**Resumen de la actividad**

En esta actividad, tendrás la oportunidad de revisar los detalles de un incidente de seguridad y documentarlo utilizando tu diario de gestión de incidentes. Anteriormente, aprendiste la importancia de la documentación en el proceso de respuesta a incidentes, así como el rol crucial que desempeña el diario de gestión de incidentes para registrar información detallada durante la gestión de estos eventos.

A lo largo de este curso, podrás aplicar tus habilidades de documentación al utilizar tu diario de gestión de incidentes. Con este diario, podrás registrar información relevante acerca de las experiencias que adquieras al analizar diversos escenarios de incidentes de seguridad a través de las actividades del curso.

Una vez que termines este curso, habrás acumulado varias entradas en tu diario de gestión de incidentes, las cuales serán de gran utilidad como referencia para recordar conceptos y herramientas específicas. Más adelante, incorporarás este documento a tu cartera de ciberseguridad, un valioso recurso que podrás compartir con posibles empleadores o reclutadores. Para una revisión detallada sobre la importancia de desarrollar una cartera profesional y las opciones disponibles para crearla, te recomendamos leer el artículo [Crear una cartera de ciberseguridad](https://www.coursera.org/learn/haz-sonar-la-alarma-deteccion-y-respuesta/resources/H3ujO).

Asegúrate de completar esta actividad y responder a las preguntas que se presentan antes de continuar. En la siguiente parte del curso, podrás ver un ejemplo terminado para compararlo con tu propio trabajo.

***Nota:*** *Puedes usar tu diario de gestión de incidentes como un espacio personal en el que puedes hacer un seguimiento de tu proceso de aprendizaje a medida que aprendes conceptos de detección y respuesta a incidentes e interactúas con diferentes herramientas de ciberseguridad. Allí puedes incluir tus observaciones, ideas y cualquier otro detalle o información relevante.*

**Escenario**

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

Una pequeña clínica de atención médica especializada en servicios de atención primaria en los Estados Unidos experimentó un incidente de seguridad un martes por la mañana, alrededor de las 9:00 a.m. Varios empleados reportaron la imposibilidad de utilizar sus computadoras para acceder a archivos como historiales médicos. Las operaciones comerciales se interrumpieron porque los empleados no podían acceder a los archivos y programas necesarios para realizar su trabajo.

Además, los empleados informaron la aparición de  una nota de rescate en sus computadoras. Este mensaje decía que todos los archivos de la empresa habían sido cifrados por un grupo organizado de hackers poco éticos, conocidos por dirigir sus ataques a organizaciones en los sectores de salud y transporte. A cambio de restablecer el acceso a los archivos cifrados, la nota de rescate exigía una gran suma de dinero por la clave de descifrado.

Los atacantes lograron acceder a la red de la empresa mediante el uso de correos electrónicos de phishing dirigidos a varios empleados de la compañía. Estos correos contenían un archivo adjunto malicioso que instala malware en la computadora del empleado una vez descargado.

Una vez que los atacantes obtuvieron acceso, desplegaron su ransomware, el cual cifró archivos críticos. La empresa se vio incapacitada para acceder a los datos críticos de pacientes, lo que causó interrupciones importantes en sus operaciones comerciales. La clínica tuvo que apagar sus sistemas informáticos y ponerse en contacto con varias organizaciones para reportar el incidente y recibir asistencia técnica.

**Instrucciones paso a paso**

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

**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: [diario de gestión de incidentes](https://docs.google.com/document/d/1jGJhQKrNz7G62RaiIj7l-OTWBTKXVaerWSCRVS0xEQE/template/preview?resourcekey=0-JXYRihuX_a13YrV6ditJ3A)

O BIEN

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

[Portfolio Activity Document an incident with an incident handler\_s journal\_Incident-handler-s-journal-](https://d3c33hcgiwev3.cloudfront.net/D-NGIY6ITQekXzwwCM3U1A_b11f0b25f44f408daec33aa2003bdff1_Portfolio-Activity-Document-an-incident-with-an-incident-handler_s-journal_Incident-handler-s-journal-.docx?Expires=1708473600&Signature=iuF-iIE177TZUbIg9pnBVTdd33rd8TNsE29z3HHZlnDG4vlMZdZzp9DXQ3c4ZXoh8VLKtwAvC4~ZIStZuFBkpWlN2V8XJRrrdMc8CUM3Raa033fFx8YM0IekOgn5Rn0GMT3FbaMCAXj7T-ZOY3Jz~d2YJ1~2cSTjyvN-LSNJapw_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

[DOCX File](https://d3c33hcgiwev3.cloudfront.net/D-NGIY6ITQekXzwwCM3U1A_b11f0b25f44f408daec33aa2003bdff1_Portfolio-Activity-Document-an-incident-with-an-incident-handler_s-journal_Incident-handler-s-journal-.docx?Expires=1708473600&Signature=iuF-iIE177TZUbIg9pnBVTdd33rd8TNsE29z3HHZlnDG4vlMZdZzp9DXQ3c4ZXoh8VLKtwAvC4~ZIStZuFBkpWlN2V8XJRrrdMc8CUM3Raa033fFx8YM0IekOgn5Rn0GMT3FbaMCAXj7T-ZOY3Jz~d2YJ1~2cSTjyvN-LSNJapw_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

Paso 2: Revisa el escenario

Revisa los detalles del escenario. Considera los siguientes puntos clave:

* Una pequeña clínica de atención médica en Estados Unidos experimentó un incidente de seguridad el martes a las 9:00 a.m., lo cual interrumpió gravemente sus operaciones comerciales.
* La causa del incidente de seguridad fue un correo electrónico de phishing que contenía un archivo adjunto malicioso. Una vez descargado, se desplegó un ransomware que cifró los archivos informáticos de la organización.
* Un grupo organizado de hackers poco éticos dejó una nota de rescate indicando que los archivos de la empresa habían sido cifrados y exigían dinero a cambio de la clave de descifrado.

Paso 3: Registra una entrada en el diario

Utiliza el diario de gestión de incidentes para documentar tu primera entrada sobre el escenario dado. Asegúrate de completar todos los campos:

1. En la sección **Fecha**, anota la fecha de la entrada en el diario. Debe ser la fecha real en la que se registra la entrada, no una ficticia.
2. En la sección **Entrada**, anota un número de entrada en el diario. Por ejemplo, si es tu primera entrada, escribe 1.
3. En la sección **Descripción**, introduce una descripción de la entrada.
4. En la sección **Herramientas utilizadas**, enumera las herramientas de ciberseguridad empleadas, en caso de que se hayan usado.
5. En la sección **Las 5 W**, anota los detalles sobre el escenario dado.
   1. ¿Quién (who) causó el incidente?
   2. ¿Qué (what) sucedió?
   3. ¿Cuándo (when) ocurrió el incidente?
   4. ¿Dónde (where) ocurrió el incidente?
   5. ¿Por qué (why) ocurrió el incidente?
6. En la fila **Notas adicionales**, anota cualquier idea o pregunta que tengas sobre la situación planteada.

**Consejo profesional: Guarda una copia de tu trabajo**

Por último, asegúrate de guardar una copia de tu diario de gestión de incidentes para poder acceder a él a medida que avances en el curso. Puedes usarla en tu cartera profesional para demostrar tus conocimientos y/o experiencia a posibles empleadores.

**Qué incluir en tu respuesta**

Asegúrate de incluir los siguientes elementos en la actividad terminada:

* La fecha y el número de la entrada.
* La descripción de la entrada.
* 1-2 frases que aborden cada una de las 5 W del escenario:
  + ¿Quién (who) causó el incidente?
  + ¿Qué (what) sucedió?
  + ¿Cuándo (when) ocurrió el incidente?
  + ¿Dónde (where) ocurrió el incidente?
  + ¿Por qué (why) ocurrió el incidente?
* 1-2 frases sobre cualquier idea o pregunta adicional acerca del escenario.