## **Plan de Recuperación ante Incidencias**

**Reportado por:**

**Germán Alberto Parra Araque**

**4Geeks Academy**

**Colombia**

[**Plan de Recuperación ante Incidencias 1**](#_8hyglkcio3pu)

[**Plan de Respuesta ante Incidentes 3**](#_xzwjukchl1cs)

[**1. Preparación 3**](#_mw108wdmgjom)

[**2. Detección y Análisis 3**](#_53se7t2bl9ql)

[**3. Contención, Erradicación y Recuperación 4**](#_kowx0kzc3svy)

[**4. Actividades Posteriores 5**](#_v4u1j4ir3fnh)

[**5. Roles y Responsabilidades 5**](#_9wksu3x8pud1)

[**6. Comunicación 6**](#_lypi3blohtq7)

[**7. Mantenimiento del Plan 6**](#_1r4s66feomuu)

[**8. Conclusión 6**](#_p5wipjxm5cvu)

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## 

## **Plan de Respuesta ante Incidentes**

**Basado en NIST SP 800-61 Rev. 3  
Banco de Teusaquillo**

### **Preparación**

**Objetivo:** Establecer las condiciones necesarias para responder eficazmente ante incidentes de ciberseguridad que puedan afectar la confidencialidad, integridad o disponibilidad de los activos tecnológicos.

**Acciones clave:**

* Mantener actualizado el servidor Debian 12, sus aplicaciones y los servicios que este aloja.
* Contar con copias de seguridad verificadas del sitio WordPress y su base de datos.
* Definir roles y responsabilidades del equipo de respuesta ante incidentes.
* Implementar herramientas de monitoreo, como revisión de logs, detección de cambios o alertas automatizadas a través de un sistema EDR o XDR.
* Establecer canales de comunicación para la coordinación durante un incidente.
* Contar con documentación técnica de la configuración de los equipos tecnológicos.
* Mantener una copia de seguridad **auth.log** alojado en otro equipo tecnológico, esta debe generarse de manera periódica.
* Definir procesos de back up sobre archivos y directorios esenciales sobre el sistema, estos se deben respaldar en un dispositivo externo al servidor

### **Detección y Análisis**

**Objetivo:** Identificar rápidamente posibles incidentes, clasificarlos correctamente y determinar su alcance e impacto.

**Indicadores comunes en el entorno evaluado:**

* Identificación de logs dentro del sistema SIEM que involucren eventos de seguridad de la información.
* Con el apoyo del sistema EDR, permitirle establecer actividades de contención y aislamiento
* Intentos de acceso remoto al servidor en horarios infrecuentes.
* Intentos fallidos de acceso que sean reiterativos a través de ssh.
* Mal rendimiento dentro del servidor.
* Denegación de servicios prestados como el servidor web, FTP o de Base de datos .
* Intentos reiterados de acceso no autorizado a interfaces web de inicio de sesión.
* Usuarios desconocidos en la base de datos mysql.
* Archivos desconocidos o sospechosos en directorios como **wp-content/uploads/**.
* Habilitación de listado de directorios del servidor web.
* Exposición de archivos sensibles, dentro del servidor web como license.txt, wp-link-opml entre otros.
* Registros anómalos en los logs del servidor web Apache.
* Cambios de configuración de archivos como **wp-config.php**, **sshd\_config** o **vsftpd.conf**

**Clasificación de incidentes según NIST:**

| **Tipo de incidente** | **Ejemplo** |
| --- | --- |
| Intrusión | Acceso remoto no autorizado a WordPress, FTP, base de datos o al sistema operativo |
| Exposición de información | Acceso público a directorios o archivos sensibles sin autenticación |
| Uso indebido del sistema | Carga de shells y scripts maliciosos |
| Alertas de seguridad | Registro de actividades en los sistemas de monitoreo de la red informática, como EDR y SIEM. |
| Denegación de servicios | Indisponibilidad del ambiente web de la empresa, a través de solicitudes maliciosas. |

Figura 1. Clasificación de incidentes.

### **Contención, Erradicación y Recuperación**

**Contención:**

* Aislar temporalmente el sistema afectado de la red, desconectándolo dentro de la misma.
* Cambiar credenciales comprometidas.
* Aplicar restricciones mediante firewall o reglas de bloqueo de IP.

**Erradicación:**

* Eliminar cualquier archivo malicioso o no autorizado.
* Corregir configuraciones inseguras (como listado de directorios habilitados, configuración de archivos de servicios, etc.).
* Actualizar todos los componentes del CMS, incluyendo plugins y temas.
* Detener procesos que generen problemas de rendimiento o generación de eventos inesperados

**Recuperación:**

* Restaurar el sistema a partir de una copia de seguridad verificada.
* Validar la funcionalidad del sistema antes de reincorporarlo al entorno de producción.
* Fortalecer medidas de seguridad para prevenir recurrencias.

### **Actividades Posteriores**

**Objetivo:** Obtener aprendizajes del incidente para mejorar las políticas, configuraciones y capacidades de respuesta futura.

**Acciones:**

* Generar un proceso de auditoría de ciberseguridad.
* Documentar de forma detallada la línea de tiempo y acciones tomadas.
* Analizar causas raíz y puntos débiles detectados.
* Actualizar configuraciones, documentación y procedimientos internos.
* Comunicar hallazgos relevantes al equipo de TI y áreas interesadas.
* Informar a partes interesadas sobre el incidente de seguridad y sus correcciones realizadas.

### **Roles y Responsabilidades**

Se definen los roles de los actores implicado en el plan de recuperación ante incidencias:

| **Rol** | **Función principal** |
| --- | --- |
| Coordinador de Respuesta | Dirige el proceso de manejo del incidente y toma decisiones clave |
| Analista de Seguridad | Ejecuta análisis técnicos y determina el alcance del incidente |
| Técnico de Infraestructura | Ejecuta restauraciones y aplica medidas de contención |
| Oficial de Cumplimiento | Evalúa implicaciones legales y coordina notificaciones externas |

Figura 2. Tabla de roles y responsabilidades

### **Comunicación**

* Establecer un canal interno de respuesta rápida ante incidentes.
* Notificar oportunamente a las partes responsables dentro de la organización.
* En caso necesario, emitir comunicados a usuarios, clientes o entidades reguladoras conforme a las políticas de cumplimiento.

### **Mantenimiento del Plan**

* Este plan debe ser revisado de manera periódica, al menos cada 6 a 12 meses.
* Deben realizarse ejercicios de simulación para validar la efectividad del proceso de respuesta al menos una vez al año.

### **Conclusión**

Este plan, basado en el estándar NIST SP 800-61 Rev. 3, proporciona una estructura sólida para la gestión de incidentes de seguridad en la infraestructura tecnológica del Banco de Teusaquillo. Su correcta aplicación permite minimizar impactos operativos, garantizar la recuperación efectiva de los sistemas y fortalecer la postura de ciberseguridad de la organización.