Política de Seguridad de la Información

Versión: 3.0

Confeccionó	Revisó	Aprobó
BDO **Consultoría Externa**	 **Carla Leiva - CISO**	 **Francisco Canale - Director**

Contenido

1. Objetivo

Definir los lineamientos generales para gestionar adecuadamente los activos de información de INTIZA y garantizar la integridad, confidencialidad y disponibilidad de la información y servicios.

2. Alcance

Esta Política involucra a todas las personas que realicen cualquier actividad para INTIZA, como los empleados efectivos, personal pasante, contratado, tercerizados o cualquier otra modalidad de empleo directa o indirectamente que pudiera generar un vínculo laboral.

3. Responsabilidades

La totalidad de las **Áreas de la organización**, al igual que el **personal contratado**, los **proveedores** y cualquier persona que preste servicios, deberán cumplir adecuadamente con la Política y sus documentos normativos dependientes.

Todo el personal de la organización, es responsable de cumplir con la presente Política y sus Normas relacionadas.

El **equipo directivo** representado por el **Comité de Seguridad** es el responsable de garantizar que la seguridad de la información se gestiona adecuadamente en toda la organización.

Seguridad de la Información es responsable de definir los lineamientos de seguridad de la información en base a las mejores prácticas y hacer cumplir los mismos mediante una correcta gestión del SGSI.

4. Desarrollo

Se definen directrices de Seguridad de la Información respecto a la utilización segura y responsable de la Información a través de las cuales se busca:

- Garantizar que los sistemas de información de la compañía tengan un nivel de seguridad adecuado a las buenas prácticas y se apliquen los estándares más avanzados en los activos tecnológicos que respalden la operación de infraestructuras críticas.
- Implementar las medidas de seguridad necesarias para proteger la confidencialidad, la integridad y la disponibilidad de la información en función de su criticidad y los riesgos existentes.
- Sensibilizar a todos los empleados, contratistas y colaboradores sobre los riesgos de seguridad de la información y garantizar que tengan los conocimientos, habilidades, experiencia y capacidades tecnológicas necesarios para respaldar los objetivos de la Compañía.
- Proporcionar procedimientos y herramientas que se adapten rápidamente a las condiciones cambiantes del entorno tecnológico y las nuevas amenazas.
- Garantizar el cumplimiento normativo asociado a las áreas de Seguridad de la Información en toda la Compañía.

4.1. Objetivos de Seguridad de la Información

INTIZA establece los siguientes objetivos de seguridad de la información como parte de su compromiso con la protección de sus activos y la gestión del riesgo:

- **Confidencialidad:** Asegurar que solo quienes estén autorizados puedan acceder a la información.
- **Integridad:** Asegurar que la información y sus métodos de procesamiento son exactos y completos.

- **Disponibilidad** de la información en sus operaciones: Asegurar que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.
- **Cumplimiento Normativo:** Cumplir con los requisitos legales, regulatorios y contractuales aplicables en materia de seguridad de la información.
- **Mejora Continua:** Monitorear, evaluar y mejorar continuamente los controles de seguridad para adaptarse a nuevos riesgos y tecnologías.
- **Concientización:** Promover una cultura de seguridad de la información en toda la organización mediante la capacitación y sensibilización de los empleados.

4.2. Directrices de Seguridad de la Información

La Seguridad de la Información en INTIZA fija los controles principales, denominados directrices:

- Se debe tratar la Información de la Compañía y de los clientes de forma ética y confidencial siguiendo el marco normativo vigente.
- Se debe utilizar la Información de forma transparente y solamente a los efectos para los cuales ha sido recolectada.
- Solamente se debe acceder a la Información y los recursos a través de la correspondiente y debida autorización.
- La identificación de cualquier colaborador debe ser única, personal e intransferible para identificarlo como responsable de las acciones efectuadas.
- El otorgamiento de accesos se debe realizar teniendo en cuenta el criterio de menor privilegio, por lo tanto, los usuarios accederán a los recursos de información que son imprescindibles para el desempeño de sus actividades.
- Se debe informar a Seguridad de la Información cualquier riesgo identificado para la Información.

- Se deben divulgar ampliamente las responsabilidades en cuanto a la Seguridad de la Información a los empleados, que deben comprender y asegurar el cumplimiento de estas directrices.

4.3. Gestión de la Seguridad de la Información

A través de los siguientes procesos, la compañía se cerciora de contar con una adecuada protección de la información:

- Clasificación de los Activos de la Información
- Gestión y Evaluación de Riesgos
- Seguridad Física aplicada a los Activos de la Información
- Seguridad en los Recursos Humanos
- Seguridad de Acceso Lógico a los Activos de la Información
- Control y Monitoreo de Seguridad
- Seguridad de Redes y Comunicaciones
- Auditoría y Registros de Eventos de Seguridad
- Gestión de incidentes de Seguridad
- Seguridad Cloud
- Seguridad en Servicios Tercerizados
- Seguridad en el Desarrollo de Software
- Gestión de Vulnerabilidades

4.3.1. Clasificación de Activos

Con el objetivo de garantizar y mantener la protección sobre los activos de la Compañía, los mismos deben ser claramente identificados en su totalidad y poseer un dueño asignado. Para ello se debe elaborar y mantener un inventario de los activos para su posterior clasificación.

Seguridad de la Información, debe administrar y gestionar la seguridad de todos los Activos de Información y administrar los Riesgos asociados a cada activo de acuerdo con la criticidad y

sensibilidad obtenida para los mismos, previniendo a su vez por medio de la implementación de restricciones y controles, la fuga de información, asegurando una correcta protección de los activos más críticos identificados a través de controles de accesos robustos.

4.3.2. Gestión de evaluación de Riesgos

Se entiende por evaluación de riesgos a la evaluación de las posibles amenazas y vulnerabilidades que podrían afectar de manera directa o indirecta a la información y/o la infraestructura tecnológica que procesa la misma, la probabilidad de ocurrencia y el impacto que podría generar.

Se evaluarán los riesgos identificándolos, cuantificándolos y priorizándolos de acuerdo con el impacto que pudiesen generar directa o indirectamente en el negocio, permitiendo así el orden de prioridades en la aplicación de controles de seguridad.

La evaluación de riesgos se debe realizar periódicamente, de manera metódica y reproducible con resultados comparables cada vez que exista un cambio significativo en la compañía, ejemplo: cambios en activos, amenazas, vulnerabilidades.

Para cada uno de los riesgos identificados durante la evaluación se necesita tomar una decisión para su tratamiento. Las posibles opciones para el tratamiento de riesgos incluyen:

- Mitigar los riesgos mediante la aplicación de los controles apropiados para reducirlos.
- Aceptar los riesgos de manera objetiva y consciente, siempre y cuando estos satisfagan los criterios de aceptación de la empresa.
- Evitar los riesgos, eliminando las acciones que dan origen a la ocurrencia de estos.
- Transferir los riesgos asociados a otras partes interesadas, por ejemplo, a compañías de seguros.

Se deben implementar controles sobre los riesgos identificados para lograr mitigar los mismos. Los controles implementados deben ser evaluados permanentemente para que puedan ser mejorados en eficiencia y efectividad al pasar el tiempo.

4.3.3. Seguridad Física aplicada a los Activos de la Información

Todo sitio, ya sea propio o de terceros, productivo o de contingencia, que procese y/o almacene datos e información de INTIZA debe cumplir con todas las medidas de seguridad física definidas por la Compañía, con el fin de asegurar una adecuada protección de todos los equipos de procesamiento de información.

Se deben implementar escritorios limpios en las instalaciones físicas de INTIZA con el fin de reducir los riesgos de acceso no autorizado, pérdida y/o daño de la información durante el horario normal de trabajo. Y fuera del mismo se debe dejar libre de información confidencial el escritorio, computadoras de escritorio o portátiles apagadas o bloqueadas, y documentos impresos bajo llave.

El acceso a las áreas seguras de INTIZA tanto por personal interno como externo deben ser previamente autorizados y registrados formalmente. El personal externo debe ser supervisado en todo momento.

4.3.4. Seguridad en los Recursos Humanos

Se deben incluir en el contrato laboral los acuerdos de propiedad intelectual, protección de datos y convenio de confidencialidad.

Se debe brindar capacitación al personal sobre temas de seguridad y protección de activos de información para que sean conscientes de las amenazas a las cuales dichos activos se encuentran expuestos, cómo éstas afectan sus labores diarias y qué medidas adoptar para proteger y prevenir la materialización de estas amenazas y lograr el uso eficiente y seguro de los activos de información.

Se debe asegurar que la desvinculación o cambio de cargos dentro de INTIZA de los empleados, contratistas y terceras partes se realice de una manera ordenada, garantizando la devolución de activos y la eliminación de derechos de acceso.

Se debe notificar a Seguridad de la Información del inicio y fin de los períodos de licencias de los empleados que cumplan tareas relacionadas al manejo de activos de información, para que este último aplique los controles de seguridad correspondientes.

4.3.5. Seguridad de Acceso lógico a los activos de información

Seguridad de la Información debe administrar la seguridad sobre los distintos tipos de accesos (locales y/o remotos), y la autenticación de usuarios y perfiles de todo el personal. La seguridad debe ser aplicada sobre todos los activos de información (aplicaciones y plataformas tecnológicas homologadas), tanto para el ambiente productivo como el de contingencia.

El acceso a cualquier activo de información debe estar limitado mediante controles de acceso adecuados según la criticidad de esta, derivada del análisis de riesgo correspondiente. La asignación de privilegios a personas se realiza basándose en la clasificación y función del trabajo que ésta desempeña.

Se debe definir el circuito formal de solicitud de cuenta de usuarios para todos los casos posibles, esta solicitud debe tener un proceso de autorización formal y documentado.

Se deben establecer controles sobre las cuentas de usuarios con privilegios especiales, contar con circuitos de solicitud y aprobación formales y los accesos quedar registrados en bitácoras de auditoría.

La asignación de derechos de acceso debe otorgarse a través de un proceso de autorización formal, verificando periódicamente los niveles y privilegios otorgados a los usuarios.

4.3.6. Control y Monitoreo de Seguridad

Los accesos y la actividad en los Activos de Información definidos como críticos deben ser monitoreados periódicamente por Seguridad de la Información, reportando los incidentes o cualquier anomalía detectada a las áreas involucradas, y procediendo a la toma de acciones necesarias para su resolución.

El monitoreo y control de los sistemas debe incluir los componentes y sistemas que actúen sobre el perímetro, redes y las comunicaciones.

Todos los usuarios, así como los clientes que estén conectados a los sistemas de INTIZA, deben estar conscientes de que sus acciones serán registradas y supervisadas. También se deberán implementar normas y procedimientos formales que regulen los procesos relacionados con el monitoreo y control de la Seguridad de la Información.

Se deben dar protección a los registros de auditoría de cada plataforma, los mismos deberán ser analizados, registrados y protegidos de modo de resguardar la información confidencial de INTIZA.

4.3.7. Seguridad de Redes y comunicaciones

Se deben establecer controles de seguridad en la infraestructura de INTIZA, para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información.

Se deben establecer requisitos para la administración y protección de todas las redes y comunicaciones informáticas, incluyendo la conectividad entre éstas aun cuando sea provista por un tercero.

Todo el tráfico entrante o saliente a redes debe estar mediado por un firewall.

El firewall debe estar configurado según los lineamientos, estándares y procedimientos documentados para prevenir ataques internos y externos.

Todos los equipos de INTIZA deben ser protegidos de los riesgos de infección por códigos maliciosos; por lo tanto, es necesario poder detectar y eliminar los virus informáticos que afecten a cualquier sistema de información.

Se debe llevar a cabo la prevención, detección y erradicación de virus informáticos que afecten a los sistemas de información o redes que procesan, almacenan o transmiten información de la INTIZA, mediante la utilización de tecnología antivirus.

4.3.8. Auditoría y Registros de eventos de seguridad

Los sistemas e infraestructura tecnológica deben ser auditables, permitiendo el seguimiento de las acciones realizadas en el ámbito de estos. Para ello es necesario configurar y analizar los registros de Logs y auditoría.

Se debe establecer qué tipo de actividad se debe registrar como mínimo para permitir el seguimiento de esa actividad en los distintos sistemas o redes que procesan, almacenan o transmiten información de INTIZA.

Todos los Activos Críticos deben ser monitoreados para evitar actividades ilícitas, anormales o no autorizadas.

Se deben definir los lineamientos para la correcta protección y almacenamiento de los registros de auditoría para su posterior análisis y consulta. Deben ser debidamente protegidos, para evitar la alteración y los accesos no autorizados a la información contenida en los mismos.

4.3.9. Gestión de incidentes de Seguridad

Los incidentes de seguridad de la información requieren una respuesta rápida y confiable. Con el objetivo de prevenir los ataques o incidentes sobre los activos de información, es necesario contar con procesos formales que sirvan de marco regulatorio para la administración y control de estos.

Los incidentes de seguridad están relacionados con accesos no autorizados, pérdidas o daños en la disponibilidad, integridad y confidencialidad de la información.

Es necesaria la formación de un equipo de respuesta a incidentes de seguridad con funciones explícitas para sus miembros, así como la forma de definir un plan de respuesta a incidentes de seguridad, es vital cuando se detectan ocurrencias de compromisos de la seguridad.

INTIZA debe contar con un proceso formal para la gestión de incidentes de seguridad, que incluya la detección, reporte, análisis, respuesta y recuperación, integrando las lecciones aprendidas para mejorar los controles de seguridad en el futuro.

4.3.10. Seguridad Cloud

Se debe cifrar toda la información sensible que esté siendo almacenada en la nube para evitar la divulgación y garantizar una gestión adecuada ya que esto podría afectar al rendimiento de los sistemas.

Se deberá garantizar la transmisión segura de los datos en toda la infraestructura de la nube, entre los entornos de la empresa y la infraestructura de la nube y/o otras redes públicas.

Implementar un DRP teniendo en cuenta la posibilidad de interrupción del proveedor de servicios de la nube completa.

Deberá proporcionar mecanismos de eliminación de datos que garanticen a la compañía que todos los datos se han eliminado de forma segura del entorno de la nube, en caso de migrar a un nuevo Proveedor, desmantelar sus recursos en la nube o salir completamente de un entorno en la nube.

4.3.11. Seguridad en Servicios Tercerizados de TI

Previa a la contratación de Servicios Tercerizados de TI debe existir una gestión de evaluación de los aspectos de seguridad inherentes al proveedor y al servicio que brindará.

Periódicamente se debe evaluar la criticidad de los servicios tercerizados teniendo en cuenta la integridad, confidencialidad y disponibilidad de la información que maneja para definir controles de acuerdo a dicha criticidad.

4.3.12. Seguridad en Desarrollo/Adquisición de Software

Los productos de software que se implementen en producción deben mantener los principios de integridad, confidencialidad y disponibilidad establecidos por esta política.

Se deben implementar metodologías que contemplen controles previos a la puesta en producción de los desarrollos/aplicaciones adquiridas, a fin de asegurar que dichos cambios o desarrollos de nuevas funcionalidades, no afecten negativamente la seguridad de la información.

Se debe mantener una clara separación de ambientes de Desarrollo, Prueba y Producción.

El ambiente de producción es aquel en el cual residen los programas ejecutables de producción y los datos necesarios para el funcionamiento de estos. Sólo el personal autorizado a efectuar los cambios en los sistemas debe contar con privilegios de escritura en los mismos.

Se debe integrar la seguridad desde el inicio del ciclo de desarrollo del software, aplicando prácticas de desarrollo seguro, revisiones de código y pruebas de seguridad para identificar vulnerabilidades en etapas tempranas del desarrollo.

Los requerimientos de seguridad y los controles requeridos deben evaluarse teniendo en cuenta el nivel de criticidad obtenido luego de un análisis de riesgo. Los mismos deben ser proporcionales en costo y esfuerzo al valor del activo que se quiere proteger y al daño potencial que pudiera ocasionar la ocurrencia de ciertos sucesos.

Las actualizaciones o modificaciones a realizar sobre los aplicativos deben registrarse adecuadamente y estar formalmente aprobadas para su ejecución por parte del propietario de la información.

4.3.13. Gestión de Vulnerabilidades y parches

Se debe implementar un proceso de gestión de la vulnerabilidad y parches que incluya el descubrimiento de la vulnerabilidad, análisis de riesgos, medidas de mitigación como también una infraestructura que permita un adecuado y continuo monitoreo, seguimiento y mejora.

Previo a la puesta en producción de los aplicativos o sistemas de información, se debe realizar un análisis de vulnerabilidades técnicas, y, establecer el plan de remediación y seguimiento de vulnerabilidades identificadas. De acuerdo con el riesgo expuesto por la vulnerabilidad, el responsable del activo de información gestionará la remediación y aceptará o no la puesta en producción.

Se deberá implementar Planes de remediación de las vulnerabilidades críticas y tomar acciones correctivas a corto y mediano plazo para remediar las mismas.

4.3.14. Protección de datos personales

INTIZA se compromete a proteger los datos personales procesados, almacenados o transmitidos por la organización, asegurando su confidencialidad, integridad y disponibilidad.

Se deben establecer procesos para la gestión de solicitudes de acceso, rectificación, eliminación y portabilidad de datos personales, de acuerdo con las leyes y regulaciones aplicables (Ejemplo: GDPR, leyes locales de protección de datos).

Se establecen las directrices y medidas específicas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales en la Política de Protección de Datos Personales. Todo el personal debe cumplir con esta política, asegurando que los datos personales se gestionen conforme a las normativas aplicables y los controles definidos.

5. Referencias

5.1. Normativa Relacionada

Categoría	Título	Código
Política	Protección de Datos Personales	PO-SI-02

5.2. Definiciones y Abreviaturas

Término	Descripción
Confidencialidad	La confidencialidad es un principio fundamental de la seguridad de la información que garantiza el necesario nivel de secreto de la información y de su tratamiento, para prevenir su divulgación no autorizada cuando está almacenada o en tránsito.
Integridad	La integridad de los datos o de la información garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada.
Disponibilidad	La disponibilidad es la característica o capacidad de asegurar la fiabilidad y el acceso oportuno a los datos y recursos que los soportan por parte de los individuos autorizados, es decir, que lo necesitan para desenvolver sus actividades.
SGSI - Sistema de Gestión de Seguridad de la Información	Un SGSI proporciona un modelo para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la protección de los activos de información para alcanzar los objetivos de negocio.
Activo	En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas) que tenga valor para la organización.

Vulnerabilidad	Fallo o debilidad de un sistema de información que pone en riesgo la seguridad de esta.
Seguridad de la Información	Conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.
Monitoreo y Control	Proceso sistemático de recolectar, analizar y utilizar información para hacer seguimiento al progreso de un programa en pos de la consecución de sus objetivos, y para guiar las decisiones de gestión.

6. Historial de Versiones

Versión	Fecha	Resumen de Cambios
1.0	01/07/2021	Creación de la política de Seguridad de la información.
1.0	28/10/2021	Aprobado por Comité de Dirección: MI-DI-01- Minuta de Directorio N° 1
2.0	07/09/2022	Se ajusta objetivo y responsabilidades y se verifica que el contenido siga vigente.
2.0	11/10/2022	Aprobado por Comité de Dirección: MI-DI-06- Minuta de Directorio N° 6

3.0	17/09/2024	Se revisó el documento. Se agregan los puntos 4.1 Objetivos de Seguridad de la Información, 4.3.14 Protección de datos personales y se completa el punto 4.3.9 Gestión de incidentes de seguridad.
3.0	08/10/2024	Aprobado por Comité de Seguridad.