Desarrollos Informáticos DEINSA Sociedad Anónima

Política de Seguridad de la Información

Julio 2025

Control de versiones

Fecha de creación	Versión	Autores	Aprobado por	Descripción	Nivel de Confidencialidad
Mayo 2024	1.0	DAB	DAB	Política de seguridad de la información	Información Interna
Octubre 2024	1.1	JCR	DAB	Ajustes estructurales y de contenido.	Información Interna
Julio 2025	2.0	JCR	DAB	Se refuerza cumplimiento normativo y se eliminan objetivos y sanciones	Información Interna

DENNIS GERARDO ALVARADO BONILLA (FIRMA)

Firmado digitalmente por DENNIS GERARDO ALVARADO BONILLA (FIRMA)
Fecha: 2025.07.14 09:59:55 -06'00'

Contenido

1 Introducción

La política de seguridad de la información de DEINSA establece los principios y lineamientos fundamentales para garantizar la protección de la confidencialidad, integridad y disponibilidad de los datos del servicio Delphos (SaaS).

En un entorno de operación basado en la nube, como el que sustenta Delphos, esta política busca asegurar que la información sensible, tanto de DEINSA como de sus clientes, esté protegida frente a accesos no autorizados, alteraciones indebidas y posibles interrupciones. Además, fomenta el cumplimiento con normativas y estándares internacionales aplicables a la seguridad de la información, promoviendo la confianza de los clientes y el fortalecimiento de la reputación de la organización.

2 Propósito y Compromiso

DEINSA se compromete a proteger la información de los clientes, empleados y otras partes interesadas, garantizando un enfoque de gestión de la seguridad de la información que respalde la confidencialidad, integridad y disponibilidad de los datos. Este compromiso se cumple mediante la implementación de controles, procesos y prácticas de seguridad que protegen el entorno operativo y la infraestructura de DELPHOS, nuestro servicio SaaS.

Para asegurar una protección robusta de la información, DEINSA se compromete a:

1. **Control de Acceso**: Aplicar principios de mínimo privilegio y autenticación fuerte para el acceso a Oracle Cloud, repositorios de código y bases de datos.
2. **Seguridad en la Nube**: Configurar y monitorear la infraestructura de Oracle Cloud con controles de seguridad avanzados, asegurando la integridad de los datos y la infraestructura.
3. **Gestión de Riesgos**: Identificar, evaluar y tratar de forma continua los riesgos que afecten a la seguridad de la información, aplicando controles de mitigación para minimizar el impacto de posibles amenazas.
4. **Gestión de Incidentes**: Implementar y seguir procedimientos claros para la detección, notificación y resolución de incidentes de seguridad, minimizando su impacto en la operación.
5. **Cumplimiento Normativo**: Asegurar el cumplimiento de leyes, acuerdos contractuales, regulaciones y estándares aplicables, incluyendo ISO 27001, y garantizar que todos los controles y políticas de seguridad se alineen con las mejores prácticas internacionales.
6. **Concienciación y Capacitación**: Promover una cultura de seguridad mediante programas de capacitación continua y sensibilización sobre seguridad de la información.
7. **Mejora Continua**: Revisar y actualizar de manera continua el SGSI para adaptarse a los cambios en el entorno de riesgos, requisitos normativos y avances tecnológicos, asegurando su eficacia y relevancia

3 Alcance de Política de Seguridad

Esta política de seguridad de la información aplica a todas las áreas, activos, procesos y sistemas incluidos dentro del alcance del Sistema de Gestión de Seguridad de la Información (SGSI) de DEINSA. En particular, se enfoca en:

- **Aplicación Organizacional**: La política es de cumplimiento obligatorio para todos los colaboradores, contratistas y terceros que accedan, gestionen o utilicen información o sistemas de DEINSA.
- **Cobertura de Activos**: Incluye la protección de la infraestructura tecnológica, datos, aplicaciones, sistemas, redes y entornos en la nube utilizados para el servicio Delphos (SaaS) y otras operaciones críticas.
- **Ámbito Operativo**: Se aplica a todas las ubicaciones físicas y remotas desde las cuales se gestionan los activos de información de DEINSA, incluyendo su infraestructura alojada en Oracle Cloud.
- **Propósito del Documento**: Este documento define los principios, lineamientos y objetivos que rigen la protección de la confidencialidad, integridad y disponibilidad de la información, en concordancia con los requisitos establecidos por el SGSI y alineados con la norma ISO 27001:202

4 Responsabilidades

La asignación de responsabilidades es esencial para garantizar la gestión eficaz de los riesgos y la protección de la información en DEINSA. Los roles clave y sus principales responsabilidades son:

- **Alta Dirección**: Supervisa y apoya la implementación efectiva de la seguridad de la información, garantizando la asignación de recursos necesarios.
- **Jefe de Seguridad Integral (CISO)**: Lidera la estrategia de seguridad, supervisa la gestión de riesgos, coordina respuestas a incidentes y asegura el cumplimiento normativo.
- **Dirección de Operaciones**: Implementa y mantiene medidas técnicas de seguridad, como firewalls, cifrado, gestión de accesos y recuperación ante desastres.
- **Especialista en Riesgos y Cumplimiento**: Garantiza el cumplimiento de regulaciones, coordina auditorías y mantiene actualizadas las políticas de privacidad y protección de datos.
- **Recursos Humanos**: Selecciona y capacita al personal en seguridad, gestiona accesos de acuerdo con las políticas, y realiza verificaciones de antecedentes.
- **Usuarios y Empleados**: Cumplen con las políticas de seguridad, informan sobre incidentes o vulnerabilidades y participan en programas de concienciación.

5 Políticas Específicas

DEINSA mantendrá un catálogo de políticas específicas que detallarán controles y procedimientos para las diferentes áreas de seguridad (como acceso, cifrado, continuidad, gestión de riesgos, respuesta a incidentes, entre otras). Estas políticas revisarán y actualizarán periódicamente.

6 Cumplimiento y Auditoría

La realización de auditorías periódicas es esencial para evaluar y mejorar la eficacia de las políticas y controles de seguridad de la información en DEINSA. Este proceso garantiza el cumplimiento de regulaciones y estándares relevantes, proporcionando información clave para la mejora continua. Los elementos principales incluyen:

Preparación y Planificación:

- Definir objetivos claros y determinar el alcance de la auditoría.
- Establecer un equipo de auditores internos o externos capacitados.
- Desarrollar un plan de auditoría alineado con los recursos y objetivos.

Evaluación y Análisis:

- Revisar las políticas, regulaciones y estándares aplicables, como ISO 27001.
- Identificar áreas críticas de enfoque, realizar pruebas técnicas, y recopilar datos mediante entrevistas y análisis de documentación.

Resultados y Seguimiento:

- Generar un informe con hallazgos, recomendaciones y acciones correctivas.
- Implementar las acciones correctivas asignando responsabilidades claras.
- Realizar auditorías de seguimiento para verificar la eficacia de las medidas tomadas.

Este enfoque sistemático permite a DEINSA mantener altos estándares de seguridad de la información y fortalecer la protección de los activos organizacionales y de sus clientes.

7 Revisión de la Política

Esta política será revisada anualmente o cuando se produzcan cambios significativos en el entorno de riesgos, las operaciones o los requisitos normativos de DEINSA.

8 Anexos

8.1 Definiciones y Términos

Acción Correctiva:

Medida implementada para eliminar las causas de una no conformidad detectada, evitando su recurrencia y asegurando el cumplimiento de las políticas y controles establecidos.

Activo de Información:

Cualquier recurso, tangible o intangible, que tiene valor para la organización y que debe ser protegido.

Confidencialidad:

Principio de seguridad que asegura que la información solo está disponible para personas autorizadas y que no se divulga a partes no autorizadas.

Control de Acceso:

Proceso que garantiza que solo personas autorizadas puedan acceder a sistemas, datos y recursos de información, de acuerdo con sus roles y responsabilidades.

Disponibilidad:

La disponibilidad se refiere a la accesibilidad y utilidad de la información cuando sea necesario. Los sistemas y datos deben estar disponibles para usuarios autorizados y las interrupciones deben minimizarse para mantener la continuidad de las operaciones.

Gestión de Riesgos:

Proceso continuo para identificar, evaluar y tratar riesgos relacionados con la seguridad de la información, minimizando su impacto potencial sobre la organización.

Integridad:

Principio de seguridad de la información que garantiza que los datos y sistemas sean precisos, consistentes y estén protegidos contra modificaciones no autorizadas, tanto intencionales como accidentales.

Seguridad de la Información:

La seguridad de la información es el conjunto de medidas y prácticas diseñadas para proteger la confidencialidad, integridad y disponibilidad de los datos y la información en una organización.