# METODOLOGÍA DE RESPUESTA A INCIDENTES

# IRM #6: DESFIGURACIÓN DE SITIOS WEB

Reacción en vivo en un servidor web comprometido.

**Autor IRM: CERT SG**
**Contribución: CERT a Dvens / Paloma Vargas**
**Versión del IRM: 2.0**
**E-Mail: cert.sg@socgen.com**
**Web: https://cert.societegenerale.com**
**Twitter: @CertSG**

**Traducción al Español**

**Paloma Amilene Vargas Alvarado**
**E-Mail: amilenhalvarado@gmail.com**
**Twitter / X: @AmileneVargas**

# Contenido

## 1. ABSTRACTO

Esta metodología de respuesta a incidentes, es una hoja de referencia dedicada a los analistas que investigan un problema preciso de seguridad.

¿QUIÉN DEBE UTILIZAR HOJAS IRM?

- Administradores.
- Centro de Operaciones de Seguridad.
- CISO y adjuntos.
- CERT (Equipo de respuesta ante emergencias informáticas).

Recuerde: Si se enfrenta a un incidente, siga el IRM y tome notas. Mantenga la calma y, si es necesario, contacte inmediatamente con el equipo de Respuesta a Incidentes o el CERT de su línea de negocio.

## 2. PASOS PARA LA GESTIÓN DE INCIDENTES

***SE DEFINEN 6 PASOS PARA GESTIONAR INCIDENTES DE SEGURIDAD***

1. Preparación: prepárese para manejar el incidente
2. Identificación: detectar el incidente
3. Contención: limitar el impacto del incidente
4. Remediación: eliminar la amenaza
5. Recuperación: recuperarse a una etapa normal
6. Lecciones aprendidas: elaborar y mejorar el proceso

IRM proporciona información detallada para cada paso del proceso de respuesta a incidentes. Los pasos provienen de la Guía de Gestión de Incidentes de Seguridad Informática del NIST.

## 2.1 PREPARACIÓN

***OBJETIVO***: ESTABLECER CONTACTOS, DEFINIR PROCEDIMIENTOS, REUNIR INFORMACIÓN PARA AHORRAR TIEMPO DURANTE UN INCIDENTE.

- Tenga esquemas actualizados que describan sus componentes aplicativos relacionados con el servidor web.
- Asegúrese de tener un mapa de red actualizado.
- Construya un sitio web de respaldo listo y preparado, en el que pueda publicar contenido.
- Defina un procedimiento para redirigir a cada visitante a este sitio web de respaldo (una página de mantenimiento estática, por ejemplo).
- Despliegue herramientas de monitoreo y prevención de intrusiones (WAF, fail2ban y similares) para detectar y prevenir cualquier actividad anormal dirigida a sus servidores web críticos.
- Exporte los archivos de registro del servidor web a un servidor externo. Asegúrese de que los relojes estén sincronizados entre cada servidor.
- Despliegue reglas de detección de explotación de vulnerabilidades y ataques basada en los registros del servidor y monitoréelas.
- Audite sus sitios web antes del lanzamiento y de forma regular (mensualmente si es posible).
- Referencie todas las fuentes de contenido estático o dinámico externo.
- Tenga los contactos operativos de su proveedor de alojamiento (hosting providers) disponibles.
- Asegúrese de que su proveedor de alojamiento aplique políticas para registrar todos los eventos y verifique su cumplimiento contractual.
- Prepare plantillas de comunicación en caso de que el incidente sea visible para los usuarios y necesite ser explicado.

## 2.2 IDENTIFICACIÓN

***OBJETIVO***: DETECTAR EL INCIDENTE, DETERMINAR SU ALCANCE E INVOLUCRAR A LAS PARTES APROPIADAS.

**Los canales habituales de detección son:**

- Monitoreo de la página web: El contenido de una página web ha sido alterado. El nuevo contenido es muy discreto (una inyección de "iframe" por ejemplo) o explícito ("Ha sido hackeado por xxx").
- Usuarios: recibe llamadas de usuarios o notificaciones de empleados sobre problemas que notan mientras navegan por el sitio web.
- Controles de seguridad con herramientas como Google SafeBrowsing.

**Verifique el incidente de desfiguración y detecte su origen:**

- Verifique los metadatos de los archivos (en particular, verifique las fechas de modificación, las firmas hash).
- Verifique los proveedores de contenido mashup.
- Verifique los enlaces presentes en el código fuente (src, meta, css, scripts).
- Verifique los archivos de registro y las alertas generadas por las reglas de detección.
- Escanee las bases de datos en busca de contenido malicioso.

**El código fuente de la página sospechosa debe analizarse cuidadosamente para identificar y delimitar el problema.**

**Asegúrese de que el problema se origine en un servidor web que pertenezca a la empresa y no en el contenido web ubicado fuera de su infraestructura, como en banners publicitarios de un tercero.**

## 2.3 CONTENCIÓN

***OBJETIVO***: MITIGAR LOS EFECTOS DEL ATAQUE EN EL ENTORNO.

- Realice una copia de seguridad de todos los datos almacenados en el servidor web para fines forenses y recolección de evidencia. La mejor práctica aquí, si es aplicable, es crear una copia completa bit a bit del disco duro utilizado por el servidor web. Esto puede ser particularmente útil para recuperar contenido eliminado.
- Verifique su mapa de arquitectura de red. Verifique que la vulnerabilidad explotada por el atacante no se encuentre en otro lugar:

    - Verifique el sistema en el que se está ejecutando el servidor web.
    - Verifique otros servicios que se ejecutan en esa máquina.
    - Verifique las conexiones entrantes y salientes realizadas desde el servidor.

**Si el origen del ataque proviene de otro sistema, investigue la máquina culpable.**

- Intente encontrar evidencia detrás de cada acción perpetrada por el atacante:
- Descubra cómo ingresó el atacante al sistema en primer lugar y corrija las causas raíz:
    - Una vulnerabilidad de componente web que permite el acceso de escritura: corrija la vulnerabilidad aplicando las remediaciones aplicables.
    - Las vulnerabilidades de plugins de CMS suelen ser explotadas por atacantes y deben identificarse y parchearse.
    - Carpeta pública abierta: hágalo privado.
    - Debilidad de SQL que permite la inyección: corrija el código.
    - Componentes mashup: corte las fuentes de mashup implicadas.
    - Una modificación administrativa por acceso físico: modifique los derechos de acceso.

**Si es necesario (problema complejo en un servidor web importante), despliegue un servidor web temporal actualizado,. El servidor debe ofrecer el mismo contenido que el de la máquina comprometida o al menos mostrar contenido legítimo, como una página de mantenimiento estática. Lo mejor es mostrar contenido estático temporal, que contenga solo código HTML. Esto evita otra infección en caso de que el atacante aún pueda aprovechar la misma vulnerabilidad.**

## 2.4 REMEDIACIÓN

***OBJETIVO***: TOMAR ACCIONES PARA ELIMINAR LA AMENAZA Y EVITAR FUTURAS DESFIGURACIONES.

- Elimine todo el contenido alterado y reemplácelo con contenido legítimo, restaurado a partir de una copia de seguridad anterior.

- Asegúrese de que este contenido esté libre de vulnerabilidades; aplique parches si es necesario.

## 2.5 RECUPERACIÓN

**OBJETIVO:** RESTAURAR EL SISTEMA A SUS OPERACIONES NORMALES.

- Cambie todas las contraseñas de usuario si el servidor web proporciona autenticación de usuario y tiene evidencia o razones para creer que las contraseñas pueden haber sido comprometidas. Esto puede requerir una campaña de comunicación con el usuario.

- Si se ha utilizado un servidor de respaldo, restaure los componentes principales del servidor web a su estado nominal.

- Monitoree de cerca los registros y las alertas para detectar nuevos ataques.

## 2.6 LECCIONES APRENDIDAS

***OBJETIVO***: DOCUMENTAR LOS DETALLES DEL INCIDENTE, DISCUTIR LAS LECCIONES APRENDIDAS Y AJUSTAR LOS PLANES Y LAS DEFENSAS.

### *Comunicación*

Si la desfiguración se ha hecho pública, considere preparar y enviar un mensaje de comunicación dedicado explicando el incidente.

### *Informe*

Se debe redactar un informe de crisis y ponerlo a disposición de todos los actores de la célula de gestión de crisis.

Se deberán describir los siguientes temas:

- Causa inicial de la infección
- Acciones y cronogramas de cada evento importante
- ¿Qué salió bien?
- ¿Qué salió mal?
- Costo del incidente
- Indicadores de compromiso

Si se identifica una vulnerabilidad, informe cualquier falla no documentada que afecte al editor de la aplicación, para que el código pueda ser revisado y reciba una corrección oficial.

### *Capitalizar*

Se deben definir acciones para mejorar los procesos de gestión de infecciones por gusanos, para aprovechar esta experiencia.

## 3. DEFINICIONES

| CONCEPTO | DESCRIPCIÓN |
|---|---|
| **IRM** | Metodología de Respuesta a Incidentes |
| **CISO** | Chief Information Security Officer (ejecutivo responsable de la seguridad de la información) |
| **CERT** | Equipo de Respuesta a Incidentes Informáticos |
| **NIST** | Instituto Nacional de Estándares y Tecnología |
| **EDR** | Detección y Respuesta de Puntos de Acceso |
| **Website Defacement (Desfiguración de sitios web)** | Un incidente de seguridad que ocurre cuando el contenido de una página web ha sido alterado. Puede ser discreto (como una inyección de iframe) o explícito. |
| **WAF (Web Application Firewall)** | Herramienta de monitoreo y prevención de intrusiones que debe desplegarse para detectar actividades anormales dirigidas a servidores web críticos. |
| **fail2ban** | Herramienta de monitoreo y prevención de intrusiones que debe desplegarse para detectar actividades anormales dirigidas a servidores web críticos. |
| **iframe injection** | Una alteración discreta del contenido de una página web, mencionada como un canal de detección de desfiguración. |
| **Google SafeBrowsing** | Una herramienta de seguridad utilizada como canal habitual para verificar la seguridad de un sitio web. |
| **Firmas hash** | Valores utilizados para verificar los metadatos de los archivos durante la identificación del origen del incidente. |
| **Copia completa bit a bit** | La mejor práctica para respaldar todos los datos almacenados en el servidor web para fines forenses y de recolección de evidencia durante la contención. |
| **Vulnerabilidades de plugins de CMS** | Fallas en los plugins del Sistema de Gestión de Contenidos. Son causas raíz común de ataques que deben identificarse y parchearse. |
| **Debilidad de SQL que permite la inyección** | Un tipo de vulnerabilidad que permite la inyección de código SQL y es una causa raíz que debe ser corregida. |
| **Mashup components/feeds** | Fuentes de contenido estático o dinámico externo que deben referenciarse y pueden necesitar ser cortadas si están implicadas en el ataque. |
| **HTML** | El lenguaje de marcado. Se recomienda que, durante la contención, el servidor temporal muestre contenido |

| | |
|---|---|
| | estático que contenga solo código HTML para prevenir nuevas infecciones |
| **Indicadores de compromiso** | Información crucial sobre el ataque que debe detallarse en el informe de crisis. |