Política General de Seguridad de la Información

Documento:	**Política General de Seguridad de la Información**
Empresa:	Innovatech Soluciones, S.L.
Versión:	1.0
Fecha de Aprobación:	18 de agosto de 2025
Propietario:	Director de Seguridad de la Información (CISO)
Próxima Revisión:	18 de agosto de 2026

1. Propósito y Alcance

1.1. Propósito

El propósito de esta política es establecer el marco de gestión para proteger la información de **Innovatech Soluciones, S.L.**, sus clientes y sus socios contra todo tipo de amenazas, ya sean internas o externas, deliberadas o accidentales. El objetivo es asegurar la continuidad del negocio, minimizar los riesgos y maximizar el retorno de las inversiones y las oportunidades de negocio.

1.2. Alcance

Esta política es de obligado cumplimiento para todos los empleados, contratistas, personal temporal y terceros que tengan acceso a los sistemas de información y a los activos de Innovatech Soluciones, S.L. Aplica a toda la información, independientemente de su formato o del medio en el que se encuentre.

2. Objetivos de la Seguridad de la Información

Innovatech Soluciones, S.L. se compromete a preservar:

- **Confidencialidad:** Asegurando que la información sea accesible únicamente por el personal autorizado.
- **Integridad:** Salvaguardando la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** Garantizando que los usuarios autorizados tengan acceso a la información y a sus activos asociados cuando lo requieran.

3. Roles y Responsabilidades

- **Director de Seguridad de la Información (CISO):** Es el máximo responsable de la definición, implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información (SGSI).
- **Departamento de TI:** Es responsable de implementar y operar los controles técnicos de seguridad definidos en esta política.
- **Todos los Empleados:** Son responsables de comprender y cumplir con esta política y los procedimientos de seguridad asociados en su trabajo diario. Deben informar de cualquier incidente de seguridad que detecten.

4. Clasificación de la Información

Toda la información gestionada por Innovatech Soluciones, S.L. debe ser clasificada según su nivel de sensibilidad. Se establecen las siguientes categorías:

- **Pública:** Información que puede ser divulgada sin restricciones.
- **Interna:** Información de uso exclusivo para los empleados de la empresa. Su divulgación no autorizada tendría un impacto moderado.
- **Confidencial:** Información sensible cuya divulgación no autorizada podría causar un daño significativo a la empresa, sus clientes o socios.
- **Restringida:** Información altamente sensible (secretos comerciales, datos estratégicos) cuya divulgación tendría un impacto grave. El acceso está limitado a roles específicos.

5. Control de Acceso

El acceso a los sistemas y a la información de Innovatech Soluciones, S.L. se basará en los principios de **mínimo privilegio** y **necesidad de saber**.

- Todo usuario debe tener una identificación única.
- Se prohíbe el uso de cuentas compartidas.
- Las contraseñas deben cumplir con una política de complejidad (longitud mínima de 12 caracteres, uso de mayúsculas, minúsculas, números y símbolos) y ser cambiadas periódicamente.
- El acceso remoto debe realizarse a través de una Red Privada Virtual (VPN) segura.

6. Seguridad Física y del Entorno

Las oficinas y centros de datos de Innovatech Soluciones, S.L. deben estar protegidos por controles de acceso físico adecuados. Se implementarán medidas para proteger los equipos contra robo, daño y acceso no autorizado. Las áreas que procesan información sensible tendrán controles de acceso más estrictos.

7. Gestión de Activos

Todos los activos de información (hardware, software, datos) deben estar inventariados y tener un propietario asignado. Los empleados son responsables de la protección de los activos que se les asignen, como los ordenadores portátiles. El uso de dispositivos personales (BYOD) para acceder a información corporativa debe ser aprobado por el departamento de TI.

8. Criptografía

La información clasificada como **Confidencial** o **Restringida** debe ser cifrada tanto en reposo como en tránsito. Se utilizarán algoritmos de cifrado robustos y aprobados por la industria.

9. Gestión de Incidentes de Seguridad

Cualquier empleado que detecte o sospeche de un incidente de seguridad de la información debe notificarlo inmediatamente al Departamento de TI a través del canal establecido. Se ha definido un procedimiento de respuesta a incidentes para asegurar que se gestionen de manera rápida y eficaz.

10. Cumplimiento

Innovatech Soluciones, S.L. se compromete a cumplir con toda la legislación aplicable, como el Reglamento General de Protección de Datos (RGPD), y con las obligaciones contractuales

en materia de seguridad.

11. Revisión y Mantenimiento de la Política

Esta política será revisada anualmente o siempre que se produzcan cambios significativos en el entorno de negocio o tecnológico.