Política de Seguridad de la Información (Pública)

Área de GRC & Ciberseguridad

01/10/2025

Versión 1.0

Aviso de confidencialidad

Versiones del documento

Versión	Fecha	Autor	Descripción
1.0	01/10/2025	Área GRC & Ciberseguridad	Creación de la política

Distribución del documento

Versión	Destinatario	Organización
1.0	Dirección Área de Ciberseguridad Área de TI, BSS IT	SAMY

Contenido

1. Compromiso de la organización

En SAMY, la seguridad de la información es un principio estratégico y una prioridad empresarial. Nuestra misión es garantizar la confidencialidad, integridad y disponibilidad de los datos de clientes, empleados y socios, apoyando la continuidad de negocio y generando confianza en todas nuestras operaciones.

Estamos comprometidos a cumplir con las mejores prácticas internacionales (ISO/IEC 27001:2022) y con la normativa legal vigente, incluyendo el Reglamento General de Protección de Datos (RGPD).

2. Principios

- **Confidencialidad**: acceso a la información únicamente por personas autorizadas.
- **Integridad**: protección frente a alteraciones no autorizadas de datos o sistemas.
- **Disponibilidad**: servicios y sistemas accesibles de forma segura cuando se necesitan.
- **Legalidad y ética:** cumplimiento estricto de la legislación aplicable y códigos éticos de la organización.
- **Mejora continua**: revisión constante de las medidas de seguridad para adaptarlas a nuevas amenazas.

3. Medidas estratégicas de seguridad

- **Gobernanza de seguridad:** políticas, roles y responsabilidades definidos y supervisados por la Dirección.

- **Gestión de riesgos:** identificación, análisis y mitigación de riesgos de ciberseguridad y continuidad de negocio.

- **Protección tecnológica:** uso de firewalls, sistemas de detección y prevención de intrusiones (IDS/IPS), cifrado en tránsito y reposo, y soluciones avanzadas de protección en endpoints y servidores.

- **Gestión de accesos:** controles de acceso basados en roles, autenticación multifactor y segregación de privilegios.

- **Protección de datos personales:** cumplimiento estricto de la normativa de privacidad y principios de minimización de datos.

- **Continuidad y resiliencia:** planes de contingencia y recuperación ante desastres, con pruebas regulares.

- **Relación con terceros:** proveedores y colaboradores sujetos a los mismos estándares de seguridad y evaluados periódicamente.

- **Concienciación y formación**: programas de capacitación continua en ciberseguridad para todo el personal.

4. Roles y responsabilidades

La organización ha definido un conjunto de roles y asociado responsabilidades para cada uno de ellos, así como para los distintos puestos de la organización

4.1. Dirección General

- Aprueba y respalda la política de seguridad de la información.
- Asigna los recursos necesarios para la implementación y mejora continua del sistema de gestión de seguridad.
- Garantiza que la seguridad de la información es un pilar estratégico de la organización.

4.2. Responsable de Seguridad de la Información (CISO / GRC)

- Lidera la estrategia de seguridad y cumplimiento normativo (ISO 27001, NIS2, RGPD).
- Supervisa la identificación y gestión de riesgos de seguridad.
- Coordina la prevención, detección y respuesta ante incidentes de ciberseguridad.
- Informa regularmente a la Dirección sobre el estado de cumplimiento y riesgos críticos.

4.3. Dirección de IT / Sistemas

- Asegura que la infraestructura tecnológica se mantenga protegida mediante controles de seguridad actualizados.
- Implementa medidas de protección en redes, servidores y aplicaciones.
- Colabora con el área de seguridad en la gestión de accesos, continuidad y resiliencia tecnológica.

4.4. Dirección de RRHH y Legal

- Integra la seguridad en los procesos de gestión de personas y en las relaciones laborales.
- Garantiza que las obligaciones legales en materia de protección de datos personales se cumplen (RGPD y normativa nacional).
- Promueve la formación y concienciación de los empleados en materia de seguridad.

4.5. Dirección Financiera y Comercial

- Gestiona la información económica y contractual de manera confidencial y segura.
- Aplica controles adecuados en las relaciones con clientes, proveedores y socios.
- Se asegura de que las decisiones financieras y comerciales respetan las políticas de seguridad y compliance.

4.6. Resto de personal

- Es responsable de cumplir con las políticas y procedimientos de seguridad establecidos.
- Debe proteger la información a la que accede en el ejercicio de sus funciones.
- Tiene la obligación de reportar de inmediato cualquier incidente o sospecha de brecha de seguridad a través de los canales habilitados.

5. Respuesta ante incidentes

SAMY dispone de procesos para la detección, notificación, gestión y recuperación ante incidentes de seguridad.

- Se incentiva la notificación temprana de cualquier sospecha de incidente.
- Contamos con canales de reporte dedicados para clientes, partners y empleados.
- Todos los incidentes son investigados y tratados con la máxima prioridad, comunicando impactos relevantes a las partes interesadas según la normativa vigente.

6. Mejora continua

- Revisión periódica de las políticas de seguridad.
- Adaptación a la evolución tecnológica y a nuevas amenazas.
- Mantener la confianza de los clientes y proteger la continuidad de los servicios.

7. Conformidad y validez

La organización ha confiado la implantación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) en el proveedor externo Qualoom Expertise Technology.

El proveedor actuará como responsable del mantenimiento operativo del SGSI de la organización, realizando tareas de actualización documental, seguimiento de controles y asesoramiento técnico.

La organización será el titular del SGSI, de su supervisión y responsable último de la seguridad de la información conservando la responsabilidad última sobre las decisiones, aprobación de políticas y cumplimiento de la norma ISO 27001.

Por ello, estando la Dirección junto con los representantes de las áreas interesadas alineados con el alcance de la presente política, autorizando su difusión así como su aplicación interna y externa si así procediera, otorgan conformidad a la misma a través de su firma.

En Madrid a [...] de octubre de [...]

Política	Organización	Responsable	Área	Firma
Revisado y aprobado por	SAMY	Marcos García Bermejo	IT	

SIMY