Política General de Seguridad de la Información de Escala 24x7

1. Introducción.

Escala 24x7 se compromete a proteger la confidencialidad, integridad y disponibilidad de toda la información que crea, recibe, mantiene y transmite, en apoyo de sus objetivos estratégicos y operacionales. Esta política establece las directrices y los principios fundamentales para la seguridad de la información en Escala 24x7, y el compromiso de implementar, mantener y mejorar continuamente un "Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001:2022.

2. Objetivo.

Los objetivos de esta política alineados a la estrategia de la organización, son:

- Establecer un marco robusto y adaptable para la implementación, operación, seguimiento, revisión, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con los requisitos de la norma ISO/IEC 27001:2022.
- Definir, asignar y comunicar de manera clara las responsabilidades y autoridades en materia de seguridad de la información en todos los niveles de la organización.
- Establecer e implementar los principios, políticas y directrices fundamentales para asegurar la protección integral de los activos de información de la organización, considerando su confidencialidad, integridad y disponibilidad.
- Garantizar el cumplimiento continuo de los requisitos legales, regulatorios y contractuales aplicables a la seguridad de la información y la privacidad de los datos, estableciendo los mecanismos necesarios para su identificación, seguimiento y evaluación.
- Integrar la seguridad de la información como un valor fundamental en la cultura organizacional, promoviendo la conciencia, la capacitación y la participación activa de todos los miembros.

3. Alcance.

Esta política aplica a toda la información de Escala 24x7 en sus operaciones globales, y a todos los empleados, contratistas, proveedores y otras partes

interesadas que acceden, utilizan o gestionan la información y los sistemas de la organización, incluyendo el alcance del SGSI:

- Servicios de Consultoría, migración a entornos cloud y modernización de aplicaciones.
- Prácticas DevOps y desarrollo de aplicaciones cloud-native.
- Seguridad en la nube, Security Assessments, Security Epics, Cloud Foundations y cumplimiento.
- Gestión de infraestructura, Resiliencia y optimización de costos.
- Análisis de datos, Inteligencia Artificial (IA), Machine Learning (ML) e IA generativa sobre plataformas AWS.

4. Principios de Seguridad de la Información.

La seguridad de la información en Escala 24x7 se basa en los siguientes principios fundamentales:

- **Confidencialidad:** La información solo será accesible a personas autorizadas. Se implementarán controles para proteger la información sensible contra la divulgación no autorizada, tanto en reposo como en tránsito.
- **Integridad:** La información será precisa y completa, y estará protegida contra modificaciones no autorizadas. Se implementarán controles para mantener la integridad de los datos durante su ciclo de vida.
- **Disponibilidad:** La información y los sistemas estarán disponibles para los usuarios autorizados cuando y donde sea necesario para sus actividades laborales. Se implementarán controles para asegurar la continuidad del negocio y la recuperación ante desastres, considerando la dependencia de los servicios SaaS.
- **Cumplimiento:** Las actividades de la organización se llevarán a cabo en cumplimiento con las leyes, regulaciones y obligaciones contractuales aplicables relacionadas con la seguridad de la información y la privacidad de los datos, incluyendo aquellas específicas para los proveedores de servicios en la nube.
- **Responsabilidad:** La seguridad de la información es responsabilidad de todos los empleados y partes interesadas. Se definirán y comunicarán claramente los roles y las responsabilidades específicas.
- **Concientización:** Se fomentará una cultura de seguridad de la información a través de la formación y la concientización continua de los empleados sobre los riesgos y las mejores prácticas.

- **Mejora Continua:** El SGSI se revisará y mejorará continuamente para adaptarse a las nuevas amenazas, vulnerabilidades y cambios en el entorno operativo y tecnológico, incluyendo la evolución de los servicios SaaS.

5. Acuerdos de Confidencialidad y Privacidad (NDA)

Escala 24x7 exige la firma de Acuerdos de Confidencialidad y Privacidad de la Información (NDA) en la contratación de todo su personal (colaboradores) y contratistas antes de que obtengan acceso a cualquier activo de información. Estos acuerdos deben estar formalmente suscritos y se darán a conocer a las partes para garantizar su cabal entendimiento y cumplimiento.

Este control es obligatorio para asegurar la protección legal de la confidencialidad y privacidad de la información manejada por la organización, extendiendo la responsabilidad sobre los datos a todos los individuos que presten servicios a Escala 24x7.

6. Responsabilidades.

- **Alta Dirección:**
    - Promover la creación y generación de políticas y controles relacionados a Seguridad de la Información de Escala 24x7 con el fin de proteger la información de los grupos de interés: clientes, proveedores, partners, colaboradores, entre otros..
    - Proporcionar los recursos necesarios para la implementación y el mantenimiento del SGSI.
    - Promover una cultura de seguridad de la información en toda la organización.
    - Proporcionar directrices y revisar periódicamente los objetivos planteados por Escala 24x7 en materia de Seguridad de la información que permitan su mejora continua.
    - Asegurar que se implemente un proceso efectivo de gestión de riesgos de seguridad de la información.
    - Promover lineamientos para que la organización cumpla con todas las leyes, regulaciones y estándares relevantes en materia de seguridad de la información.

- **Equipo de Seguridad de la Información:**
    - Liderar el ciclo de vida completo del Sistema de Gestión de Seguridad de la Información (SGSI), desde su concepción y desarrollo hasta su implementación, mantenimiento continuo y supervisión rigurosa para asegurar su eficacia y alineación con los objetivos organizacionales.
    - Proporcionar asesoramiento experto y estratégico a la dirección sobre todos los aspectos relacionados con la seguridad de la información, facilitando la toma de decisiones informadas y la comprensión de los riesgos y oportunidades.
    - Orquestar y armonizar las iniciativas y actividades de seguridad de la información en todas las áreas de la organización, promoviendo una cultura de seguridad cohesiva y garantizando la integración de la seguridad en los procesos de negocio.
    - Identificar, evaluar, tratar y monitorear los riesgos de seguridad de la información de manera proactiva, implementando estrategias y controles efectivos para proteger los activos de la organización.
    - Velar por la adhesión estricta a las políticas, normas y estándares de seguridad de la información establecidos, así como a las regulaciones y leyes aplicables, asegurando un entorno de operación seguro y conforme.
    - Planificar, coordinar y ejecutar la respuesta ante incidentes de seguridad de la información, desde la detección y análisis hasta la contención, erradicación, recuperación y lecciones aprendidas, minimizando el impacto en la organización.
- **Gerentes y Líderes de Área:**
    - Asegurar que el personal bajo su supervisión maneje y proteja la información de acuerdo con las políticas y normativas de seguridad establecidas por la organización.
    - Reportar de manera oportuna y precisa cualquier incidente de seguridad o incumplimiento de las normativas identificadas.

- Contribuir activamente en las evaluaciones de riesgos de seguridad de la información y participar en las revisiones periódicas para fortalecer la postura de seguridad de la organización.

- **Empleados, contratistas y otras partes interesadas:**

  - Conocer, comprender y cumplir con las políticas, normas y procedimientos de seguridad de la información establecidos por la organización.
  - Proteger sus nombres de usuario, contraseñas y otros métodos de autenticación, evitando compartirlos y asegurándose de que sean robustos.
  - Utilizar los sistemas, la información y los activos de la organización de manera ética, legal y de acuerdo con las políticas de uso aceptable.
  - Reportar de inmediato a los canales designados por la organización, cualquier actividad sospechosa, evento de seguridad o vulnerabilidad detectada.
  - Asegurar la seguridad de los dispositivos que utilizan para acceder a la información y los sistemas de la organización, aplicando las medidas de seguridad recomendadas.
  - Seguir las mejores prácticas de seguridad en todas las interacciones con los sistemas y la información, como tener precaución con los enlaces y archivos adjuntos, y evitar el acceso a sitios web no seguros.
  - Manejar la información sensible con el cuidado adecuado, evitando su divulgación no autorizada y asegurando su almacenamiento y transmisión segura.
  - Cuando sea requerido, participar en los programas de formación y concienciación sobre seguridad de la información para mantenerse informados sobre las amenazas y las mejores prácticas.
  - En caso de un incidente de seguridad, deben cooperar plenamente con las investigaciones llevadas a cabo por la

organización. El canal oficial para el reporte de incidentes es la Mesa de Ayuda de Escala 24x7.

7. Programa de Formación y Concientización en Seguridad y Privacidad de la Información

El desarrollo y mantenimiento de una cultura de seguridad proactiva es fundamental para proteger los activos de Escala 24x7. Para ello, se establece un Programa de Formación y Concientización obligatorio y periódico dirigido a todos los empleados y contratistas. Este programa está estructurado de la siguiente manera:

- **Frecuencia**: Se llevará a cabo una capacitación formal y obligatoria al menos de forma trimestral, además de la formación de inducción inicial para nuevos ingresos.
- **Alcance**: El programa cubre pero no se limita a los temas que se mencionan a continuación:
    - **Creación de Conciencia sobre Amenazas:** El personal aprenderá a reconocer los peligros más comunes, incluyendo el phishing (correos electrónicos fraudulentos), el malware (software malicioso) y las técnicas de ingeniería social (manipulación psicológica para obtener información).
    - **Desarrollo de Habilidades de Protección:** Se enseñarán prácticas seguras para la rutina diaria, tales como el uso de contraseñas robustas y únicas, la identificación de enlaces sospechosos, el manejo seguro de dispositivos y la correcta clasificación de la información.
    - **Minimización del Riesgo de Fuga de Datos:** La formación instruirá a los empleados sobre cómo proteger sus credenciales de acceso y evitar ataques diseñados para sustraer información confidencial, garantizando el manejo cuidadoso de la información sensible.
    - **Fomento de una Cultura de Seguridad y Responsabilidad:** Se promoverá la seguridad de la información como una responsabilidad de todos, no solo del Equipo de Seguridad de la Información, convirtiendo a cada empleado en la primera línea de defensa de la organización.
- **Cumplimiento Regulatorio:** El programa de formación asegurará el cumplimiento continuo de los requisitos legales, regulatorios y contractuales , incluyendo aquellos específicos para la protección y privacidad de datos, tales como el GDPR y otras normativas aplicables .

Se garantizará que todo el personal entienda y cumpla con las regulaciones de ciberseguridad exigidas por las industrias pertinentes.

8. Cumplimiento.

- El cumplimiento de esta Política de Seguridad de la Información, así como de las políticas, procedimientos y estándares relacionados, es una obligación para todos los colaboradores, contratistas y terceros que accedan a los activos de información de la empresa. El incumplimiento de estas directrices puede acarrear la aplicación de medidas disciplinarias, las cuales serán determinadas de acuerdo con la gravedad de la infracción y las normativas internas vigentes. Adicionalmente, es importante destacar que el incumplimiento de las políticas de seguridad de la información puede generar consecuencias legales y regulatorias para la empresa y para los individuos involucrados, de acuerdo con la legislación aplicable. Para ello, Escala 24x7 tiene establecido un procedimiento disciplinario formal dentro del Sistema de Gestión de Seguridad de la Información.
- Esta Política de Seguridad de la Información estará accesible para su consulta en el Sistema de Gestión de Seguridad de la Información (SGSI) y en el portal web de la empresa, asegurando su amplia disponibilidad para todos los interesados. Asimismo, esta política forma parte integral del programa de capacitaciones de la organización, garantizando que los usuarios comprendan sus responsabilidades y obligaciones en materia de seguridad de la información. Cualquier modificación o actualización que se realice a esta política será comunicada de manera oportuna a través de los canales de comunicación establecidos por la empresa.

9. Mejora continua

Escala 24x7 realiza análisis continuo de los incumplimientos, no conformidades o hallazgos identificados en auditorías internas / externas u otras fuentes, en pro de mejorar de forma continua los controles que rigen su Sistema de Gestión de Seguridad de la Información. Este ciclo de mejora permitirá identificar la causa raíz e implementar acciones correctivas / preventivas y/o reportar a las autoridades competentes, de ser necesario.

10. Políticas relacionadas.

En la Política de Seguridad de la Información de Escala 24x7 han sido consideradas aquellas políticas que proporcionan principios y guía en aspectos específicos de la seguridad de la información, y que se alinean con los objetivos y estrategias del negocio, como lo son: Política de segregación de funciones, Clasificación de la información, Gestión de identidades, Plan de Continuidad del Negocio (BCP), Programa de Capacitación en Seguridad, Acuerdos de Confidencialidad y No Divulgación, Gestión de incidentes, Política de seguridad de la información en las relaciones con los proveedores, Políticas de privacidad, Código de ética, Confidencialidad, Anticorrupción y Soborno, Teletrabajo, Procesos disciplinarios, Gestión de accesos, Eliminación de la información y Gestión de cambios.

11. Control de Proveedores

Escala 24x7 a través del área de Compliance es responsable de la revisión y evaluación inicial de todos los proveedores para verificar el cumplimiento con nuestros estándares de seguridad y normativas. Para los proveedores críticos, esta gestión se eleva a un ciclo anual de revisión, donde solicita y revisa el informe de control interno SOC 2 siempre y cuando el proveedor disponga de dicho informe, a fin de determinar su nivel de cumplimiento, dejando como evidencia de la revisión, un informe que incluye las conclusiones, el reporte SOC 2 del proveedor y los planes de acción requeridos en caso de identificar falencias. En su defecto se podrá solicitar cumplimiento de otras normativas o estándares del mercado.

12. Otros documentos y/o estándares de seguridad relacionados:

- Norma ISO/IEC 27001:2022.
- Leyes de protección de datos personales GDPR.
- Gestión de Riesgos - ISO/IEC 27005.
- Continuidad del Negocio - ISO 22301.

13. Revisión.

Esta política será revisada y actualizada periódicamente por la Alta Dirección de Escala 24x7, al menos anualmente o cuando ocurran cambios significativos en la organización, sus operaciones, la tecnología utilizada o el

entorno legal y regulatorio, para asegurar su continua adecuación, eficacia y alineación con los objetivos de la organización.

Aprobado por: Harold Barber DocuSigned by: Harold Barber FFA4D554670A426...

Cargo: COO & CFO

Versión 8

Fecha de Aprobación: 10/24/2025 | 18:49:24 PDT

Próxima Revisión: Octubre 2026