Desarrollos Informáticos DEINSA Sociedad Anónima

Política de Seguridad de la Información

Agosto 2026

Control de Versiones

Fecha	Versión	Autores	Aprobado por	Descripción	Nivel de Confidencialidad
Mayo 2024	1.0	DAB	DAB	Política de seguridad de la información	Información Interna
Julio 2025	2.0	JCR	DAB	Se refuerza cumplimiento normativo y se eliminan objetivos y sanciones	Información Interna
Agosto 2026	3.0	JCR	DAB	Actualización por transición de SGSI a SIG (integración con la Política de Continuidad v2.0 e ISO 22301	Información Interna

DENNIS GERARDO ALVARADO BONILLA (FIRMA)

Firmado digitalmente por DENNIS GERARDO ALVARADO BONILLA (FIRMA)
Fecha: 2026.08.11 08:31:07 -06'00'

Tabla de contenido

1 Introducción

La presente Política de Seguridad de la Información de DEINSA establece los principios fundamentales para garantizar la protección de la confidencialidad, integridad y disponibilidad de los datos del servicio Delphos (SaaS), dentro del Sistema Integral de Gestión (SIG).

El SIG de DEINSA integra las normas internacionales ISO/IEC 27001:2022 (Seguridad de la Información) e ISO 22301:2019 (Continuidad del Negocio)

En un entorno de operación centralizado en la nube (Oracle Cloud Infrastructure - OCI) y bajo un modelo operativo de teletrabajo distribuido, esta política busca asegurar que la información sensible esté protegida frente a accesos no autorizados, alteraciones indebidas, fuga de datos y ciberataques, promoviendo el cumplimiento normativo, la resiliencia operativa y la confianza de nuestras partes interesadas.

2 Propósito y Compromiso

DEINSA se compromete a proteger la información de sus clientes, colaboradores y partes interesadas, garantizando un enfoque transversal de gestión de la seguridad que respalde las operaciones de la plataforma SaaS DELPHOS.

Para asegurar una protección robusta y alineada a los objetivos corporativos, DEINSA se compromete a:

1. Control de Acceso: Aplicar el principio de mínimo privilegio, segregación de funciones y autenticación fuerte para el acceso a la consola de Oracle Cloud, repositorios de código y bases de datos.
2. Seguridad en la Nube: Configurar y monitorear proactivamente la infraestructura en Oracle Cloud mediante controles de seguridad avanzados y arquitecturas seguras por diseño.
3. Gestión Unificada de Riesgos: Identificar, evaluar y tratar de forma continua los riesgos de seguridad de la información y riesgos de continuidad del necio de forma unificada como parte del SIG.
4. Gestión de Incidentes de Seguridad: Implementar procedimientos para la detección, notificación, contención y resolución de incidentes de seguridad de la información, sirviendo de enlace con los planes de gestión de crisis y continuidad corporativa.
5. Cumplimiento Normativo y Legal: Garantizar el cumplimiento de leyes, regulaciones, acuerdos contractuales y estándares aplicables, tales como ISO 27001, ISO 22301 y garantizar que todos los controles y políticas de seguridad se alineen con las mejores prácticas internacionales..
6. Concienciación y Cultura Digital: Capacitar y sensibilizar continuamente al personal en materia de ciberseguridad, protección de datos y buenas prácticas en teletrabajo.
7. Mejora Continua: Evaluar periódicamente la eficacia de los controles de seguridad y ajustar el SIG ante cambios en el entorno tecnológico, normativo o de amenazas.

3 Alcance de Política de Seguridad

Esta política es de cumplimiento obligatorio para todas las áreas, activos, procesos y colaboradores incluidos dentro del alcance del Sistema Integral de Gestión (SIG) de DEINSA.

- Aplicación Organizacional: Obligatorio para colaboradores (bajo modalidad 100% teletrabajo), contratistas, consultores y terceros que gestionen o accedan a datos y sistemas dentro del alcance del SIG de DEINSA.
- Cobertura de Activos: Comprende la infraestructura tecnológica en Oracle Cloud Infrastructure (OCI), repositorios de código fuente, bases de datos multitenant, endpoints corporativos y datos de clientes asociados al servicio DELPHOS (SaaS).

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:

- Gerencia General: Asigna recursos financieros y humanos, aprueba la dirección estratégica del SIG y lidera la respuesta corporativa ante emergencias mayores.
- Responsable de Seguridad de la Información: Lidera la estrategia de seguridad, supervisa los riesgos de seguridad, coordina la respuesta a incidentes tecnológicos y tiene la potestad de vetar cambios en producción que no cumplan los criterios de seguridad.
- Responsable de Continuidad del Negocio: Lidera el Análisis de Impacto en el Negocio (BIA), mantiene los planes BCP/DRP y custodia las copias de seguridad offline independientes de la infraestructura primaria.
- Especialista en Riesgos y Cumplimiento: Garantiza el cumplimiento de regulaciones, coordina auditorías y mantiene actualizadas las políticas de privacidad y protección de datos.
- Dirección de Operaciones y Especialistas Técnicos: Implementan medidas técnicas de seguridad y ejecutan mantenimientos, respaldos y procedimientos en la nube.
- Usuarios y Empleados: Cumplen con las políticas de seguridad, reportan debilidades o incidentes y participan en las capacitaciones obligatorias.

5 Políticas Específicas

DEINSA mantendrá un catálogo estructurado de políticas específicas, procedimientos e instrucciones de trabajo que integran el SIG. Toda la documentación deberá ser revisada y actualizada formalmente al menos una vez al año, o bien cuando se presenten cambios significativos.

6 Cumplimiento y Auditoría

El cumplimiento de esta política y de las normativas aplicables se valida mediante un esquema sistemático de evaluación:

- Auditorías Integradas**:** Realización de auditorías internas unificadas al menos una vez al año para evaluar simultáneamente el cumplimiento de los controles de seguridad (ISO 27001) y resiliencia (ISO 22301).
- Evaluaciones Técnicas**:** Pruebas periódicas de seguridad, análisis de código y simulacros técnicos sobre la infraestructura en OCI.
- Gestión de Hallazgos: Toda desviación, vulnerabilidad crítica o No Conformidad detectada se administrará en el módulo "Observaciones" de DELPHOS. Se aplicará el análisis de causa raíz (5 porqués) para implementar Acciones Correctivas (AC) que eviten la reincidencia.

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 la causa raíz de una no conformidad detectada en el SIG, evitando su recurrencia.
- Activo de Información: Recurso tangible o intangible (datos, bases de datos, código fuente, repositorios) que posee valor para la organización y sus clientes.
- Confidencialidad: Propiedad que asegura que la información solo esté accesible para personas, procesos o sistemas autorizados.
- Control de Acceso: Conjunto de mecanismos que restringen el acceso lógico o físico a sistemas y datos según roles y privilegios autorizados.
- Disponibilidad: Accesibilidad y usabilidad de la información y servicios cuando sea requerido por los usuarios autorizados.
- Integridad: Salvaguarda de la exactitud y completitud de la información frente a modificaciones no autorizadas o accidentales.
- Sistema Integral de Gestión (SIG): Marco único de gobernanza que unifica la gestión de seguridad de la información (ISO 27001) y la continuidad del negocio (ISO 22301) en DEINSA.