Plan de Recuperación y Contingencia SOC

Security operations center (SOC)
REALTIME CONSULTING & SERVICES
https://www.rt.com.co/
soc@rt.com.co

Tabla de Contenido

Plan de Recuperación de Desastres: Falla de Firewall, Servidor y Almacenamiento . 3

1. Introducción 3

2. Alcance 3

3. Estrategias de Recuperación 3

3.1 Falla de Firewall 3

3.2 Falla de Servidor 4

3.3 Falla de Almacenamiento 4

4. Roles y Responsabilidades 5

4.1 Nivel 1: Operación y Monitoreo 5

4.2 Nivel 2: Análisis y Diagnóstico 5

4.3 Nivel 3: Proveedor HostDime 5

5. Comunicación Durante el Incidente 5

6. Conectividad 5

7. Documentación y Actualización 6

Plan de Recuperación de Desastres: Falla de Firewall, Servidor y Almacenamiento

---

Objetivo: Definir el proceso de recuperación ante desastres para fallas críticas en la infraestructura de un centro de datos, centrado en la recuperación de firewalls, servidores y sistemas de almacenamiento. Este documento servirá como referencia para integrar controles y estrategias implementadas por el proveedor HostDime.

---

1. Introducción

Los desastres pueden originarse por fallos de hardware, ataques cibernéticos, errores humanos o desastres naturales. Este plan tiene como fin garantizar la continuidad del negocio y minimizar el impacto en las operaciones mediante un enfoque sistemático y estructurado.

---

2. Alcance

Este documento cubre los procedimientos para:

- **Falla de firewall:** Interrupciones en la protección de red y acceso a servicios.
- **Falla de servidores:** Interrupción de aplicaciones y servicios críticos.
- **Falla de almacenamiento:** Pérdida o corrupción de datos almacenados.

---

3. Estrategias de Recuperación

3.1 Falla de Firewall

Controles Implementados:

- **Redundancia Activa-Pasiva:** Configuración de firewalls en modo HA (Alta Disponibilidad).
- **Respaldos (Snapshots) de Configuración:** Copias automáticas de configuraciones críticas.
- **Backup de Configuración:** Respaldo periódico en almacenamiento seguro.

Proceso de Recuperación:

1. Identificar la falla (hardware o software).
2. Activar el firewall de respaldo (si está configurado en HA).
3. Restaurar la configuración desde el último backup.
4. Realizar pruebas de conectividad y validación de políticas.

3.2 Falla de Servidor

Controles Implementados:

- **Virtualización:** Uso de entornos virtualizados para migración rápida.
- **Balanceo de Carga:** Para redistribuir el tráfico y evitar puntos únicos de fallo.
- **Backup de Sistemas y Datos:** Copias de seguridad programadas de todas las máquinas.

Proceso de Recuperación:

1. Analizar el origen del fallo (hardware o software).
2. Migrar las máquinas virtuales afectadas a servidores disponibles.
3. Restaurar desde la copia de seguridad más reciente si es necesario.
4. Validar la funcionalidad de las aplicaciones y servicios afectados.

3.3 Falla de Almacenamiento

Controles Implementados:

- **Redundancia RAID:** Configuración para tolerancia a fallos.
- **Almacenamiento Replicado:** Replicación automática entre centros de datos.
- **Respaldos (Snapshots) y Backups:** Instantáneas periódicas para recuperación rápida.

Proceso de Recuperación:

1. Identificar la causa de la falla (disco, controlador, etc.).
2. Activar almacenamiento replicado o restaurar desde snapshot.
3. Verificar la integridad de los datos y la continuidad de las operaciones.
4. Sustituir componentes defectuosos si es necesario.

4. Roles y Responsabilidades

4.1 Nivel 1: Operación y Monitoreo

- Monitorear alertas de infraestructura.
- Escalar incidentes al Nivel 2.

4.2 Nivel 2: Análisis y Diagnóstico

- Diagnosticar el problema y aplicar soluciones iniciales.
- Restaurar servicios utilizando backups y snapshots.

4.3 Nivel 3: Proveedor HostDime

- Proveer soporte avanzado para la recuperación.
- Sustituir hardware defectuoso.
- Gestionar la replicación y restauración a nivel de infraestructura.

---

5. Comunicación Durante el Incidente

1. Notificar a los equipos afectados y partes interesadas.
2. Enviar actualizaciones periódicas sobre el progreso de la recuperación.
3. Emitir un informe final detallando las causas y soluciones aplicadas.

---

6. Conectividad

1. Si falla la conexión de la VPN Site to Site establecida entre Real Time y HostDime, se tiene una conexión alterna, asignada por un proveedor ISP diferente para mantener alcance a la herramienta de monitoreo.
2. En dado caso que las dos VPN fallen se genera una comunicación directa al firewall de HostDime a través de una VPN SSL, donde se tiene el alcance a todas las herramientas del SOC.
3. Por fallas eléctricas en la sede principal se tiene una sede alterna en cota con el fin de que la operación no se vea afecta y se tenga acceso a través de la VPN SSL.

---

7. Documentación y Actualización

- Registrar el incidente en un sistema de gestión de eventos.
- Actualizar este documento con información específica provista por HostDime.
- Realizar revisiones periódicas para asegurar la efectividad del plan.

Notas: Este documento se actualizará según los procedimientos generados por HostDime ya que toda la infraestructura que se tiene para el SOC depende esta arrendada con este datacenter.