PLAN DE MANEJO DE EMERGENCIAS, BCP Y DRP

Incendio en el Data Center

JOSE FRANCISCO OCHOA ORNELAS LDSW

Plan de Manejo de Emergencias, BCP y DRP

Riesgo seleccionado: Incendio en el Data Center

1. Análisis de Riesgo

1.1 Identificación del Riesgo

Riesgo: Incendio en el Data Center ubicado en Zapopan, Jalisco.

Causas posibles:

- Fallas eléctricas en servidores, UPS o infraestructura de potencia.
- Cortocircuitos en contactos, canalizaciones o cableado envejecido.
- Sobrecalentamiento de los equipos (AC de precisión fallando).
- Error humano (malas prácticas de cableado o mantenimiento).
- Incendio externo propagado desde comercios o domicilios vecinos.
- Descargas eléctricas o variaciones extremas de voltaje.

Activos afectados:

- 30 servidores Dell EMC PowerEdge R540
- Arreglo Dell EMC SC7020 con 30 SSD
- UPS Toshiba G9000 500 kVA
- Aire acondicionado Stulz Mini Space
- Switches Dell
- Servicios ERP, inventarios, punto de venta, cuentas por cobrar, nómina, compras, logística
- Datos operativos críticos de la compañía

1.2 Valoración del Impacto

Se evalúan dimensiones: económica, operativa, reputacional, legal.

DIMENSIÓN	IMPACTO	JUSTIFICACIÓN
ECONÓMICA	Muy alto	Pérdida de infraestructura >15 M MXN
OPERATIVA	Crítico	ERP fuera de línea
REPUTACIONAL	Alto	Pérdida de confiabilidad
LEGAL	Medio	Incumplimiento de obligaciones

1.3 Probabilidad

Probabilidad estimada:

- Zona urbana con flujo eléctrico variable.
- Cargas altas por UPS de 500 kVA.
- Mucho polvo ambiental en Guadalajara.

Probabilidad asignada: 3 (Media)

1.4 Nivel de Riesgo

Se usa matriz 5×5:

Riesgo = Impacto (5) × Probabilidad (3) = 15 → Riesgo Alto

2. Costo del Incidente

CONCEPTO	COSTO APROXIMADO
30 SERVIDORES DELL R540	$6,000,000 MXN
ARREGLO SC7020 + SSD	$2,500,000 MXN
UPS G9000 500 KVA	$2,300,000 MXN
STULZ PRECISION	$500,000 MXN
SWITCHES DELL	$350,000 MXN
CABLEADO Y SENSORES	$400,000 MXN
PÉRDIDAS OPERATIVAS 3 DÍAS	$9,000,000 MXN
TOTAL	$21,050,000 MXN

3. Plan de Manejo de Emergencias (CEM)

Fase 1: Mitigación

Acciones preventivas:

Infraestructura

- Instalación de sistema de supresión contra incendios de agente limpio (FM-200 o Novec1230).
- Sensores de humo de alta sensibilidad.
- Cableado certificado LSZH.
- Separación eléctrica en racks + canalización metálica.
- Mantenimiento trimestral del aire acondicionado de precisión.
- Sistema de monitoreo ambiental 24/7 (temperatura, humedad, partículas).
- UPS con bypass y pruebas de carga regulares.

Organización

- Capacitación anual del personal en NFPA 75 y 76.
- Restricción de acceso a personal autorizado.
- Revisiones de auditoría internas semestrales.

Fase 2: Preparación

- Diseño y difusión de un Plan de Respuesta a Incendios del Data Center.
- Rutas de evacuación señalizadas.
- Extintores CO_2 y de agente limpio, con recarga anual.
- Simulacros semestrales.
- Directorio de emergencia (Protección Civil Zapopan, Bomberos, CFE, Seguridad Privada).
- Copias del BCP y DRP impresas y digitales fuera del sitio.

Fase 3: Respuesta

Acciones inmediatas ante un evento:

1. Activación automática del sistema de supresión.
2. Corte inmediato de energía del Data Center.
3. Evacuación del personal.
4. Llamada a Bomberos y Protección Civil.
5. Activación del Equipo de Continuidad de Negocio.
6. Comunicación a dirección general y sucursales.
7. Activación del centro alterno (ver BCP).

Fase 4: Recuperación

- Evaluación de daños del recinto por parte de una brigada técnica.
- Restauración del sitio o traslado definitivo al centro alterno.
- Restauración del ERP y sistemas críticos desde backups.
- Reinstalación de infraestructura dañada.
- Informe final y actualización del BCP/DRP.

4. Plan de Continuidad de Negocio (BCP)

PROCESO	RTO	RPO	DEPENDENCIA
ERP VENTAS	4 hrs	30 min	Servidores/SC7020
INVENTARIOS	4 hrs	30 min	ERP
CONTABILIDAD	12 hrs	4 hrs	Servidores
LOGÍSTICA	12 hrs	2 hrs	ERP
FACTURACIÓN	8 hrs	1 hr	ERP

5. Plan de Recuperación de Desastres (DRP)

Objetivos:

- Restablecer ERP crítico en < 4 horas (RTO).
- Pérdida máxima de información: < 30 minutos (RPO).
- Reanudar operaciones completas en < 24 horas.

5.2 Procedimiento de Recuperación

Fase 1: Activación del DRP

- Director de TI declara desastre tras informe de brigada.
- Se activa el sitio alterno.
- Se notifica a todas las sucursales.

Fase 2: Recuperación Tecnológica

1. Levantar entornos virtuales en sitio alterno.
2. Restaurar la base de datos ERP desde réplica/logs.
3. Reconfigurar comunicaciones WAN.
4. Validar operación en dos sucursales piloto.
5. Desplegar acceso a todo el país.

Fase 3: Restauración al sitio original

- Daños reparados → se revierte operación al Data Center primario.
- Replicación inversa de datos.
- Pruebas de integridad y operación.

6. Conclusiones

El incendio es un riesgo de impacto crítico para este Data Center, capaz de paralizar completamente la operación nacional de la empresa.
La combinación de un Plan de Manejo de Emergencias, un BCP sólido basado en ISO 22301 y un DRP alineado a buenas prácticas NFPA y CEM permite garantizar que la organización pueda mantenerse operativa incluso ante un evento mayor, asegurando continuidad, estabilidad, integridad de los datos y confianza para clientes y proveedores.

7. Referencias (APA 6)

INCIBE. (2019). Fases de un plan de continuidad de negocio.

MTNET. (2017). Pasos básicos para diseñar un plan de recuperación.

RiesgosCero. (s.f.). Guía para gestionar un plan según ISO 22301.