseguridad; estarán determinadas por las siguientes directrices:

- Prevalecerá sobre las políticas, normas, procesos y procedimientos de Seguridad de la Información y Ciberseguridad existentes a nivel de la Alta Dirección, Vicepresidencias, Gerencias, Direcciones, filiales, áreas, aliados, terceros, y líneas de negocio.

- Cumplir los requisitos legales, regulatorios y contractuales del negocio frente al manejo Seguro de la Información y Ciberseguridad.

- Deberá contar con el desarrollo conjunto y en equipo con las Vicepresidencias, Gerencias, Direcciones, filiales y áreas para garantizar el progreso de las diferentes disposiciones e infraestructura de datos, técnicas y parámetros de la Seguridad de la Información y Ciberseguridad.

- Se adoptara el modelo de Gobierno de Seguridad de la Información y Ciberseguridad de datos bajo la presente Política.

- El incumplimiento de las disposiciones establecidas en la presente Política de Seguridad de la Información y Ciberseguridad tendrá como resultado la aplicación de medidas, de acuerdo a la matriz de sanciones, conforme a la magnitud y característica del aspecto no cumplido.

- Estructurará de manera específica las políticas, normas, planes, procesos, procedimientos y acciones alienadas a los objetivos y controles de la norma ISO/IEC 27001:2013 que deben poseer las áreas para el desarrollo de sus actividades dentro de un marco adecuado de Seguridad de la Información y Ciberseguridad.

  Fortalecer el Sistema de Gestión de Seguridad de la información y Ciberseguridad bajo la norma ISO/IEC 27001:2013; aplicable bajo los

lineamientos del Modelo Integrado de Gestión Empresarial, la política del Sistema Integrado de Gestión de la organización y los acuerdos interinstitucionales. Incluyendo revisiones, pruebas, actualización y cambios significativos de forma periódica, buscando siempre la mejora continua.

- Definir la Seguridad de la Información y Ciberseguridad para los ambientes donde se procesan activos de información e infraestructura de T.I. áreas, sedes, empresas, filiales, terceros, aliados, proveedores y demás grupos de interés.

- Implementar los procedimientos de comunicación adecuados, según sea el caso con las áreas, sedes, empresas, filiales, terceros, aliados, proveedores y demás grupos de interés.

- Comunicar a todas las áreas, sedes, empresas, filiales, terceros, aliados, proveedores y demás grupos de interés, sobre sus responsabilidades en el Sistema de Gestión de Seguridad de la Información (SGSI) y Ciberseguridad por medio de actividades de concientización y capacitación.

- Fortalecer la cultura del Sistema de Gestión de Seguridad de la Información (SGSI) y Ciberseguridad a todas las áreas, sedes, empresas, filiales, terceros, aliados, proveedores y demás grupos de interés.

- Incluir todos los cambios que se realizan sobre los procesos informáticos que componen los sistemas de información, activos de información e infraestructura de T.I, de las Vicepresidencias, Gerencias, Direcciones, áreas, filiales y demás grupos de interés.

- Impartir las características de la Administración de la Seguridad Física que deben acompañar al ambiente informático (cámaras, controles de acceso y vigilancia, seguridad electrónica y biométrica, bitácoras, GPS, dataswift).

- Definir del marco de control que asegure la continuidad de los procesos informáticos.

- Disponer las pautas de seguridad en los dispositivos de comunicaciones, medios magnéticos, discos duros extraíbles de estado sólido y mecánico, memorias usb y demás dispositivos removibles donde se almacene información para todas las Vicepresidencias, Gerencias, Direcciones, áreas, filiales y demás grupos de interés.

- Mitigar el impacto de los riesgos operacionales debido al mal uso de los activos de información e infraestructura de T.I. Para todas las Vicepresidencias, Gerencias, Direcciones, áreas, filiales y demás grupos de interés.

- Disponer las pautas del manejo de la información, transmisión, confidencialidad, almacenamiento, intercambio, modificación, copias y borrado de la información.

- Implantar los parámetros de identidad y acceso de la información para las áreas, sedes, empresas, filiales, terceros, aliados, proveedores y demás grupos de interés.

- Establecer los parámetros del Sistema de Gestión de Seguridad de la Información (SGSI) y Ciberseguridad orientado al trabajo remoto para las Vicepresidencias, Gerencias, Direcciones, demás áreas, sedes, filiales, terceros, aliados, proveedores y grupos de interés.

Control de Cambios:

Versión	Descripción del Cambio	Fecha del Cambio
1.0	Creación documento inicial	17/07/2015
2.0	Actualización definiciones y lineamientos estratégicos e inclusión objetivos de seguridad de la información	06/06/2019
3.0	Actualización lineamientos estratégicos	22/05/2020
4.0	Actualización del objetivo, alcance, definiciones, lineamientos. Actualización del nombre de la Política, como seguridad de la Información y Ciberseguridad.	14/09/2022