# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

OFITECO, es una ingeniería internacional de origen español creada en el año 1971 y con presencia permanente en España, Perú, Argelia e Israel; y experiencia en otros países, entre ellos: Portugal, Canadá, Arabia Saudí, Colombia, Ecuador, Chile, Bolivia, Argentina, Uruguay, Costa Rica, Guatemala, Panamá, Honduras, Polonia, Georgia y Albania.

OFITECO tienen como misión el crecimiento sostenido y rentable como organización y el incremento de su posición de liderazgo a nivel mundial en la prestación de servicios de valor añadido en la redacción de proyectos de ingeniería civil, instrumentación, auscultación, supervisión y dirección de obras de infraestructuras de obras públicas y control de calidad de materiales.

**OFITECO** considera que la Seguridad de la Información debe ser una prioridad en la organización. Para ello la **Dirección** asume la responsabilidad de la Gestión de la Seguridad de la Información de los procesos y actividades que se desarrollan en las instalaciones de la Sede Central y con la total participación de los mandos directivos y de todo el personal se compromete a:

- ✓ Mantener y revisar periódicamente un **Sistema de Gestión de Seguridad de la Información** (SGSI), conforme con la norma internacional ISO 27001, cuyo alcance es aplicable al sistema de alojamiento en los centros de procesamiento de datos que sustentan las actividades de desarrollo de sistemas inteligentes de tráfico y transporte, sistemas de seguridad, así como el control de procesos interno y externo.

- ✓ **Mejorar de forma permanente la eficacia** del SGSI implantado, aplicando las acciones determinadas tras analizar los resultados del desempeño de la seguridad de la información y la información obtenida en las auditorías y en las revisiones periódicas.

- ✓ Impulsar una cultura proactiva de mejora gestionando los **riesgos y oportunidades** coherentes con el contexto y partes interesadas de la organización.

- ✓ Establecer, planificar y revisar **objetivos** coherentes con la presente Política, teniendo en cuenta los requisitos de seguridad de la información aplicables, los resultados de la apreciación y tratamiento de los riesgos, y realizar el seguimiento de las acciones que se determinen para su consecución.

- ✓ Garantizar la **confidencialidad** de la información en todo momento.

- ✓ Asegurar la **integridad** de la información de todos los procesos que la gestionan, procesan y almacenan.

- ✓ Garantizar la **disponibilidad** de la información mediante las adecuadas medidas de respaldo y continuidad del negocio.

- ✓ **Gestionar** de forma lógica y eficaz cualquier **incidente** o debilidad que pueda comprometer o haya comprometido la confidencialidad, integridad y/o disponibilidad de la información.

- ✓ Asegurar que todo el personal dentro del alcance del SGSI dispone de la adecuada **formación** y **concienciación** en materia de seguridad de la información.

- ✓ Cumplir con los requisitos legales y contractuales aplicables en materia de seguridad de la información.
  - o REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
  - o Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
  - o Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual
  - o Real Decreto-ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual
  - o Real Decreto 3/2010, de 8 de enero, de desarrollo del Esquema Nacional de Seguridad modificado por el Real Decreto 951/2015, de 23 de octubre.

La estructura de nuestro sistema de gestión de forma que sea fácil de comprender. Nuestro sistema de gestión tiene la siguiente estructura:

- Procedimientos
- Políticas
- Normas y códigos

Nuestra política se desarrolla aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad: a través del procedimiento PG-001 Gestión de Seguridad de la Información.

b) Análisis y gestión de los riesgos: a través del procedimiento PG-001 Gestión de Seguridad de la Información

c) Gestión de personal: a través del procedimiento PG-001 Gestión de Seguridad de la Información

d) Profesionalidad: a través del procedimiento PG-001 Gestión de Seguridad de la Información

e) Autorización y control de los accesos: a través de los documentos Código de conducta informática, IT-SIS-205-PROC-USER-VPN_Acceso portal VP y IT-SIS-206-PROC-USER-VPN-DT_Acceso portal VPN – DT.

f) Protección de las instalaciones: a través del documento Código de conducta informática

g) Adquisición de productos: a través del procedimiento PG-110 Compras y subcontratación.

h) Seguridad por defecto: a través del procedimiento PG-001 Gestión de Seguridad de la Información

i) Integridad y actualización del sistema: a través del procedimiento PG-001 Gestión de Seguridad de la Información

j) Protección de la información almacenada y en tránsito: a través del del documento Código de conducta informática

k) Prevención ante otros sistemas de información interconectados mediante el Código de conducta informática, la Política de comunicación y difusión corporativa, el Protocolo de tratamiento de información confidencial, la IT-SIS-214-PROC-USER - Intercambio información-upload y la IT-SIS-215-PROC-USER - Intercambio información-FTP

l) Registro de actividad: a través del procedimiento PG-001 Gestión de Seguridad de la Información

m) Incidentes de seguridad: a través de las IT-SIS-212-PROC-USER_ CAU SICE e IT-SIS-500-PROC-OPER

n) Continuidad de la actividad: a través de los documentos PE-DT-014 - Plan De Contingencia Sistema Informáticos DT e IT-SIS-500_PROC-OPER-PLAN_CONTINGENCIA_SSI

o) Mejora continua del proceso de seguridad: a través del procedimiento E PG-001 Gestión de Seguridad de la Información

**Roles y responsabilidades**

La gestión de nuestro sistema se encomienda al Responsable de Gestión y el sistema estará disponible en nuestro sistema de información en un repositorio, al cual se puede acceder según los perfiles de acceso concedidos según nuestro procedimiento en vigor de gestión de los accesos. Estos principios son asumidos por la Dirección, quien dispone los medios necesarios y dota a sus empleados de los recursos suficientes para su cumplimiento, plasmándolos y poniéndolos en público conocimiento a través de la presente Política Integrada de Sistemas de Gestión. Los roles o funciones de seguridad definidos son:

| Función | Deberes y responsabilidades |
|---|---|
| Responsable de la información | ✓ Tomar las decisiones relativas a la información tratada<br>✓ Determinar los requisitos de la información tratada |
| Responsable de los servicios | ✓ Coordinar la implantación del sistema<br>✓ Mejorar el sistema de forma continua<br>✓ Determinar los requisitos de los servicios tratados |

| | |
|---|---|
| Responsable de la seguridad | ✓ Determinar la idoneidad de las medidas técnicas<br>✓ Proporcionar la mejor tecnología para el servicio<br>✓ Determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. |
| Responsable del sistema de información | ✓ Coordinar la implantación del sistema<br>✓ Mejorar el sistema de forma continua<br>✓ Operar el sistema de información, atendiendo a las medidas de seguridad determinadas por el responsable de seguridad. |

Esta definición se completa en los perfiles de puesto y en los documentos del sistema. El procedimiento para su designación y renovación será la ratificación en el comité de seguridad. El comité para la gestión y coordinación de la seguridad es el órgano con mayor responsabilidad dentro del sistema de gestión de seguridad de la información, de forma que todas las decisiones más importantes relacionadas con la seguridad se acuerdan por este comité. Los miembros del comité de seguridad de la información son:

- Responsable de la información.
- Responsable de los servicios.
- Responsable de la seguridad.
- Responsable del sistema.

Estos miembros se designan por el comité, único órgano que puede nombrarlos, renovarlos y cesarlos. El comité de seguridad es un órgano autónomo, ejecutivo y con autonomía para la toma de decisiones y que no tiene que subordinar su actividad a ningún otro elemento de nuestra empresa. La toma de decisiones se realizará mediante la votación de los miembros y con el único requisito de mayoría simple. En caso de conflicto entre los diferentes responsables, éste será resuelto por el superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Responsable de Seguridad. Está política se complementa con el resto de las políticas, procedimientos y documentos en vigor para desarrollar nuestro sistema de gestión

La Dirección de **OFITECO**, confía en que cada persona de la Empresa comprenda la trascendencia de los compromisos indicados, los asuma y los incorpore a su trabajo, formando parte de la gestión general y diaria.

**Jürgen Fleitz**
**Director General**

Alcobendas (Madrid), 05 de julio de 2021