Introducción

La misión de **IRONTEC** es ofrecer soluciones tecnológicas abiertas e innovadoras, gracias a un equipo motivado y cualificado, que ayude a los/las clientes/as a ser más competitivos/as mediante un modelo de negocio creciente, sostenible e íntegro que genere riqueza en el entorno.

Nuestra visión es ser la empresa tecnológica de referencia que destaca por su calidad al servicio del negocio de clientes/as satisfechos/as.

En **IRONTEC**, la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

Consciente de las necesidades actuales, **IRONTEC** implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

Esto implica que los departamentos dentro del alcance deben aplicar las medidas mínimas de seguridad exigidas a todos los activos bajo su responsabilidad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los sistemas administrados por **IRONTEC** y los desarrollos de software realizados serán llevados a cabo con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

La Política de Seguridad de la Información de **IRONTEC** se encuentra soportada por políticas, normas y procedimientos específicos que guiarán el manejo adecuado de la información. Se establecen políticas de seguridad de la información fundamentadas en los dominios y objetivos de control de la norma internacional UNE-EN ISO IEC 27001, la cual

nos permite identificar y minimizar los riesgos a que está expuesta nuestra información y sus procesos de gestión.

IRONTEC establece, define y revisa unos objetivos dentro de su Sistema de Gestión de Seguridad de la Información (SGSI) encaminados a mejorar su seguridad, entendiéndola como la conservación de la confidencialidad, disponibilidad e integridad de su información, así como de los sistemas que la soportan, aumentando la confianza de clientes y clientas, personal y otras partes interesadas; junto con el cumplimiento de todos los requisitos legales, reglamentarios y contractuales que le sean de aplicación.

IRONTEC, establece la función de Seguridad de la Información en la Entidad, con el objetivo de:

1. Minimizar el riesgo en las funciones más importantes y críticas
2. Cumplir con los principios de seguridad de la información
3. Cumplir con los principios de la función administrativa
4. Mantener la confianza de sus clientes y clientas, socios y personal
5. Apoyar la innovación tecnológica
6. Implementar el sistema de gestión de seguridad de la información ajustado a las necesidades y dimensión de la entidad
7. Proteger los activos de información
8. Establecer las políticas e instrucciones en materia de seguridad de la información
9. Garantizar la continuidad del negocio frente a incidentes

Para el desarrollo del SGSI nos hemos basado en el ciclo PDCA, desde la planificación, la realización de las acciones planificadas, la comprobación de cómo se han llevado a cabo y finalmente la implementación de los cambios pertinentes para lograr una mejora continua y minimizar el riesgo de futuros fallos.

Todo el personal interno, empresas proveedoras, y en general quienes tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información de **IRONTEC**, deben adoptar los contenidos del presente documento y en los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

Alcance

El diseño, implantación y mantenimiento del SGSI se apoyará en los resultados de un proceso continuo de análisis y gestión de riesgos del que se derivan las actuaciones a desarrollar en materia de seguridad dentro del alcance de su sistema, que es:

- Registro y mantenimiento de dominios y certificados SSL
- Provisión y mantenimiento de servidores dedicados, máquinas virtuales, infraestructura cloud y almacenamiento.
- Gestión de copias de seguridad
- Desarrollo e ingeniería de software

de acuerdo a la declaración de aplicabilidad vigente.

Responsabilidad

La responsabilidad general de la seguridad de la información recaerá sobre la persona Responsable de Gestión del Sistema de Seguridad de la Información, que contará con el CISO (Director de Seguridad de la Información) como parte de su equipo, siendo la responsabilidad última de la Dirección como máximo responsable del SGSI.

Datos de carácter personal

IRONTEC trata datos de carácter personal. El documento de seguridad, al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y las personas responsables correspondientes. Todos los sistemas de información de **IRONTEC** se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de

Seguridad. En concreto, se atenderá a lo dispuesto por el Reglamento UE 2016/679 y la Ley Orgánica 3/2018 sobre Protección de Datos Personales.

Marco legal y regulatorio

El marco legal y regulatorio en el que desarrollamos nuestras actividades es:

- 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
- 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
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- REGLAMENTO (UE) 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Reglamento Europeo eIDAS).
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de

Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.

- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

Propiedad intelectual

Se protegerá adecuadamente la propiedad intelectual de **IRONTEC**, tanto propia como la de terceros (derechos de autor de software o documentos, derechos de diseño, marcas registradas, patentes, licencias, código fuente, entre otros). El material registrado con derechos de autor no se debe copiar sin la autorización del propietario, siguiendo la Ley de Propiedad Intelectual.

Liderazgo y compromiso de la dirección

La Dirección de **IRONTEC** se compromete a facilitar y proporcionar los recursos necesarios para el establecimiento, implantación, mantenimiento y mejora del SGSI de la entidad, así como a demostrar liderazgo y compromiso respecto a éste, a través de la constitución del Comité de Calidad y Seguridad que tendrá la responsabilidad de:

- Asegurar el establecimiento de la presente política y los objetivos de la seguridad

de la información, y que estos sean compatibles con la estrategia de **IRONTEC** de fomento del software libre en la sociedad

- Asegurar la integración y el cumplimiento de los requisitos aplicables del SGSI en los procesos de la entidad
- Asegurar que los recursos necesarios para el SGSI estén disponibles
- Comunicar la importancia de una gestión de la seguridad eficaz y conforme con los requisitos del SGSI
- Asegurar que el SGSI consigue los resultados previstos
- Dirigir y apoyar a las personas para contribuir a la eficacia del SGSI
- Promover la mejora continua

La Dirección de **IRONTEC** tendrá potestad de modificar la Política de Seguridad de la Información de acuerdo con las necesidades de revisión establecidas periódicamente o a la aplicabilidad de las mismas.

Obligaciones del personal

El personal de **IRONTEC** tiene la obligación de conocer esta Política de Seguridad de la Información, que es de obligado cumplimiento dentro del alcance identificado, siendo responsabilidad del Comité de Calidad y Seguridad disponer los medios necesarios para que la información llegue a los afectados y las afectadas.

Se espera que todas las personas de **IRONTEC** se rijan por el SGSI definido y cumplan sus funciones y obligaciones en materia de seguridad de la información, y en concreto que reporten los incidentes en materia de seguridad utilizando las directrices establecidas por **IRONTEC** y mantengan la confidencialidad debida, y las buenas prácticas en el manejo de datos de carácter personal, de equipos y de contraseñas.

Las personas con responsabilidad en el desarrollo de software y uso, operación o administración de sistemas TIC dentro del alcance recibirán formación para desarrollo seguro de aplicaciones y el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. Se establecerá un programa de concienciación continua para atender a cada integrante de **IRONTEC**, en particular a las nuevas incorporaciones.

Roles

En IRONTEC hemos definido roles para nuestro sistema de información certificado en el Esquema Nacional de Seguridad. Los roles o funciones de seguridad definidos son:

FUNCIÓN	DEBERES Y RESPONSABILIDADES
Responsable de la información	Tomar las decisiones relativas a la información tratada
Responsable de los servicios	Coordinar la implantación del sistema Mejorar el sistema de forma continua
Responsable de la seguridad	Determinar la idoneidad de las medidas técnicas Proporcionar la mejor tecnología para el servicio
Responsable del sistema	Coordinar la implantación del sistema Mejorar el sistema de forma continua Implantación, gestión y mantenimiento de las medidas de seguridad.
Dirección	Proporcionar los recursos necesarios para el sistema Liderar el sistema

Esta definición de deberes y responsabilidades se completa en los perfiles de puesto y en los documentos del sistema Registro de responsables, roles y responsabilidades.

Comité de Seguridad

El comité de seguridad de IRONTEC es el órgano con mayor responsabilidad dentro del sistema de gestión de seguridad de la información para ENS y está formado por el responsable de la información, el responsable del servicio, el responsable de seguridad y el responsable de los sistemas de información. 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

La gestión de la seguridad ENS se encomienda al responsable de seguridad que informará al comité de seguridad ENS de las necesidades de la emisión de políticas y procedimientos complementarios a las políticas de seguridad corporativa para asegurar el cumplimiento de la normativa española.

Estos miembros se designan por el Comité de dirección, único órgano que puede nombrarlos, renovarlos y cesarlos.

Estructuración de la documentación del sistema

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

Políticas de seguridad

La presente política de seguridad se complementa con el resto de políticas de seguridad de la información, y en especial con las relativas a:

a) Organización e implantación del proceso de seguridad

b) Análisis y gestión de los riesgos

c) Gestión de personal

d) Profesionalidad

e) Autorización y control de los accesos

f) Protección de las instalaciones

g) Adquisición de productos

h) Seguridad por defecto

i) Integridad y actualización del sistema

j) Protección de la información almacenada y en tránsito

k) Prevención ante otros sistemas de información interconectados

l) Registro de actividad

m) Incidentes de seguridad

n) Continuidad de la actividad

o) Mejora continua del proceso de seguridad

Terceras partes

Las terceras partes relacionadas con **IRONTEC**, dentro del alcance, firman con la empresa un acuerdo que protege los activos de **IRONTEC** y la información intercambiada.

Cuando **IRONTEC** utilice servicios o ceda información a terceras partes, se les hará

partícipes de esta Política de Seguridad. Dicha tercera parte quedará sujeta a las obligaciones establecidas en esta Política, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.