Desarrollos Informáticos DEINSA Sociedad Anónima

Política de Continuidad del Negocio

Mayo 2026

Control de Versiones

Fecha	Versión	Autores	Aprobado por	Descripción	Nivel de Confidencialidad
Mayo 2024	1.0	DAB		Documento inicial	Información Interna
Mayo 2026	2.0	JCR / AAB	DAB	Actualización integral para cumplimiento de ISO 22301:2019 e integración al SIG.	Información Interna

DENNIS GERARDO ALVARADO BONILLA (FIRMA)

Firmado digitalmente por DENNIS GERARDO ALVARADO BONILLA (FIRMA)
Fecha: 2026.06.08 08:02:50 -06'00'

Tabla de contenido

1 Propósito

Establecer un marco sólido para la planificación, implementación y gestión de medidas que aseguren la continuidad de las operaciones y servicios de DEINSA ante interrupciones inesperadas, protegiendo los intereses de la empresa, empleados y clientes.

2 Alcance

Abarca todos los procesos críticos, especialmente la plataforma SaaS DELPHOS alojada en la nube de ORACLE y los servicios asociados que ofrecemos a nuestros clientes. Considera el contexto de sede en Costa Rica e infraestructura en centros de datos en Estados Unidos.

3 Objetivos

1. Garantizar la resiliencia operativa y el mantenimiento de funciones críticas.
2. Proteger la reputación corporativa y la confianza del cliente.
3. Cumplir con requisitos regulatorios de privacidad, ciberseguridad y acuerdos de confidencialidad.

4 Responsabilidades

1. Gerencia General

Responsabilidad final de la gestión, asignación de recursos (humanos y financieros) y liderazgo estratégico.

2. Director de Operaciones

Supervisar la infraestructura tecnológica, coordinar con proveedores de tecnología (Oracle Cloud) y ejecutar estrategias de recuperación de desastres (DRP).

3. Responsable de Continuidad

Desarrollo y actualización del BIA, estrategias de recuperación y asegurar la disponibilidad de copias de los planes fuera de los sistemas primarios.

4. Responsable de Seguridad de la Información

Asegurar que los controles de seguridad (ISO 27001) se mantengan operativos durante una contingencia.

5. Equipo de Continuidad

Activar el BCP, tomar decisiones clave y comunicarse con partes interesadas.

- Recuperación: Restauración de sistemas, datos y operaciones tras un evento disruptivo.
- Respuesta ante Emergencias: Intervención rápida y coordinación con servicios externos.

5 Principios de la Política

- Integración Estratégica: La continuidad es parte fundamental de la estrategia corporativa y las decisiones de inversión de DEINSA.
- Evaluación Continua: Identificación proactiva de riesgos y vulnerabilidades (fallos de infraestructura, ciberataques, desastres naturales).
- Mejora Continua: Revisión sistemática basada en lecciones aprendidas y resultados de pruebas.

6 Directrices de Continuidad

La Alta Dirección de DEINSA establece las siguientes directrices de continuidad:

1. Identificación y Análisis de Impacto (BIA)

Es obligatorio realizar anualmente un Análisis de Impacto en el Negocio (BIA) para identificar procesos críticos, interdependencias y activos de TI fundamentales como la plataforma DELPHOS y sus bases de datos. El BIA deberá determinar formalmente los tiempos de recuperación (RTO) y puntos de recuperación (RPO) aceptables para la operación.

2. Gestión Integral de Riesgos

La organización deberá ejecutar evaluaciones de riesgos para identificar amenazas externas e internas, incluyendo ciberataques, fallas de infraestructura en la nube y desastres naturales.

3. Desarrollo de Estrategias y Planes de Respuesta

Se instruye la creación y mantenimiento de Planes de Continuidad del Negocio (BCP) y Planes de Recuperación de Desastres (DRP) que contengan procedimientos técnicos paso a paso para la restauración de servidores, bases de datos SQL Server y servicios en Oracle Cloud.

4. Disponibilidad de Información Documentada Crítica

Por instrucción superior, el Responsable de Continuidad deberá garantizar que existan copias de alta disponibilidad de todos los planes de emergencia (BCP/DRP) fuera de los sistemas primarios y de la herramienta Delphos. Estas copias (digitales fuera de línea o impresas) deben estar bajo custodia del equipo de continuidad para asegurar su acceso inmediato ante una interrupción total de servicios.

5. Gestión de Continuidad con Terceros

La Gerencia de Operaciones deberá evaluar y monitorear a los proveedores críticos, estableciendo acuerdos de Servicio de Continuidad del Negocio (BCS). Se dará prioridad absoluta a la resiliencia de la infraestructura en Oracle Cloud por ser el pilar de la plataforma SaaS.

6. Programa de Pruebas y Validación

Es imperativo ejecutar ejercicios regulares basados en diversos escenarios de crisis para validar la efectividad de las estrategias de recuperación. Los resultados de estos ejercicios deberán documentarse como evidencias del SIG para alimentar el proceso de mejora continua.

7. Cumplimiento Legal y Normativo

DEINSA garantizará el cumplimiento estricto de la Ley de Protección de Datos Personales de Costa Rica y las regulaciones internacionales de privacidad aplicables en las regiones donde operan nuestros clientes. Todo plan de continuidad deberá respetar los acuerdos de confidencialidad y seguridad de la información vigentes.

8. Mantenimiento y Actualización

Los planes y políticas deberán revisarse formalmente ante cualquier cambio significativo en el entorno tecnológico o tras la detección de áreas de mejora en auditorías internas y externas.

7 Gestión de Incidentes y Comunicación

- Comunicación Interna: Uso de canales designados, actualizaciones regulares y sesiones virtuales durante una crisis.
- Comunicación Externa: Notificación proactiva a clientes y socios mediante portales de información y redes sociales.
- Reporte de Incidentes: Uso obligatorio de la mesa de ayuda en Delphos para recopilar datos sobre causas, impactos y acciones tomadas.

8 Formación y Concienciación

- Programa de Pruebas: Ejecución de ejercicios periódicos (recuperación de sistemas, ejercicios de respuesta) con participación del personal.
- Capacitación: Entrenamiento en procedimientos de crisis y uso de herramientas de apoyo (comunicación de emergencia, software de gestión).
- Campañas: Sensibilización mediante boletines para fortalecer la cultura de resiliencia.

9 Cumplimiento y Auditoría

- Monitoreo de Cumplimiento: El Responsable de Continuidad y el RSI evaluarán periódicamente el acatamiento de esta política.
- Auditorías: Se realizarán auditorías internas sistemáticas y, cuando se requiera, auditorías externas para validar la conformidad del sistema con la norma ISO 22301 y los requisitos del SIG.
- No Conformidades y Mejora: Cualquier hallazgo, desviación o falla se gestionará según el Procedimiento para la gestión de No Conformidades, Acciones Correctivas y Oportunidades de Mejora.

10 Sanciones y Consecuencias

El incumplimiento de los protocolos y a las directrices de seguridad y continuidad, está sujeto a las medidas correctivas y sanciones establecidas en el reglamento interno de DEINSA

11 Revisión y Actualización

Esta política se revisará anualmente o cada vez que ocurra un cambio significativo en el entorno operativo (infraestructura de TI) o regulatorio. Las auditorías internas y externas validarán su eficacia.