1. Área responsable.

Sistemas de la Información.

2. Realizó.

- Oficial de Seguridad Informática (TISO).
- Sr. Business Process Specialist.
- Gerente Sr. de Sistemas de Información.

3. Autorizó.

- CEO.
- CTO.

4. Objetivo.

Establecer los principios generales y compromisos de la organización para proteger sus activos de información frente a amenazas internas o externas, deliberadas o accidentales, asegurando la confidencialidad, integridad y disponibilidad de la información conforme a los requisitos de la Norma ISO/IEC 27001:2022.

5. Alcance.

El Sistema de Gestión de Seguridad de la Información (SGSI) aplica a todos los procesos, activos, personas y tecnologías involucradas en el tratamiento de información dentro de la organización, incluyendo:

- Plataformas tecnológicas para la gestión de información interna.
- Desarrollos internos y tercerizados para automatizaciones e integraciones del negocio.
- Servicios de terceros contratados para el tratamiento de información.
- Oficinas físicas.
- Servicios en la nube dedicados a la interoperabilidad de plataformas internas.

La determinación y aplicación de los controles de seguridad para estos activos y procesos se encuentran detallados y formalizados en el documento **FT-89-SGE-SI DECLARACIÓN DE APLICABILIDAD (SOA) V1.0 16/01/2026**, el cual forma parte integral del presente alcance.

6. Políticas.

6.1. Roles y responsabilidades.

- **CEO:** Responsable de la seguridad de la información como parte del liderazgo organizacional para implementar el SGSI y la cultura de seguridad de la información.
- **CTO:** Responsable de la gestión de la infraestructura tecnológica y del cumplimiento de los requisitos técnicos del SGSI.

- **CFO:** Asegurar la asignación de recursos financieros necesarios para la seguridad de la información y la implementación del SGSI.
- **Head of People:** Responsable de asignar los recursos humanos necesarios para apoyar las responsabilidades dedicadas a las operaciones de ciberseguridad así como la capacitación necesaria en temas de seguridad de la información.
- **Gerente Sr de Sistemas de Información:** Responsable de la supervisión operativa del SGSI.
- **Oficial de Seguridad Informática (TISO):** Responsable técnico de la implementación de controles de seguridad de la información/ciberseguridad y de la gestión diaria del SGSI.
- **Sr Business Process Specialist:** Alinear los procesos de negocio con los controles del SGSI y apoyar en la gestión de riesgos operativos.
- **Comité de Seguridad de la Información:** Responsables de revisar y aprobar políticas, supervisar la implementación del SGSI y evaluar su eficacia.
- **Colaboradores:** Responsable de cumplir con las políticas y procedimientos de seguridad de la información aplicables a sus funciones.

6.2. Contexto de la Organización y Partes Interesadas.

La organización ha determinado en el **FT-42-SGE FODA SGC/SGSI (I)** los aspectos externos e internos que son relevantes para su propósito y que afectan a su capacidad para lograr los resultados previstos, además se han identificado las partes interesadas y sus requisitos dentro del **FT-41-SGE PARTES INTERESADAS SGC/SGSI (I).** Este análisis será revisado anualmente o ante cambios eventualmente significativos en la organización o su entorno.

6.3. Compromiso de la Alta Dirección.

La Alta Dirección, conformada por el CEO, CTO, CFO, Head of People y Gerente Senior de Sistemas de Información, se compromete a:

- Apoyar el establecimiento, implementación, mantenimiento y mejora continua del SGSI.
- Asegurar la integración de los requisitos del SGSI en los procesos de la organización.
- Cumplir con los requisitos aplicables, incluidos los legales, contractuales y regulatorios.
- Promover una cultura de seguridad de la información en toda la organización.
- Proporcionar los recursos necesarios para la implementación y mantenimiento del SGSI.
- Comunicar la importancia de una gestión eficaz de la seguridad de la información a la organización.

6.4. Cumplimiento legal.

La organización ha identificado las leyes y regulaciones aplicables en las jurisdicciones donde mantiene operaciones o relaciones comerciales, considerando su relevancia para los

objetivos del Sistema de Gestión de Seguridad de la Información (SGSI) y su impacto en el tratamiento de datos personales y la protección de la información. Este cumplimiento normativo forma parte integral de los compromisos asumidos por Tecnomotum y será objeto de revisión periódica o cuando se presenten cambios significativos en el marco legal o en las actividades de la organización.

- Tecnomotum reconoce la información personal como un activo crítico. En cumplimiento con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), la organización se compromete a garantizar la privacidad, integridad y disponibilidad de los datos de nuestros colaboradores, proveedores y clientes.

Para asegurar este cumplimiento dentro del SGSI, se establecen las siguientes directrices obligatorias:

- **Gobernanza y Responsabilidad:** Se designa a un responsable para supervisar el cumplimiento legal, gestionar las solicitudes de Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) y asegurar que el tratamiento se limite a las finalidades declaradas.

- **Transparencia (Aviso de Privacidad):** Todo tratamiento de datos personales debe estar respaldado por un Aviso de Privacidad integral, puesto a disposición del titular previo a la recolección de su información. En caso de tratarse de datos sensibles, financieros o patrimoniales, se deberá obtener el consentimiento expreso y por escrito.

- **Medidas de Seguridad:** Tecnomotum implementará controles técnicos, administrativos y físicos proporcionales al riesgo. Estas medidas no serán inferiores a las aplicadas a la información confidencial de la propia empresa y se alinearán con los controles establecidos por el SGSI.

- **Gestión de Terceros:** Toda transferencia de datos a proveedores o socios de negocio debe estar regulada mediante cláusulas contractuales de confidencialidad, seguridad y protección de datos, asegurando que el tercero asuma las mismas obligaciones de seguridad que Tecnomotum.

- **Ciclo de Vida y Retención:** Los datos personales se conservarán únicamente durante el tiempo necesario para cumplir con la finalidad del tratamiento y las obligaciones legales aplicables. Al finalizar dicho periodo, se procederá al bloqueo y posterior supresión segura de la información.

- **Respuesta a Incidentes:** Ante cualquier vulneración de seguridad que afecte significativamente los datos personales, se activará el Proceso de Respuesta a

Incidentes, notificando de manera inmediata a los titulares afectados y, de ser requerido, a las autoridades competentes.

6.5. Principios de Seguridad de la Información.

Tecnomotum reconoce el valor y significado de la Seguridad de la información que consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como la de los sistemas implicados en su tratamiento, dentro de una organización. Al igual que adopta los siguientes principios para gestionar la seguridad de la información:

- **Confidencialidad:** Garantizar que la información solo sea accesible por personas autorizadas.
- **Integridad:** Asegurar que la información y sus métodos de proceso sean exactos y completos.
- **Disponibilidad:** Asegurar que los usuarios autorizados tengan acceso a la información y a los activos asociados cuando sea necesario.

6.6. Objetivos de Seguridad de la Información.

Tecnomotum establece los siguientes objetivos medibles de seguridad de la información:

1. Garantizar la identificación y mitigación oportuna de vulnerabilidades en los activos tecnológicos, asegurando que los riesgos detectados sean atendidos dentro de los tiempos de respuesta establecidos por la organización.
2. Mantener una configuración de seguridad estandarizada y robusta en todos los sistemas y dispositivos, verificando constantemente su alineación con las guías de seguridad establecidas por la organización para reducir la superficie de ataque.
3. Asegurar que todo el personal reciba formación continua y sensibilización en materia de seguridad de la información, fomentando una cultura de prevención ante las amenazas actuales.
4. Garantizar que el acceso a los sistemas y aplicaciones institucionales esté protegido mediante mecanismos de autenticación seguros, restringiendo el uso de la información sólo a usuarios autorizados.
5. Asegurar una respuesta eficiente ante incidentes de seguridad, garantizando que los eventos detectados sean contenidos, analizados y cerrados en los tiempos definidos para minimizar el impacto operativo.
6. Mantener un proceso de revisión y auditoría constante sobre los controles de seguridad, asegurando el cumplimiento de los planes de evaluación aprobados y la mejora continua del sistema.
7. Garantizar que todos los proyectos de desarrollo de software incorporen controles y revisiones de seguridad desde su concepción hasta su despliegue, cumpliendo con las directrices definidas por la organización de desarrollo seguro.
8. Asegurar que todos los equipos de cómputo y dispositivos institucionales cuenten con herramientas de protección contra software malicioso activas y actualizadas para

prevenir infecciones y ataques externos.

9. Controlar la vigencia y seguridad de las credenciales de acceso mediante la rotación periódica de contraseñas, asegurando que el personal cumpla con los estándares de seguridad definidos para sus cuentas de usuario.

Estos objetivos serán medidos periódicamente y revisados anualmente por la Alta Dirección.

6.7. Gestión de riesgos.

La organización ha establecido y mantiene un proceso de gestión de riesgos de seguridad de la información que:

- Sigue la metodología documentada en el **PR-04-SGE GESTIÓN DE RIESGOS.**
- Establecer criterios para la aceptación de riesgos, considerando:
  - Impacto potencial en la confidencialidad, integridad y disponibilidad de la información.
  - Impacto financiero y reputacional.
  - Requisitos legales y regulatorios aplicables.
- Identificar, analizar, evaluar y tratar los riesgos de seguridad de la información.
- Documentar el resultado del proceso de gestión de riesgos.
- Revisar los riesgos al menos anualmente o ante eventuales cambios significativos.

6.8. Cumplimiento de los Controles del Anexo A.

La organización implementa y mantiene los controles de seguridad descritos en el Anexo A de la norma ISO/IEC 27001:2022, conforme a las directrices de ISO/IEC 27002:2022. Estos controles se aplican de acuerdo con la evaluación de riesgos y el tratamiento de riesgos documentado en el SGSI.

La selección y justificación de los controles aplicables y no aplicables se documenta en la **FT-89-SGE-SI DECLARACIÓN DE APLICABILIDAD (SOA) (REGISTRO) (I)** que es revisada y aprobada por la Alta Dirección al menos anualmente y debido a cambios significativos en el SGSI.

6.8.1. Controles específicos para la gestión del SGSI.

6.8.1.1. Gestión del control de acceso.

Tecnomotum implantará y mantendrá un marco de control de acceso basado en el principio de mínimo privilegio y la autenticación de toda entidad. Todo acceso a los sistemas de información y a los datos se controlará mediante procedimientos formales de registro, modificación y baja de usuarios.

Los derechos de acceso sólo se concederán previa aprobación documentada tanto del propietario del recurso como del equipo de Sistemas de la información.

La autenticación multifactor será obligatoria para todo acceso a sistemas y/o plataformas y acceso a cuentas privilegiadas. Se realizarán revisiones periódicas del acceso a los sistemas de información para garantizar que solo los responsables tengan acceso a los recursos y se validen los derechos a estos.

Las revisiones periódicas de los accesos se realizarán al menos semestralmente, con revocación inmediata de los derechos de acceso en caso de cese o cambio de función.

La organización mantendrá registros de auditoría de todos los cambios de control de acceso, con alertas automáticas de intentos de acceso sospechosos o escaladas de privilegios no autorizadas.

Las políticas de contraseñas aplicarán requisitos de autenticación fuerte, incluyendo longitud mínima, complejidad y cambios periódicos de contraseña, con controles técnicos que impidan la reutilización de contraseñas.

6.8.1.2. Seguridad física y ambiental.

La organización debe implantar y mantener controles de seguridad físicos y controles de seguridad física y ambiental apropiados para impedir el acceso físico no autorizado, daño, robo, compromiso o interferencia a los activos de información y a las instalaciones de procesamiento de la información. Los perímetros de seguridad estarán claramente definidos y protegidos mediante controles de seguridad por niveles que incluyan de acceso, cámaras de vigilancia y personal de seguridad cuando proceda.

Todos los accesos físicos se registrarán y supervisarán, con revisiones periódicas de los registros de acceso e investigación inmediata de los incidentes de seguridad.

Se aplicarán controles para proteger contra amenazas ambientales como incendios, inundaciones o cortes de electricidad, con pruebas y mantenimiento periódicos de todos los sistemas de protección.

Las zonas seguras estarán protegidas por controles de entrada adecuados para garantizar que sólo pueda acceder el personal con autorización previa considerando controles adicionales para las zonas que contengan información sensible o sistemas críticos.

6.8.1.3. Gestión y clasificación de activos.

La organización debe mantener un inventario exhaustivo de todos los activos de información incluidos los activos físicos y lógicos, con una propiedad clara y responsabilidades de seguridad definidas.

Todos los activos de información se clasifican en función de su sensibilidad, criticidad y requisitos legales utilizando el esquema de clasificación definido por la organización. Los propietarios de los activos serán responsables de garantizar que se apliquen los procedimientos de tratamiento en función del nivel de clasificación del activo.

El inventario de activos se revisará y actualizará periódicamente, con procesos formales de conciliación para identificar y abordar cualquier discrepancia. Se aplicarán procedimientos de tratamiento para protegerlos contra la divulgación, modificación o destrucción no autorizada a lo largo del ciclo de vida de los activos, incluido el almacenamiento seguro, transmisión y eliminación segura de los mismos.

6.8.1.4. Criptografía y gestión de llaves.

Tecnomotum implantará y mantendrá controles criptográficos para proteger la confidencialidad, integridad y autenticidad de la información durante todo su ciclo de vida. Todos los datos sensibles se cifran tanto en tránsito y en reposo utilizando algoritmos y protocolos de cifrado considerados robustos en materia de seguridad de la información.

La organización mantendrá una política formal de gestión de claves que cubra todo el ciclo de vida de la clave criptográfica, incluida la generación, distribución, almacenamiento, uso y destrucción. Las claves criptográficas estarán protegidas contra acceso no autorizado, pérdida y compromiso mediante mecanismos aplicables de almacenamiento seguro de claves.

Se llevarán a cabo evaluaciones periódicas de las implementaciones criptográficas para garantizar la alineación con las normas y mejores prácticas actuales del sector, con procedimientos documentados para la transición a controles criptográficos más estrictos cuando sea necesario.

6.8.1.5. Operaciones de seguridad.

Tecnomotum establecerá y mantendrá procedimientos operativos documentados para todas las instalaciones de procesamiento de información para asegurar operaciones correctas y seguras.

Se implementarán procedimientos de gestión de cambios para controlar todos los cambios en las instalaciones y sistemas de procesamiento de información, con los requisitos apropiados de pruebas, documentación y aprobación.

Los entornos de desarrollo, pruebas y operación estarán separados para reducir los riesgos de acceso o cambios no autorizados a los sistemas operativos.

Se implementarán controles de monitoreo de sistemas y seguridad para detectar actividades no autorizadas de procesamiento de información, con revisión y análisis regular de los registros del sistema.

Se implementará protección contra malware a través de un enfoque de defensa en profundidad que incluya protección de endpoints, filtrado de correo electrónico, filtrado web y capacitación regular en concientización de seguridad para todos los usuarios.

6.8.1.6. Desarrollo, mantenimiento y adquisición de sistemas.

Los requisitos de seguridad se identificarán e integrarán en todas las etapas del ciclo de vida del desarrollo de sistemas, desde la planificación y el diseño hasta la implementación y el mantenimiento.

Todos los sistemas nuevos o los cambios significativos en los sistemas existentes se someterán a pruebas de seguridad y a una revisión de seguridad formal antes de su despliegue en los entornos de producción.

Se seguirán los principios de desarrollo seguro, incluyendo la validación de entradas, la codificación de salidas y la gestión segura de sesiones.

Se llevarán a cabo evaluaciones de vulnerabilidades y pruebas de penetración periódicas en todos los sistemas, con la remediación oportuna de las vulnerabilidades identificadas en base a la evaluación de riesgos.

6.8.1.7. Gestión de proveedores.

La organización establecerá y mantendrá requisitos de seguridad de la información para las relaciones con los proveedores con el fin de mitigar los riesgos asociados con el acceso de los proveedores a los activos de la organización.

Los contratos o acuerdos formales incluirán requisitos de seguridad específicos, incluyendo las obligaciones de notificación de incidentes, los requisitos de protección de datos y las cláusulas de derecho de auditoría.

La prestación de servicios de los proveedores se supervisará y revisará periódicamente, y se llevarán a cabo evaluaciones formales de los controles de seguridad implementados por los proveedores al menos anualmente.

Los cambios en los servicios de los proveedores se gestionarán mediante procedimientos formales de gestión de cambios, y se realizarán evaluaciones de impacto para los cambios significativos.

6.8.1.8. Transferencia de Información.

Toda transferencia de información, ya sea dentro de la organización o con terceros externos, deberá realizarse mediante mecanismos seguros que aseguren la protección de la información en tránsito.
Los principios que se deberán aplicar son:

- Uso de cifrado adecuado (TLS, VPN, cifrado de archivos) en función de la clasificación y sensibilidad de la información.
- Control de accesos y autenticación previa para el intercambio de información sensible.
- Validación y autorización previa de los canales de transferencia utilizados, con preferencia por soluciones aprobadas por el área de seguridad de la información.
- Registro y trazabilidad de las transferencias de información relevantes, a través de sistemas de monitoreo o bitácoras de auditoría que permitan un seguimiento posterior si es necesario.
- Prohibición de uso de plataformas no autorizadas o personales para transferencias de datos corporativos.
- Responsabilidad de los usuarios en asegurar que la información transferida cumpla con las políticas internas de seguridad y privacidad.
- Aplicación de medidas correctivas en caso de incidentes relacionados con transferencias no autorizadas, incluyendo su reporte inmediato al área correspondiente y el seguimiento conforme a los procedimientos establecidos en el SGSI.

6.8.1.9. Configuración y Tratamiento Seguro de los Dispositivos Finales de los Usuarios.

Todos los dispositivos utilizados para acceder o gestionar información de la organización deberán configurarse siguiendo las mejores prácticas de seguridad:

- Aplicación de configuraciones seguras de acuerdo con guías internas y estándares de seguridad (CIS Benchmarks, Hardening Guides).

- Instalación y actualización de soluciones de protección contra malware y amenazas avanzadas (EDR).
- Habilitación de cifrado en almacenamiento local de los dispositivos (Full Disk Encryption).
- Gestión centralizada de dispositivos a través de soluciones MDM (Mobile Device Management) o EMM (Enterprise Mobility Management).
- Gestión de borrado seguro de información previa a la baja o reasignación de los dispositivos.
- Configuración y/o uso de herramienta para la prevención de fuga de información (DLP).

6.8.1.10. Seguridad de la red.

Las redes corporativas deberán estar protegidas mediante controles de defensa en profundidad, con especial atención a los siguientes aspectos:

- Segmentación de redes para separar entornos críticos, usuarios, y zonas expuestas a Internet.
- Configuración segura de dispositivos de red y protección perimetral (firewalls, proxies, IDS/IPS).
- Acceso remoto únicamente mediante VPN corporativa y autenticación multifactor (MFA).
- Monitorización continua del tráfico de red y detección de actividades anómalas.
- Prohibición de redes inalámbricas inseguras o no gestionadas.

6.8.1.11. Gestión de respaldo.

La gestión de respaldo deberán garantizar la disponibilidad e integridad de la información crítica:

- Definición de frecuencias de respaldo acorde a la criticidad de los sistemas, servicios o activos de información.
- Almacenamiento seguro de copias de respaldo en ubicaciones distintas o fuera de línea.
- Protección de las copias mediante cifrado, autenticación y controles de acceso.
- Verificaciones de la eficacia del proceso de respaldo.
- Registro y control de los medios de respaldo.
- Asignación clara de responsabilidades para la ejecución, monitoreo y verificación de los respaldos.
- Política de retención y eliminación segura de copias de respaldo, que defina los tiempos de conservación en función de criterios legales, operativos o

contractuales.

6.8.1.12. Clasificación y tratamiento de la información.

La información deberá clasificarse siguiendo un esquema corporativo que define los niveles de sensibilidad y criticidad, tales como:

- Información Pública.
- Información de Uso Interno.
- Información Confidencial.
- Información Restringida.

Cada clase de información tendrá definidos controles de acceso, mecanismos de protección y requisitos de manejo, almacenamiento, transferencia y eliminación seguros.

De igual forma, toda transferencia de información, ya sea interna o hacia partes externas, debe realizarse exclusivamente a través de canales autorizados que garanticen la Confidencialidad, Integridad y Disponibilidad. Es obligatorio el uso de mecanismos de cifrado robusto para datos en tránsito y la implementación de protocolos de autenticación mutua, especialmente cuando la información esté clasificada como Confidencial o Restringida. Queda estrictamente prohibido el uso de herramientas de intercambio no corporativas o medios físicos sin cifrar; asimismo, cualquier comunicación de datos críticos con terceros deberá estar respaldada por acuerdos de transferencia formalizados y cláusulas de confidencialidad vigentes.

6.8.1.13. Gestión de las vulnerabilidades técnicas.

La organización implementará un proceso continuo y proactivo de gestión de vulnerabilidades que incluya:

- Identificación y monitoreo de nuevas vulnerabilidades aplicables al entorno tecnológico.
- Evaluación de riesgos asociados a las vulnerabilidades detectadas.
- Priorización y tratamiento oportuno de las vulnerabilidades según criticidad.
- Aplicación de actualizaciones de seguridad y parches en plazos establecidos.
- Realización de escaneos periódicos de vulnerabilidades en infraestructuras y aplicaciones.

6.8.1.14. Desarrollo seguro.

Los procesos de desarrollo de software y evolución de aplicaciones deberán integrar prácticas de seguridad desde las etapas iniciales:

- Aplicación de metodologías DevSecOps.
- Definición de requisitos de seguridad en la fase de diseño.
- Análisis de código estático (SAST) y dinámico (DAST).
- Control de versiones y revisión de código fuente.
- Gestión segura de dependencias y librerías de terceros.
- Pruebas de seguridad antes de la puesta en producción.
- Segregación de ambientes de desarrollo, pruebas y producción.

6.8.1.15. Gestión de continuidad del negocio.

La organización desarrollará, mantendrá y probará regularmente planes de continuidad del negocio para asegurar la disponibilidad continua de las instalaciones críticas de procesamiento de información.

Se llevarán a cabo análisis de impacto en el negocio para identificar las funciones críticas del negocio y sus dependencias de los sistemas de información.

Se definirán los objetivos de tiempo de recuperación **(RTO)** y los objetivos de punto de recuperación **(RPO)** para todos los sistemas y procesos críticos dentro de la herramienta BIA.

Se implementarán procedimientos de copia de seguridad regulares con pruebas periódicas de la restauración de las copias de seguridad.

Se identificarán y mantendrán instalaciones de procesamiento alternativas para respaldar los requisitos de continuidad del negocio, con pruebas regulares de los procedimientos.

6.9. Gestión de Incidentes de Seguridad.

La organización establece un proceso definido para la gestión de incidentes de seguridad que considera lo siguiente:

- Canales y mecanismos para el reporte de incidentes de seguridad.
- Roles y responsabilidades en la gestión de incidentes.
- Proceso de clasificación, respuesta, contención, investigación y resolución de incidentes.
- Métricas para la evaluación de la eficacia de la gestión de incidentes.
- Proceso para documentar lecciones aprendidas y mejoras.

Todos los incidentes de seguridad deben ser reportados inmediatamente siguiendo el procedimiento establecido.

6.10. Evaluación del Desempeño y Mejora Continua.

La organización:

- Evalúa periódicamente el desempeño y la eficacia del SGSI mediante:
  - Monitorización y medición de los objetivos de seguridad.
  - Auditorías internas programadas según el "Plan de Auditorías Internas".
  - Revisiones por la Dirección al menos una vez al año.
- Documenta los resultados de estas evaluaciones y las acciones resultantes.
- Implementa acciones correctivas para las no conformidades identificadas.
- Se compromete a la mejora continua de la idoneidad, adecuación y eficacia del SGSI.

6.11. Requisitos Documentales.

El SGSI incluye la siguiente documentación obligatoria:

- Política de Seguridad de la Información.
- Alcance del SGSI.
- Objetivos de seguridad de la información.
- Metodología y resultados de la evaluación y tratamiento de riesgos.
- Declaración de Aplicabilidad.
- Políticas y procedimientos específicos necesarios para la operación del SGSI.
- Registros requeridos por la norma ISO/IEC 27001:2022.

La documentación se gestiona según el **PR-01-SGE CONTROL DE INFORMACIÓN DOCUMENTADA (I)** que establece los controles para la creación, actualización, revisión, aprobación, distribución y control de versiones.

6.12. Difusión y Concienciación.

Esta política será comunicada a todas las partes interesadas pertinentes, incluyendo empleados, contratistas y proveedores. Además, se establecerán programas de formación y concienciación en seguridad de la información que incluirán:

- Formación inicial para nuevos empleados.
- Formación y concienciación periódica para todo el personal.
- Formación especializada para roles específicos de seguridad.
- Comunicaciones regulares sobre amenazas emergentes y buenas prácticas.

6.13. Revisión de la Política.

La presente política, al igual que todos los documentos relacionados del SGSI (Políticas, Procesos, Instrucciones de trabajo u cualquier otro formato aceptado) será revisada anualmente, como parte de la Revisión por la Dirección, o ante cambios significativos en la

organización, en el contexto del SGSI o en los requisitos aplicables, para asegurar su continua idoneidad, adecuación y eficacia.

6.14. Tratamiento de Exenciones y Excepciones .

Con carácter general, todos los usuarios, proveedores y terceros que acceden a la información o a los activos tecnológicos de la organización deberán cumplir con lo establecido en la Política de Seguridad de la Información.

No obstante, se reconoce que pueden existir situaciones excepcionales en las que el cumplimiento estricto de determinados controles de seguridad no sea viable o adecuado por razones justificadas de negocio, operativas o técnicas.

En estos casos, se deberá seguir el siguiente procedimiento:

- Toda solicitud de exención o excepción a esta política deberá presentarse de forma documentada, indicando:
  - La descripción del control o requisito al que se solicita excepción.
  - La justificación detallada del motivo de la excepción.
  - El periodo de vigencia estimado de la excepción.
  - Los riesgos asociados derivados de no aplicar el control correspondiente.
  - Las medidas compensatorias que se proponen para mitigar dichos riesgos.
- La solicitud deberá ser evaluada y analizada por el Responsable de Seguridad de la Información (TISO) o el Comité de Ciberseguridad.
- En caso de ser aprobada, la excepción se documentará formalmente, definiendo:
  - El alcance y período de vigencia.
  - Las condiciones asociadas y controles alternativos.
  - El responsable de su revisión y seguimiento.
- Las excepciones tendrán carácter temporal y deberán revisarse periódicamente, quedando sujetas a revocación si cambian las circunstancias que motivaron su aprobación.
- Las excepciones no documentadas y no aprobadas se considerarán incumplimientos de la presente política.

6.15. Cumplimiento de políticas, reglas y estándares de seguridad de seguridad de la información

Se garantiza que todos los activos de información, procesos y personas operen de acuerdo con de las políticas, reglas y estándares de seguridad de la información establecidos por la organización mediante los siguientes lineamientos de cumplimiento:

a) **Revisiones de Gestión** (Cumplimiento Administrativo)

Los propietarios de los procesos y jefes de área deberán realizar revisiones periódicas para asegurar que el personal a su cargo cumple con las políticas de seguridad.

Frecuencia: Al menos una vez al año o cuando ocurran cambios significativos en el proceso.
Metodología: Verificación de registros de capacitación, firmas de acuerdos de confidencialidad y cumplimiento de protocolos operativos.
Reporte: Cualquier desviación debe documentarse y notificarse al Oficial de Seguridad de la Información (TISO).

b) **Revisiones de Cumplimiento Técnico** (Hardening y Configuración)

El equipo de TI y Ciberseguridad verificará que los sistemas están configurados según los estándares de seguridad establecidos.

Verificación Técnica: Se utilizarán herramientas automáticas, así como procesos manuales para validar configuraciones de firewalls, sistemas operativos, bases de datos y aplicaciones.
Pruebas de Vulnerabilidad: Se realizarán escaneos de vulnerabilidades con una frecuencia trimestral para identificar fallos técnicos que contravengan las políticas.
Pruebas de penetración: Se llevará a cabo un test de penetración anual por parte de un tercero independiente para validar la eficacia de los controles.

c) Auditoría Interna

Para asegurar que las políticas y normas técnicas se cumplen, el programa de auditoría interna integrará los siguientes elementos:

Planificación basada en Riesgos: El programa de auditoría dará prioridad a las áreas donde el incumplimiento de las políticas del control 5.36 represente un mayor riesgo para la confidencialidad, integridad o disponibilidad de la información.
Independencia y Objetividad: Los auditores internos no auditan su propio trabajo. Esto garantiza que la revisión del cumplimiento de las políticas sea imparcial y crítica.
Criterios de Auditoría: Se utilizarán como referencia las políticas internas y el propio Anexo A.

6.16. Sanciones por incumplimiento.

El incumplimiento de las disposiciones establecidas en esta Política de Seguridad de la Información se considerará una infracción de las normas internas de la organización y podrá conllevar la aplicación de medidas disciplinarias o contractuales, en función de la gravedad del hecho y de lo dispuesto en la normativa interna y en la legislación vigente.

Los procedimientos a seguir en estos casos serán los siguientes:

- Cualquier incumplimiento detectado deberá ser comunicado al Responsable de Seguridad de la Información o al área de People, siguiendo los canales de reporte establecidos.
- El incidente o incumplimiento será evaluado por las áreas competentes (Seguridad de la Información, People, Legal) para determinar:
  - La naturaleza del incumplimiento.
  - La intencionalidad o negligencia asociada.
  - El impacto o daño causado a la organización.
  - El historial previo del infractor.
- En función de la evaluación realizada, se podrán aplicar las siguientes acciones correctivas o sancionadoras:
  - Formación o concientización adicional en materia de seguridad.
  - Advertencia formal por escrito.
  - Suspensión temporal de accesos o funciones.
  - Sanciones disciplinarias conforme a la normativa laboral.
  - Rescisión de la relación contractual, en los casos más graves.
  - Acciones legales, si el incumplimiento constituye delito o infracción legal.
- Todas las acciones correctivas o sancionadoras deberán respetar la normativa laboral, contractual y de protección de datos aplicable.
- La reincidencia o la resistencia deliberada a cumplir con las normas de seguridad podrá agravar la sanción correspondiente.

7. Anexos.

- **FT-42-SGE FODA SGC/SGSI (I)**
- **FT-41-SGE PARTES INTERESADAS SGC/SGSI (I)**
- **PR-04-SGE GESTIÓN DE RIESGOS (I)**
- **FT-89-SGE-SI DECLARACIÓN DE APLICABILIDAD (SOA) (REGISTRO) (I)**
- **PR-01-SGE CONTROL DE INFORMACIÓN DOCUMENTADA (I)**