POLÍTICA DE **SEGURIDAD DE ZITU INFORMATIKA S.L.**

- ENTRADA EN VIGOR -

Esta Política de Seguridad es efectiva desde la fecha de aprobación y hasta que sea reemplazada por una nueva Política.

INTRODUCCIÓN

ZITU INFORMATIKA S.L. (en adelante, "ZITU") sustenta el cumplimiento de sus objetivos en el uso de los sistemas y servicios de Tecnologías de la Información y las Comunicaciones (TIC). Por tanto, dichos sistemas deben ser gestionados con el máximo rigor y responsabilidad, aplicando las medidas necesarias para protegerlos frente a posibles riesgos que pudieran materializarse comprometiendo la disponibilidad, integridad, confidencialidad, autenticidad y/o trazabilidad.

El propósito de la gestión de la seguridad en ZITU es asegurar la fiabilidad de los datos y la continuidad operativa de los servicios a través de un enfoque preventivo que incluya la supervisión constante de las actividades y la capacidad de responder eficazmente ante cualquier incidente de seguridad. Los sistemas y servicios TIC deben mantenerse protegidos frente a amenazas en constante evolución capaces de afectar a las dimensiones de seguridad y para ello, resulta esencial adoptar una estrategia y compromiso firme en la seguridad, orientada a garantizar la continuidad, calidad y protección de los servicios prestados. Dado el contexto, los procesos y activos de información en ZITU deben ser conformes con el conjunto de medidas y requisitos establecidos por el RD 311/2022, de 3 de mayo; por el que se regula el Esquema Nacional de Seguridad (ENS).

Todo el personal debe cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. En consecuencia, ZITU debe estar preparada para prevenir, detectar, reaccionar y recuperarse ante incidentes.

PREVENCIÓN

El personal que interviene en el uso, gestión o administración de los sistemas de información debe prevenir y evitar cualquier circunstancia que pueda afectar a cualquier dimensión de seguridad. Para ello, ZITU implementa las medidas de seguridad exigidas por el ENS y cualesquiera controles adicionales que se identifiquen a través del análisis y evaluación de amenazas y riesgos. De igual forma, los roles, responsabilidades y obligaciones en materia de seguridad que sean asignados al personal, se definen, comunican y documentan de manera clara y accesible. Con la finalidad de garantizar el cumplimiento preventivo, resulta necesario:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

DETECCIÓN

Tomando en cuenta que los servicios son susceptibles de degradarse como consecuencia de incidentes, resulta imprescindible monitorizar de forma continua la operación de los sistemas y servicios con el fin de detectar a tiempo cualquier anomalía o desviación que pueda afectar a los niveles de prestación establecidos; estableciendo mecanismos de detección, análisis y reporte que notifiquen a los responsables designados de forma regular y cuando se produzcan desviaciones.

RESPUESTA

Los incidentes de seguridad son gestionados adecuadamente a través de los mecanismos necesarios para asegurar un óptimo tratamiento. Además, se contemplan protocolos para el intercambio de información relacionada con los incidentes tomando en consideración a los Equipos de respuesta a Emergencias Informáticas (CERT).

RECUPERACIÓN

Puesto que se debe garantizar la disponibilidad de los servicios críticos, se identifican y analizan las necesidades, los requisitos y las capacidades del negocio, especialmente en aquellos servicios cuya operación dependa de las TIC; aumentando así la resiliencia de los sistemas ante los incidentes.

ALCANCE

Esta Política tiene su aplicación en "*El sistema de información que da soporte a las infraestructuras, servicios y procesos para el desarrollo de software, según Declaración de Aplicabilidad vigente*". De esta manera, aplica a todos los sistemas TIC de ZITU y a todos sus miembros, sin excepciones.

SISTEMA DE INFORMACIÓN

Para garantizar que el proceso de seguridad es controlado, actualizado y mejorado de forma continua, se implanta y documenta un Sistema de Información. De esta forma, el contenido de la Política de Seguridad, así como los procedimientos, guías y registros complementarios forman parte de la documentación controlada en ZITU.

FINALIDAD DE ZITU COMO ORGANIZACIÓN

MISIÓN	Desarrollar soluciones de software seguras y personalizadas que impulsen la transformación digital de nuestros clientes, garantizando la protección y confidencialidad de la información.
VISIÓN	Consolidarnos como empresa de referencia en el desarrollo de software seguro y de confianza, certificada en el Esquema Nacional de Seguridad, ofreciendo servicios tecnológicos innovadores y alineados con las mejores prácticas en ciberseguridad.
VALORES	· Seguridad: protegemos la información de nuestros clientes como un activo esencial. · Confianza: trabajamos con transparencia y responsabilidad. · Innovación: mejoramos continuamente nuestros procesos y servicios. · Compromiso: impulsamos el cumplimiento normativo y la calidad del servicio. · Colaboración: fomentamos el trabajo en equipo y la mejora continua.

MARCO NORMATIVO (*)

Marco	Resumen
Reglamento (UE) 2016/679 (RGPD)	La normativa aplicable establece obligaciones para la protección de datos personales y la privacidad de las personas, define derechos y responsabilidades para quienes gestionan información, e impone medidas de seguridad para garantizar las distintas dimensiones de seguridad de la información. Asimismo, regula la prestación de servicios electrónicos y el comercio en línea, y pretende proteger los derechos de propiedad intelectual sobre obras, programas y contenidos, asegurando su uso legítimo y la salvaguarda de los derechos de autores y titulares.
Ley Orgánica 3/2018 (LOPDGDD)	
Real Decreto 311/2022, Esquema Nacional de Seguridad (ENS)	
Ley 34/2002, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE) (Revisión vigente desde 23 de Enero de 2025)	
Real Decreto Legislativo 1/1996, de Propiedad Intelectual (y modificaciones posteriores del texto refundido)	

(*) Sin perjuicio del marco normativo identificado, se tendrán en cuenta las modificaciones y derogaciones de dicha normativa que afecten a esta Política de Seguridad. Además, ZITU establece un proceso documentado en su Sistema de Información específico para la identificación y evaluación de requisitos legales.

ORGANIZACIÓN DE LA SEGURIDAD

COMITÉ DE SEGURIDAD		
Rol (ENS)	**Designación**	**Cargo / Puesto**
Responsable de la Información	Iñaki Ugarteburua	CEO
Responsable de Seguridad	Iñigo Sanz	Responsable de Sistemas
Responsable del Servicio	Aitor Alkorta	Responsable de Proyecto
Responsable del Sistema	Iñigo Sanz	Responsable de Sistemas

ROLES: FUNCIONES Y RESPONSABILIDADES (*)

Responsable de la Información

- Asumir la responsabilidad última de cualquier negligencia o error que conlleve un incidente.
- Establecer los requisitos de seguridad sobre la información.
- Categorizar los sistemas.
- Determinar los niveles de seguridad de la información.
- Determinar niveles de seguridad en cada dimensión.
- Facilitar los recursos necesarios para la respuesta ante incidentes.
- Adoptar las medidas necesarias sobre los datos personales.

Responsable del Servicio

- Asumir la responsabilidad sobre el uso que se haga de los servicios y de su protección.
- Establecer los requisitos de seguridad del servicio.
- Asegurar el tratamiento de los datos personales.
- Planificar, gestionar y colaborar en la identificación y aprobación de los riesgos.
- Proteger el uso de los servicios.

Responsable de Seguridad

- Participar en la elaboración y revisión (cuando proceda) de políticas, procedimientos, guías, normativas y cualquier documentación controlada del Sistema de Información.
- Promover la formación y concienciación en materia de seguridad de la información en la ZITU, garantizando la participación y la eficacia de dichas acciones.
- Categorizar el Sistema, determinar el apetito de riesgo y realizar (o revisar, según necesidad) la evaluación de riesgos y el tratamiento de estos.
- Reportar al CEO las decisiones e incidentes (y eventos que se consideren relevantes) en materia de seguridad.
- Facilitar y comunicar de forma regular al Comité de Seguridad las actualizaciones pertinentes del sistema.

Responsable del Sistema

- Tomar las decisiones operativas en relación con la arquitectura y mantenimiento del sistema.
- Tomar parte en la elaboración de la documentación operativa sobre seguridad.
- Monitorizar el Sistema de Información
- Reportar periódicamente al resto de responsables los cambios, avances y/o estado de los sistemas, así como del Sistema de Información.
- Solicitar autorización del Responsable de la Información y/o del Servicio para determinadas tareas recogidas en la documentación del Sistema de Información. (*)

(*) Excepcionalidad en la asignación de roles

Dado el contexto de ZITU y debido a la ausencia de recursos humanos para la separación de los roles de Responsable del Sistema y Responsable de Seguridad, se aplican medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades previsto en el artículo 11 del ENS. Dichas medidas compensatorias se evidencian en el Sistema de Información.

COMITÉ DE SEGURIDAD

El Comité de Seguridad es la herramienta para atender las inquietudes de la dirección y los diferentes departamentos y procesos de ZITU, garantizando la coordinación entre los distintos roles de seguridad con la finalidad de mantener una comunicación fluida del estado de la seguridad. Asimismo, los miembros del comité participan, según necesidad, en la aprobación de la normativa de seguridad, liderando la definición y aprobación de la Política, que es revisada periódicamente (al menos anualmente y siempre que se produzcan cambios). Además, promueve la planificación de las auditorías necesarias para verificar el cumplimiento de ZITU con los requisitos aplicables. En términos generales, el Comité de Seguridad debe velar por la seguridad de la información en todos los procesos y proyectos de ZITU en todas sus fases (planificación, operación, monitorización, evaluación…).

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad la revisión anual de esta Política de Seguridad y la propuesta de revisión o mantenimiento de esta. La Política será aprobada por el CEO de ZITU y ampliamente difundida entre las partes interesadas.

DATOS DE CARÁCTER PERSONAL

ZITU solo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y estos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, se adoptan las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso. Se mantienen actualizados los registros de actividad, así como la inclusión de nuevos tratamientos derivados ad hoc.

GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política de Seguridad deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad define las metas, expectativas y modo de gestión en relación con la seguridad en ZITU. Asimismo, de dicha política emanan distintas normativas y/o políticas, fichas de proceso, instrucciones técnicas, guías y registros; que forman parte del Sistema de Información de ZITU. La información recogida en los citados documentos estará disponible a las partes interesadas internas y externas que lo precisen, según el caso.

OBLIGACIONES DEL PERSONAL

Todos los miembros de ZITU deben conocer y cumplir esta Política de Seguridad y cualquier otro documento que forme parte del Sistema de Información, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a todas las partes afectadas.

Se establece un plan de formación y concienciación continua que implica a todos los miembros de ZITU, adaptando los contenidos y recursos según las necesidades de cada puesto. Las personas con responsabilidad en el uso, operación o administración de sistemas TIC reciben formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar sus funciones. Dicha formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

TERCERAS PARTES

Cuando ZITU preste servicios a otros organismos o maneje información de otras entidades, se les hará partícipes de esta Política de Seguridad, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

En el caso que ZITU utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de cualquier otro documento controlado referido a la normativa que atañe a dichos servicios o información. Esta tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias; además, se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política. Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad y del Responsable del Sistema que precise los riesgos en que se incurre y la forma de tratarlos que debe ser aprobado por el CEO de ZITU.