OFITECO

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, Colombia, Guatemala y Argelia; representación en Iraq y Qatar; y experiencia en otros países, entre ellos: Angola, Arabia Saudí, Honduras, Israel, Panamá, Polonia y Uruguay.

OFITECO tiene 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 infraestructura 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.

- Preservar la **confidencialidad** de la información en todo momento.

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

- Mantener la **trazabilidad** de la información en todo momento.

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

- **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.

    - 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
    - Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
    - Real Decreto Legislativo 1/ 1996, de 12 de abril, Ley de Propiedad Intelectual
    - Real Decreto-ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual
    - Ley 5/2014, de 4 de abril, que regula la actividad de la Seguridad Privada.
    - Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, establecido en el artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Nuestro sistema de gestión tiene la siguiente estructura:

- Procedimientos
- Políticas
- Normas y códigos

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 y la IT-IS-101-PROC-OPER-COMITÉ_SEGURIDAD_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 y la IT-IS-101-PROC-OPER-COMITÉ_SEGURIDAD_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 Guía de usuarios de los Sistemas de Información (VINCI), IT-SIS-205-PROC-USER-VPN.
f) Protección de las instalaciones: a través del documento Guía de usuarios de los Sistemas de Información (VINCI).
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 Guía de usuarios de los Sistemas de Información (VINCI).
k) Prevención ante otros sistemas de información interconectados mediante: la Guía de usuarios de los Sistemas de Información (VINCI), la IT-SIS-100-PROC-USER-CODIGO-CONDUCTA-INFORMATICA, la Política de comunicación y difusión corporativa, la Política de Protección de Datos y Tratamiento de Información Confidencial y Sensible.
l) Registro de actividad: a través del procedimiento PG-001 Gestión de Seguridad de la Información.
m) Incidentes de seguridad: a través de la IT-SIS-212-PROC-USER_ CAU_SICE e IT-SIS-500-PROC-OPER.
n) Continuidad de la actividad: a través de los documentos IT-SIS-500_PROC-OPER-PLAN_CONTINGENCIA_SSI, IT-SIS-529-PROC-OPER-PLAN_RESPUESTA_INCIDENTES_SEGURIDAD y la IT-SIS-525-PROC-OPER-GESTION_INCIDENTES_SEGURIDAD_GDPR.
o) Mejora continua del proceso de seguridad: a través del procedimiento PG-001 Gestión de Seguridad de la Información.

El sistema estará disponible en un repositorio, al cual se puede acceder según los perfiles de acceso concedidos según nuestro procedimiento de gestión de los accesos.

El procedimiento IT-IS-101-PROC-OPER-COMITE_SEGURIDAD_INFORMACION recoge toda la información relativa al **Comité de Seguridad de la Información,** en adelante **CSI**.

Los roles o funciones de seguridad definidos, que se completan en los perfiles de puesto y los documentos del sistema, son:

Función	Deberes y responsabilidades
Responsable de Seguridad de la Información / CISO	Determinar la idoneidad de las medidas técnicas Proporcionar la mejor tecnología para el servicio Determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
Responsable del Sistema de Información / CIO	Coordinar la implantación del sistema. Mejorar el sistema de forma continua Operar el sistema de información, atendiendo a las medidas de seguridad determinadas por el responsable de seguridad.

El procedimiento para su designación y renovación será la ratificación en el **CSI,** único órgano que puede nombrarlos, renovarlos y cesarlos. El Comité de Seguridad es el órgano con mayor responsabilidad dentro del sistema de gestión de seguridad de la información, de forma que las decisiones más importantes relacionadas con la seguridad se acuerdan por este Comité. Los miembros del Comité de Seguridad son:

- Responsable de Seguridad de la Información
- Responsable de Sistemas de Información
- Responsable de Protección de datos
- Responsable de RRHH
- Responsable de Cumplimiento normativo
- Responsable de Asesoría jurídica
- Responsable de Desarrollo de negocio
- Responsable de Aprovisionamiento
- Responsable de Calidad
- Responsable de Administración y Finanzas
- Responsable de Dirección Técnica

El **CSI** es un órgano autónomo y ejecutivo 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 de la Alta Dirección.

Está política se complementa con el resto de las políticas, procedimientos y documentos en vigor para desarrollar nuestro sistema de gestión.

Todos los miembros de la Organización tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del **CSI** disponer los medios necesarios para que la información llegue a los afectados.

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

Alcobendas, 1 de septiembre de 2024

Jürgen Fleitz
Director General