ÍNDICE

1. Introducción

Este informe describe el Plan de Recuperación ante Incidentes (PRI) que tiene como objetivo restaurar los servicios críticos de la empresa tras un incidente de seguridad. El plan está basado en las mejores prácticas de respuesta a incidentes y en la norma **ISO 27001**, con el fin de garantizar la continuidad de las operaciones y minimizar el impacto de cualquier ataque o incidente en la infraestructura de TI.

2. Objetivos del Plan de Recuperación Ante Incidentes

- **Identificar** los incidentes de seguridad en sus primeras etapas.
- **Contener** el incidente para evitar su propagación.
- **Erradicar** la causa raíz del incidente.
- **Recuperar** los servicios críticos lo más rápido posible.

- **Prevenir** futuros incidentes de la misma índole.
- **Mantener** la continuidad de los servicios esenciales.

3. Estrategia de Respuesta a Incidentes

3.1. Preparación

- Capacitar al personal en el manejo de incidentes.
- Asegurarse de que las herramientas de respuesta y los recursos estén disponibles.
- Tener sistemas de respaldo actualizados y almacenados en ubicaciones externas.

3.2. Identificación del Incidente

- Monitorear los logs del sistema, las alertas del firewall y el tráfico de red.
- Clasificar el incidente según su gravedad.
- Notificar inmediatamente a los equipos de seguridad y la gerencia.

3.3. Contención

- Aislar el sistema comprometido.
- Implementar controles temporales para mitigar los efectos del ataque (por ejemplo, bloquear direcciones IP comprometidas).

3.4. Erradicación

- Investigar el incidente y eliminar los archivos maliciosos y las configuraciones alteradas.
- Aplicar parches y soluciones a las vulnerabilidades explotadas.

3.5. Recuperación

- Restaurar los servicios críticos utilizando copias de seguridad.
- Verificar la integridad de los servicios restaurados y monitorear para asegurarse de que no haya signos de actividad maliciosa.

3.6. Lecciones Aprendidas y Prevención

- Analizar el incidente para identificar qué falló y cómo se puede mejorar.
- Reforzar las políticas de seguridad y las configuraciones del sistema.

4. Continuidad de los Servicios Críticos

4.1. Servicios Críticos para la Empresa

Los servicios más críticos incluyen:

- **Base de datos**: Para almacenar la información vital de la empresa.
- **Correo electrónico**: Para la comunicación interna y externa.
- **Aplicaciones web**: Para acceder a los sistemas internos y servicios web.
- **Acceso remoto**: Servicios como SSH y VPN.
- **Sistemas de respaldo**: Para garantizar que los datos puedan ser restaurados.

4.2. Plan de Respaldo y Recuperación

- **Respaldo diario**: Realizar copias de seguridad regulares de los servicios más críticos.
- **Almacenamiento fuera del sitio**: Mantener copias de seguridad en una ubicación externa.
- **Pruebas de restauración**: Verificar regularmente que las copias de seguridad sean válidas.

5. Mecanismos de Protección de Datos

5.1. Cifrado de Datos Sensibles

- **Cifrado en tránsito**: Usar HTTPS y VPN para proteger la información sensible.
- **Cifrado en reposo**: Asegurar que los datos sensibles estén cifrados cuando están almacenados.

5.2. Control de Acceso Estricto

- **Autenticación multifactor (MFA)**: Implementar MFA en todos los servicios críticos.
- **Principio de menor privilegio**: Limitar el acceso solo a los usuarios que lo necesiten.
- **Auditoría de acceso**: Realizar auditorías periódicas para revisar cuentas de usuario y permisos.

6. Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI)

6.1. Análisis de Riesgos

- **Identificación de riesgos**: Evaluar las amenazas y vulnerabilidades en la infraestructura.
- **Valoración del impacto**: Determinar el impacto potencial de cada riesgo.
- **Planes de mitigación**: Implementar medidas para reducir la probabilidad y el impacto de los riesgos.

6.2. Políticas de Seguridad

- **Política de contraseñas**: Crear normas estrictas para la creación y gestión de contraseñas.
- **Política de respaldo**: Definir procedimientos claros para la realización de copias de seguridad y su recuperación.

6.3. Planes de Acción para Proteger Información Crítica

- **Redundancia de servicios**: Implementar alta disponibilidad para los servicios más críticos.
- **Monitoreo continuo**: Monitorear todos los servicios de manera continua para detectar posibles fallos o amenazas.

Este informe debe servir como base para la creación de un entorno más seguro en la empresa, garantizando que todos los servicios esenciales estén protegidos y que exista un plan claro para responder ante futuros incidentes.