# METODOLOGÍA DE RESPUESTA A INCIDENTES

# IRM #4 RESPUESTA A INCIDENTES DDOS

Pautas para manejar Incidentes de Denegación de Servicio Distribuido.

**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** ..... 3
**2. PASOS PARA LA GESTIÓN DE INCIDENTES** ..... 4
**2.1 PREPARACIÓN** ..... 5
**2.2 IDENTIFICACIÓN** ..... 7
**2.3 CONTENCIÓN** ..... 9
**2.4 REMEDIACIÓN** ..... 10
**2.5 RECUPERACIÓN** ..... 11
**2.6 LECCIONES APRENDIDAS** ..... 12
**3. DEFINICIONES** ..... 13

## 1. ABSTRACTO

Esta metodología de respuesta a incidentes, es una hoja de consulta dedicada a los encargados 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.

**Soporte del Proveedor de Servicios de Internet (ISP).**

- Contacte a su ISP para comprender los servicios de mitigación de DDoS que ofrece (gratuitos y de pago) y qué proceso debe seguir.
- Si es posible, suscríbase a una conexión a Internet redundante y a un proveedor de servicios Anti-DDoS.
- Establezca contactos con su ISP y entidades de aplicación de la ley30. Asegúrese de tener la posibilidad de usar un canal de comunicación fuera de banda (por ejemplo: teléfono).
- Asegúrese de que su ISP y servicio de mitigación de DDoS tengan soporte telefónico 24/7.

**Inventario**.

- Cree una lista blanca de las direcciones IP y protocolos que debe permitir si está priorizando el tráfico durante un ataque.
- No olvide incluir a sus clientes críticos, socios clave, etc.
- Documente los detalles de su infraestructura de TI, incluidos propietarios de negocio, direcciones IP e IDs de circuito, configuraciones de enrutamiento (AS, etc); prepare un diagrama de topología de red y un inventario de activos.

**Infraestructura de Red.**

- Diseñe una buena infraestructura de red sin Puntos Únicos de Falla ni cuellos de botella.
- Implemente un Firewall de Aplicaciones Web (WAF) para proteger contra DDoS a nivel de aplicación.
- Distribuya sus servidores DNS y otros servicios críticos (SMTP, etc.) a través de diferentes Sistemas Autónomos (AS).
- Refuerce la configuración de los componentes de red, SO y aplicaciones que puedan ser objeto de DDoS.
- Establezca una línea de base del rendimiento actual de su infraestructura, para que pueda identificar el ataque de manera más rápida y precisa.
- Si su negocio depende de Internet, considere comprar productos o servicios especializados de mitigación de DDoS.
- Confirme las configuraciones de tiempo de vida (TTL) de DNS para los sistemas que podrían ser atacados. Reduzca los TTLs, si es necesario, para

facilitar la redirección de DNS si las direcciones IP originales son atacadas. 600 es un buen valor de TTL.
- Dependiendo de la criticidad de sus servicios, considere configurar un respaldo al que pueda cambiar en caso de problemas.

**Contactos Internos.**

- Establezca contactos para sus equipos de IDS, firewall, sistemas y red.
- Colabore con las líneas de negocio para comprender las implicaciones comerciales (por ejemplo, pérdida de dinero) de los escenarios probables de ataque DDoS.
- Involucre a su equipo de planificación de BCP/DR (Planificación de Continuidad del Negocio / Recuperación ante Desastres) en incidentes DDoS.

## 2.2 IDENTIFICACIÓN

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

**Comunicación.**

- Prepare una plantilla de comunicación interna y externa sobre incidentes DDoS.
- Identifique el canal donde se publicará esta comunicación.
- La fase de "preparación" debe considerarse como el elemento más importante de una respuesta exitosa a incidentes DDoS.

**Analizar el ataque**.

- Tenga en cuenta que el ataque DDoS podría ser una cortina de humo que esconde un ataque más sofisticado y dirigido.
- Revise el análisis de su servicio anti-DDoS y los informes de su centro de depuración (scrubbing centre):
    - Comprenda el flujo lógico del ataque DDoS e identifique los componentes de la infraestructura afectados por él.
    - Comprenda si usted es el objetivo del ataque o una víctima colateral.
- Revise los archivos de carga y de registro de servidores, enrutadores, firewalls, aplicaciones y otra infraestructura afectada.
- Identifique qué aspectos del tráfico DDoS lo diferencian del tráfico benigno:
    - Direcciones IP de origen, AS, etc
    - Puertos de destino
    - URLs
    - Banderas de protocolo

Se pueden usar herramientas de análisis de red para revisar el tráfico:
→**Tcpdump, Tshark, Snort, Netflow, Ntop, MRTG, Cacti, Nagios**

Si es posible, cree una firma NIDS (Sistema de Detección de Intrusiones en Red) para enfocar y diferenciar entre tráfico benigno y malicioso.

**Involucrar a Actores Internos y Externos.**

- Contacte a sus equipos internos para conocer su visibilidad del ataque.
- Contacte a su ISP para solicitar ayuda. Sea específico sobre el tráfico que le gustaría controlar:
    - Bloques de red involucrados
    - Direcciones IP de origen
    - Protocolos
- Notifique a los equipos ejecutivos y legales de su compañía.

**Verificar los Antecedentes.**

- Averigüe si la compañía recibió una demanda de extorsión como precursora del ataque:
    - Busque correos electrónicos en su puerta de enlace de correo electrónico de seguridad basándose en una lista de palabras clave.
    - Algunos actores de amenazas envían demandas de extorsión directamente a las direcciones de correo electrónico en los registros Whois del sitio web objetivo.

- Busque reivindicaciones del ataque en Redes Sociales.
- Busque si alguien podría tener algún interés en amenazar a su compañía:
    - Competidores
    - Grupos con motivación ideológica (hacktivistas)
    - Antiguos empleados

## 2.3 CONTENCIÓN

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

- Si el cuello de botella es una característica particular de una aplicación, deshabilite temporalmente esa característica.
- Intente limitar o bloquear el tráfico DDoS lo más cerca posible de la "nube" de la red a través de un enrutador, firewall, balanceador de carga, dispositivo especializado, etc.
- Termine las conexiones o procesos no deseados en servidores y enrutadores y ajuste su configuración TCP/IP.
- Si es posible, cambie a sitios o redes alternas utilizando DNS u otro mecanismo. "Blackhole" (agujero negro) el tráfico DDoS dirigido a las direcciones IP originales.
- Configure un canal de comunicación alternativo entre usted y sus usuarios/clientes (por ejemplo: servidor web, servidor de correo, servidor de voz, etc.).
- Si es posible, enrute el tráfico a través de un servicio o producto de depuración de tráfico (traffic-scrubbing) mediante DNS o cambios de enrutamiento (por ejemplo: enrutamiento sinkhole).
- Configure filtros de egreso para bloquear el tráfico que sus sistemas podrían enviar en respuesta al tráfico DDoS (por ejemplo: tráfico backsquatter), para evitar añadir paquetes innecesarios a la red.
- En caso de intento de extorsión, intente ganar tiempo con el defraudador. Por ejemplo, explique que necesita más tiempo para obtener la aprobación de la gerencia.

**Si el cuello de botella está del lado del ISP o del servicio anti-DDoS, solo ellos pueden tomar acciones eficientes. En ese caso, trabaje en estrecha colaboración con su ISP y/o proveedor anti-DDoS y asegúrese de compartir información de manera eficiente.**

## 2.4 REMEDIACIÓN

***OBJETIVO***: TOMAR ACCIONES PARA DETENER LA CONDICIÓN DE DENEGACIÓN DE SERVICIO.

- Contacte a su ISP y/o proveedor anti-DDoS y asegúrese de que implementen medidas de remediación. Para su información, algunas de las posibles medidas son:
  - Filtrado (si es posible a nivel Tier1 o 2)
  - Depuración de tráfico / Sinkhole / Clean-pipe
  - Balanceo / División / Conmutación de IP pública
  - Enrutamiento Blackhole

**Las acciones de remediación técnica pueden ser implementadas principalmente por su ISP y/o proveedor anti-DDoS.**

SI EL ATAQUE TUVO UN IMPACTO MAYOR, PUEDE QUE TENGA QUE HACER UN REPORTE DE INCIDENTE A LOS REGULADORES.

SI LOS PATROCINADORES DEL DDOS HAN SIDO IDENTIFICADOS, CONSIDERE INVOLUCRAR A LAS FUERZAS DEL ORDEN.

**ESTO DEBE REALIZARSE BAJO LA DIRECCIÓN DE LOS EQUIPOS EJECUTIVOS Y LEGALES DE SU COMPAÑÍA.**

## 2.5 RECUPERACIÓN

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

**Evaluar el fin de la Condición DDoS.**

- Asegúrese de que los servicios impactados sean accesibles nuevamente.
- Asegúrese de que el rendimiento de su infraestructura haya vuelto a su línea de base de rendimiento.

**Revertir las Medidas de Mitigación.**

- Vuelva a dirigir el tráfico a su red original.
- Reinicie los servicios detenidos.

**Asegúrese de que las acciones relacionadas con la recuperación se decidan de acuerdo con los equipos de red. El levantamiento de servicios podría tener efectos secundarios inesperados.**

## 2.6 LECCIONES APRENDIDAS

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

Informe a su jerarquía, subsidiarias y socios para compartir las mejores prácticas aplicadas en este incidente y hacer cumplir reglas similares en otras ubicaciones.

***Informe***

Se debe redactar un informe de crisis y ponerlo a disposición de todos los actores del incidente.

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

***Lecciones Aprendidas***

Se deben definir acciones para mejorar los procesos de gestión de DDoS para capitalizar esta experiencia. Considere qué relaciones dentro y fuera de sus organizaciones podrían ayudarlo con futuros incidentes.

## 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 Emergencias Informáticas. |
| **CSIRT** | Equipo de respuesta a Incidentes de Seguridad, implícito como sinónimo/similar a CERT en la accesión de red phone. |
| **NIST** | Instituto Nacional de Estándares y Tecnología |
| **TLP** | Indica que la información puede ser distribuida sin restricciones |
| **DDoS (Distributed Denial of Service) / Denegación de Servicio Distribuida** | Un ataque en el que múltiples sistemas informáticos comprometidos atacan un solo objetivo, causando una Denegación de Servicio (DoS) para los usuarios legítimos |
| **ISP (Internet Service Provider) / Proveedor de Servicios de Internet** | La entidad a contactar para comprender los servicios de mitigación de DDoS y obtener soporte. |
| **Web Application Firewall (WAF) / Firewall de Aplicaciones Web** | Un tipo de firewall que ayuda a proteger contra DDoS a nivel de aplicación. |
| **Single Point of Failure (SPOF) / Punto Único de Falla** | Un componente de infraestructura cuya falla detiene el funcionamiento de todo el sistema. La infraestructura debe diseñarse sin ellos |
| **AS (Autonomous System) / Sistema Autónomo** | Una colección de redes IP que tienen una política de enrutamiento claramente definida, que se utiliza en la configuración de enrutamiento y debe usarse para distribuir servicios críticos. |
| **DNS Time-to-Live (TTL) / Tiempo de Vida de DNS** | Un valor en la configuración de DNS que determina cuánto tiempo un respondedor de DNS debe almacenar en caché una consulta antes de que expire. Se recomienda bajarlo (ej: 600) para facilitar la redirección si las IP originales son atacadas. |

| | |
|---|---|
| **NIDS (Network Intrusion Detection System) / Sistema de Detección de Intrusiones en Red** | Una herramienta que se puede usar para crear una firma para diferenciar entre tráfico benigno y malicioso. |
| **Tcpdump y Tshark** | Analizadores de paquetes/captura de tráfico. |
| **Snort** | Un sistema de prevención y detección de intrusiones de red (NIPS/NIDS). |
| **Netflow** | Un protocolo de red desarrollado por Cisco para recopilar información de tráfico IP. |
| **Ntop, MRTG, Cacti, Nagios:** | Herramientas de monitoreo y visualización de tráfico y rendimiento de red. |
| **Traffic-scrubbing Service / Servicio de Depuración de Tráfico** | Un servicio o producto al que se puede enrutar el tráfico para limpiarlo del tráfico malicioso de DDoS (a menudo a través de cambios de DNS o enrutamiento). |
| **Sinkhole Routing / Enrutamiento Sinkhole** | Una técnica de enrutamiento para redirigir el tráfico malicioso, a menudo como parte de un servicio de depuración. |
| **Blackhole Routing / Enrutamiento Blackhole** | La práctica de tirar todo el tráfico dirigido a una dirección IP específica. |
| **Out-of-band communication channel / Canal de comunicación fuera de banda** | Un método de comunicación separado de la red principal que puede estar bajo ataque (ej: teléfono). |
| **Blacksquatter traffic / Tráfico Blacksquatter** | El tráfico que los sistemas pueden enviar en respuesta al tráfico DDoS; la configuración de filtros de egreso ayuda a bloquearlo. |