Sistema de Gestión Integral

# Política de Seguridad de la Información y Ciberseguridad

## 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 ..... 2
2. Objetivos ..... 2
2.1. Objetivo General: ..... 2
2.2. Objetivos Específicos: ..... 2
3. Alcance ..... 3
4. Roles y responsabilidades ..... 3
4.1. Comité de Seguridad/Ciberseguridad de la Información: ..... 3
5. Cumplimiento General de la Política ..... 4
6. Políticas para Gestionar la Seguridad y Ciberseguridad de la Información. ..... 4
6.1. Política 1: Gestión de Seguridad de la Información. ..... 4
6.2. Política 2: Administración del Riesgo en Seguridad de la Información. ..... 5
6.3. Política 3: Seguridad de la Información en los Procesos Asociados a Personas. ..... 5
6.4. Política 4: Administración y Protección de Activos de Información: ..... 5
6.5. Política 5: Control de Acceso Lógico: ..... 6
6.6. Política 6: Gestión de Operaciones y Comunicaciones: ..... 6
6.7. Política 7: Cifrado: ..... 6
6.8. Política 8: Seguridad Física y Entorno: ..... 6
6.9. Política 9: Incidentes de Seguridad de la Información: ..... 7
6.10. Política 10: Desarrollo Seguro y Mantenimiento de los Sistemas de Información: ..... 7
6.11. Política 11: Seguridad de la Información Relaciones con Terceras Partes: ..... 7
6.12. Política 12: Dispositivos Móviles Corporativos: ..... 8
6.13. Política 13: Cumplimiento Corporativo Estándares y Certificaciones: ..... 8
6.14. Política 14: Continuidad del Negocio: ..... 8
6.15. Política 15: Seguridad Trabajo en Casa: ..... 8
6.16. Política 16: Inteligencia de Amenaza Corporativa: ..... 9
7. Periodicidad de revisión. ..... 9
8. Control de cambios ..... 9

# 1. Introducción

Las Políticas para gestionar la seguridad de la información y ciberseguridad de **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 estas políticas para proporcionar directrices clave en la gestión de seguridad de la información y ciberseguridad. El objetivo es cultivar una cultura de seguridad en todos los procesos de la entidad como parte de nuestra estrategia, asegurando 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 todas estas partes.

# 2. Objetivos

A continuación, se detalla los siguientes objetivos:

## 2.1. Objetivo General:

Determinar las Políticas generales de Seguridad y Ciberseguridad para que la información 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:

- Preservar la confidencialidad, la integridad y la disponibilidad de la información de los IVRs transaccionales y los IVRs financieros sujetos a las normativas ISO 27001 y PCI-DSS.
- Reducir en un 13% respecto al año 2023 el número de incidentes de seguridad de la información/ciberseguridad en la Organización. Logrando esfuerzos en conjunto entre todas las áreas, fortaleciendo el sistema de seguridad de la información y creando ambientes más seguros.
- Asegurar la disponibilidad de los IVRs transaccionales y financieros en un 99,9%, alineándola con el alcance de nuestro sistema de gestión de seguridad de la información.
- Fortalecer la cultura de seguridad de la información y ciberseguridad a nivel general.
- Establecer un respaldo sólido para la administración de riesgos centrada en los activos, con el propósito de resguardar la información contra posibles amenazas.
- Realizar la planificación y acompañamiento a la organización para la migración segura a la nube, adoptando las mejores prácticas de ISO 27017 y ISO 27018, así como la regulación Circular Básica Jurídica (C.E. 029/14) con sus respectivas Circulares Externas 029/14 y 005/19 de la SFC (Superintendencia Financiera de Colombia).
- Establecer y mantener una gestión de identidades y accesos con terceros, garantizando un proceso seguro de asignación y rotación de credenciales.
- Diseñar y llevar a cabo simulacros de manera controlada con el propósito de evaluar la eficacia de los planes de respuesta y las plataformas de ciberseguridad. Ajustando y perfeccionar los protocolos correspondientes para garantizar la creación de entornos seguros en **EMTELCO S.A.S.**
- Desarrollar y aplicar protocolos exhaustivos de seguridad para fortalecer la colaboración con clientes, proveedores y otras entidades externas.

- Establecer las bases para el desarrollo, implementación, mantenimiento y cumplimiento de la Seguridad de la Información mediante un Sistema de Gestión que la integre en toda la organización.

## 3. Alcance

Las Políticas para gestionar la Seguridad de la Información y Ciberseguridad aplica a todos los empleados, clientes, 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 Políticas aplican a la información en custodia de nuestros clientes, así como la creada, procesada, o utilizada en la Organización.

Las Políticas para gestionar la seguridad y ciberseguridad tendrán como referencia las normas ISO 27001, PCI-DSS en sus versiones vigentes y aquellas que aporten para las buenas prácticas de la organización. Y los estándares ISO 27032, NIST sp800, sp1800, CIS y COBIT 5.

## 4. Roles y responsabilidades

**EMTELCO S.A.S.** establece el Comité de Seguridad/Ciberseguridad 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. Todos los actores participantes deben conocer dicha política. Aclaramos que las funciones del comité y demás mencionados en la política se encuentra en el Manual de Seguridad de la Información en la Política 1: Gestión de la seguridad de la información.

### 4.1. Comité de Seguridad/Ciberseguridad de la Información:

El Comité de Seguridad y Ciberseguridad 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 (Asistencia Necesaria).
- Vicepresidencia de Tecnología (Asistencia Necesaria).
- Vicepresidencia de Talento Humano. (Asistencia Necesaria).
- Vicepresidencia de Operaciones y Desarrollo de Negocios (Asistencia Necesaria).
- Vicepresidencia Administrativo y Financiero (Asistencia Necesaria).
- Vicepresidencia de Nuevos Negocios.
- Director Automatización y Ciencias de Datos.
- Dirección Unidad XP, Marca y Producto.
- Dirección Operaciones y Desarrollo de CX Bogotá.
- Dirección Operaciones y Desarrollo de CX Tigo.
- Dirección Operaciones y Desarrollo de CX Medellín.
- Dirección Operaciones y Desarrollo de CX Ventas.
- Dirección Operaciones y Desarrollo de CX Premisas.
- Gerencia de Ingeniería y Desarrollo (Asistencia Necesaria).

- Gerencia de Tecnología. (Asistencia Necesaria).
- Gerencia de Relaciones Laborales.
- Gerencia de Proyectos y Procesos.
- Gerencia de Seguridad de la Información y Continuidad de Negocio (Asistencia Necesaria).

El Comité sesionará cada vez que se requiera, previa convocatoria de algunos miembros, de acuerdo con la disponibilidad de los integrantes, sin embargo, cada sesión debe contar con la presencia de los miembros de "asistencia necesaria ". Podrán asistir otros funcionarios en las sesiones del grupo de seguridad de la información para participar en aquellos temas a tratar que se consideren convenientes para su intervención.

## 5. Cumplimiento General de la Política

Los cumplimientos de la Política General de Seguridad de la Información y Ciberseguridad, 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 leyes vigentes asociadas a la organización por parte de los empleados de la Compañía, además de las consecuencias legales, podría dar lugar a la imposición de la sanción correspondiente, de acuerdo con lo dispuesto en el contrato de trabajo, Convención Colectiva de Trabajo, Reglamento Interno de Trabajo y la reglamentación legal vigente.

## 6. Políticas para Gestionar la Seguridad y Ciberseguridad de la Información.

Estas políticas entran en vigor a partir de su fecha de aprobación por el comité de seguridad de la información e integradas a La política del sistema de gestión integral de **EMTELCO S.A.S.**

A continuación, se detallan los lineamientos para cumplir las políticas de seguridad y Ciberseguridad de la información de **EMTELCO S.A.S.**

### 6.1. Política 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 PCI-DSS, ISO 27001, ISO 27017, ISO 27018 y Circular Básica Jurídica (C.E. 029/14) con sus respectivas Circulares Externas que correspondan de la SFC (Superintendencia Financiera de Colombia); y aquellas que puedan surgir y que apliquen; permitiendo garantizar la seguridad de la información de la compañía y de nuestros clientes, soportando la misión y objetivos estratégicos de **EMTELCO S.A.S.**

Esta Política de Seguridad de la Información debe ser comunicada y socializada con empleados y terceros para asegurar la debida gestión de la seguridad de la información 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 y Ciberseguridad 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 de **EMTELCO S.A.S.**

Cualquier inquietud acerca de la aplicabilidad de está 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.

### 6.2. Política 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 de Cumplimiento.

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. Política 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 y retirar el talento humano. Considerando que las cláusulas de confidencialidad, políticas, estándares y lineamientos de seguridad de la Información sean asociados a 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 y ciberseguridad, compartidos desde la Gerencia de Seguridad de la Información. Estas capacitaciones y boletines de sensibilización tendrán como alcance a los empleados nuevos y antiguos de la organización.

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. Política 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 que se encuentre en repositorio único expuesto por la Vicepresidencia de Tecnología.

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 que comprometan a la seguridad en los activos asociados a su cargo se debe referir a un incumplimiento a “5. Cumplimiento general de la política”.

### 6.5. Política 5: Control de Acceso Lógico:

La Organización por medio de la Vicepresidencia de Tecnología y Gerencia de Tecnología 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 y Ciberseguridad para su administración. Es responsabilidad del funcionario cualquier acción que sea realizada con su identificador de usuario 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, y Direcciones de Operaciones 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. Las áreas mencionadas anteriormente, notificaran al tercero la necesidad por buenas prácticas de hacer la rotación de credenciales, no superando los siguientes ANS para:

- Cuentas asociadas por usuario, 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. Política 6: Gestión de Operaciones y Comunicaciones:

La Organización desde la Gerencia de Seguridad de la Información junto con las Vicepresidencia de Tecnología, Vicepresidencia de Operaciones y Desarrollo de Negocios, y Dirección de Centro de Inteligencia Digital DIX deberán incluir controles de seguridad en las operaciones de los activos de procesamiento de información, así como las comunicaciones de acuerdo con su nivel de criticidad con el fin de salvaguardar confidencialidad, integridad y disponibilidad de la información de la compañía y sus clientes.

### 6.7. Política 7: Cifrado:

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 de acuerdo con las necesidades y requerimiento que soliciten los clientes; garantizando que la información sensible de la compañía sea cifrada y debidamente protegida al momento de transmitirse por cualquier medio. Así mismo, la información en reposo debe contar con las buenas prácticas de cifrado, bajo aquellas solicitudes contractuales con clientes.

### 6.8. Política 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 siempre debe ser portado en un lugar visible.

Se debe establecer perímetros y sistemas que controlen las condiciones de seguridad física de acuerdo con el "Plan de emergencia y evacuación del **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 y Gerencia de Seguridad y Salud en el Trabajo. Adicional, se debe tomar todas las medidas necesarias para el cumplimiento de los estándares, lineamientos y buenas prácticas asociadas a los requerimientos explícitos de nuestros clientes.

### 6.9. Política 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 directrices 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 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 seguridad de los activos de información de tal forma que se puedan tomar acciones correctivas adecuadas; en caso de requerir sanciones referirse a "5. Cumplimiento general de la política".

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

Los desarrollos realizados por los proveedores o in house deben estar alineados a la Política de uso de software y Política de Protección de Datos Personales, desde la Vicepresidencia de Tecnología y Gerencia de Ingeniería y Desarrollo. El área de Seguridad de la Información debe velar que se ejecuten los lineamientos asociados al desarrollo seguro en las aplicaciones, aplicaciones web, entornos de pruebas en desarrollo y código seguro en 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. Para esto, la organización contara como guía la adopción de las buenas prácticas soportado en OWASP, NIST, ISO, CIS, entre otros.

Así mismo, el proceso y adopción de buenas prácticas en el desarrollo seguro de aplicaciones, por medio de la Gerencia de Ingeniería y Desarrollo deberá vigilar el cumplimiento por terceros para la integración con servicios con **EMTELCO S.A.S.**, minimizando riesgos por obsolescencia tecnológica. Para el proceso de credenciales brindadas por el tercero, seguir las recomendaciones de "Política 5: Control de Acceso Lógico".

### 6.11. Política 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 implemento 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 y se tomarán las medidas consignadas en "5. Cumplimiento de la política general de seguridad de la información". 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.**

Los empleados responsables de la supervisión de cualquier contrato o acuerdo con terceros deben asegurar la divulgación de las políticas y lineamientos de seguridad de la Información 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. Política 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 (celulares, Tablet, portátiles, entre otros), con el fin de facilitar y cubrir las necesidades labores 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.

### 6.13. Política 13: Cumplimiento Corporativo Estándares y Certificaciones:

La Organización por medio de la Vicepresidencia de Tecnología, Dirección de Centro de Inteligencia Digital DIX, 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 de la norma PCI-DSS e ISO 27001, con el objetivo de mantener la certificación vigente de acuerdo con la versión correspondiente en el mercado y alineado a la visión estratégica de la organización.

Así mismo, con la adopción a las recomendaciones de seguridad y ciberseguridad mencionadas por la SFC (Superintendencia Financiera de Colombia) en la Circular Básica Jurídica (C.E. 029/14), incluyendo las Circulares Externas que corresponden.

### 6.14. Política 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 revisara y aprobara 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.

### 6.15. Política 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 de Cumplimiento. 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. Política 16: Inteligencia de Amenaza Corporativa:

La Organización desde la Vicepresidencia de Tecnología, Gerencia de Seguridad de la Información y el grupo corporativo Millicom, 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 y el Manual de Seguridad de la Información y ciberseguridad se revisará anualmente o antes frente a un cambio diferencial en la organización que afecte el alcance, cumplimiento y conformidad de la norma ISO 27001 y/o PCI-DSS y frente al Sistema de gestión integral.

## 8. Control de cambios.

La presente Política para la gestión de seguridad de la información. Rige a partir de la fecha de su publicación, sin embargo, Emtelco 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<br>Flor Neusa | Vicepresidente Tecnología<br>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<br>Duvan Hernandez | Gerente I+D<br>Director de Servicios Tecnológicos. | Leonardo Jaimes<br>Flor Neusa | Vicepresidente Tecnología<br>Gerente I+D | 20/10/2023 | 01/02/2024 |
| 8 | Ajustes:<br>Objetivos Específicos.<br>Miembros del Comité de Seguridad.<br>Políticas 1, 2, 5, 7, 10, 11, 13 y 14.<br><br>Añadido:<br>Política 16. | Dilan Muñoz | Gerente de Seguridad de la Información y Continuidad del Negocio | Leonardo Jaimes | Vicepresidente Tecnología | Maritza Garzón | Presidencia | 02/02/2024 | A la fecha |

| Aprobado por | Cargo | Firma |
|---|---|---|
| Leonardo Jaimes Gamboa | Vicepresidente de Tecnología | |
| Maritza Garzón Vargas | Presidencia | |
| **Revisado por** | **Cargo** | **Firma** |
| Flor Neusa | Gerente de Ingeniería y Desarrollo | |
| Duván Hernandez | Gerente de Tecnología | |

| | | |
|---|---|---|
| Juan D. Adarve Vergara | Vicepresidente de Operaciones y Desarrollo de Negocios |  |
| Juan E. Jaramillo Toro | Vicepresidente de Talento Humano |  |
| Carlos M. Arango Franco | Vicepresidencia Administrativa y Financiera |  |
| **Elaborado por** | **Cargo** | **Firma** |
| Dilan Muñoz | Gerente de Seguridad de la Información y Continuidad del Negocio |  |