Sistema de Gestión Integral

Política: SGSI Sistema de Gestión de Seguridad de la Información

Vicepresidencia de Tecnología

emtelco

Sede Aguacatala, Medellín / Calle 17A Sur # 48 - 35 / Código Postal: 050022 / Teléfono: 604 389 7000
Sede Olaya, Medellín / Calle 14 # 52A - 174 / Código Postal: 050024 / Teléfono: 604 389 7000
Sede I&R Olaya, Medellín / Calle 14 # 52A -198 / Código Postal: 050024 / Teléfono: 604 389 7000
Sede el Dorado, Bogotá / Calle 52A # 85A - 61, Piso 4 / Código Postal: 111071 / Teléfono: 601 486 3500
Sede Modelo, Barranquilla / Carrera 67 # 48 - 07 Edificio Puerto Digital / Código Postal: 080002 / Teléfono: 604 389 7000 Ext. 5580

Contenido

1. Introducción

La Política que ayuda en la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) para **EMTELCO S.A.S.** representan un compromiso ético y de responsabilidad adoptado por nuestra organización. Buscamos crear un entorno seguro para gestionar información propia, de clientes y de terceros, prescindiendo de su ubicación.

Hemos establecido esta Política para proporcionar directrices claves para el SGSI. El objetivo es adoptar una cultura de seguridad en todos los procesos de la entidad como parte de nuestra estrategia, velando que los datos estén protegidos de manera adecuada.

Proteger la información es una prioridad para **EMTELCO S.A.S**., y esto incluye los datos de nuestros colaboradores, el estado, clientes, comunidad, socios y proveedores. Este compromiso se realiza para cumplir con requisitos contractuales, operar nuestro negocio de manera efectiva y mantener la confianza depositada en nosotros por las partes interesadas.

El presente documento establece la Política de Seguridad de la Información de manera resumida y con una visión de alto nivel, reflejando el compromiso de la organización con la confidencialidad, integridad y disponibilidad de la información en el marco de su responsabilidad corporativa. Este documento está dirigido tanto al público interno como externo con fines informativos. Para detalles más específicos y operativos, se podrá consultar el **Manual del Sistema de Gestión de Seguridad de la Información (SGSI)**, el cual describe el cumplimiento de las directrices del Sistema de Gestión de Seguridad de la Información. Sin embargo, dicho manual es de uso exclusivo para el personal corporativo interno.

2. Objetivos

2.1. Objetivo General:

Determinar las Directrices generales para el Sistema de Gestión de Seguridad de la Información (SGSI) que maneja **EMTELCO S.A.S.** bien sea propia, en custodia o compartida con terceros, cumpla con los controles de seguridad implementados en la organización y alojada en cualquier sistema de información.

2.2. Objetivos Específicos:

- Identificar, analizar, evaluar y tratar los riesgos relacionados con la seguridad de la información para garantizar la confidencialidad, integridad y disponibilidad de los activos críticos de la organización.
- Garantizar que todos los procesos, controles y procedimientos de seguridad de la información cumplan con las normativas legales, estándares internacionales y políticas internas aplicables.
- Detectar, responder, mitigar y aprender de los incidentes de seguridad de la información de manera eficaz para minimizar su impacto y prevenir su recurrencia.
- Garantizar la continuidad operativa de los procesos críticos de la organización mediante la implementación de planes de continuidad y recuperación ante desastres alineados con la estrategia del negocio.
- Promover una cultura organizacional de seguridad de la información mediante la formación continua y la sensibilización de todos los empleados, contratistas y partes interesadas.

3. Alcance

Las Directrices para gestionar el Sistema de Gestión de Seguridad de la Información (SGSI) aplica a todos los empleados, clientes, contratistas, proveedores y entes externos de **EMTELCO S.A.S.** que acceden, de manera interna o externa, a cualquier activo de información de la organización, o que se encuentra bajo su responsabilidad, independiente de su ubicación.

Así mismo, las presentes Directrices aplican a la información en custodia de nuestros clientes, así como la creada, procesada, o utilizada en la Organización.

Las Directrices para gestionar el SGSI adoptará las buenas prácticas como referencia las normas, leyes y demás aplicables que se encuentran definidos en el normograma corporativo de **EMTELCO S.A.S.**

4. Roles y responsabilidades

EMTELCO S.A.S. establece el Comité de Seguridad de la Información para evaluar y aprobar las estrategias e iniciativas de control, con el fin de tomar decisiones que permitan minimizar la exposición de la organización a los riesgos asociados con seguridad de la información; ha definido roles específicos garantizando la madurez del sistema de gestión seguridad de la información a través de la creación del Comité de Seguridad. Todos los actores participantes deben conocer la Política actual. Aclaramos que las funciones del comité y demás mencionados en la Política se encuentran detallas a un nivel más bajo en el Manual de Seguridad de la Información en la Directriz 1: Gestión de la seguridad de la información, solo disponible para conocimiento y acceso interno del personal de **EMTELCO S.A.S.**

4.1. Comité de Seguridad de la Información:

El Comité de Seguridad de la Información de **EMTELCO S.A.S.** es un grupo interdisciplinario conformado por representantes de diferentes áreas y miembros de la organización como sigue:

- Presidencia.
- Vicepresidencia de Tecnología.
- Vicepresidencia de Operaciones y Desarrollo de Negocios.
- Gerencia de Ingeniería y Desarrollo.
- Gerencia de Tecnología.
- Gerencia de Seguridad de la Información y Continuidad de Negocio.

El Comité sesionará trimestralmente, con previa convocatoria desde la Gerencia de Seguridad de la Información y Continuidad del Negocio, contando con la disponibilidad de los integrantes, Sin embargo, cada sesión debe contar con la presencia de los miembros mencionados anteriormente. Sin limitarse a estos, la participación de otros integrantes se restringirá únicamente a quienes ocupen cargos de Vicepresidente o Director, y solo en aquellos temas en los que se considere conveniente su intervención.

5. Cumplimiento General de la Política

Los cumplimientos de la Política General del Sistema de Gestión de Seguridad de la Información (SGSI), Política de Uso de Software y Política de Protección de Datos Personales, son de carácter obligatorio. Todos y cada uno de los empleados de la organización, clientes y entes externos, deben entender su rol y asumir su responsabilidad respecto a los riesgos en el acceso, uso, manejo, administración y protección de los activos de información, además estarán sometidos a las acciones legales y/o disciplinarias que sean pertinentes.
El incumplimiento de las Políticas vigentes asociadas a la organización por parte de los empleados de la Compañía, además de las consecuencias legales, dará lugar a la imposición de la sanción o acciones disciplinarias correspondientes, de acuerdo con lo dispuesto en el contrato de trabajo, Convención Colectiva de Trabajo, Reglamento Interno de Trabajo y la reglamentación legal vigente.

6. Directrices para Gestionar el SGSI.

Estas Directrices entran en vigor a partir de su fecha de aprobación por el comité de seguridad de la información e integrada al Sistema de Gestión Integral (SGI) de **EMTELCO S.A.S.**

A continuación, se detallan los lineamientos para cumplir las Directrices del Sistema de Gestión de Seguridad de la Información (SGSI) de **EMTELCO S.A.S.**

6.1. Directriz 1: Gestión de Seguridad de la Información.

La organización debe implementar y mantener un área de Seguridad de la Información con responsabilidades claramente definidas; y asociadas a la adopción de las buenas prácticas de seguridad de las normas que se encuentran dentro del normograma corporativo de la compañía en el SGI); y aquellas que puedan surgir y que apliquen; permitiendo garantizar una compañía segura y de nuestros clientes, soportando la misión y objetivos estratégicos de **EMTELCO S.A.S.**

El área de Seguridad de la Información deberá ser integrada en los procesos de Gestión de Proyectos y en la planeación de los sistemas informáticos corporativos para contribuir al análisis y la identificación de riesgos que puedan comprometer la prestación del servicio; así mismo, como aportar en los controles que se pueden implementar para minimizar o erradicar el riesgo.

Esta Directriz de Seguridad de la Información debe ser comunicada y socializada con empleados y terceros para asegurar el correcto proceso del SGSI de **EMTELCO S.A.S.,** su revisión se realiza mínimo una vez al año o antes si lo amerite, con el fin de asegurar su conveniencia, adecuación, modificación, aplicación y eficacia. Todo cambio en la Política de Seguridad de la Información debe ser aprobado por la Presidencia, Vicepresidencia de Operaciones y Desarrollo de Negocios, Vicepresidencia de Tecnología, Vicepresidencia de Talento Humano, Vicepresidencia Administrativa y Financiera, Gerencia de Ingeniería y Desarrollo, Gerencia de Tecnología y Gerencia de Seguridad de la Información y Continuidad del Negocio de **EMTELCO S.A.S.**

Cualquier inquietud acerca de la aplicabilidad de esta política puede ser comunicada a la Gerencia de Seguridad de la Información y Continuidad del Negocio, a través del correo electrónico corporativo gruposeguridadinformatica@emtelco.com.co

El área de Seguridad de la Información de la compañía, ha designado el correo a continuación para reportar cualquier tipo de incidente de seguridad y/o ciberseguridad real NO operativo, donde se puedan tomar las acciones preventivas correspondientes:

seussocseginfo@experiencia.emtelco.com.co

Entendiendo como alcance de incidentes reales de seguridad de la información:

a) **Infección por malware:** Presencia de virus u otro software malicioso en cualquier activo de información de la organización.
b) **Amenazas a la infraestructura:** Identificación de posibles ataques o intentos de daño a la infraestructura corporativa.
c) **Divulgación o filtración de datos:** Exposición no autorizada de información de la organización, clientes o proveedores fuera de los entornos o aplicaciones aprobadas por el equipo de Tecnología.
d) **Acceso indebido:** Detección de accesos no autorizados a sistemas, aplicaciones u otros activos tecnológicos.
e) **Alteración de datos:** Modificación o alteración no autorizada de la información.
f) **Ataques por correo electrónico:** Intentos de phishing, suplantación de identidad, estafas, correos fraudulentos u otros ataques por email.
g) **Pérdida o robo de dispositivos:** Hurto, extravío o acceso no autorizado a dispositivos o estaciones de trabajo que contengan información de la organización.
h) **Evento de ciberseguridad:** Reporte de eventos como ataques de denegación de servicio (DoS) o la detección de vulnerabilidades.

6.2. Directriz 2: Administración del Riesgo en Seguridad de la Información.

La Organización desde la Vicepresidencia de Tecnología, Gerencia de Seguridad de la Información, Gerencia de Tecnología y Gerencia de Ingeniería y Desarrollo, deberán administrar las amenazas y vulnerabilidades de seguridad que estén asociados a los activos de información; garantizando los criterios básicos necesarios para la valoración y tratamiento del riesgo de seguridad en **EMTELCO S.A.S.** junto con el Oficial Profesional de Responsabilidad Social Empresarial.

Se deben realizar revisiones periódicas de vulnerabilidades por el área de Seguridad de la Información, apoyando en el cierre de cualquier riesgo o amenaza expuesta en un activo de información. Junto con un plan de trabajo entre las Vicepresidencia de Tecnología, Gerencia de Tecnología y Gerencia de Ingeniería y Desarrollo.

6.3. Directriz 3: Seguridad de la Información en los Procesos Asociados a Personas.

La Organización a través de la Vicepresidencia de Talento Humano, debe establecer prácticas formales para seleccionar, vincular, mantener, retirar y mantener comunicación con el talento humano, garantizando que las cláusulas de confidencialidad, políticas, estándares y lineamientos de seguridad de la información estén correctamente integradas en sus procesos.

EMTELCO S.A.S. por medio de las áreas de Comunicaciones, Gestión de Aprendizaje y Cultura y Cambio serán responsables de promover mecanismos de capacitación, relacionados con temas de seguridad de la información, compartidos desde la Gerencia de Seguridad de la Información. Estas capacitaciones y boletines de sensibilización tendrán como alcance a todo los empleados activos de la organización. Asimismo, en conjunto con el equipo de Formación en las plataformas corporativas, se deberá impartir un curso evaluable sobre seguridad de la información, con el objetivo de medir el nivel de conocimiento y cultura.

Todo empleado de la organización debe devolver los activos y accesos asignados para su función luego de que exista un cambio de área o terminación de contrato laboral. Este proceso debe ser definido por la Vicepresidencia de Talento Humano con el fin de notificar este tipo de cambios a las partes interesadas.

6.4. Directriz 4: Administración y Protección de Activos de Información:

La Organización desde la Vicepresidencia Administrativa y Financiera, Vicepresidencia de Tecnología, Gerencia Administrativo y Logístico, y Gerencia de Tecnología deberán garantizar que los activos de información reciban un apropiado nivel de acceso, protección, clasificación y tratamiento; mediante un inventario de activos que se encuentre en repositorio único y accesible por las personas estrictamente necesarias.

Todo activo de información debe ser utilizado únicamente con fines laborales, desde su creación, procesamiento, almacenamiento y retiro de la red de **EMTELCO S.A.S.** El buen uso, protección e integridad; debe ir respaldado mediante un acta de entrega al responsable del activo.

El uso de las herramientas instaladas en los equipos de trabajo, recursos compartidos, sitios web para compartir información, uso de móviles que entrega **EMTELCO S.A.S.** solamente es de uso exclusivo para su labor. El uso de herramientas o ajustes de configuración que puedan atentar contra la confidencialidad, integridad y/o disponibilidad en los activos asociados a su cargo; será de manera directa un incumplimiento a la Directriz y Política del Sistema de Gestión de Seguridad de la Información (SGSI), por lo que se tomaran las acciones correspondiente con el área de Relaciones Laborales y/o autoridades externas competentes.

Así mismo los responsables del proceso con el apoyo del área de Seguridad de la Información, deberán adoptar las buenas prácticas de configuración (hardening) en los activos de información, tomando como referencia los marcos de la CIS, NIST, etc.

6.5. Directriz 5: Control de Acceso Lógico:

La Organización por medio de la Vicepresidencia de Tecnología, Gerencia de Tecnología, Gerencia de Ingeniería y Desarrollo TIC deberá implementar controles que garanticen que solo el personal autorizado acceda a la información de acuerdo con sus responsabilidades. **EMTELCO S.A.S.** es el responsable de mantener la seguridad en el acceso, uso de recursos de red, privilegios, uso de contraseñas seguras, control de acceso a la red y autenticación de usuarios para conexión externas; estas mencionadas anteriormente facilitan a los empleados su correcta labor dentro de la organización.

Se debe seguir un procedimiento documentado para las contraseñas de carácter crítico y cuentas técnicas, las cuales deben cumplir con los lineamientos y ser auditadas desde el área de Seguridad de la Información. Es responsabilidad del funcionario cualquier acción realizada con su identificador de usuario de red sobre los sistemas de información y plataformas del negocio; debido a que las contraseñas o cualquier otro método utilizado para el proceso de identificación y autenticación de usuarios se considera información de carácter confidencial e intransferible.

Para las relaciones comerciales y contractuales con terceros (clientes, proveedores, etc.), **EMTELCO S.A.S.** desde la Vicepresidencia de Operaciones y Desarrollo de Negocios, Vicepresidencia de Tecnología, Direcciones de Operaciones, Gerencia de Tecnología, Gerencia de Ingeniería y Desarrollo, Gerencia de Seguridad de la Información, y los que aplique a nivel interno, se ha definido un proceso de responsabilidad compartida con respecto a la asignación de credenciales para usuarios, cuentas técnicas y/o servicios integrados sobre plataformas de propiedad o licenciadas por el tercero (clientes, proveedores, etc.). El responsable que corresponda, deberá notificar al tercero la necesidad de adoptar buenas prácticas haciendo rotación de credenciales, no superando los siguientes ANS para:

- Cuentas asociadas a usuarios, deben ser cambiadas en un plazo no mayor a 90 días.
- Cuentas técnicas o de servicios (APIs, webservices, etc.), deben ser cambiadas en un plazo no mayor a los 365 días.

6.6. Directriz 6: Gestión de Operaciones y Comunicaciones Tecnológicas:

La Organización desde la Gerencia de Tecnología junto con las Vicepresidencia de Tecnología, Gerencia de Seguridad de la Información y Continuidad del Negocio deberán incluir controles de seguridad en las operaciones de los activos de procesamiento de información, así como las comunicaciones en red de acuerdo con su nivel de criticidad con el fin de salvaguardar los pilares de confidencialidad, integridad y disponibilidad de la organización y sus clientes. El equipo de trabajo en las operaciones junto con el área de Seguridad de la Información, no deberán aceptar el uso de software no autorizado, obsoleto, sin licencia o con alto riesgo de ciberseguridad que pueda atentar con la confidencialidad, integridad y disponibilidad de la compañía; heredados en la prestación de servicio con clientes, aliados, proveedores o los que aplique.

6.7. Directriz 7: Cifrado de la Información:

La Organización a través de la Vicepresidencia de Tecnología, Gerencia de Seguridad de la Información, Gerencia de Ingeniería y Desarrollo, y Gerencia de Tecnología deberá usar mecanismos de cifrado y administración de claves criptográficas, adoptando las recomendaciones y buenas prácticas de los estándares de la industria; garantizando que la información sensible de la compañía tanto en tránsito y reposo se encuentre debidamente cifrada y protegida por cualquier medio de información. La compañía no debe permitir la implementación de estándares obsoletos que atente con la confidencialidad de los datos Se deberá exigir los protocolos adecuados a clientes, aliados, proveedores y los que aplique.

6.8. Directriz 8: Seguridad Física y Entorno:

La Organización desde la Vicepresidencia Administrativa y Financiera, y Gerencia de Administrativos y Logísticos deberán fijar controles y criterios para prevenir acceso no autorizado a los activos, edificios e instalaciones a través de la Política de Seguridad en Sedes; con el fin de proteger, resguardar la información ante amenazas mal intencionadas o naturales.

Es necesario que el personal de **EMTELCO S.A.S.** tenga un identificador de tipo físico, que permita el acceso a las oficinas, recintos e instalaciones para uso explícito de su labor. Dicho identificador es personal e intransferible y es obligatorio ser portado en un lugar visible del cuerpo.

Se debe establecer perímetros y sistemas que controlen las condiciones de seguridad física de acuerdo con el "Plan de emergencia y evacuación de **EMTELCO S.A.S.**", protegiendo al empleado contra daños, inundaciones, terremotos, explosión y otras formas de desastre natural o creada por el hombre, con el apoyo desde la Vicepresidencia de Talento Humano, Vicepresidencia de Tecnología, Gerencia de Seguridad y Salud en el Trabajo y Gerencia de Seguridad de la Información y de Continuidad del Negocio. Adicional, se debe tomar todas las medidas necesarias para el cumplimiento de los estándares, lineamientos y buenas prácticas asociadas a los requerimientos contractuales de nuestros clientes.

6.9. Directriz 9: Incidentes de Seguridad de la Información:

La Organización por medio de la Vicepresidencia de Tecnología, Gerencia de Seguridad de la Información y Gerencia de Tecnología deberán proveer una estrategia de alcance para: identificar, atender, responder y tomar medidas preventivas y correctivas; respondiendo de manera eficaz y eficiente a los incidentes de seguridad que afecten o pudieran afectar negativamente los activos de información de **EMTELCO S.A.S.**

Todos los empleados, visitantes y proveedores deben ser conscientes de reportar a través de un procedimiento formal cualquier tipo de incidente que pueda tener impacto en la confidencialidad, integridad y/o confidencialidad de los datos corporativos de tal forma que se puedan tomar acciones correctivas adecuadas. Así mismo, toda

persona interna o externa que realice una acción que atente con la prestación de los servicios o el buen nombre de **EMTELCO S.A.S.**, será sometida de manera directa a un proceso de descargo disciplinario con el área de Relaciones Laborales o autoridades judiciales externas correspondientes.

El área de Seguridad de la Información de la compañía, ha designado el correo a continuación para reportar cualquier tipo de incidente de seguridad y/o ciberseguridad real NO operativo, donde se puedan tomar las acciones preventivas correspondientes:
seussocseginfo@experiencia.emtelco.com.co

Entendiendo como alcance de incidentes reales de seguridad de la información:

a) **Infección por malware:** Presencia de virus u otro software malicioso en cualquier activo de información de la organización.
b) **Amenazas a la infraestructura:** Identificación de posibles ataques o intentos de daño a la infraestructura corporativa.
c) **Divulgación o filtración de datos:** Exposición no autorizada de información de la organización, clientes o proveedores fuera de los entornos o aplicaciones aprobadas por el equipo de Tecnología.
d) **Acceso indebido:** Detección de accesos no autorizados a sistemas, aplicaciones u otros activos tecnológicos.
e) **Alteración de datos:** Modificación o alteración no autorizada de la información.
f) **Ataques por correo electrónico:** Intentos de phishing, suplantación de identidad, estafas, correos fraudulentos u otros ataques por email.
g) **Pérdida o robo de dispositivos:** Hurto, extravío o acceso no autorizado a dispositivos o estaciones de trabajo que contengan información de la organización.
h) **Evento de ciberseguridad:** Reporte de eventos como ataques de denegación de servicio (DoS) o la detección de vulnerabilidades.

6.10. Directriz 10: Desarrollo Seguro y Mantenimiento de los Sistemas de Información:

La Organización designará como responsables a la Vicepresidencia de Tecnología, Vicepresidencia de Talento Humano, Dirección de Centro de Experiencia Marca y Producto, Dirección de Operaciones y Desarrollo de Negocios, Gerencia de Ingeniería y Desarrollo TIC y Gerencia de Gestión del Talento deben estar alineados a la Política de Uso de Software y Política de Protección de Datos Personales. El área de Seguridad de la Información debe velar que se ejecuten y adopten los lineamientos asociados al desarrollo seguro en las aplicaciones bajo demanda del negocio, bajo entornos de prueba, desarrollo y producción; con el fin de prevenir vulnerabilidades que puedan afectar el funcionamiento y/o protección de los datos alojados o en circulación por medio de la aplicación; así mismo como a la infraestructura que ejecuta la aplicación. Para esto, los responsables mencionados anteriormente deberán adoptar como guía las buenas prácticas soportado en OWASP, NIST, ISO, entre otros.

Así mismo, el proceso y adopción de buenas prácticas en el desarrollo seguro para las aplicaciones, por medio de los responsables que apliquen deberán vigilar el cumplimiento por terceros contratados para la integración o desarrollos con servicios para **EMTELCO S.A.S.**, minimizando riesgos por obsolescencia tecnológica. Así mismo, siguiendo las recomendaciones de la "Directriz 5: Control de Acceso Lógico".

6.11. Directriz 11: Seguridad de la Información Relaciones con Terceras Partes:

La Organización por medio de la Vicepresidencia de Tecnología, Vicepresidencia Administrativa y Financiera, y Gerencia de Compras implementará dentro de la estrategia, controles de seguridad en los acuerdos con terceras partes y conexión remota, donde estos serán evaluados periódicamente por el área de Seguridad de la

Información, en caso de un uso inadecuado por parte del proveedor y/o Tercero, todo acceso será retirado. La organización podrá capturar y guardar cualquier evidencia cuando se sospeche que se esté ejecutando un mal uso de los recursos, abuso, fraude u otro crimen que involucre los sistemas informáticos, acorde con las leyes aplicables, partiendo del hecho que los activos de información son un recurso de **EMTELCO S.A.S.;** así mismo se iniciarán las acciones legales correspondiente con el tercero por los daños ocasionados.

Los empleados responsables de la supervisión de cualquier contrato o acuerdo con terceros deben asegurar la divulgación de la Política del Sistema de Gestión de Seguridad de la Información (SGSI) a dichas partes y deben velar porque el acceso a la información por parte de los terceros se realice de manera segura, de acuerdo con los lineamientos establecido.

Todos los contratos o acuerdos de colaboración suscritos entre la Organización y cualquier tercero deben contener acuerdos de confidencialidad y responsabilidad, así como derechos de autor y propiedad intelectual acordes con los accesos requeridos a los recursos y activos de información de la compañía, siguiendo los lineamientos establecidos por la Gerencia de Tecnología. En estos contratos o acuerdos deben incluir las consecuencias por incumplimiento a los acuerdos pactados, así mismo, si el tercero contratado tiene otro tercero que le apoye en sus funciones, debe existir una relación comercial bajo un acuerdo contractual con cláusulas de confidencialidad.

6.12. Directriz 12: Dispositivos Móviles Corporativos:

La Organización desde la Vicepresidencia Administrativa y Financiera, y Vicepresidencia de Tecnología da la posibilidad a sus empleados de hacer uso de las capacidades de red que tiene la compañía para la conexión de sus dispositivos móviles corporativos (portátiles o tables para los que aplica), con el fin de facilitar y cubrir las necesidades laborales del día a día.

El propósito de esta Política es dictar los lineamientos para el acceso de los usuarios autorizados a los servicios de conectividad de la compañía usando sus dispositivos corporativos que se les fueron asignados. NO está autorizado, el uso de dispositivos móviles personales en las áreas de trabajo de la operación; así mismo, cualquier otro que pueda ser usado para extracción o filtración de información de la compañía, sin la debida autorización del área de Seguridad de la Información. Estas acciones, serán consideradas un incumplimiento a la Política del Sistema de Gestión de Seguridad de la Información (SGSI) y se hará el respectivo proceso con el área de Relaciones Laborales.

6.13. Directriz 13: Cumplimiento Corporativo Estándares y Certificaciones:

La Organización por medio de la Vicepresidencia de Tecnología, Dirección de Centro de Experiencia Marca y Producto, Gerencia de Aseguramiento y Gerencia de Seguridad de la Información, junto con las diferentes áreas de apoyo que correspondan dentro del proceso, deberán garantizar el cumplimiento de los estándares y normas, aplicables y definidos en el normograma corporativo por el equipo del Sistema de Gestión Integral (SGI) Incluyendo las certificaciones del sello de cumplimiento ISO/IEC 27001 y PCI-DSS..

6.14. Directriz 14: Continuidad del Negocio:

La Organización desde la Vicepresidencia de Tecnología y Gerencia de Continuidad del Negocio deberá desarrollar un plan de contingencia tecnológica, que permita restablecer los servicios de acuerdo con los ANS y porcentajes de recuperación en las operaciones establecidas con los clientes.

Desde la Vicepresidencia de Operaciones y Desarrollo de Negocios, Vicepresidencia de Tecnología, Direcciones de Operaciones y Gerencia de Continuidad del Negocio revisará y aprobará un proceso de continuidad de

negocio para recuperar los procesos críticos de la organización en el menor tiempo posible (RTO) (RPO) y mantenerse operativa. Para esto **EMTELCO S.A.S.** debe tener: un Análisis de riesgos de interrupción, Estrategias de recuperación de continuidad, planes de respuesta ante una crisis, material de sensibilización, informes de prueba, modelo de gobierno y una Política de Continuidad de Negocio.

Junto con el apoyo de Seguridad de la Información y las demás áreas que correspondan, se deben desarrollar escenarios de recuperación seguros que cuenten con los controles idóneos de seguridad y eviten una afectación mayor en lo correspondiente a disponibilidad, integridad y/ confidencialidad.

6.15. Directriz 15: Seguridad Trabajo en Casa:

Desde la Vicepresidencia de Tecnología, Vicepresidencia de Talento Humano, Gerencia de Relaciones Laborales y Gerencia de Seguridad de la Información se debe implementar, desarrollar, mantener y actualizar la estrategia segura que apoye la Política para el trabajo en casa entendiendo los riesgos inherentes y/o residuales que conlleva este escenario junto con el Oficial Profesional de Responsabilidad Social Empresarial. Adicionalmente se establecieron los trabajos seguros para este esquema con nuestros controles integrados a la normatividad vigente y la Circular Externa 024 del 21 de octubre de 2021 de la Superintendencia Financiera de Colombia.

6.16. Directriz 16: Inteligencia de Amenaza Corporativa:

La Organización desde la Vicepresidencia de Tecnología, Gerencia de Seguridad de la Información y casa matriz, implementará, mantendrá y actualizará una estrategia integral de inteligencia de amenazas para anticipar, identificar y mitigar proactivamente posibles riesgos cibernéticos. Esta iniciativa incluirá la recopilación y análisis continuo de información relacionada con amenazas potenciales, el monitoreo de la actividad en línea y la colaboración con fuentes de inteligencia externas. Además, se establecerán procedimientos robustos para la respuesta rápida ante incidentes, garantizando la adaptabilidad de nuestras defensas en un entorno cibernético en constante evolución.

7. Periodicidad de revisión.

La Política del Sistema de Gestión de Seguridad de la Información (SGSI) se revisará anualmente o antes frente a un cambio diferencial en la organización que afecte el alcance, cumplimiento y conformidad, de lo establecido de las directrices corporativas.

8. Control de cambios.

La presente Política del Sistema de Gestión de Seguridad de la Información (SGSI),rige a partir de la fecha de su publicación, sin embargo, **EMTELCO S.A.S.** se reserva el derecho de cambiar, modificar o eliminar, en su totalidad o parcialmente, y en cualquier momento y sin previo aviso, de forma unilateral. Todo cambio será publicado y notificado en el Sistema de Gestión Integral (SGI).

Control de Cambios									
Versión	Naturaleza del cambio	Elaboró		Revisó		Aprobó		Vigencia	
		Nombre	Cargo	Nombre	Cargo	Nombre	Cargo		
5	6.15 Periodicidad de revisión política de seguridad de la información. Se incluye la palabra Ciberseguridad en los objetivos generales y específicos.	Laura Velez	Jefe de seguridad de la información y continuidad de negocio	Leonardo Jaimes Juan F. Sanchez	Director Tecnología Gerente Infraestructura	Maritza Garzón	Gerente General	18/07/2020	2/08/2021
6	Cambio de nombre del documento de Política general de seguridad de la información por Políticas de gestión para la seguridad de la información. 6.15Política 15: Política de trabajo en casa.	Laura Velez	Gerente de seguridad de la información y continuidad de negocio	Leonardo Jaimes Juan F. Sanchez Carlos Lopez	Vicepresidente Tecnología Gerente Infraestructura Gerente I+D	Maritza Garzón	Presidencia	2/08/2021	16/08/2022
7	Objetivo específico alcance de migración	Laura María	Gerente de seguridad de la información y continuidad de negocio	Leonardo Jaimes Flor Neusa	Vicepresidente Tecnología Gerente I+D	Maritza Garzón	Presidencia	16/08/2022	10/10/2023
7.1	Revisión y ajuste de formato	Dilan Muñoz	Gerente de seguridad de la información y continuidad de negocio	Flor Neusa Duvan Hernandez	Gerente I+D Director de Servicios Tecnológicos.	Leonardo Jaimes Flor Neusa	Vicepresidente Tecnología Gerente I+D	20/10/2023	01/02/2024
8	Ajustes: Objetivos Específicos. Miembros del Comité de Seguridad. Políticas 1, 2, 5, 7, 10, 11, 13 y 14. Añadido: Política 16.	Dilan Muñoz	Gerente de Seguridad de la Información y Continuidad del Negocio	Leonardo Jaimes	Vicepresidente Tecnología	Maritza Garzón	Presidencia	02/02/2024	17/03/2025

9	Ajustes: Objetivos específicos. Actualización de cargos. Miembros del comité. Modificación de textos y contenido. Cambio de políticas a directrices.	Dilan Muñoz	Gerente de Seguridad de la Información y Continuidad del Negocio	Mario Montoya	Vicepresidente Tecnología	Juan D. Adarve	Presidencia	18/03/2025	A la fecha

9. Aprobación de la Política

El cuadro a continuación contiene la matriz de aprobación a la Política del Sistema de Gestión de Seguridad de la Información (SGSI).

RESPONSABLE	CARGO	FIRMA
Aprobador	Presidencia	
Consultado	Vicepresidente de Tecnología	
Informado	Vicepresidente de Talento Humano	
	Vicepresidente de Administrativa y Financiera	
	Gerente de Ingeniería y Desarrollo TIC	
	Gerente de Tecnología	
Responsable	Gerente de Seguridad de la Información y Continuidad del Negocio	