

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

EMT:Publica

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 Tecnología, Seguridad y Desarrollo: 3

5. Cumplimiento General de la Política 4

6. Directrices para Gestionar el SGSI. 4

6.1. Directriz 1: Gobierno y Organización de Seguridad de la Información. 4

6.2. Directriz 2: Administración del Riesgo en Seguridad de la Información. 5

6.3. Directriz 3: SGSI en los Procesos Asociados a Personas. 5

6.4. Directriz 4: Administración y Protección Física a los Activos. 5

6.5. Directriz 5: Control de Acceso Lógico: 5

6.6. Directriz 6: Gestión de Infraestructura y Conectividad Tecnológica: 6

6.7. Directriz 7: Cifrado de la Información: 6

6.8. Directriz 8: Seguridad Física y Entorno: 6

6.9. Directriz 9: Incidentes de Seguridad de la Información: 7

6.10. Directriz 10: Desarrollo de Aplicaciones y Mantenimiento a los Sistemas: 7

6.11. Directriz 11: Relaciones Seguras con Terceras Partes: 7

6.12. Directriz 12: Dispositivos Móviles Corporativos: 8

6.13. Directriz 13: Cumplimiento Corporativo Estándares y Certificaciones: 8

6.14. Directriz 14: Continuidad del Negocio: 8

6.15. Directriz 15: Seguridad de Trabajo en Casa: 8

6.16. Directriz 16: Inteligencia de Amenaza: 8

6.17. Directriz 17: Tecnologías Emergentes: 9

7. Periodicidad de revisión. 9

8. Control de cambios. 9

1. Introducción

Emtelco establece la presente Política del Sistema de Gestión de Seguridad de la Información (SGSI) como expresión de su compromiso con la protección de la información propia, de sus clientes y de terceros, independientemente de su formato, ubicación o medio de tratamiento.

La organización gestiona los riesgos de seguridad de la información y adopta medidas administrativas, humanas, físicas y tecnológicas orientadas a preservar la confidencialidad, integridad y disponibilidad de la información, cumplir los requisitos aplicables y promover la mejora continua.

Esta Política presenta los compromisos generales de **emtelco** y está dirigida a colaboradores, clientes, proveedores y demás partes interesadas. Los criterios operativos y técnicos se desarrollan en el *Manual del Sistema de Gestión de Seguridad de la Información (SGSI)* y en la documentación interna correspondiente.

2. Objetivos

A continuación, se detalla los siguientes objetivos:

2.1. Objetivo General:

Establecer los compromisos y principios generales mediante los cuales **emtelco** gestiona los riesgos de seguridad de la información y protege la información propia, en custodia o compartida con terceros, durante todo su ciclo de vida y con independencia del medio o entorno en el que sea tratada.

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

Esta Política aplica a todos los colaboradores, contratistas, proveedores, clientes y demás partes interesadas que accedan, administren, custodien, procesen, almacenen, transmitan o utilicen información de **emtelco** o información entregada a la organización.

Su aplicación comprende la información en medios físicos o digitales, los activos tecnológicos, las instalaciones, los servicios en la nube, los ambientes de trabajo remoto y las tecnologías implementadas para apoyar los procesos y servicios de la organización. Los controles se aplicarán de acuerdo con el alcance definido, los riesgos identificados y los requisitos legales, regulatorios, contractuales y organizacionales correspondientes.

4. Roles y responsabilidades

La Presidencia y Junta Directiva, orienta y respalda el Sistema de Gestión de Seguridad de la Información (SGSI), promoviendo su integración con la estrategia y los procesos de la organización. **Emtelco** cuenta con instancias de gobierno y con responsabilidades formalmente asignadas para dirigir, implementar, supervisar y mejorar la seguridad de la información, la ciberseguridad y la continuidad del negocio.

Los líderes de proceso son responsables de gestionar los riesgos y controles asociados con la información bajo su responsabilidad. Todos los colaboradores, contratistas y terceros deben conocer y cumplir las directrices que les sean aplicables, proteger la información y reportar oportunamente los eventos o situaciones que puedan afectar su seguridad.

4.1. Comité de Tecnología, Seguridad y Desarrollo:

El Comité de **emtelco** es un grupo interdisciplinario conformado por representantes de diferentes áreas y miembros de la organización como sigue:

- ✓ Presidencia.
- ✓ Vicepresidente de Tecnología.
- ✓ Gerente de Ingeniería y Desarrollo.
- ✓ Gerente de Tecnología.
- ✓ Gerente de Seguridad de la Información y Continuidad del Negocio.
- ✓ Vicepresidente de Operaciones *(Bajo necesidad)*.
- ✓ Vicepresidente de Talento Humano *(Bajo necesidad)*.
- ✓ Vicepresidente Administrativo y Financiero *(Bajo necesidad)*.

El Comité sesionará mensualmente, con previa convocatoria desde la Presidencia y/o Vicepresidencia de Tecnología, 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 estratégicos o decisivos, y solo en aquellos temas en los que se considere conveniente su intervención.

5. Cumplimiento General de la Política

El cumplimiento de esta Política y de las directrices asociadas es obligatorio para las personas y terceros incluidos en su alcance. Cada parte debe conocer sus responsabilidades y actuar de manera diligente en el acceso, uso, almacenamiento, transferencia, administración y protección de la información.

El incumplimiento podrá dar lugar a las medidas contractuales, administrativas, disciplinarias o legales aplicables, según la naturaleza de la relación, la gravedad de la situación y los procedimientos establecidos por la organización.

6. Directrices para Gestionar el SGSI.

Estas Directrices entran en vigor a partir de su fecha de aprobación por el Comité e integrada al Sistema de Gestión Integral (SGI) de **emtelco**.

A continuación, se detallan los lineamientos para cumplir las Directrices del Sistema de Gestión de Seguridad de la Información (SGSI) definido por la organización.

6.1. Directriz 1: Gobierno y Organización de Seguridad de la Información.

La organización mantiene una estructura de gobierno con responsabilidades definidas para orientar, implementar, supervisar y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI). La seguridad de la información se integra en los procesos, proyectos, cambios tecnológicos y decisiones que puedan afectar la información o la prestación de los servicios.

La organización promueve la asignación de recursos, la formación del personal, la evaluación periódica del desempeño y la comunicación de las directrices aplicables a colaboradores y terceros.

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, ha designado el correo a continuación para reportar cualquier tipo de incidente de seguridad y/o ciberseguridad real NO operativo, con el objetivo de tomar las acciones preventivas o reactivas correspondientes: *seussocseginfo@experiencia.emtelco.com.co*.

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

- **Infección por malware:** Presencia de virus u otro software malicioso en cualquier activo de información de la organización.
- **Amenazas a la infraestructura:** Identificación de posibles ataques o intentos de daño a la infraestructura corporativa.
- **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.
- **Acceso indebido:** Detección de accesos no autorizados a sistemas, aplicaciones u

otros activos tecnológicos.

- **Alteración de datos:** Modificación o alteración no autorizada de la información.
- **Ataques por correo electrónico:** Intentos de phishing, suplantación de identidad, estafas, correos fraudulentos u otros ataques por email.
- **Pérdida o robo de dispositivos:** Hurto, extravío o acceso no autorizado a dispositivos o estaciones de trabajo que contengan información de la organización.
- **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 gestiona los riesgos de seguridad de la información mediante una metodología formal que permite identificar, analizar, evaluar, tratar y monitorear los eventos que puedan afectar la información, los activos tecnológicos y los servicios.

Los controles y planes de tratamiento se establecen de manera proporcional al nivel de riesgo, el contexto del servicio y los requisitos aplicables. Los riesgos que permanezcan después de implementar los controles deben ser conocidos y aceptados por las instancias con autoridad para ello.

6.3. Directriz 3: SGSI en los Procesos Asociados a Personas.

La organización incorpora requisitos de seguridad de la información durante la selección, vinculación, permanencia, cambio de funciones y retiro del personal, de acuerdo con la criticidad del cargo y la información a la que pueda acceder.

Emtelco promueve la formación y concientización continua, establece compromisos de confidencialidad y gestiona oportunamente la devolución de activos y la modificación o retiro de los accesos cuando cambie o finalice la relación laboral o contractual.

6.4. Directriz 4: Administración y Protección Física a los Activos.

La organización identifica, inventaría, clasifica y protege los activos de información de acuerdo con su valor, sensibilidad, criticidad y los riesgos asociados. Cada activo debe contar con un responsable y utilizarse únicamente para los fines autorizados.

La información debe almacenarse, compartirse, conservarse y eliminarse mediante recursos autorizados y controles adecuados durante todo su ciclo de vida. Los activos asignados a colaboradores o terceros deben ser custodiados y devueltos cuando finalice la necesidad que dio origen a su entrega.

6.5. Directriz 5: Control de Acceso Lógico:

La organización controla el acceso a la información y a los recursos tecnológicos mediante mecanismos de identificación, autenticación y autorización, aplicando los principios de necesidad de conocer, mínimo privilegio y segregación de funciones.

Los accesos deben ser autorizados, individuales, trazables y revisados periódicamente. Las credenciales son confidenciales e intransferibles, y deben administrarse conforme con los requisitos de seguridad definidos por la organización. Se aplicarán mecanismos reforzados de autenticación cuando el riesgo, la criticidad del recurso o las condiciones de

acceso lo requieran.

Las cuentas predeterminadas, genéricas, técnicas o de servicio deben administrarse bajo controles especiales que reduzcan el riesgo de uso indebido o acceso no autorizado.

Para las relaciones comerciales y contractuales con terceros (clientes, proveedores, etc.), **emtelco** 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 Infraestructura y Conectividad Tecnológica:

La organización implementa controles para proteger la infraestructura tecnológica, las redes, las comunicaciones y los servicios de procesamiento de información, de acuerdo con su criticidad y nivel de exposición.

Los activos tecnológicos deben contar con configuraciones seguras, actualizaciones, protección contra amenazas, segmentación, monitoreo, respaldo y gestión controlada de cambios. Antes de su puesta en operación deben eliminarse, modificarse o deshabilitarse las cuentas, credenciales, servicios y configuraciones predeterminadas que no sean necesarias o que puedan representar un riesgo.

6.7. Directriz 7: Cifrado de la Información:

La organización aplica mecanismos criptográficos para proteger la información durante su almacenamiento y transmisión, de acuerdo con su clasificación, los riesgos identificados y los requisitos legales, regulatorios y contractuales aplicables.

Los mecanismos de cifrado, certificados y claves criptográficas deben mantenerse vigentes, administrarse de forma segura y ajustarse a estándares reconocidos. No se permite el uso de mecanismos criptográficos obsoletos, vulnerados o no autorizados.

6.8. Directriz 8: Seguridad Física y Entorno:

La organización establece controles físicos y ambientales para prevenir el acceso no autorizado, la pérdida, el daño, la interferencia o la afectación de la información y de los recursos tecnológicos.

El acceso a instalaciones y áreas restringidas debe ser autorizado, controlado y monitoreado. Los colaboradores, visitantes y terceros deben cumplir las medidas establecidas para la identificación, el ingreso, la permanencia y el retiro de personas,

equipos y elementos, de acuerdo con la criticidad de cada espacio y los requisitos aplicables.

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

La organización mantiene procesos para identificar, reportar, analizar, contener, resolver y aprender de los eventos e incidentes que puedan afectar la confidencialidad, integridad o disponibilidad de la información y de los servicios.

Los colaboradores, contratistas, proveedores y demás partes interesadas deben reportar oportunamente cualquier situación sospechosa mediante los canales oficiales definidos. La organización conservará las evidencias necesarias, realizará los escalamientos correspondientes y comunicará los incidentes a clientes, autoridades u otras partes cuando exista una obligación aplicable.

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*.

6.10. Directriz 10: Desarrollo de Aplicaciones y Mantenimiento a los Sistemas:

En **emtelco** incorporamos requisitos de seguridad durante el diseño, adquisición, desarrollo, prueba, implementación, mantenimiento y retiro de aplicaciones y sistemas de información. Las soluciones internas y las suministradas por terceros deben someterse a revisiones y pruebas proporcionales a su criticidad y nivel de riesgo.

Los ambientes de desarrollo, pruebas y producción deben mantenerse separados. Antes de la puesta en producción deben retirarse los datos, cuentas, credenciales, funciones de depuración y configuraciones de prueba que no sean necesarias. Las credenciales, claves y secretos no deben incorporarse directamente en el código fuente ni mantenerse en repositorios no autorizados.

6.11. Directriz 11: Relaciones Seguras con Terceras Partes:

La organización incorpora requisitos de seguridad de la información, confidencialidad, continuidad, protección de datos y gestión de incidentes en los acuerdos con terceros, de acuerdo con la naturaleza del servicio y el nivel de exposición asociado.

Los terceros deben cumplir las directrices aplicables, proteger la información, limitar el acceso al propósito autorizado y comunicar oportunamente los eventos que puedan afectar a **emtelco** o a sus clientes. La organización clasifica y evalúa a sus proveedores de manera proporcional al riesgo, supervisa los servicios relevantes y puede solicitar acciones de mejora o adoptar medidas cuando se identifiquen desviaciones.

Cuando se utilicen servicios en la nube, se deben definir las responsabilidades de las partes y evaluar las condiciones de seguridad, privacidad, disponibilidad, ubicación, conservación y eliminación de la información.

6.12. Directriz 12: Dispositivos Móviles Corporativos:

Los dispositivos móviles corporativos utilizados para acceder a información o servicios de **emtelco** deben estar autorizados, administrados y protegidos mediante controles acordes con el riesgo.

Los usuarios son responsables de su custodia y uso adecuado. La conexión de dispositivos personales a los recursos corporativos no está permitida, salvo que exista una necesidad justificada, una autorización previa y los controles de seguridad correspondientes. La pérdida, extravío o posible compromiso de un dispositivo debe reportarse inmediatamente.

6.13. Directriz 13: Cumplimiento Corporativo Estándares y Certificaciones:

La organización gestiona el cumplimiento de los requisitos legales, regulatorios, contractuales, normativos y organizacionales aplicables a la seguridad de la información. Asimismo, adopta estándares y buenas prácticas reconocidos que fortalecen la protección de la información y la confianza de las partes interesadas.

La organización mantiene certificaciones y evaluaciones de cumplimiento dentro de alcances formalmente definidos. La información sobre el alcance y los controles aplicables se administra mediante la documentación oficial correspondiente y podrá ser suministrada a las partes autorizadas cuando resulte procedente.

6.14. Directriz 14: Continuidad del Negocio:

La organización gestiona la continuidad del negocio para fortalecer su capacidad de respuesta y recuperación ante eventos que puedan interrumpir los procesos y servicios críticos.

La organización identifica los impactos potenciales, establece estrategias y planes de continuidad y recuperación, asigna responsabilidades y realiza ejercicios periódicos para verificar su eficacia. Las prioridades y tiempos de recuperación se determinan de acuerdo con la criticidad de los procesos, los riesgos y los compromisos establecidos con los clientes.

6.15. Directriz 15: Seguridad de Trabajo en Casa:

La organización aplica sus políticas y controles de seguridad de la información en los escenarios de trabajo en casa autorizados. La habilitación de esta modalidad debe considerar los riesgos del servicio, los requisitos contractuales y las condiciones legales aplicables.

La organización implementa medidas para proteger los equipos, la información, las comunicaciones y los accesos remotos, y establece responsabilidades de confidencialidad y uso adecuado para el personal. Cuando el servicio involucre información o recursos de un cliente, se atenderán las condiciones acordadas en la relación contractual.

6.16. Directriz 16: Inteligencia de Amenaza:

La organización desarrolla actividades de inteligencia de amenazas para identificar y analizar oportunamente riesgos cibernéticos que puedan afectar la organización, sus

servicios o sus partes interesadas.

La información obtenida se utiliza para fortalecer la gestión de riesgos, la detección de eventos, la respuesta a incidentes y la mejora de los controles de seguridad, considerando fuentes internas y externas confiables.

6.17. Directriz 17: Tecnologías Emergentes:

La organización promueve la adopción responsable, segura y controlada de tecnologías emergentes que apoyen la innovación y la mejora de sus procesos y servicios. Toda tecnología nueva o en evolución debe ser evaluada antes de su adquisición, desarrollo, integración o uso, considerando los riesgos de seguridad, privacidad, continuidad, cumplimiento y dependencia tecnológica.

El uso de estas tecnologías debe contar con una finalidad autorizada, responsables definidos, protección adecuada de la información y supervisión humana cuando sus resultados puedan afectar a personas, clientes, terceros o procesos relevantes. No se permite procesar información confidencial, datos personales, credenciales o información de clientes en herramientas no autorizadas.

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** 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	24/02/2025
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	25/02/2025	07/09/2026
10	Actualización general de las directrices del Sistema de Gestión de Seguridad de la Información (SGSI) e inclusión de tecnologías emergentes.	Dilan Muñoz	Gerente de Seguridad de la Información y Continuidad del Negocio	Mario Montoya	Vicepresidente Tecnología	Juan D. Adarve	Presidencia	08/09/2026	A la fecha