POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

ELABORADO POR	REVISADO POR	APROBADO POR
Firma: Fabian A. Llantén **Nombre:** Fabian Llantén	**Firma:** **Nombre:** Rubén Darío Camayo Medina	**Firma:** **Nombre:** Tatiana Iveth Moreno Palacios
Cargo: Tecnólogo Oficina Tecnologías de la información	**Cargo:** Director Oficina Tecnologías de la información	**Cargo:** Gerente
Fecha:30/12/2025	**Fecha:** 30/12/2025	**Fecha:** 30/12/2025

CONTROL DE MODIFICACIONES

VERSIÓN	FECHA	CAMBIOS REALIZADOS	INCORPORÓ
01	19/10/2019	Creación del documento	Ana María Guevara
02	30/12/2025	Actualización del documento	Rubén Darío Camayo Medina

TABLA DE CONTENIDO

1. OBJETIVO

Establecer los lineamientos para la implementación, operación y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI) de EMTEL S.A. E.S.P., con el fin de proteger los activos de información, garantizar la confidencialidad, integridad y disponibilidad de la información, asegurar la continuidad de los sistemas y apoyar el cumplimiento de los objetivos institucionales.

2. ALCANCE

La presente política aplica a todos los procesos de EMTEL S.A E.S.P. y sus integraciones.

3. RESPONSABLE

La implementación, administración y cumplimiento de esta política es responsabilidad de:

Gerencia: Aprobar la política y asignar los recursos necesarios.

Área de Tecnologías de la Información (TI): Administrar el SGSI, definir controles y realizar el seguimiento.

Jefes de Proceso: Garantizar el cumplimiento de la política en sus áreas.

Área administrativa: Apoyar la gestión del SGSI mediante la definición y aplicación de controles administrativos, contractuales y de gestión del talento humano.

Usuarios de la información: Cumplir los lineamientos establecidos y reportar incidentes de seguridad.

4. DEFINICIONES

A. Datos Sensibles: Datos cuya divulgación, modificación o pérdida puede generar impactos legales, operativos o financieros para la empresa o para terceros.
B. Clasificación de la Información: Proceso mediante el cual se categoriza la información según su nivel de criticidad y sensibilidad.
C. ISO/IEC 27001: Norma internacional que define los requisitos para gestionar y proteger la seguridad de la información en una organización, asegurando su confidencialidad, integridad y disponibilidad.
D. Seguridad: Conjunto de medidas, controles y prácticas destinadas a proteger la información y los sistemas frente a accesos no autorizados, uso indebido, alteración, pérdida o interrupción, garantizando su confidencialidad, integridad y disponibilidad.

E. Incidente: Evento o situación, real o potencial, que puede comprometer la confidencialidad, integridad o disponibilidad de la información, de los sistemas de información.

5. NORMATIVIDAD

La presente política da cumplimiento, entre otras, a las siguientes normas y disposiciones:

- ISO/IEC 27001 – Sistema de Gestión de Seguridad de la Información
- ISO/IEC 27002 – Controles de Seguridad de la Información
- ISO/IEC 27005 – Gestión del Riesgo de Seguridad de la Información
- ISO/IEC 27032 – Ciberseguridad
- Ley 1581 de 2012 – Protección de Datos Personales
- Decreto 1078 de 2015 – Sector TIC
- Lineamientos de Gobierno Digital
- Modelo Integrado de Planeación y Gestión – MIPG

6. CONDICIONES GENERALES

EMTEL S.A. E.S.P., consciente de la importancia de la información como activo estratégico, establece y respalda la definición, implementación, operación y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI), alineado con los objetivos institucionales y la normatividad vigente.

La gestión de la seguridad de la información en EMTEL está orientada a reducir los riesgos que puedan afectar sus activos de información, garantizando niveles adecuados de confidencialidad, integridad y disponibilidad.

La presente política se basará en los siguientes lineamientos generales para cumplir con el objetivo.

Gestión de activos.

Los activos de información deberán ser identificados, clasificados y protegidos de acuerdo con su criticidad y nivel de sensibilidad.

Cada proceso misional es responsable de la gestión y protección de los datos sensibles bajo su custodia.

EMTEL S.A. E.S.P. protegerá los datos mediante un trabajo articulado entre los diferentes procesos de la empresa y la Oficina de Tecnologías de la Información, aplicando controles

técnicos, organizativos y operativos orientados a prevenir accesos no autorizados, la pérdida, la divulgación o la alteración de los datos sensibles.

Control de acceso

El acceso a la información y a los sistemas de información de la Empresa será autorizado conforme a las funciones del usuario, aplicando el principio de mínimo privilegio.

Uso de recursos tecnológicos

Los recursos tecnológicos institucionales deberán ser utilizados exclusivamente para fines laborales y conforme al documento PO.04.TI.(V2) POLITICA DE CONTROL DECONTENIDO WEB.

Dispositivos externos

El uso de dispositivos de almacenamiento y equipos externos estará restringido de acuerdo al documento PO.03.TI.(V2) POLITICAS CONTROL DE DISPOSITIVOS.

Seguridad en redes y navegación

Se implementarán controles técnicos y administrativos orientados a proteger la red institucional, prevenir accesos no autorizados, descargas de software malicioso y la fuga de información, garantizando un uso seguro y adecuado de los recursos.

Capacitación

EMTEL S.A E.S.P. promoverá programas continuos de capacitación y sensibilización en seguridad de la información y ciberseguridad para la oficina de Tecnologías de la Información, quien replicará estos conocimientos a las demás áreas de la Empresa.

GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD

EMTEL contará con un Plan de Respuesta a Incidentes de Ciberseguridad que establezca los mecanismos para la identificación, análisis, contención, erradicación, recuperación y cierre de los incidentes de seguridad de la información, con el fin de minimizar su impacto y fortalecer la mejora continua del SGSI.

Las fases del plan se definen:

Identificación del incidente

Se identifica un incidente, real o potencial, a partir de sistemas de monitoreo, alertas, reportes de usuarios o notificaciones de terceros, y se notifica de forma inmediata a la Oficina de Tecnologías de la Información para su evaluación inicial.

Análisis y clasificación

En esta etapa se evalúa el impacto sobre la confidencialidad, integridad y disponibilidad de la información. Con base en este análisis, el incidente se clasifica según su nivel de criticidad y se prioriza su atención de acuerdo con la gravedad y urgencia del caso.

Contención y erradicación

Se restablecen los sistemas, servicios e información afectados por el incidente. Las actividades incluyen la restauración de la información desde respaldos seguros, la validación de la integridad de los datos, la reactivación de los servicios y la verificación de que las vulnerabilidades asociadas al incidente hayan sido mitigadas.

Recuperación

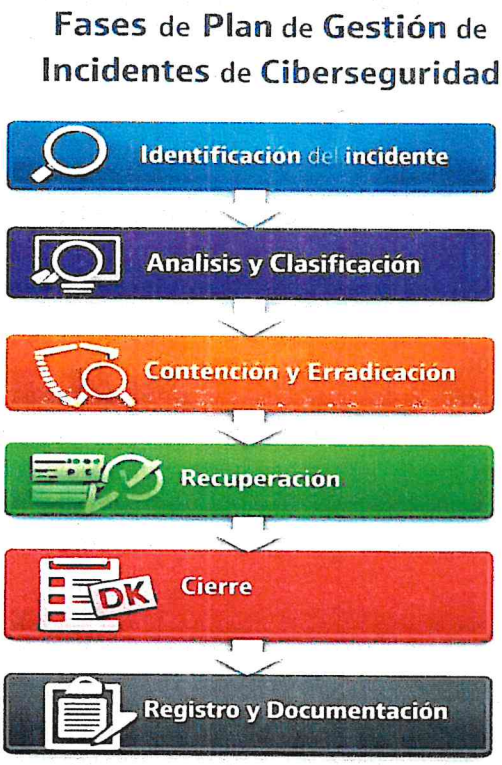
Se ejecutan las acciones necesarias para restablecer de manera controlada la operación normal de los sistemas, servicios y procesos afectados por el incidente de ciberseguridad. La recuperación incluye la restauración de sistemas y aplicaciones, la validación del correcto funcionamiento de la infraestructura tecnológica, la verificación de la integridad y disponibilidad de la información.

Cierre

El cierre del incidente se realiza una vez confirmada la solución total del evento y la normalización de los servicios. En esta etapa se validan las acciones ejecutadas, se confirman los resultados obtenidos y se da por finalizada la atención del incidente.

Registro y documentación

Todas las actividades relacionadas con la gestión del incidente deben ser documentadas de manera formal. La Oficina de TI registrará la información en la bitácora, incluyendo la descripción del incidente y las acciones realizadas.



7. DESCRIPCION DE ACTIVIDADES

No.	NOMBRE DE LA ACTIVIDAD	ACTIVIDAD / DESCRIPCIÓN	RESPONSABLE	REGISTRO/ DOCUMENTO
1	Identificación de activos	Identificar y clasificar los activos de información	Oficina TI	FR.12.TI. Inventario de activos
3	Implementación de controles	Aplicar controles técnicos de seguridad	Oficina TI	N/A
4	Atención de incidentes	Reportar y atender incidentes de seguridad	Oficina TI	FR.11.TI. Registro de incidentes
5	Auditoría y mejora	Evaluar el SGSI y aplicar mejoras	Oficina TI	FR.04.CT. Informes de auditoría

8. ACCIONES CONTINGENTES

EMTEL S.A. E.S.P. definirá y aplicará acciones contingentes orientadas a asegurar la continuidad de los servicios, la protección de los activos de información y la rápida recuperación ante eventos que afecten la seguridad de la información o la operación de los sistemas.

Ante la detección de un incidente de seguridad de la información, la Oficina de Tecnologías de la Información activará de manera inmediata el Plan de Respuesta a Incidentes de Ciberseguridad, priorizando la atención según el nivel de criticidad identificado.

Cuando sea necesario, se procederá al aislamiento lógico o físico de los sistemas, equipos o redes comprometidas, con el fin de evitar la propagación del incidente y proteger el resto de la infraestructura tecnológica.

Se realizará la restauración de la información y los sistemas afectados a partir de copias de seguridad previamente validadas, garantizando la integridad, disponibilidad y consistencia de los datos.

Cuando la magnitud del incidente lo requiera, se gestionará el apoyo de proveedores especializados, fabricantes, entidades reguladoras o equipos externos de respuesta, garantizando la adecuada atención del evento.

Durante la contingencia se implementarán controles de monitoreo intensivo sobre los sistemas y redes afectados, con el fin de detectar comportamientos anómalos y prevenir recurrencias.

Todas las acciones contingentes ejecutadas deberán ser registradas y documentadas. Posteriormente, se analizarán las causas del incidente y se definirán acciones correctivas y preventivas que fortalezcan el SGSI y reduzcan la probabilidad de eventos similares.

9. DOCUMENTOS DE REFERENCIA

- Procedimientos del SGSI
- Manual de Gobierno Digital
- Normas ISO/IEC 27001, 27002, 27005 y 27032

10. REGISTROS DE CALIDAD

- FR.12.TI. Inventario de activos.
- FR.11.TI. Registro de incidentes
- FR.04.CT. Informes de auditoría

11. ANEXOS

N.A.