POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. Objeto y alcance

ZUNIBAL reconoce plenamente las implicaciones en términos de seguridad de la información asociadas a su operación y su compromiso con las partes interesadas. La finalidad fundamental de esta política es asegurar el compromiso para la debida salvaguarda de los activos de información y la continuidad de los servicios ofrecidos, al contar con la capacidad necesaria para prevenir, detectar, responder y recuperarse ante posibles incidentes de seguridad. Con este fin, la organización adopta las medidas de seguridad necesarias para mantener un nivel de riesgo que se considere aceptable. Igualmente, reconoce la importancia de monitorear el desempeño de los servicios, analizar las vulnerabilidades identificadas y establecer respuestas efectivas a los incidentes.

Es responsabilidad de ZUNIBAL asegurar que la seguridad se encuentre integrada en todas las etapas del ciclo de vida de los sistemas de información. Esto abarca desde la concepción hasta la retirada del servicio, incluyendo decisiones relativas a la adquisición y las actividades operativas. Los requisitos de seguridad vinculados a cada fase son identificados y considerados en la planificación y desarrollo de proyectos.

Este documento se dirige a todo el personal de ZUNIBAL, así como al conjunto total de partes interesadas.

2. Ámbito de aplicación

De acuerdo con la Política de Seguridad de la Información, se establecen medidas de seguridad que deben ser aplicadas a todos los sistemas, servicios y recursos relacionados con Tecnologías de la Información y Comunicación (TIC) utilizados por ZUNIBAL para respaldar sus procesos organizativos, y que afecten a los diversos elementos de información asociados.

Los recursos TIC de la entidad tienen como finalidad proporcionar soporte a las operaciones, así como a las actividades de gestión esenciales para su funcionamiento. Estos recursos abarcan tanto los sistemas centrales como los departamentales, estaciones de trabajo, ordenadores, impresoras, dispositivos de salida y otros periféricos, redes internas y externas, servicios de comunicación y sistemas de almacenamiento propiedad de ZUNIBAL.

Esta política no solo se aplica al personal interno de la organización, sino que también es vinculante para todas las personas, entidades, instituciones o unidades y servicios, tanto internos como externos, que hagan uso de los recursos TIC y tengan acceso a los elementos de información de la entidad. Esto incluye a quienes se conecten directa o indirectamente a dichos recursos, ya sea de manera remota o mediante dispositivos ajenos, y engloba especialmente los servicios ofrecidos a través de Internet. En el contexto de esta actividad, se considerará a estos individuos como usuarios, de acuerdo con los términos establecidos en esta política.

3. Principios de seguridad de la información

La presente política, en conjunto con su normativa correspondiente, se fundamenta en principios esenciales de protección con el objetivo de asegurar que la organización pueda alcanzar sus metas a través de la correcta gestión de los sistemas de información.

Estos principios fundamentales, que deben ser tenidos en cuenta en todas las decisiones relacionadas con la seguridad de la información, se describen a continuación:

3.1 Enfoque integral de la seguridad

La seguridad se aborda como un proceso global que involucra a todos los elementos humanos, materiales, organizativos y tecnológicos relacionados con el sistema. Por tanto, es crucial tomar las medidas apropiadas para que todos los actores involucrados en el proceso sean conscientes de la Política de Seguridad de Información y ejecuten sus responsabilidades de acuerdo con ella. La coordinación entre todos los participantes es aplicable a todas las iniciativas y acciones emprendidas por ZUNIBAL.

3.2 Gestión de riesgos

El análisis y gestión de riesgos desempeñan un rol crucial en la seguridad de la información. Es esencial mantener los niveles de riesgo dentro de límites aceptables a través de la implementación continua de medidas de seguridad apropiadas y actualizadas. Esto asegura una proporcionalidad entre la naturaleza de los datos y procesos de tratamiento, los riesgos a los que están expuestos, y las medidas de seguridad correspondientes.

3.3 Prevención y recuperación ante incidentes

La seguridad de los sistemas debe abarcar la prevención, detección y recuperación con el propósito de evitar que las amenazas se materialicen o tengan un impacto significativo en los datos manejados por los sistemas de información o en los servicios ofrecidos. Esto se logra a través de medidas preventivas, incluyendo disuasión y reducción de exposición; medidas de detección que son complementadas con respuestas efectivas para abordar incidentes de seguridad, y medidas de recuperación que permiten la restauración de servicios e información. El sistema garantiza la preservación de datos y la disponibilidad de servicios a lo largo del ciclo de vida de la información.

3.4 Múltiples capas de defensa

El sistema debe contar con una estrategia de protección que consiste en múltiples capas de seguridad dispuestas de tal manera que, si una de ellas falla debido a un incidente inevitable, se tenga tiempo suficiente para una respuesta adecuada, reduciendo la probabilidad de que todo el sistema se vea comprometido y minimizando el impacto final. Estas capas de defensa incluyen medidas organizativas, físicas y lógicas.

3.5 Revisión periódica y mejora continua

ZUNIBAL revisa y actualiza regularmente las medidas de seguridad implementadas para asegurar que continúen siendo efectivas ante la evolución constante de los riesgos y los sistemas de protección.

4. Liderazgo y compromiso

La Dirección de ZUNIBAL demuestra su liderazgo y compromiso con los principios fundamentales de seguridad de la información mediante la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), sobre el que asume las siguientes responsabilidades:

- Establecer y alinear la Política de Seguridad de la Información y la Normativa de Seguridad de la Información con la dirección estratégica de la organización.
- Garantizar la disponibilidad de los recursos necesarios para el funcionamiento efectivo del SGSI.
- Comunicar la importancia de una gestión eficiente del sistema y del cumplimiento de los requisitos establecidos a todos los niveles de la organización.
- Proporcionar dirección y apoyo a las personas que contribuyen al funcionamiento del SGSI, promoviendo una cultura de seguridad de la información.
- Colaborar con otras áreas de gestión pertinentes para fortalecer su liderazgo en sus respectivas áreas de responsabilidad, garantizando la integración de la seguridad de la información en todos los procesos.
- Asegurar que el SGSI alcance los resultados previstos en términos de protección de la información y continuidad de los servicios.
- Promover la mejora continua en el ámbito de la seguridad de la información, respaldando iniciativas que conduzcan a una mayor eficacia y eficiencia en la gestión de la seguridad.

5. Política de gestión

La Dirección de ZUNIBAL reconoce la necesidad de garantizar el cumplimiento de los niveles definidos de confidencialidad, integridad y disponibilidad para sus activos de información. Esto es esencial para llevar a cabo las actividades de la compañía y alcanzar los objetivos estratégicos, así como para demostrar su capacidad para una gestión eficiente de los servicios ofrecidos a los clientes.

Con el propósito de lograr estas metas, se ha desarrollado e implementado el Sistema de Gestión de Seguridad de la Información (SGSI), que proporciona un marco de referencia sólido para el manejo seguro de los activos de la compañía. Además, este sistema actúa como garantía para asegurar la confianza y satisfacción de todas las partes interesadas, al integrar una metodología segura para la prestación de servicios.

Para reforzar su compromiso, y teniendo en cuenta que la seguridad de la información se orienta a garantizar la continuidad de las operaciones de la organización y mitigar el

riesgo al prevenir y, en caso necesario, reducir el impacto de los incidentes de seguridad, ZUNIBAL establece los siguientes objetivos estratégicos en materia de seguridad de la información, en sintonía con el contexto y la dirección estratégica de la empresa:

- Promover una cultura organizativa en la que la seguridad de la información sea un pilar fundamental y se encuentre arraigada en todas las prácticas y procesos de gestión de la organización.
- Proteger la confidencialidad, disponibilidad e integridad de los datos de la organización para respaldar la estrategia empresarial, así como cumplir con los requerimientos legales y contractuales vigentes.
- Realizar análisis y gestión de riesgos centrados en la seguridad de la información.
- Utilizar de manera óptima los recursos destinados a la seguridad para respaldar los objetivos del negocio.
- Aprovechar de manera eficiente y efectiva el conocimiento y la infraestructura de seguridad existente.
- Salvaguardar los recursos de información y la tecnología utilizada por ZUNIBAL contra amenazas tanto internas como externas, sean intencionadas o accidentales.
- Establecer procesos de monitorización y reporte para garantizar el cumplimiento de los objetivos de seguridad de la información y asegurar una respuesta adecuada ante incidentes.
- Garantizar la resiliencia de la organización y sus sistemas de información frente al cambio climático o desastres naturales.

6. Organización de la seguridad

Para cumplir con todos estos objetivos durante todas las fases del ciclo de vida de la información y asignar de manera apropiada las responsabilidades para su implementación, ZUNIBAL establece una estructura que fomenta la coherente aplicación de la política de seguridad de la información. Esta estructura se adapta eficazmente a los frecuentes cambios tecnológicos y organizacionales del entorno donde lleva a cabo su actividad de negocio.

En consecuencia, ZUNIBAL establece el siguiente comité y roles relacionados con la supervisión y gestión de la seguridad de la información:

- Comité de Seguridad de la Información.
- Responsable de Seguridad.
- Responsable de Sistemas de Información.
- Responsable del SGSI.

7. Datos de carácter personal

ZUNIBAL lleva a cabo tratamiento de datos personales y mantiene un Registro de Actividades de Tratamiento que documenta estos procesos e identifica a los responsables correspondientes. Cada uno de sus sistemas de información se ajusta a los niveles de seguridad requeridos según la normativa, considerando la naturaleza y el propósito de los datos personales involucrados.

Las medidas de seguridad implementadas en conformidad con esta política de seguridad de la información, así como las evaluaciones de riesgos realizadas para cumplir con las obligaciones del Reglamento General de Protección de Datos, se coordinan de manera efectiva con el Responsable de Seguridad y el Comité de Seguridad de la Información. Esto garantiza que la protección de los datos personales se integre plenamente en el marco del SGSI y que se cumplan las normativas de privacidad aplicables.

8. Obligaciones de los usuarios

Es una responsabilidad de todos los miembros de ZUNIBAL conocer y cumplir rigurosamente con la Política de Seguridad de la Información y la Normativa de Seguridad que emana de esta política. La Dirección se encarga de garantizar que estas políticas lleguen a todos los interesados, facilitando los medios necesarios para su difusión y comprensión.

Es de vital importancia que todos los empleados de la organización sean plenamente conscientes de la relevancia de preservar la seguridad de los sistemas de información. Cada persona desempeña un papel esencial en el mantenimiento y mejora de la seguridad en ZUNIBAL.

En consecuencia, se establece un programa de concienciación continua que abarca a todos los miembros de la organización, con especial énfasis en aquellos que se han unido recientemente. Aquellas personas con responsabilidades relacionadas con la utilización, administración u operación de sistemas de tecnologías de la información y comunicación (TIC) reciben formación específica en la gestión segura de estos sistemas, según sea necesario para cumplir con sus tareas. Esta capacitación es obligatoria antes de asumir cualquier responsabilidad, ya sea en su primer puesto o en caso de cambio de roles o responsabilidades dentro de la organización.

9. Responsabilidades de los usuarios en caso de incumplimiento

El Comité de Seguridad de la Información está capacitado para evaluar si el personal de la organización está incumpliendo alguna de las obligaciones establecidas en la presente política, así como en la normativa y las instrucciones adicionales relacionadas.

En el caso de identificarse algún incumplimiento, se implementan medidas tanto preventivas como correctivas con el objetivo principal de preservar y proteger los

sistemas de información y las redes de la organización. Estas medidas se aplicarán sin menoscabo de las posibles consecuencias disciplinarias que puedan derivarse.

Una vez confirmado un incumplimiento de la Política de Seguridad de la Información, el Comité sigue los procedimientos establecidos para iniciar las acciones disciplinarias correspondientes. El procedimiento que seguir y las sanciones a aplicar se ajustan a la legislación vigente que regula el régimen disciplinario del personal empleado en la organización.

10. Relación con terceras partes

Cuando ZUNIBAL brinda servicios a otros organismos o maneja información procedente de ellos, el responsable de esta relación se encarga de informarles sobre la Política de Seguridad de la Información, así como de aquellas normas e instrucciones que sean necesarias a compartir. Además, se establecen canales de comunicación y coordinación entre los respectivos Responsables de Seguridad de la Información con el propósito de asegurar una colaboración efectiva en materia de seguridad. También se implementan procedimientos para la respuesta ante posibles incidentes de seguridad, lo que permite reaccionar de manera rápida y eficiente en caso de que ocurran eventos que pongan en riesgo la seguridad de la información.

Cuando ZUNIBAL utiliza servicios de terceros o comparte información con ellos, se establecen acuerdos contractuales que obligan a estos terceros a cumplir con las obligaciones y medidas de seguridad especificadas en dichos contratos. Estos terceros pueden implementar sus propios procedimientos operativos para garantizar el cumplimiento de estas obligaciones. Además, se pueden establecer procedimientos específicos para prevenir, detectar, informar y resolver incidentes de seguridad en colaboración con los terceros. El objetivo es asegurar que el personal de estos terceros esté debidamente informado y capacitado en materia de seguridad, al menos al mismo nivel que se establece en la presente política de seguridad.

En particular, los terceros deben garantizar el cumplir con medidas de seguridad basadas en estándares que puedan ser auditables, y podrán estar sujetos a controles y revisiones realizados por terceros certificados que verifiquen su cumplimiento con estas políticas.

Si una tercera parte no puede cumplir con algún aspecto de esta política de seguridad, se solicita un informe a su Responsable de Seguridad donde se identifiquen los riesgos involucrados y las medidas para abordarlos. Este informe debe ser aprobado por ZUNIBAL antes de continuar con la relación o el servicio en cuestión.

zunibal@zunibal.com www.zunibal.com +34 944 977 010