

plan de recuperacion de incidentes



4 geeks academy

Contenido

[1. Objetivo del Plan 2](#_Toc191383646)

[2. Alcance 2](#_Toc191383647)

[3. Fases del Plan de Recuperación 2](#_Toc191383648)

[Preparación 2](#_Toc191383649)

[Contención 3](#_Toc191383650)

[Erradicación 3](#_Toc191383651)

[Recuperación 3](#_Toc191383652)

[Lecciones Aprendidas 3](#_Toc191383653)

[4. Responsabilidades 4](#_Toc191383654)

[5. Cronograma 4](#_Toc191383655)

[6. Revisión y Actualización del Plan 4](#_Toc191383656)

# Objetivo del Plan

El objetivo de este plan es establecer un conjunto de procedimientos y acciones a seguir para recuperar la seguridad y la integridad del servidor FTP tras el incidente de acceso no autorizado, así como para prevenir futuros incidentes.

# Alcance

Este plan se aplica al servidor FTP afectado y a todos los sistemas y datos relacionados. También incluye la capacitación del personal y la revisión de políticas de seguridad.

# Fases del Plan de Recuperación

## Preparación

- Revisión de Políticas de Seguridad : Actualizar las políticas de seguridad de la organización para incluir directrices específicas sobre el uso de servidores FTP.

- Capacitación del Personal : Realizar sesiones de capacitación sobre seguridad informática y mejores prácticas para el manejo de datos sensibles.

- Implementación de Herramientas de Monitoreo : Asegurar que se utilicen herramientas de monitoreo de seguridad para detectar accesos no autorizados en tiempo real.

## Contención

- Deshabilitar Acceso Anónimo : Inmediatamente deshabilitar el acceso anónimo al servidor FTP.

- Revisar Configuraciones de Seguridad : Auditar la configuración del servidor FTP y aplicar las mejores prácticas de seguridad.

- Bloquear Direcciones IP Sospechosas : Identificar y bloquear las direcciones IP que intentaron acceder al servidor de manera no autorizada.

## Erradicación

- Eliminar Archivos Comprometidos : Identificar y eliminar cualquier archivo que haya sido comprometido o descargado durante el incidente.

- Actualizar Software : Asegurarse de que el software del servidor FTP y cualquier otro software relacionado estén actualizados con los últimos parches de seguridad.

- Revisar y Fortalecer Políticas de Contraseñas : Implementar políticas de contraseñas más estrictas para el acceso al servidor.

## Recuperación

- Restaurar Servicios : Una vez que se hayan implementado las medidas de seguridad, restaurar el acceso al servidor FTP con autenticación de usuario.

- Monitoreo Continuo : Implementar un monitoreo continuo del servidor para detectar cualquier actividad sospechosa.

- Revisar Logs : Continuar revisando los logs del servidor para identificar cualquier intento de acceso no autorizado posterior al incidente.

## Lecciones Aprendidas

- Reunión de Evaluación : Realizar una reunión con el equipo de TI y otros interesados para discutir el incidente, las acciones tomadas y las lecciones aprendidas.

- Documentación : Documentar el incidente y las acciones tomadas en un informe final que se compartirá con la alta dirección.

# Responsabilidades

- Equipo de TI : Responsable de la implementación de las medidas de contención, erradicación y recuperación.

- Administrador de Sistemas : Responsable de la configuración y seguridad del servidor FTP.

- Gerente de Seguridad : Responsable de la supervisión del proceso de recuperación y de la capacitación del personal.

# Cronograma

|  |  |  |  |
| --- | --- | --- | --- |
| Fase | Actividad | Responsable | Fecha Límite |
| Preparación | Revisión de políticas de seguridad | Gerente de Seguridad | 20 de febrero 2025 |
| Preparación | Capacitación del personal | Administrador de TI | 25 de febrero 2025 |
|  |  |  |  |
| Contención | Deshabilitar acceso anónimo | Administrador de TI | 14 de febrero 2025 |
| Contención | Bloquear IPs sospechosas | Administrador de TI | 16 de febrero 2025 |
| Erradicación | Eliminar archivos comprometidos | Administrador de TI | 14 de febrero 2025 |
| Recuperación | Reunión de evaluación | Administrador de TI |  |
| Lecciones Aprendidas | Reunión de evaluación | Gerente de Seguridad | 30 de febrero 2025 |

# Revisión y Actualización del Plan

Este plan debe ser revisado y actualizado anualmente o después de cualquier incidente significativo para asegurar su efectividad y relevancia.