PLAN DE RECUPERACIÓN ANTE INCIDENTES

1. Introducción

Este plan detalla los procedimientos de recuperación ante incidentes de seguridad para garantizar la restauración efectiva de los servicios críticos y la mitigación de impactos en la infraestructura tecnológica.

2. Objetivos

- Restaurar los servicios críticos en el menor tiempo posible.
- Minimizar la pérdida de datos y la interrupción operativa.
- Mitigar riesgos y prevenir incidentes futuros.
- Establecer procedimientos claros de respuesta y recuperación.

3. Alcance

Este plan aplica a los siguientes servicios críticos:

- **Servidor web (Apache, Nginx).**
- **Base de datos (MySQL, PostgreSQL).**
- **Acceso remoto y autenticación (SSH, VPN).**
- **Firewall y seguridad perimetral.**
- **Sistema de almacenamiento y copias de seguridad.**

---

4. Clasificación de Incidentes

Categoría	Descripción	Ejemplo
Crítico	Impacto directo en operaciones y datos sensibles	Exfiltración de datos, ransomware
Alto	Afectación parcial de servicios críticos	Ataques DDoS, acceso no autorizado

Medio	Interrupción menor sin pérdida de datos	Caída temporal del servidor web
Bajo	Incidente sin impacto significativo	Intentos fallidos de acceso

---

5. Procedimientos de Recuperación

5.1. Identificación y Contención

1. **Detección del incidente:**
   - Monitoreo de logs (/var/log/syslog, /var/log/auth.log).
   - Alertas de IDS/IPS (Snort, OSSEC).
   - Reportes de usuarios y sistemas de monitoreo.
2. **Contención inmediata:**
   - Desconectar servidores comprometidos de la red.
   - Bloquear direcciones IP maliciosas (iptables, ufw).
   - Revocar accesos comprometidos (passwd -l usuario).

5.2. Análisis Forense y Evaluación de Daños

1. **Revisión de actividad sospechosa:**
   - Comprobación de cambios en archivos (auditd, inotify).
   - Identificación de procesos anómalos (ps aux --forest).
2. **Determinación del alcance:**
   - Evaluación de datos comprometidos.
   - Análisis de integridad con Tripwire.
   - Creación de snapshots para investigación.

5.3. Restauración de Servicios Críticos

1. **Servidor web:**
   - Verificación de configuraciones (apache2ctl configtest).
   - Restauración desde backup (rsync, tar).

2. **Base de datos:**
    - Recuperación desde última copia (mysqldump --restore).
    - Validación de integridad (CHECK TABLE).
3. **Accesos y autenticación:**
    - Rotación de credenciales y claves SSH.
    - Reconfiguración de firewall y VPN.

5.4. Medidas Preventivas y Monitoreo Post-Incidente

1. **Refuerzo de Seguridad:**
    - Aplicación de parches y actualizaciones (apt update && apt upgrade).
    - Implementación de autenticación multifactor (MFA).
    - Configuración de reglas estrictas en firewall (ufw default deny).
2. **Monitoreo continuo:**
    - Uso de herramientas SIEM para detección temprana.
    - Análisis periódico de vulnerabilidades (OpenVAS, Nessus).
3. **Pruebas y Simulaciones:**
    - Ejecución de simulacros de recuperación.
    - Evaluaciones de seguridad trimestrales.

---

6. Conclusión y Recomendaciones

- Se ha establecido un procedimiento detallado para la identificación, contención y recuperación de incidentes.
- Se recomienda actualizar este plan periódicamente con base en nuevas amenazas y cambios en la infraestructura.
- La capacitación del equipo es clave para una respuesta efectiva ante incidentes futuros.

Este plan garantiza la continuidad operativa y la resiliencia ante amenazas de seguridad.