Política para gestionar la Seguridad y Ciberseguridad de la información.

Vicepresidencia de Tecnología

Contenido

Introducción

Las Políticas para gestionar la seguridad y ciberseguridad de la información de **EMTELCO S.A.S** son una declaración de la conducta ética y responsable adoptada por la Organización, con el fin de proveer un ambiente seguro en el manejo de la información propia, de clientes y de terceras personas sin importar donde se encuentra alojada.

EMTELCO S.A.S. ha establecido las presentes Políticas, en donde se definen los lineamientos principales para el establecimiento de la gestión de ciberseguridad y seguridad de la Información, con el fin de establecer una cultura de seguridad en todos los procesos de la entidad, ya que, esta debe siempre estar protegida en forma adecuada.

Es prioridad para **EMTELCO S.A.S.** proteger la información que nuestros colaboradores, estado, clientes, comunidad, socios, proveedores; para el cumplimiento de los requisitos contractuales, operación del negocio y la confianza depositada por ellos en nosotros

1. Objetivos

A continuación, se detalla los siguientes objetivos:

1.1. 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.

1.2. Objetivos Específicos

- Preservar la confidencialidad, la integridad y la disponibilidad de la información de los IVR transaccionales de pago con tarjeta de crédito y los IVR financieros que se encuentren bajo la norma ISO 27001 y PCI DSS 3.2.
- Reducir en la Organización en un 30% con respecto al año 2021 el número de incidentes de seguridad de la información/Ciberseguridad; estableciendo esfuerzos en conjunto entre todas las áreas para fortalecer el sistema de seguridad de la Información generando ambientes más seguros
- Garantizar la disponibilidad del IVR transaccionales de pago con tarjeta de crédito y los IVR financieros de acuerdo con el alcance de nuestro sistema de gestión de seguridad de la Información, cuando sea requerido y utilizado para gestionar pasarelas de pago.
- Fundamentar el desarrollo, implantación, mantenimiento y cumplimiento de la Seguridad de la información por medio de un Sistema de Gestión que la despliegue en la organización.
- Fundamentar la gestión de riesgos en los activos para la protección de la información frente a amenazas.
- Definir un plan de educación de Ciberseguridad de la información y cultura para la protección de la información.

- Realizar escenarios ágiles y seguros para Emtelco S.A.S con ANS óptimos para anticipar, resistir y recuperarse frente a condiciones adversas.
- Realizar la planificación y acompañamiento a la organización para la migración a la nube de manera segura mediante las buenas prácticas de ISO 27017 y 27018.

2. Alcance

Las Políticas para gestionar la Seguridad y ciberseguridad de la información aplica a todos los empleados, clientes, proveedores y entes externos de **EMTELCO S.A.S** que acceden, ya sea interna o externamente, a cualquier activo de información de la organización, o que lo tienen bajo su responsabilidad, independiente de su ubicación.

Así mismo, la presente 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 20071, PCI DSS en sus versiones vigentes y aquellas que aporten para las buenas prácticas de la organización.

3. 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.

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 **EMTELCO S.A.S.** como sigue:

- Presidente (Asistencia Necesaria)
- Vicepresidencia de Tecnología (Asistencia Necesaria)
- Vicepresidencia de Talento Humano. (Asistencia Necesaria)
- Vicepresidencia de Operaciones y Desarrollo de Negocios (Asistencia Necesaria)
- Vicepresidencia Estrategia y Transformación
- Vicepresidencia Administrativo y Financiero.
- Vicepresidencia de Nuevos Negocios.
- Vicepresidencia Experiencia al Cliente.
- Director Automatización y Ciencias de Datos.
- Dirección Dix

- Vicepresidente de Operaciones y Desarrollo de Negocios (Asistencia Necesaria)
- Dirección Operaciones y Desarrollo de Negocios Bogotá.
- Dirección Operaciones y Desarrollo de Negocios Tigo.
- Dirección Operaciones y Desarrollo de Negocios Medellín.
- Dirección Operaciones y Desarrollo de Negocios – Venta por resultados.
- Dirección Operaciones y Desarrollo de Negocios – I&R
- Gerencia de Ingeniería y Desarrollo.
- Gerencia de Infraestructura Tecnológica. (Asistencia Necesaria)
- Gerencia de Relaciones Laborales.
- Dirección de Servicios Tecnológicos y Digitales (Asistencia Necesaria)
- 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.

4. Cumplimiento general de la política

Los cumplimientos de la Política General de Seguridad de la Información, 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 y el numeral numero 5

5. 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

5.1. Políticas para la gestión de seguridad de la información.

La organización debe implementar y mantener un área de seguridad informática con responsabilidades claramente definidas y asociadas a las buenas prácticas de seguridad de las normas PCI-DSS, ISO 27001, buenas prácticas de la norma ISO 27017 y 27018 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 cuando 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 Gerencia General 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 de negocio a través del correo electrónico GrupoSeguridadInformatica@emtelco.com.co

5.2 Política 2: Administración del Riesgo en seguridad de la información.

La Organización debe 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**

Se deben realizar revisiones periódicas de vulnerabilidades por el área de seguridad informática, apoyando en el cierre de cualquier riesgo o amenaza expuesta en un activo de información.

5.3 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 es responsable de promover mecanismos de capacitación relacionados con los temas del área de seguridad informática. Estas capacitaciones y boletines de sensibilización son entregados a la Vicepresidencia De Talento Humano y Comunicaciones; y en conjunto se capacitará 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.

5.4 Política 4: Administración y protección de activos de información

La organización debe 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 "**4. Cumplimiento general de la política"**

5.5 Política 5: Control de acceso lógico

La organización debe 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 a su correcta labor dentro de la organización.

Se debe seguir procedimiento documentado para las contraseñas de carácter crítico y cuentas técnicas, las cuales deben cumplir con los lineamientos definidos por el área de seguridad informática 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.

5.6 Política 6: Gestión de operaciones y comunicaciones.

La organización debe 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.

5.7 Política 7: Cifrado y criptografía.

EMTELCO S.A.S a través de esta política debe 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.

5.8 Política 8: Seguridad Física y entorno.

La organización debe 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. 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.

5.9 Política 9: Incidentes de seguridad de la información

La organización debe 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 "**4. Cumplimiento general de la política".**

5.10 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. El área de Seguridad Informática 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 inyección de código, desbordamiento de buffer, almacenamiento de cifrado inseguro, comunicación insegura, vulnerabilidades críticas expuestas, Cross-site scripting (XSS), cross-site request forgery (CSRF), control de acceso inapropiado, entre otros.

5.11 Política 11: Seguridad de la información relaciones terceras partes y proveedores.

EMTELCO S.A.S debe incluir controles de seguridad de la información en los acuerdos con terceras partes y conexión remota, los cuales serán evaluados periódicamente por el área de seguridad informática, en caso de un uso inadecuado por parte del proveedor, todo acceso

será retirado y se tomarán las medidas consignadas en "4. Cumplimiento de la política generalde seguridad de la información". **EMTELCO S.A.S.** podrá capturar y guardar cualquier evidenciacuando se sospeche que se esté llevando a cabo 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 Vicepresidencia de Tecnología. En estos contratos o acuerdos se 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, se debe firmar un acuerdo de confidencialidad adicional.

5.12 Política 12: Política de dispositivos Móviles

Emtelco S.A.S, 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, 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

5.13 Política 13: Mantenimiento PCI DSS Emtelco S.A.S.

EMTELCO S.A.S, a través del área de seguridad informática debe garantizar el cumplimiento de los estándares de la norma PCI DSS, con el objetivo de mantener la certificación de acuerdo con la versión que se encuentre vigente en el mercado y alineado a la visión estratégica.

5.14 Política 14: Continuidad de negocio

Emtelco S.A.S debe desarrollar un plan de contingencia tecnológica, que permita restablecer los servicios de acuerdo con los ANS, porcentajes de operación establecidos con los clientes.

La organización debe establecer 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 debe tener: un Análisis de riesgos de interrupción, Estrategias de recuperación de continuidad, planes de respuesta ante un evento o catástrofe, material de sensibilización, Informes de prueba, Modelo de Gobierno y una política de continuidad de negocio.

5.15 Política 15: Política para el trabajo incluyendo entornos seguros Emtelco S.A.S

Desde el sistema de gestión de seguridad de la información, se debe implementar, desarrollar y mantener la estrategia segura que apoye la Política para el teletrabajo entendiendo los riesgos inherentes y/o residuales que conlleva este escenario. 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 Periodicidad de revisión

La política y el manual de seguridad de la información se revisará anualmente o si existe un cambio diferencial en la organización que afecte el alcance, cumplimiento y conformidad de la norma ISO 27001y frente al Sistema de gestión integral.

7 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		
1	Política seguridad de la información Versión 1.0 - Creación de la primera versión de la política de seguridad de la información.	Laura María Vélez Carvajal	Coordinadora - Seguridad informática	Juan David Carrasquilla	Director de Tecnología	Maritza Garzón Vargas	Gerente General	22/06/2017	24/08/20188
2	Ítem #5. Leyes colombianas para el cumplimiento de la política. Política 13: Continuidad del negocio.	Laura María Vélez Carvajal	Coordinadora - Seguridad informática	Leonardo Jaimes Gamboa Juan Fernando Sanchez	Gerente I+D. Gerente Infraestructura	Maritza Garzón Vargas Juan David Carrasquilla	Gerente General Director de Tecnología	24/08/2018	23/09/2019
3	Ítem #5. Leyes colombianas para el cumplimiento de la política. Política 13: Continuidad del negocio. 6.12 Política 12: Política de dispositivos Móviles.	Laura María Vélez Carvajal	Coordinadora - Seguridad informática	Leonardo Jaimes Gamboa Juan Fernando Sanchez	Gerente I+D. Gerente Infraestructura	Maritza Garzón Vargas Comité de seguridad de asistencia necesaria	Gerente General Comité Directivo	23/09/2019	21/01/2020
4	Objetivos Generales Objetivos específicos Comité de seguridad: Cambio de nombres de cargos Cumplimiento de la política de seguridad de la información	Laura María Vélez Carvajal	Coordinadora - Seguridad informática	Leonardo Jaimes Gamboa Juan Fernando Sanchez	Gerente I+D. Gerente Infraestructura	Maritza Garzón Vargas Comité de seguridad de asistencia necesaria	Gerente General Comité Directivo	21/01/2020	18/07/2020
5	6.15 Periodicidad de revisión política de seguridad de la información. Se incluye la palabra Ciberseguridad en los objetivos generales y específicos.	Laura María Vélez Carvajal	Jefe de seguridad de la información y continuidad de negocio	Leonardo Jaimes Gamboa Juan Fernando Sanchez	Director Tecnología Gerente Infraestructura	Maritza Garzón Vargas Comité de seguridad de asistencia necesaria	Gerente General Comité Directivo	18/07/2020	02/08/2021
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 María Vélez Carvajal	Gerente de seguridad de la información y continuidad de negocio	Leonardo Jaimes Gamboa Juan Fernando Sanchez Carlos Lopez	Director Tecnología Gerente Infraestructura Gerente I+D	Maritza Garzón Vargas Comité de seguridad de asistencia necesaria	Gerente General Comité Directivo	02/08/2021	16/08/2021
7	Objetivo específico alcance de migración	Laura María	Gerente de seguridad de la	Leonardo Jaimes	Director Tecnología	Maritza Garzón	Gerente General	16/08/2021	A la fecha

	on premise cloud Política 1 Políticas para la gestión de seguridad de la información.	Vélez Carvajal	información y continuidad de negocio	Gamboa Juan Fernando Sanchez Carlos Lopez	Gerente Infraestructura Gerente I+D	Vargas Comité de seguridad de asistencia necesaria	Comité Directivo		

Como aprobación

Aprobado por	Cargo	Firma	Fecha
Leonardo Jaimes Gamboa	Vicepresidente de Tecnología		16/08/2022
Maritza Garzón Vargas	Presidente		16/08/2022

Revisado por	Cargo	Firma	Fecha
Duván Ovidio Hernandez Pedraza	Director de Servicios Tecnológicos y Digitales		16/08/2022
Edgar Castañeda Zambrano	Gerente Ingeniería y Desarrollo		16/08/2022
Juan David Adarve Vergara	Vicepresidente de Operaciones y Desarrollo de Negocios		16/08/2022
Juan Eduardo Jaramillo Toro	Vicepresidente de Talento Humano		16/08/2022

Elaborado por	Cargo	Firma	Fecha
Laura María Vélez Carvajal	Gerente de seguridad de la información y continuidad de negocio		16/08/2022