EML
PUBLICIDAD & MERCADEO
HEALTHCARE

Política de SGSI

EML S.AS.
Bogotá - Colombia

1. Objetivo

La alta dirección de **EML S.A.S**, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus servicios con sus clientes y proveedores, todo enmarcado en el cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

El objetivo de este documento es establecer las políticas, prácticas y lineamientos internos aplicables para el Sistema de Gestión de Seguridad de la Información de ahora en más SGSI para **EML S.A.S**.

2. Alcance

El siguiente documento impacta a los procesos y controles que sirven para el cumplimiento del Sistema de Gestión de la Seguridad de la Información, incluidos en el alcance definido por la organización.

3. Lineamientos

Contexto de la organización (Cláusula 4)

3.1 Comprender a la organización y su contexto (Requisito 4.1)

EML S.A.S ha determinado los asuntos internos y externos que son relevantes para su propósito y que intervienen en el logro de los resultados esperados.

Para esto, se aplicaron los siguientes análisis:

Análisis del entorno

Esto incluye cualquier cosa **fuera** de la organización que pueda influir en su operación.

Político Política gubernamental	**Económico** Economía y finanzas	**Socioambiental** Cultura y naturaleza	**Tecnológico** Avances e innovación	**Legal** Leyes y regulaciones
Cambios en la legislación. Cambios en los tratados comerciales. Acuerdos internacionales. Conflictos internos y externos. Movimientos Políticos	Ciclo económico. Financiación. Tributarios. Ataques o perdidas de información de entidades bancarios a las que pertenece EML.	Nivel de experiencia y/o Expertise. Nivel de ingresos. Desastres naturales.	Nuevo hardware. Nuevas tecnologías para el software. Reemplazo de las tecnologías. Riesgos asociados a la innovación u obsolescencia de las tecnologías.	Propiedad intelectual. Salud y seguridad laboral. Regulación de sectores. Cambios en las leyes de privacidad y protección de datos en los países donde opera EML podrían requerir ajustes en las políticas de seguridad de la información para cumplir con nuevas regulaciones. Salario mínimo. Licencias.

Análisis FODA

Esto incluye cualquier cosa **fuera** y **dentro** de la organización que pueda influir en su operación.

Fortalezas	**Debilidades**
Administrativas • Personal directivo, administrativo y producción • Voluntad gerencial de contar con equipos y licencias actualizadas y legalizadas • Voluntad gerencial de calidad total y procesos de formación	Administrativas • Proceso de facturación electrónica dependiente de una sola persona • No implementación aun del software de nómina al 100%

• Voluntad gerencial de contar con todos los manuales requeridos de políticas, funciones, procesos de producción, logística, seguridad de la información • Trayectoria de más de 20 años • Licencias para equipos de producción al día (Windows, office, Adobe, banco de imágenes, sonidos, etc.) • Adquisición de herramienta Office365 para mejorar productividad Producción • Procesos de auditoría de producción (GEPRO), ventas (GECO), tráfico • Equipo multidisciplinario • Potencial mejoría de productividad con próxima implementación de office 365 y metodologías ágiles Mercadeo • Certificación en Veeva e Iqvia • Personal de contenidos bilingüe	• Desconocimiento de las funcionalidades del software de nómina • No cumplimiento al 100% de las políticas del Sistema General de Seguridad y Salud en el Trabajo • Deficiente concientización por parte del personal sobre la importancia y ejecución de pausas activas • Demoras en las respuestas ante solicitud de deficiencias en el funcionamiento de los equipos de cómputo • Dificultad en la centralización física de los equipos de cómputo, sus configuraciones y reparaciones/mantenimiento por el teletrabajo • No contamos con Políticas de Seguridad de la Información aun en ejecución • Ausencia de procesos de auditorías sobre los diferentes procesos de las Políticas de Seguridad de la Información • Políticas y cultura de backup ineficiente • Deficiencias en los procesos de selección del personal (pruebas psicotécnicas) • Manuales de funciones incompletos según el cargo • Deficiencias en la disponibilidad de la información oportuna para la toma de decisiones con respecto a la renovación de contratos • Deficiencia de programas continuos de capacitación, entrenamiento y retroalimentación en las diferentes áreas de producción/administrativas • Manuales de procesos incompletos

	• No hay un adecuado sistema de seguimiento y control de las tareas asignadas • Deficiente gestión de las tareas asignadas en tiempo y calidad • Existen políticas internas escritas, pero no se ejecutan metodológicamente, no hay conciencia • Pobre divulgación y comunicación corporativa Producción • No presencialidad del personal • Deficiencias en sistemas eficientes y seguros de comunicación (chats, correos electrónicos) • Se siguen cometiendo los mismos errores básicos (diseño/contenidos) que hace veinte años • Aun no hay plena conciencia de la importancia en el correcto nombramiento y archivo de los trabajos • Equipo de Ejecutivos de Cuenta aún en proceso de formación • Inadecuada implementación de estrategias de planeación y seguimiento de licitación de cuentas, proyectos complejos y/o extensos • Deficiente estructuración de presentación de licitaciones y campañas • Producción creativa aun por debajo del nivel esperado/requerido • Equipo de TyD en proceso de formación • Deficiente comunicación entre áreas de soporte • No contamos con una eficiente herramienta de planeación de proyectos

	• Pasividad e indiferencia del personal ante su capacidad de aportar soluciones a los potenciales problemas. Mercado • Bajo posicionamiento de la División de Marketing Digital • Bajo posicionamiento de la División de Marketing Experiencial • Bajo porcentaje de ganancia de licitaciones y campañas • Baja penetración en el mercado healthcare no farmacéutico y OTC • Inadecuado posicionamiento en web (SEO-SEM) del sitio web corporativo.
Oportunidades	**Amenazas**
Administrativas • Digitalización del mercado • Presencia en el mercado de agencias que aún no tiene políticas de Seguridad de la Información Producción • Incremento significativo en el uso de plataformas como Veeva e Iqvia • Incremento en el uso de herramientas digitales Mercado • Exigencias del sector farmacéutico por contar con proveedores que dispongan de políticas de seguridad de la información, licencias de software, legalización de las relaciones laborales de los empleados • Comportamiento del dólar en operaciones internacionales	Administrativas • Pandemia • Digitalización y teletrabajo como riesgo de ciberseguridad • Presencia creciente en el mercado farmacéutico de Agencias de Publicidad Multinacionales Producción • No presencialidad del personal • Vulnerabilidad de los equipos de cómputo (seguridad física/cibernética/cambios de voltaje) Mercado • Incertidumbre del mercado por Pandemia • Baja demanda de servicios para eventos presenciales • Inestabilidad de la economía • Desempleo

• Baja penetración del mercado internacional de habla hispana • LinkedIn como herramienta de promoción B2B • Teléfonos corporativos como herramienta de promoción de los servicios de EML (estado de WhatsApp) • Buen nivel de posicionamiento con Sanofi en Centroamérica • Necesidad del mercado de servicios de marketing experiencial	

3.2 Comprender a las partes interesadas (Requisito 4.2)

La organización ha determinado las partes interesadas que son pertinentes para el SGSI y sus requisitos para la seguridad de la información.

Identificar a las partes interesadas

Categoría	Interesados detectados
Partes internas	Alta dirección
	Comité de Seguridad de Información
	OSI (Oficial de Seguridad de la Información)
	Líderes de procesos / servicios
	Personal operativo de los procesos / servicios
Partes externas	Clientes
	Proveedores

Analizar los requisitos de las partes interesadas que se abordan en el SGSI

- ALTA DIRECCIÓN Y/O COMITÉ DE SEGURIDAD DE LA INFORMACIÓN
  - Un ambiente de trabajo seguro y apropiado.
  - Un SGSI exitoso.
  - Empleados concientizados e involucrados.
- OSI (Oficial de Seguridad de la Información)
  - Implementar y mantener el SGSI.
  - Cumplimiento normativo.
  - Mejoramiento continuo del SGSI.
- LÍDERES DE PROCESOS / SERVICIOS
  - Protección de la información involucrada en los procesos / servicios.
  - Documentación pertinente sobre los procesos / servicios.
  - Atención de los incidentes reportados en los procesos / servicios.
- EMPLEADOS (Personal operativo de los procesos / servicios)
  - Un ambiente de trabajo seguro y apropiado.
  - Recibir capacitación y apoyo requeridos.
  - Recibir claramente sus objetivos laborales.
  - Oportunidades para el avance y desarrollo profesional.

- ➔ CLIENTES
    - Productos y servicios con soporte y mantenimiento:
        - de acuerdo con los requisitos contractuales,
        - de acuerdo con los requisitos legales aplicables,
        - de acuerdo con los requisitos adicionales de la industria aplicables.
    - Disponibilidad de los sistemas alcanzados por el SGSI.
    - Cumplir con los requisitos de seguridad de la información.
- ➔ PROVEEDORES
    - Cumplir con los acuerdos contractuales.
    - Cumplir con los acuerdos de confidencialidad firmados.
    - Cumplir con los requisitos de seguridad de la información.
    - Cumplir con los requerimientos y cumplimiento de la documentación requerida para el proceso de inscripción de proveedores.

3.3 Determinar el alcance del SGSI (Requisito 4.3)

La información relacionada a los análisis internos y externos han ayudado a delimitar el alcance del SGSI con respecto a:

- ➔ Características del negocio
- ➔ Procesos operativos
- ➔ Estructura organizacional de SI
- ➔ Ubicación

Características del negocio

El producto y/o servicio provisto por **EML S.A.S.** que es alcanzado por el SGSI es:

- ➔ Almacenamiento y tratamiento de los datos.
- ➔ Entrega final de proyectos a clientes

Procesos operativos

Aquí se declaran los procesos de la operación que son relevantes para el alcance del SGSI de **EML S.A.S.**

Procesos operativos	Area	Procesos con dependencia / interacción
Proceso de etiquetado y almacenamiento de archivos.	Areas administrativas y de producción.	Proceso de almacenamiento y control de la información sensible de EML
Proceso de depuración y back-up de la información.	Áreas administrativas y de producción.	Proceso de escritorio limpio.
Proceso de control de acceso.	Áreas administrativas y de producción.	Proceso de ajuste y actualización de credenciales.
Proceso de acción ante incidentes de seguridad de la información	Toda la empresa	Políticas y procesos del comité de emergencias

Ubicación

La infraestructura (física y/o lógica) donde se desarrollan los procesos alcanzados corresponden a la siguiente ubicación:

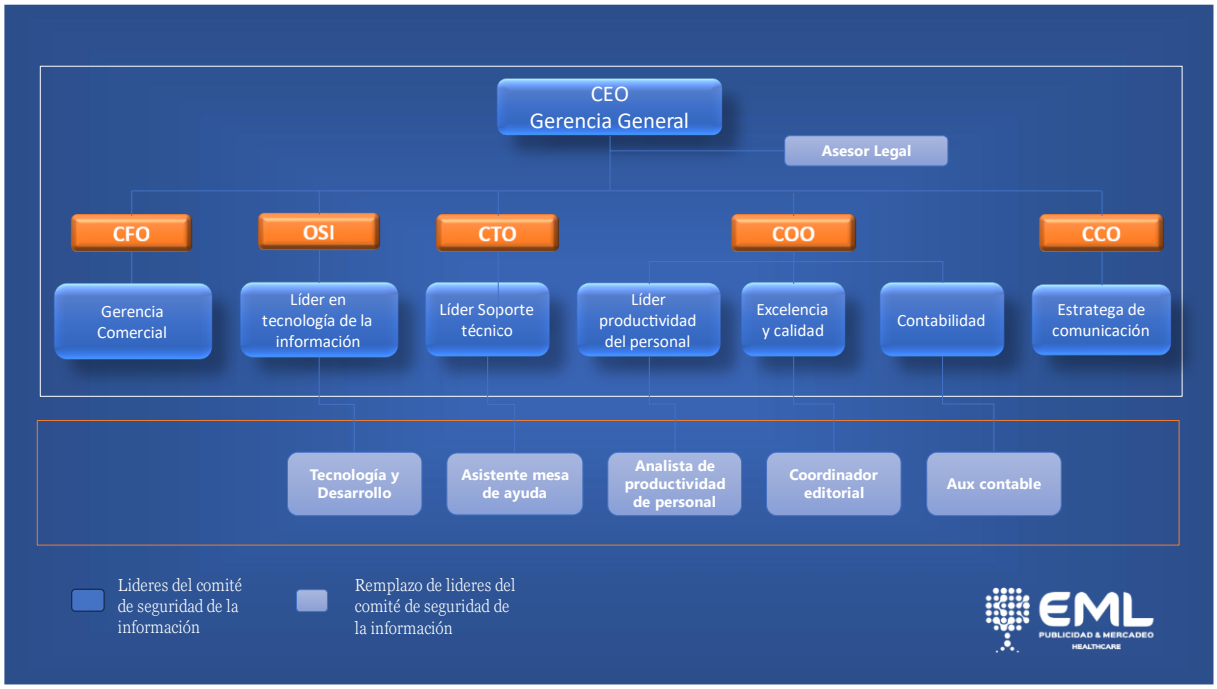
- ➔ Colombia/Servidor propio NAS
- ➔ Microsoft 365/OneDrive.

Considerando la información definida en los puntos anteriores, se establece el siguiente enunciado de alcance:

El alcance del Sistema de Gestión de Seguridad de la Información (SGSI) de EML S.A.S se extiende a los procesos operativos llevados a cabo en la infraestructura física y lógica ubicada en Colombia, incluyendo un servidor propio NAS, así como en la plataforma Microsoft 365/OneDrive. Este SGSI tiene como objetivo principal asegurar la confidencialidad, integridad y disponibilidad de la información relacionada con la producción y clientes de EML S.A.S, abarcando tanto los datos almacenados localmente en el servidor NAS como aquellos gestionados a través de la plataforma Microsoft 365/OneDrive. El SGSI se implementará para proteger los activos de información críticos, garantizar el cumplimiento normativo y promover un entorno seguro para el desarrollo de las operaciones de la organización.

Estructura organizacional

EML define una estructura organizacional que incluye roles de seguridad de la información que están alineados al contexto de la organización, los cuales se muestran en el siguiente organigrama:



3.4 Sistema de gestión de la seguridad de la información (Requisito 4.4)

EML establece, implementa, mantiene y mejora continuamente un SGSI siguiendo los lineamientos de esta política e incluyendo los procesos necesarios y sus interacciones.

Liderazgo (Cláusula 5)

3.5 Liderazgo y compromiso (Requisito 5.1)

La alta dirección y los c-levels de EML demuestran su liderazgo y compromiso con el SGSI mediante las siguientes acciones:

- ➔ Definiendo la política (véase sección 3.6) y los objetivos de seguridad de la información (véase sección 3.9) de manera que se encuentren alineados con la estrategia de la empresa.
- ➔ Asegurando la integración de la seguridad dentro de los procesos de la organización mediante la aprobación y comunicación de documentos del SGSI.
- ➔ Garantizando los recursos necesarios para el SGSI mediante la aprobación de un presupuesto.
- ➔ Garantizando que el SGSI logre sus resultados esperados mediante las revisiones periódicas del sistema, como lo son las auditorías, los indicadores y métricas, entre otros.
- ➔ Dirigiendo a la empresa a tomar acciones que aporten al éxito del SGSI y promuevan la mejora continua.

3.6 Política general de seguridad de la información (Requisito 5.2)

La Seguridad de la Información en **EML** es parte fundamental del negocio para así entregar confianza a nuestros clientes y usuarios sobre las tecnologías de la información que operamos. La data, con base en nuestra clasificación de la información, es gestionada con los más altos estándares según las mejores prácticas disponibles en el mercado, lo cual es una base para nuestro crecimiento y sustentabilidad organizacional.

La Seguridad de la Información en EML es posible dado el compromiso de la alta dirección promoviendo una cultura de mejora continua, facilitando los recursos y herramientas necesarias.

La alta dirección entiende y atiende la importancia y beneficios de mantenerse en cumplimiento, no solo con los requerimientos de ISO 27001 y mejores prácticas de seguridad, sino además con otros requisitos legales, contractuales y gubernamentales relevantes para el contexto de la organización.

En EML nuestras políticas y procedimientos en cuanto a la Seguridad de la Información son del conocimiento general de los empleados, cuando aplique. En la medida de lo posible y con base al Plan de Comunicación del SGSI definido, nuestras partes interesadas clave serán informadas de nuestros lineamientos y mejores prácticas.

3.7 Roles, responsabilidades y autoridades (Requisito 5.3)

La alta dirección de EML ha definido los roles y asignado sus responsabilidades asociadas al SGSI dentro del documento de Descriptivo de Roles y Responsabilidades que establece, entre otras cosas, lo siguiente:

- ➔ Todos los roles necesarios para llevar a cabo las actividades requeridas por la ISO 27001.
- ➔ Las responsabilidades que asume cada uno de los roles involucrados en el SGSI.

- La responsabilidad del Oficial de Seguridad de la Información (OSI), en conjunto con el Comité de Seguridad es, entre otras, velar por el cumplimiento del SGSI y de informar sobre su desempeño a la alta dirección y a la organización.

Así como también dentro de la Política del Comité de Seguridad de la Información donde se establecen las funciones de los integrantes del comité definido por la organización.

Planificación (Cláusula 6)

3.8 Acciones para tratar los riesgos y oportunidades (Requisito 6.1)

3.8.1 General (Requisito 6.1.1)

EML planifica la gestión de riesgos y oportunidades del SGSI, tomando como base lo analizado en 6.1 Comprender a la organización y de su contexto (véase sección 3.1) y 6.2 Comprender las necesidades y expectativas de las partes interesadas (véase sección 3.2).

Esta planificación está orientada a:

- Evitar o reducir efectos no deseados, que se demuestra con el análisis, evaluación y tratamiento de riesgos.

- Fortalecer el SGSI apoyando el logro de los resultados previstos y la mejora continua.

Esta planificación tiene como objetivos:

- Definir las acciones para evaluar y tratar los riesgos y oportunidades.

- Definir la forma en que se integrarán e implementarán estas acciones dentro de los procesos del SGSI.

- Definir la forma en que serán medidas estas acciones en cuanto a su efectividad.

3.8.2 Evaluación de los riesgos de seguridad de la información (Requisito 6.1.2)

EML dispone de la realización de una evaluación de riesgos, que considera lo siguiente:

- Definir los criterios de aceptación y de evaluación de los riesgos.

- Establecer una metodología objetiva para la evaluación de los riesgos que arroje resultados consistentes, válidos y comparables.

- Identificar y analizar riesgos de seguridad de la información (asociados a la pérdida de confidencialidad, integridad y disponibilidad) y a sus responsables dentro del SGSI.

- Determinar el nivel de riesgo mediante la valorización de su probabilidad e impacto.

- Evaluar los riesgos comparando los resultados del análisis con los criterios establecidos en la metodología y priorizándolos.

Estas actividades se encuentran documentadas en la Metodología de Gestión de Riesgos y en los registros asociados:

- Módulo de OneDrive de la cuenta de Líder en tecnologia de la información

3.8.3 Tratamiento de los riesgos de seguridad de la información (Requisito 6.1.3)

EML establece el tratamiento de los riesgos de seguridad de la Información, que considera lo siguiente:

- Tomar los resultados de la evaluación de riesgos para seleccionar opciones de tratamiento.
- Asociar los controles de seguridad del anexo A de la ISO 27001 para implementar la opción de tratamiento seleccionada, verificando que no existan omisiones.
- Elaborar la declaración de aplicabilidad donde se indiquen los controles necesarios ya implementados dentro de EML identificar aquellos que sean necesarios implementar y los que no para el SGSI, así como la justificación de su inclusión/exclusión para ambos casos.
- Proponer un plan de tratamiento y documentarlo.
- Obtener la aprobación de los responsables de riesgos sobre el plan de tratamiento y sus riesgos residuales.

Estas actividades se encuentran documentadas en la Metodología de Gestión de Riesgos y en los registros producidos como resultado del proceso:

- Módulo de Backup del equipo de líder en la tecnologia de la información
- Declaración de aplicabilidad
- Reporte de análisis de riesgos
- Minuta de sesión de comité

3.9 Objetivos de seguridad de la información y planificación para alcanzarlos (Requisito 6.2)

EML establece sus objetivos de seguridad bajo un enfoque de alto nivel, pero estrechamente relacionados a los objetivos organizacionales. Los objetivos del SGSI deben:

- Ser consistentes con la Política de Seguridad de la Información.
- Estar relacionados directamente con las métricas del SGSI, lo cual permite su medición, si aplica.
- Contemplar los resultados de la evaluación y los planes de tratamiento de los riesgos.

- ➔ Ser monitoreados, publicados y comunicados según lo establece el Plan de Comunicación del SGSI.
- ➔ Estar disponibles y documentados.
- ➔ Ser actualizados, cuando sea requerido.

Se determina dentro de la Metodología de Indicadores de Seguridad de la Información qué se hará, qué recursos se usarán, quién será el responsable, cuándo y cómo se evaluarán los objetivos y sus métricas.

EML declara los siguientes objetivos de seguridad de la información alineados al SGSI y a su estrategia:

- ➔ Garantizar la integridad y confidencialidad de los datos y dispositivos corporativos permanentemente.
- ➔ Garantizar que la información sensible, como datos de clientes, diseños de productos y procesos de producción, se mantenga confidencial y solo esté disponible para aquellos que tengan autorización.
- ➔ Asegurar que la información no se vea comprometida y que cualquier modificación no autorizada sea detectada.
- ➔ Desarrollar y mantener un plan de respuesta a incidentes para abordar cualquier evento de seguridad de la información de manera eficiente y minimizar el impacto en la producción y los clientes.

3.10 Planificación de cambios (Requisito 6.3)

EML determina que cualquier cambio que se considere necesario para el SGSI, éste debe llevarse a cabo de manera planificada. Además, debe ser aprobado por la alta dirección y comunicado a la organización y partes interesadas.

Soporte (Cláusula 7)

3.11 Recursos (Requisito 7.1)

EML dedica un presupuesto que le permita asegurar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI, el cual debe ser aprobado por la alta dirección.

Este presupuesto y su aprobación deben permanecer como información documentada.

Asimismo, se garantiza la participación del recurso humano necesario para el SGSI y se dispone de los recursos de infraestructura tecnológica que soportan la operación.

3.12 Competencia (Requisito 7.2)

EML dispone lo siguiente:

- ➔ Ha determinado las competencias necesarias de las personas que operan y asumen funciones específicas dentro del SGSI, las cuales han sido definidas en el descriptivo de roles y responsabilidades.

- Ha asegurado el cumplimiento de estas competencias mediante la capacitación y concientización del personal, lo que se ha documentado en el programa de capacitación. Este puede ser actualizado si se detectan deficiencias en el conocimiento del personal, de manera que se consideren capacitaciones adicionales.

- Ha realizado una investigación de las competencias y habilidades de los candidatos previo a su contratación, lo cual se define en el procedimiento de preselección y selección de personal.

3.13 Concientización (Requisito 7.3)

El personal de EML debe cumplir con los siguientes puntos:

- Conocer la Política General de Seguridad de la Información (véase sección 6.6). Para ello, el responsable a cargo del SGSI envía la política mediante INTRANET Y CANALES DE TEAMS a todo el personal de la empresa.

- Conocer su contribución para la efectividad y mejora continua del SGSI. Para ello, el personal recibe charlas de concientización de manera periódica, las cuales se documentan en el programa de capacitación.

- Conocer las sanciones a las que están sujetos al no aportar a la efectividad y mejora continua del SGSI. Para ello, se puede consultar la política de seguridad de la información.

3.14 Comunicación (Requisito 7.4)

Las comunicaciones internas y externas son planificadas y ejecutadas con base a lo definido en el Plan de Comunicación del SGSI. La actualización de este documento se realiza conforme a las operaciones de la empresa.

Este plan define lo siguiente:

- Qué se va a comunicar

- Cuando se va a comunicar

- A quién va dirigido

- Cómo se va a comunicar

3.15 Información documentada (Requisito 7.5)

3.15.1 General (Requisito 7.5.1)

El SGSI cuenta con:

- Los documentos y registros que son requisito de la norma.
- Los documentos que sin ser requisito de la norma son usados por EML S.A.S para asegurar la efectividad del SGSI.

3.15.2 Creación y actualización (Requisito 7.5.2)

EML dispone para la creación y actualización de sus documentos del SGSI lo siguiente:

- La identificación y descripción del documento, esto puede ser título, fecha de elaboración, autor, código, entre otros.
- La definición de formatos ya sea en medio electrónico o físico.
- La especificación de los responsables de elaborar, revisar y aprobar los documentos, los cuales deben ser adecuados con respecto a los roles del SGSI.

3.15.3 Control de la información documentada (Requisito 7.5.3)

EML se asegura que la documentación del SGSI cumpla con lo siguiente:

- Es compartida a las personas pertinentes y está disponible para su consulta mediante un acceso controlado.
- Estar protegida contra pérdida de confidencialidad e integridad.
- Tener condiciones adecuadas de almacenamiento y conservación.
- Tener control de los cambios a los documentos, así como condiciones adecuadas de retención y disposición.
- Identificar y controlar la documentación de origen externo, que la organización determine que es necesaria para la planificación, operación y mantenimiento del SGSI.

Operación (Cláusula 8)

3.16 Control y planificación operacional (Requisito 8.1)

EML planifica, implementa y controla las políticas y procedimientos necesarios donde se establecen los criterios pertinentes para cumplir los requisitos del SGSI y las acciones de la sección 3.8 de esta política.

Además, la empresa implementa planes para alcanzar los objetivos de seguridad de la información determinados en la sección 3.9 de esta política. Esto se encuentra como información documentada en el Listado de Métricas e Indicadores.

3.17 Evaluación de los riesgos de seguridad de la información (Requisito 8.2)

La evaluación de riesgos debe ser periódica por lo que EML ha definido aplicarla cada año, o cuando se produzcan modificaciones importantes como la ampliación del alcance de sistema de gestión, mecanismos de seguridad para infraestructura física y lógica de la información entre otros.

Las condiciones para la aplicación adecuada de estas evaluaciones son especificadas en la Metodología de Gestión de Riesgos.

Asimismo, los resultados de las evaluaciones de riesgos se encuentran disponibles como información documentada y en los registros asociados:

- ➔ Módulo de OneDrive del equipo de Lider en tecnologia de la información.

3.18 Tratamiento de los riesgos de seguridad de la información (Requisito 8.3)

EML implementa el plan de tratamiento de riesgos, con base en lo definido en el módulo de Riesgos de la plataforma Hackmetrix también en la estructura de carpetas de OneDrive del equipo de Lider en tecnologia de la información.

La implementación de los controles seleccionados en tu declaración de aplicabilidad para el tratamiento de riesgos deja registros que evidencian su realización.

Evaluación del desempeño (Cláusula 9)

3.19 Seguimiento, medición, análisis y evaluación (Requisito 9.1)

EML mide y evalúa el desempeño de la seguridad de la información y la efectividad del SGSI, para lo cual determina:

- ➔ Qué requiere ser monitoreado y medido, incluyendo los procesos y controles de la seguridad de información.
- ➔ Los métodos aplicados para monitorear, medir, analizar y evaluar que te aseguren resultados válidos.
- ➔ Quién es el responsable y cuándo se llevará a cabo el seguimiento y las mediciones.
- ➔ Quién es el responsable y cuándo se llevará a cabo el análisis y la evaluación de los resultados del seguimiento y las mediciones.

Las actividades descritas anteriormente se ejecutan según lo dispone la Metodología de Indicadores de Seguridad de la Información. Asimismo, los registros asociados se encuentran en el Listado de Métricas e Indicadores.

3.20 Auditorías internas (Requisito 9.2)

EML ha definido realizar auditorías internas anualmente para asegurar que el SGSI:

- Cumpla con los requerimientos del negocio y los lineamientos del estándar ISO 27001.
- Se encuentra implementado y se mantiene de manera efectiva.

Adicionalmente, la empresa debe:

- Planificar, establecer, implementar y mantener un programa de auditoría donde se defina la frecuencia, los métodos, las responsabilidades, los requisitos y la elaboración de reportes, tomando en cuenta la importancia de los procesos involucrados y los resultados de auditorías previas.
- Definir los criterios y alcance de la auditoría.
- Seleccionar auditores objetivos e imparciales.
- Seleccionar auditores certificados para la correcta implementación de una auditoría interna.
- Comunicar los resultados de las auditorías a la alta dirección y al comité de seguridad.
- Mantener evidencia de la planificación y ejecución de la auditoría en los registros asociados:
    - Plan y programa de auditoría.
    - Informe de auditoría interna.

Además, **EML S.A.S.** establece los siguientes criterios que debe cumplir el responsable de realizar las auditorías internas:

- El auditor interno debe mostrar que cuenta con experiencia y conocimiento para realizar auditorías de seguridad de la información (de ser posible, debe proporcionar los certificados pertinentes que lo comprueben).
- El auditor interno debe saber aplicar sus conocimientos sobre auditorías en cualquier proceso de la empresa para verificar el cumplimiento total del sistema de gestión de seguridad de la información.
- El auditor interno debe demostrar independencia de las funciones o procesos sobre los que se realizará la auditoría.
- El auditor interno debe tener un buen conocimiento de los requisitos y procesos involucrados en la auditoría de certificación.

3.21 Revisión por la alta dirección (Requisito 9.3)

3.21.1 General (Requisito 9.3.1)

La alta dirección y el comité que conforman a EML S.A.S. realizan una revisión trimestral del SGSI para garantizar su conveniencia, continuidad, vigencia, adecuación y efectividad.

3.21.2 Insumos para la revisión por la dirección (Requisito 9.3.2)

La revisión por la dirección comprende lo siguiente:

- ➔ El seguimiento de las acciones de revisiones previas.
- ➔ Cambios significativos internos y externos de la organización, relevantes para el SGSI.
- ➔ Cambios en las necesidades y expectativas de las partes interesadas que son relevantes para el SGSI.
- ➔ Los resultados de la retroalimentación sobre el desempeño de la Seguridad de la Información en la empresa:
    - ◆ No conformidades y acciones correctivas.
    - ◆ Resultados de auditorías internas y externas.
    - ◆ Resultados de métricas e indicadores.
    - ◆ Cumplimiento de los objetivos.
- ➔ Retroalimentación de las partes interesadas esta información se obtiene por medio de encuestas de clima laboral para la retroalimentación de los colaboradores, minutas de comité de seguridad, y un buzón de quejas y sugerencias habilitado en la página web para cualquier parte interesada externa, por medio del siguiente correo electrónico: eml@eml.co o monicafranco@eml.co
- ➔ Los resultados de la valoración y gestión de riesgos del SGSI y el estado del plan de tratamiento.
- ➔ Oportunidades de mejora continua.

3.21.3 Resultados de la revisión por la dirección (Requisito 9.3.3)

EML S.A.S genera la minuta de sesión de comité como información documentada donde incluye los resultados de la revisión y las decisiones para el mantenimiento y mejora continua del SGSI.

Mejora (Cláusula 10)

3.22 Mejora continua (Requisito 10.1)

EML S.A.S realiza acciones de mejora continua sobre la idoneidad, adecuación y efectividad del SGSI y deja registro de esto en los siguientes documentos:

- Procedimiento de Acciones Correctivas y de Mejora
- Plan de Tratamiento de Acciones Correctivas y de Mejora

3.23 No conformidad y acción correctiva (Requisito 10.2)

Al presentarse una no conformidad, la empresa:

- ➔ Toma las acciones para controlarla, corregirla y atender las consecuencias de ésta.

- ➔ Evalúa si es posible eliminar la causa de la no conformidad, mediante su revisión, determinación de sus causas y verificación de no conformidades similares.
- ➔ Implementa las acciones necesarias.
- ➔ Revisa la efectividad de las acciones realizadas.
- ➔ Realiza cambios sobre el SGSI, si es requerido.

La organización deja registro de esto en los siguientes documentos:

- Procedimiento de Acciones Correctivas y de Mejora
- Plan de Tratamiento de Acciones Correctivas y de Mejora
- Análisis Causa Raíz

EML S.A.S. asegura que las acciones correctivas aplicadas son acordes y proporcionales a las no conformidades que se encontraron.

4. Versionado

Elaborado por:	María Alejandra Zúñiga – líder en tecnología de la información
Aprobado por:	• Comité de Seguridad
Fecha de aprobación:	22/02/2024
Clasificación de esta información:	• Información Organizacional