# METODOLOGÍA DE RESPUESTA A INCIDENTES

# IRM #10 INGENIERÍA SOCIAL

¿Cómo manejar un Incidente de Ingeniería Social (Teléfono o Correo Electrónico)?

**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 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.

- Aumente la concienciación de los usuarios y las políticas de seguridad.

Nunca proporcione información personal o corporativa a una persona no identificada. Esto podría incluir identificadores de usuario, contraseñas, información de cuentas, nombre, dirección de correo electrónico, números de teléfono (móvil o fijo), dirección, número de seguridad social, cargos, información sobre clientes, la organización o los sistemas de TI.
El objetivo del ingeniero social es robar recursos humanos, secretos corporativos o datos de clientes/usuarios.
Reporte cualquier evento sospechoso a su gerente, quien lo remitirá al CISO para tener un informe centralizado.

- Tenga un proceso definido para redirigir cualquier solicitud "extraña" a un teléfono "rojo", si es necesario.

- Prepárese para manejar la conversación con ingenieros sociales para identificar qué información podría ayudar a rastrear al atacante y sus objetios.

- Consulte con su departamento legal para ver qué acciones están permitidas y qué reacciones pueden manejar.

**Teléfono Rojo**:

El número de teléfono rojo debe estar claramente etiquetado como "Ingeniería Social".

El número de teléfono debe ser fácil de identificar en el directorio telefónico global de su empresa, pero no deben mostrarse solicitudes sobre la marcación inversa.

La línea telefónica roja siempre debe grabarse con fines de recopilación de pruebas.

## 2.2 IDENTIFICACIÓN

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

- Llamada telefónica / alguien que no conoce lo llama a usted/su servicio, solicitando información detallada.
    - Si el contacto trabaja fuera de la empresa y solicita información que podría ser valiosa para un competidor, deniegue sus solicitudes y vaya a la parte 2.3 (Contención).
    - Si el contacto dice ser un empleado de su empresa, pero el número de teléfono está oculto o no es interno, proponga devolver la llamada al número declarado en el directorio. Si el supuesto atacante acepta, devuelva la llamada para verificar. Si rechaza esta opción, vaya a la parte 2.3 (Contención).
    - El atacante podría utilizar varias técnicas para incitar a su víctima a hablar (miedo, curiosidad, empatía).
    - No divulgue información en ningún caso.
    - Escuche atentamente sus solicitudes y al final pida un número de teléfono para devolver la llamada o una dirección de correo electrónico para responder.
    - Tome notas y mantenga la calma, incluso si el atacante está gritando o amenazando; recuerde que intenta utilizar las debilidades humanas

- Si puede ir más allá, la siguiente información será valiosa:
    - El nombre del corresponsal.
    - Información/personas solicitadas
    - Acento, habilidades lingüísticas
    - Lenguaje de la industria y conocimiento organizacional
    - Ruidos de fondo
    - Hora y duración de la llamada
- Correo electrónico / Alguien que no conoce solicita información detallada
    - Si el contacto tiene una dirección de correo electrónico "fuera de la empresa" y solicita información que podría ser valiosa para un competidor, vaya a la parte 2.3 (Contención).
    - Si el contacto utiliza una dirección de correo electrónico interna, pero está solicitando información extraña, pídale algunas explicaciones y use el directorio de la empresa para obtener el nombre de su gerente, a quien pondrá en copia.
    - Eventualmente, notifique a la alta dirección para informarles que se ha encontrado un incidente relacionado con un ataque de ingeniería social. Ellos podrían comprender los objetivos según el contexto.

## 2.3 CONTENCIÓN

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

En este paso, debe estar bastante seguro de que está lidiando con un ataque de ingeniería social.
Acciones para todos los empleados:

**Llamada telefónica.**

Si el atacante le insista a dar un número de teléfono, siga estos pasos:

- Use la "línea de teléfono rojo" de su CERT/CSIRT, si existe.
- Dele el número con un nombre inventado.
- Llame inmediatamente a su equipo CERT/CSIRT explicando lo sucedido y el nombre inventado elegido.
- Si el atacante lo presiona demasiado y no le da tiempo para encontrar el número de Teléfono Rojo, pídale que le devuelva la llamada más tarde, fingiendo una reunión.

Si el atacante quiere comunicarse con alguien, siga estos puntos:

- Ponga en espera al atacante y llame al equipo CERT/CSIRT explicando lo sucedido.
- Transfiera la conversación del atacante al equipo CERT/CSIRT (no le dé el número).

**Correo electrónico.**

- Reenvíe a su equipo de seguridad todos los correos electrónicos, incluyendo los encabezados (envíelos como documentos adjuntos) para fines de investigación. Podría ayudar a rastrear al atacante.

Acciones para el CERT o equipo de respuesta a incidentes:

**Llamada telefónica.**

- Reanude la conversación con el atacante y utilice una de estas técnicas:
    - Suplante la identidad de las personas con las que el atacante desea hablar.
    - Reduzca la velocidad y haga que la conversación se prolongue e incite al atacante a cometer errores.
    - Explíquele al atacante la ingeniería social está prohibido por la ley, castigado con sanciones y que el equipo de abogados se encargará del problema sin continúa.

Si se ha utilizado el número de teléfono trampa, prepárese para "quemarlo", cree otro y muéstrelo en el directorio.

**Correo electrónico.**

- Recopile tanta información como sea posible sobre la dirección de correo electrónico.
- Analice los encabezados del correo electrónico e intente localizar la fuente.
- Busque la dirección de correo electrónico con herramientas de Internet.
- Geo localice al usuario detrás de la dirección de correo electrónico.

Agregue todos los ataques de ingeniería social para visualizar el esquema.

## 2.4 REMEDIACIÓN

***OBJETIVO***: TOMAR ACCIONES PARA ELIMINAR LA AMENAZA Y EVITAR INCIDENTES FUTUROS.

**Se pueden intentar algunas posibles acciones de remediación:**

- Alertar a las fuerzas del orden y/o presentar una denuncia.
- Discutir el problema en círculos de confianza para saber si la empresa se enfrenta sola a este problema.
- Amenazar al atacante con acciones legales si puede ser identificado.
- Reportar las direcciones de correo electrónico utilizadas por el atacante a los equipos de abuso del proveedor.

## 2.5 RECUPERACIÓN

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

Notifique a la alta dirección las acciones y decisiones tomadas sobre el caso de ingeniería social.

*Para obtener más detalles sobre la autenticación y la recuperación de la infraestructura, consulte el compromiso de malware a gran escala IRMXXX.*

## 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 y subsidiarias sobre el incidente; esto podría ayudar a evitar ataques similares más adelante.

***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

***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 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** | Protocolo de Semáforo (usado para clasificar la sensibilidad de la información; en este caso: CLEAR) |
| **Indicators of compromise (IOCs)** | Indicadores de compromiso (pistas forenses o técnicas de un ataque). |
| **Headers (Email Headers)** | Encabezados de correo electrónico (información técnica utilizada para rastrear el origen). |
| **Geolocalize** | Localizar geográficamente (aplicado al usuario detrás de una dirección de correo electrónico). |
| **Social Engineering** | Ingeniería Social. Técnica de manipulación que explota el comportamiento humano para obtener información confidencial o acceso a sistemas y recursos valiosos. |
| **Threat** | Amenaza (lo que se busca remover). |
| **Phishing/Spoofing/Vishing** | El documento cubre ataques por e-mail y phone call que son las principales vías de Phishing, Spear Phishing y Vishing |