

1. Introducción y Propósito

El presente Plan de Continuidad de Negocio tiene como propósito asegurar la operación ininterrumpida de los servicios tecnológicos migrados a la nube, garantizando la disponibilidad, seguridad y estabilidad requeridas para las operaciones internas de la empresa.

Este PCN sigue los lineamientos de **ISO 22301**, priorizando la resiliencia, recuperación ante desastres y respuesta oportuna ante eventos que comprometan la continuidad operativa.

2. Alcance

El PCN cubre los siguientes elementos:

- Servicios migrados a la nube (aplicaciones críticas, bases de datos y almacenamiento).
 - Infraestructura virtual (VMs, redes, IAM, monitoreo).
 - Servicios complementarios (VPN, autenticación, respaldos).
 - Personal de TI, DevOps, Seguridad y Mesa de Ayuda.
-

3. Prioridades de Continuidad y Recuperación

3.1 MTOD y RPO

Actividad Clave	Impacto Potencial	MTOD	RPO
Acceso a aplicaciones críticas tras la migración	Interrupción del servicio, pérdida de clientes	4 horas	1 hora
Gestión de identidades IAM	Riesgo de seguridad, accesos no autorizados	6 horas	2 horas
Base de datos en la nube	Pérdida de integridad de datos	4 horas	1 hora
Red privada virtual (VPN)	Imposibilidad de operación remota	12 horas	4 horas
Automatizaciones CI/CD	Retrasos en entregas	24 horas	12 horas

4. Recursos Críticos

4.1 Humanos

- Cloud Architect
- Administradores de sistemas
- Ingeniero DevOps
- Especialista en Seguridad
- Mesa de Ayuda

4.2 Infraestructura

- Servidores cloud (IaaS / PaaS)
- Servicios de IAM
- Sistemas de monitoreo y logs
- Conectividad redundante
- Respaldos en frío y caliente

4.3 Información

- Configuraciones de infraestructura
- Políticas de seguridad
- Bases de datos sincronizadas
- Documentación técnica
- Scripts IaC (Terraform / CloudFormation)

5. Estrategias de Continuidad y Recuperación

Prioridad	Estrategia	Responsable	RTO
1. Servicios críticos	Failover automático a zona secundaria, restauración inmediata	Cloud Architect	4 hrs
2. IAM	Activación de políticas de emergencia, restauración de roles	Seguridad TI	6 hrs
3. BD	Recuperación desde snapshots automáticos	Administrador BD	4 hrs
4. VPN	Redireccionamiento a túnel alternativo	Redes TI	12 hrs
5. CI/CD	Activación de pipelines alternos	DevOps	24 hrs

6. Plan de Respuesta a Incidentes

1. Activación del comité de crisis
2. Notificación a stakeholders
3. Evaluación del incidente
4. Aplicación de estrategias de continuidad

5. Recuperación y monitoreo
 6. Normalización de operaciones
 7. Revisión y mejora del PCN
-

7. Pruebas y Actualización del PCN

- **Simulacros:** cada 6 meses
- **Prueba de restauración:** anual
- **Actualización del plan:** tras cambios críticos