Plan de Recuperación para la Continuidad de los Servicios Críticos

Marco de Referencia: ISO/IEC 27001

Este plan se desarrolla conforme a las mejores prácticas de la ISO/IEC 27001, norma internacional para la gestión de seguridad de la información, asegurando que la continuidad de los servicios críticos sea gestionada de forma estructurada y efectiva.

---

1. Introducción

Este documento establece un plan para garantizar la continuidad operativa de los servicios críticos de la empresa en caso de un incidente de seguridad, en cumplimiento con los controles específicos de la ISO/IEC 27001 relacionados con la continuidad del negocio (A.17) y la gestión de incidentes de seguridad (A.16).

---

2. Objetivos del Plan

- Restaurar los servicios críticos en los tiempos definidos por el RTO (Recovery Time Objective) y el RPO (Recovery Point Objective).
- Proteger la confidencialidad, integridad y disponibilidad de la información afectada.
- Asegurar la comunicación efectiva con los interesados internos y externos.
- Prevenir futuros incidentes mediante medidas de mejora continua.

---

3. Servicios Críticos Identificados

De acuerdo con el análisis de impacto en el negocio (BIA, por sus siglas en inglés) realizado bajo la norma ISO/IEC 27001:

1. **Servicio Web (Apache)**: Portal principal y servicios de cara al cliente.
2. **Base de Datos (MySQL)**: Contiene información sensible de clientes y operaciones.
3. **Acceso Remoto (SSH)**: Acceso administrativo a servidores críticos.
4. **Registros del Sistema**: Evidencias de actividad que sustentan análisis forenses.

---

4. Escenarios de Impacto y Niveles de Amenaza

Escenarios de Impacto

1. **Eliminación de registros críticos**:
    - Impacto: Pérdida de trazabilidad y evidencia forense.
    - Nivel de Amenaza: Alto (Afecta la capacidad de respuesta y recuperación).
2. **Acceso no autorizado mediante SSH**:
    - Impacto: Riesgo de control total del sistema por un atacante.
    - Nivel de Amenaza: Crítico (Compromiso completo de la infraestructura).
3. **Compromiso del servicio web (Apache)**:
    - Impacto: Interrupción del servicio y posible exfiltración de datos.
    - Nivel de Amenaza: Alto (Impacto en la disponibilidad y confidencialidad).
4. **Contraseñas débiles en MySQL**:
    - Impacto: Acceso no autorizado a datos sensibles.
    - Nivel de Amenaza: Alto (Confidencialidad en riesgo).
5. **Presencia de archivos maliciosos**:
    - Impacto: Escalación de privilegios y persistencia de amenazas.
    - Nivel de Amenaza: Crítico (Permite ataques adicionales).

---

5. Estrategias de Recuperación

5.1. Preparación Previa al Incidente

En línea con los controles A.12.3 (Respaldo de la Información) y A.16.1.4 (Evaluación de Impacto), se implementan las siguientes acciones:

1. **Gestión de Copias de Seguridad**
    - Política de respaldos incremental (diaria) y completa (semanal).
    - Almacenamiento externo en ubicaciones seguras: local, nube y fuera del sitio.
    - Pruebas periódicas de restauración.
2. **Plan de Gestión de Activos**
    - Inventario actualizado de sistemas críticos.
    - Identificación de propietarios y responsables de cada servicio.
3. **Capacitación del Personal**

    - Entrenamiento continuo sobre gestión de incidentes y continuidad del negocio.
    - Simulacros de recuperación al menos una vez al trimestre.
4. **Fortalecimiento de Controles Técnicos**

    - Implementación de autenticación por llaves SSH (privada/pública).
    - Supervisión activa mediante herramientas como Wazuh o OSSEC.
    - Restricción de accesos a servicios sensibles (MySQL y FTP a localhost).

5.2. Respuesta Inmediata al Incidente

Paso 1: Activar el Equipo de Respuesta a Incidentes (IRT)

- Notificar a los interesados clave de acuerdo con el proceso definido (A.16.1.1).
- Convocar al IRT para evaluar el alcance del incidente.

Paso 2: Aislar el Sistema Comprometido

- Bloquear accesos no autorizados mediante firewall y desconexión de la red.
- Asegurar los servicios afectados para prevenir una escalación del impacto.

Paso 3: Preservar Evidencia Forense

- Crear imágenes del sistema afectado para análisis posterior.

Asegurar los registros disponibles mediante:
```
chattr +i /var/log/*
```

Paso 4: Neutralizar la Amenaza

Identificar y eliminar el archivo malicioso detectado:
```
rm -f /etc/rmt
```

- Deshabilitar cuentas comprometidas y cambiar contraseñas de emergencia.

5.3. Recuperación y Restauración de Servicios

Servicio Web (Apache):

1. Restaurar configuración desde respaldo seguro.
2. Aplicar reglas de firewall para limitar accesos no autorizados.
3. Reiniciar y validar integridad del servicio.

Base de Datos (MySQL):

1. Restaurar datos críticos desde copia de seguridad.
2. Configurar acceso restringido a localhost.
3. Establecer contraseñas robustas y únicas para cada usuario.

SSH (Acceso Remoto):

Deshabilitar autenticación por contraseña:
PasswordAuthentication no

1.
2. Implementar autenticación basada en llaves.
3. Establecer Fail2Ban para mitigar intentos de fuerza bruta.

Registros del Sistema:

1. Configurar almacenamiento remoto y centralizado de logs.
2. Implementar monitoreo de integridad con herramientas como AIDE.

---

6. Plan de Recuperación Post-Incidente

Análisis Posterior al Incidente (A.16.1.6)

1. Documentar el impacto del incidente.
2. Evaluar efectividad del plan de recuperación y realizar ajustes necesarios.
3. Presentar informe al comité de seguridad de la información.

Revisión de Controles y Medidas Preventivas

1. Actualizar los controles basados en la evaluación post-incidente.
2. Reforzar la capacitación de los empleados en gestión de incidentes.
3. Alinear mejoras con los objetivos de seguridad definidos en el ISMS (Sistema de Gestión de Seguridad de la Información).

---

7. Conclusión

Este plan asegura que la empresa está preparada para responder eficazmente a incidentes de seguridad, restaurar sus servicios críticos y fortalecer su postura de seguridad. La adopción de controles basados en la ISO/IEC 27001 garantiza un enfoque estructurado y confiable en la gestión de incidentes y continuidad del negocio.