**Resumen de la actividad**

En esta actividad, responderás a un incidente de phishing que involucra un hash de archivo malicioso. Se trata del mismo hash de archivo SHA256 que investigaste y verificaste como malicioso en una [actividad anterior](https://www.coursera.org/learn/haz-sonar-la-alarma-deteccion-y-respuesta/quiz/wXUdm/actividad-investiga-un-hash-de-archivo-sospechoso). Seguirás las instrucciones del manual de estrategias para investigar y resolver el ticket de alerta del incidente.

Anteriormente, aprendiste cómo los manuales de estrategias detallan las acciones necesarias paso a paso para responder adecuadamente a un incidente de seguridad. Una acción coordinada, efectiva y rápida es clave durante la respuesta a un incidente. Un manual de estrategias puede ayudar a los equipos de seguridad a minimizar el impacto de un incidente y reducir el tiempo de respuesta a este. Como analista de seguridad, estos manuales pueden servirte de guía para apoyar eficazmente los esfuerzos de respuesta a incidentes de una organización.

**Escenario**

Revisa el siguiente escenario. Luego, completa las instrucciones paso a paso.

Eres analista de nivel uno del centro de operaciones de seguridad (SOC) en una empresa de servicios financieros. Anteriormente, recibiste una alerta de phishing sobre la descarga de un archivo sospechoso en la computadora de un empleado. Al investigar el hash del archivo adjunto del correo electrónico, se verificó que este es malicioso. Ahora, que dispones de esta información, debes seguir el proceso de tu organización para completar la investigación y resolver la alerta.

Las políticas y procedimientos de seguridad de la empresa para la que trabajas describen cómo responder a alertas específicas, incluyendo qué hacer cuando recibes una de phishing.

En el manual de estrategias, se detalla un diagrama de flujo e instrucciones que te ayudarán a completar la investigación y resolver la alerta. Al final de tu investigación, actualizarás el ticket con tus conclusiones sobre el incidente.

***Nota***: *Utiliza el diario de gestión de incidentes que iniciaste en* [*una actividad anterior*](https://www.coursera.org/learn/haz-sonar-la-alarma-deteccion-y-respuesta/exam/ghRgc/actividad-documenta-un-evento-en-un-diario-de-gestion-de-incidentes) *para tomar notas durante la actividad y hacer un seguimiento de tus hallazgos.*

**Instrucciones paso a paso**

Sigue las instrucciones y responde la pregunta para completar la actividad. Luego, dirígete al siguiente elemento del curso para comparar tu trabajo con un ejemplo completo.

**Paso 1: Accede a la plantilla**

Para utilizar la plantilla de este elemento del curso, haz clic en el enlace de abajo y selecciona “Usar plantilla”.

Enlace a la plantilla: [**Ticket de alerta**](https://docs.google.com/document/d/1C_oSppUijx8i9vkeB2p631-kexuyCVAzco4f2FqFcTs/template/preview?usp=sharing&resourcekey=0-TC8vTWWW_7owixVHFJSrcw)

O BIEN

Si no tienes una cuenta de Google, puedes descargar la plantilla directamente desde el siguiente archivo adjunto.

[Activity Use a playbook to respond to a phishing incident\_Alert-ticket](https://d3c33hcgiwev3.cloudfront.net/h2NBScIxTL2BAwsqvSntRQ_bb8b598715c242249bb16854435a99f1_Activity-Use-a-playbook-to-respond-to-a-phishing-incident_Alert-ticket.docx?Expires=1708732800&Signature=OWfTM6lBjo7htaGhkn4QACNZMHSGo-v7yO5gdqrKwhpgMbVSgj-H9SSlHqxPk27TIOjkcL6mUQlGW4nVQWf25ivumfYUFds6~jsbFOqiLhu23Zh-uF38CYWixWmMG5FER-mG0u1-mv0gLnEzqCwCQDUHMlk0e~cK-QY8uYHjbic_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

[DOCX File](https://d3c33hcgiwev3.cloudfront.net/h2NBScIxTL2BAwsqvSntRQ_bb8b598715c242249bb16854435a99f1_Activity-Use-a-playbook-to-respond-to-a-phishing-incident_Alert-ticket.docx?Expires=1708732800&Signature=OWfTM6lBjo7htaGhkn4QACNZMHSGo-v7yO5gdqrKwhpgMbVSgj-H9SSlHqxPk27TIOjkcL6mUQlGW4nVQWf25ivumfYUFds6~jsbFOqiLhu23Zh-uF38CYWixWmMG5FER-mG0u1-mv0gLnEzqCwCQDUHMlk0e~cK-QY8uYHjbic_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

**Paso 2: Accede a los materiales de apoyo**

Los materiales de apoyo te ayudarán a completar esta actividad. Manténlos abiertos a medida que avances en los siguientes pasos.

Enlace a los materiales de apoyo: [**Manual de estrategias de phishing (con diagrama de flujo)**](https://docs.google.com/document/d/1rOSSCtLsiWVjAjTdJtWrSrvqpiXHissEAqiy5KD4Kv4/template/preview?usp=sharing)

O BIEN

Si no tienes una cuenta de Google, puedes descargar los materiales de apoyo directamente desde el siguiente archivo adjunto.

[Activity Use a playbook to respond to a phishing incident\_Phishing-incident-response-playbook](https://d3c33hcgiwev3.cloudfront.net/OVko3IcgQRKhhz29N_xIKA_129a6785dd68412faf84a4a1c33981f1_Activity-Use-a-playbook-to-respond-to-a-phishing-incident_Phishing-incident-response-playbook.docx?Expires=1708732800&Signature=dVfuSFOaBlyqDKJW~shLuu3WXWBWycx5yXQtjjS6EPu8BhOFq-mLwibhedFyLIkcGLoH1sDAzGsNCUmIdZy86O8yQ4j~OigjzJeWz-2SgSGilciFXlB1CtMzmUkfsKi8ywPTK3w79EQ5lVOo9-U8t1~Q6hfyfklaagBtYEHH0MI_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

[DOCX File](https://d3c33hcgiwev3.cloudfront.net/OVko3IcgQRKhhz29N_xIKA_129a6785dd68412faf84a4a1c33981f1_Activity-Use-a-playbook-to-respond-to-a-phishing-incident_Phishing-incident-response-playbook.docx?Expires=1708732800&Signature=dVfuSFOaBlyqDKJW~shLuu3WXWBWycx5yXQtjjS6EPu8BhOFq-mLwibhedFyLIkcGLoH1sDAzGsNCUmIdZy86O8yQ4j~OigjzJeWz-2SgSGilciFXlB1CtMzmUkfsKi8ywPTK3w79EQ5lVOo9-U8t1~Q6hfyfklaagBtYEHH0MI_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

Paso 3: Revisa el manual de estrategias y el diagrama de flujo

Antes de empezar a investigar la alerta, tómate un tiempo para revisar el manual de estrategias y el diagrama de flujo, ya que los utilizarás a lo largo de la investigación.

Las instrucciones del **manual de estrategias de phishing** proporcionan pautas detalladas por escrito sobre cada paso representado en el diagrama de flujo.

El **diagrama de flujo de phishing** proporciona una descripción general de alto nivel y una representación visual de la secuencia de pasos y subpasos que deberás seguir para responder a una alerta de phishing.

***Nota****: Los pasos en este manual de estrategias no son una guía definitiva para responder a un incidente de phishing. Las organizaciones tienen sus propias políticas, estándares y procedimientos que determinan las acciones de respuesta esperadas ante incidentes.*

Paso 4: Actualiza el estado del ticket de alerta

En la plantilla de **ticket Alerta**, comienza la investigación actualizando la lista desplegable **Estado del ticket** a **Investigando**.

Paso 5: Evalúa la alerta

Para este ejercicio, comienza con el segundo paso del manual de estrategias, **Evalúa la alerta**, porque ya has recibido y accedido al ticket de alerta de phishing.

Como analista de seguridad, querrás entender las causas que activaron  la alerta. Crea una nueva entrada en tu diario de gestión de incidentes para registrar los datos y anotar tus observaciones e ideas. Consultarás estas notas a medida que avances en los siguientes pasos del manual de estrategias.

A continuación, evalúa el contenido del **ticket de alerta,** incluido el contenido en la sección **Información adicional**. Estos son algunos ejemplos de elementos que debes examinar cuando evalúes los detalles del ticket de alerta:

* **Gravedad de la alerta**: De acuerdo con las instrucciones del manual de estrategias, una gravedad de alerta Media o Alta es una buena indicación de que un ticket podría requerir una atención prioritaria.
* **Datos del remitente**: Analizar los datos del remitente de un correo electrónico es importante porque podría revelar inconsistencias que pueden indicar un intento de suplantación de identidad. Con frecuencia, los correos electrónicos de phishing intentan hacerse pasar por entidades de confianza. Por ejemplo, si hay una falta de coincidencia entre la dirección de correo electrónico del remitente y el nombre del remitente, es una buena indicación de que el correo electrónico podría ser un correo electrónico de phishing.
* **Cuerpo del mensaje**: Es importante analizar el cuerpo del mensaje (y el asunto) de un correo electrónico porque los correos electrónicos de phishing suelen contener errores gramaticales u ortográficos, lo que puede ser un indicio de un intento de phishing.
* **Archivos adjuntos o enlaces**: Los correos electrónicos de phishing contienen enlaces o archivos adjuntos maliciosos que se utilizan para robar información confidencial o descargar software o código malicioso en el dispositivo del destinatario. Verifica si se ha adjuntado un archivo a este correo electrónico.

Una vez que hayas evaluado el contenido del ticket de alerta, responde a las 5 W de este incidente para recopilar la información a fin de comprender la naturaleza de la alerta. Las 5 W son:

* ¿Quién (who) causó el incidente?
* ¿Qué (what) sucedió?
* ¿Cuándo (when) ocurrió el incidente?
* ¿Dónde (where) ocurrió el incidente?
* ¿Por qué (why) sucedió?

Al final de este paso, deberías tener 2-3 razones por las que crees que la alerta de phishing es o no legítima.

Paso 6: Determina si la alerta debe elevarse a un nivel superior

Después de evaluar los datos de la alerta, utiliza los **pasos 3.0** y **3.1** del manual de estrategias de phishing para determinar si el correo electrónico contiene enlaces o archivos adjuntos y si estos son maliciosos. Recuerda que ya determinaste que el correo electrónico contiene un archivo adjunto que se ha verificado como malicioso a través de su hash de archivo.

Si decidiste que la alerta debe elevarse a un nivel superior, continúa con el **paso 3.2**,. De lo contrario, sigue con el **paso 4**.

Paso 7: Actualiza el estado del ticket de alerta

Ahora, que examinaste los datos del correo electrónico, completa el paso final del manual de estrategias y actualiza el ticket de alerta en la plantilla de actividad. Dependiendo de si deseas elevar o cerrar la alerta:

* En la columna **Estado del ticket** de la plantilla del ticket de alerta, actualiza el estado del ticket a **Cerrado** o **Elevado**.
* En la columna **Comentarios de ticket** de la plantilla del ticket de alerta, utiliza los datos que hayas encontrado para explicar los pasos a seguir y por qué decidiste elevar o cerrar el ticket. Incluye 2-3 razones por las que crees que esta alerta debería elevarse o cerrarse.