# Plan de Recuperación ante Incidentes y Continuidad de Servicios Críticos

## 1. Introducción y Alcance

El presente plan tiene como objetivo establecer las medidas y procedimientos necesarios para recuperar de forma rápida y ordenada los sistemas afectados por un incidente de seguridad o fallo operativo, garantizando la continuidad de los servicios críticos de la empresa. El plan abarca:

* Identificación y priorización de servicios críticos.
* Procedimientos de respuesta y recuperación ante incidentes.
* Estrategias de backup, redundancia y failover.
* Comunicación interna y con terceros para coordinación en la respuesta.

## 2. Objetivos del Plan

* **Minimizar el Tiempo de Inactividad:** Reducir al mínimo la interrupción de los servicios críticos durante y después de un incidente.
* **Preservar la Integridad de los Datos:** Garantizar que los datos sensibles y críticos se mantengan protegidos y se recuperen de forma íntegra.
* **Coordinar una Respuesta Efectiva:** Definir roles y responsabilidades para una respuesta coordinada y rápida ante incidentes.
* **Asegurar la Comunicación:** Establecer protocolos de comunicación interna y externa para informar a los usuarios y partes interesadas durante el incidente.
* **Evaluar y Mejorar Continuamente:** Realizar pruebas y actualizaciones periódicas del plan para adaptarlo a nuevas amenazas y cambios en la infraestructura.

## 3. Identificación de Servicios Críticos

Antes de la implementación del plan, se debe realizar un inventario de los sistemas y servicios considerados críticos. Entre ellos se incluyen:

* **Bases de Datos:** Servidores MySQL u otros, que alojan información esencial de la empresa.
* **Servicios de Autenticación:** Sistemas SSH, LDAP o similares, necesarios para el acceso seguro a la infraestructura.
* **Servidores Web y Aplicaciones:** Sitios web, aplicaciones internas y portales de clientes.
* **Sistemas de Comunicación:** Herramientas de correo electrónico y mensajería interna.
* **Redes y Conectividad:** Equipos de red, firewalls y otros dispositivos de infraestructura.

## 4. Equipo de Respuesta y Roles

Se conformará un Equipo de Respuesta a Incidentes (ERI) con roles claramente definidos:

* **Coordinador de Incidentes:** Responsable de dirigir y supervisar todas las acciones durante el incidente.
* **Analista Forense y de Seguridad:** Encargado de identificar el origen y alcance del incidente, y recopilar evidencias.
* **Administrador de Sistemas:** Responsable de la recuperación y puesta en marcha de los servicios afectados.
* **Comunicaciones:** Encargado de informar a la dirección y coordinar la comunicación interna y externa.
* **Soporte Técnico:** Personal encargado de la asistencia en tiempo real para la reconfiguración y monitoreo de servicios críticos.

## 5. Procedimientos de Respuesta y Contención

### 5.1 Detección y Notificación

* **Monitoreo Continuo:** Utilizar herramientas como Fail2ban, Wireshark, y sistemas de auditoría (Lynis, OpenVAS) para detectar anomalías.
* **Alerta Temprana:** Configurar notificaciones automáticas que informen al ERI de cualquier comportamiento anómalo o acceso no autorizado.
* **Registro de Incidentes:** Documentar de forma detallada la hora de detección, la naturaleza del incidente y las primeras evidencias recopiladas.

### 5.2 Contención Inmediata

* **Aislamiento de Sistemas:** Limitar el acceso a los sistemas afectados, aplicando reglas de firewall o desconectando segmentos de red si es necesario.
* **Detención de Accesos Maliciosos:** Bloquear cuentas comprometidas y detener servicios que presenten comportamiento anómalo mediante comandos como systemctl stop.
* **Revisión de Logs:** Analizar los logs del sistema para entender el alcance del incidente y evitar su propagación.

## 6. Procedimientos de Recuperación

### 6.1 Recuperación de Sistemas Afectados

* **Restauración de Backups:** Utilizar copias de seguridad previamente configuradas para restaurar los servicios críticos sin pérdida de datos. Es fundamental que las copias de seguridad se realicen de forma regular y se almacenen en ubicaciones seguras.
* **Reconfiguración de Servicios:**
  + Actualizar contraseñas y claves de autenticación.
  + Reestablecer configuraciones de seguridad en servicios como FTP, SSH y servidores web.
  + Verificar la integridad de archivos críticos (ej. wp-config.php).
* **Verificación de Integridad:** Ejecutar escaneos con herramientas de seguridad (Nikto, OpenVAS) para confirmar que no quedan vulnerabilidades residuales.

### 6.2 Continuidad Operativa y Failover

* **Sistemas Redundantes:** Implementar redundancia en servicios críticos, de modo que si un sistema falla, un servidor de respaldo asuma la carga.
* **Balanceo de Carga:** Configurar mecanismos de balanceo de carga para distribuir el tráfico y garantizar la disponibilidad continua de los servicios.
* **Procedimientos de Failover:** Establecer protocolos automáticos y manuales para el cambio a sistemas de respaldo sin afectar la operatividad de la empresa.

## 7. Comunicación y Coordinación

### 7.1 Comunicación Interna

* **Alertas y Actualizaciones:** El coordinador de incidentes deberá informar de forma periódica al equipo y a la dirección sobre el estado del incidente.
* **Canal de Comunicación:** Utilizar plataformas seguras (mensajería cifrada, correo interno) para coordinar la respuesta en tiempo real.

### 7.2 Comunicación Externa

* **Informar a Clientes y Socios:** En caso de que el incidente afecte servicios externos, se debe preparar un comunicado para clientes y socios, asegurando la transparencia y las medidas correctivas adoptadas.
* **Colaboración con Autoridades:** Notificar a las autoridades competentes en caso de que el incidente involucre accesos o actividades delictivas.

## 8. Pruebas y Actualización del Plan

* **Pruebas de Simulacro:** Realizar simulacros periódicos para evaluar la eficacia del plan, identificando áreas de mejora.
* **Revisión y Actualización:** Actualizar el plan al menos una vez al año o cada vez que se realicen cambios significativos en la infraestructura o se identifiquen nuevas amenazas.
* **Documentación Continua:** Registrar las lecciones aprendidas en cada simulacro o incidente real para mejorar continuamente las respuestas y procedimientos.

## 9. Herramientas de Apoyo

Para facilitar la detección, contención y recuperación se utilizarán las siguientes herramientas:

* **Monitoreo y Alerta:** Fail2ban, Wireshark, Nagios o Zabbix.
* **Análisis y Auditoría:** Lynis, OpenVAS, Nikto.
* **Gestión de Backups:** Software de backup automatizado (ejemplo: Bacula, Veeam) y almacenamiento en ubicaciones seguras.
* **Sistemas de Redundancia:** Herramientas de balanceo de carga y configuraciones de failover (HAProxy, Keepalived).

## 10. Conclusiones

Este plan de recuperación ante incidentes se orienta a asegurar que, en caso de un evento adverso, la empresa pueda responder de forma coordinada y eficaz, garantizando la continuidad de los servicios críticos. La combinación de procedimientos de contención, recuperación y comunicación, junto con la implementación de redundancias y herramientas de monitoreo, ofrece una estrategia integral para minimizar el impacto del incidente y mantener la operatividad de la infraestructura.