

# Manual de estrategias de phishing

Versión 1.0

Objetivo	2
Uso de este manual de estrategias	2
Paso 1: Recibes una alerta de phishing	2
Paso 2: Evalúa la alerta	2
Paso 3.0: ¿El correo electrónico contiene enlaces o archivos adjuntos?	3
Paso 3.1: ¿Los enlaces o archivos adjuntos son maliciosos?	3
Paso 3.2: Actualiza el ticket de alerta y escálalo	3
Paso 4: Cierra el ticket de alerta	3
Diagrama de flujo de phishing (versión 1.0)	4

**Comentado [1]:** Acá es medio raro en el inglés también, porque lo está dando como un paso a seguir y la recepción del ticket de alerta no es un paso a seguir, sino un hecho. Después, para seguir con la segunda persona que usa el original, cambié todos los pasos a eso.

**Comentado [2R1]:** ¡Ok!

## Objetivo

Ayudar a los analistas de SOC de nivel 1 a proporcionar una respuesta adecuada y oportuna a un incidente de phishing.

## Uso de este manual de estrategias

Sigue los pasos de este manual de estrategias en el orden en que se enumeran. Ten en cuenta que los pasos pueden superponerse.

### Paso 1: Recibes una alerta de phishing

El proceso comienza cuando recibes un ticket de alerta que indica que se ha detectado un intento de phishing.

### Paso 2: Evalúa la alerta

Al recibir la alerta, investiga sus detalles y cualquier información de registro relevante. Parte de la información que debes evaluar incluye:

1. **Gravedad de la alerta**
  - **Baja:** No requiere escalar la alerta
  - **Media:** Puede requerir elevar la alerta
  - **Alta:** Requiere ser elevada inmediatamente al personal de seguridad apropiado
2. **Datos del destinatario**
  - Dirección de correo electrónico del destinatario
  - Dirección IP del destinatario
3. **Datos del remitente**
  - Correo electrónico del remitente
  - Dirección IP del remitente
4. **Asunto**
5. **Cuerpo del mensaje**
6. **Archivos adjuntos o enlaces.**

Nota: **No** abras enlaces ni archivos adjuntos en tu dispositivo a menos que estés utilizando un entorno autorizado y aislado.

### Paso 3.0: ¿El correo electrónico contiene enlaces o archivos adjuntos?

Los correos electrónicos de phishing pueden contener archivos adjuntos maliciosos o enlaces que intentan obtener acceso a los sistemas. Después de examinar los detalles de la alerta, determina si el correo electrónico contiene enlaces o archivos adjuntos. Si los tiene, **no** abras enlaces ni archivos adjuntos y continúa con el **Paso 3.1**. Si el correo electrónico no contiene enlaces o archivos adjuntos, continúa con el **Paso 4**.

### Paso 3.1: ¿Los enlaces o archivos adjuntos son maliciosos?

Una vez que hayas identificado que el correo electrónico contiene archivos adjuntos o enlaces, determina si estos son maliciosos. Comprueba la reputación del enlace o archivo adjunto a través de sus valores hash utilizando herramientas de inteligencia sobre amenazas como VirusTotal. Si has confirmado que el enlace o archivo adjunto **no es malicioso**, continúa con el **Paso 4**.

### Paso 3.2: Actualiza el ticket de alerta y escálalo

Si confirmaste que el enlace o el archivo adjunto es **malicioso**, proporciona un resumen de tus hallazgos y la razón por la que estás elevando el ticket. Actualiza el estado del ticket a **Escalado** y notifica a un analista de SOC de nivel 2 de que elevaste el ticket.

### Paso 4: Cierra el ticket de alerta

Actualiza el estado del ticket a **Cerrado** si:

- Confirmaste que el correo electrónico no contiene enlaces ni archivos adjuntos o
- Confirmaste que el enlace o archivo adjunto **no es malicioso**.

Incluye un breve resumen de los hallazgos de tu investigación y la razón por la que cerraste el ticket.

## Diagrama de flujo de phishing (versión 1.0)

