**Escenario**

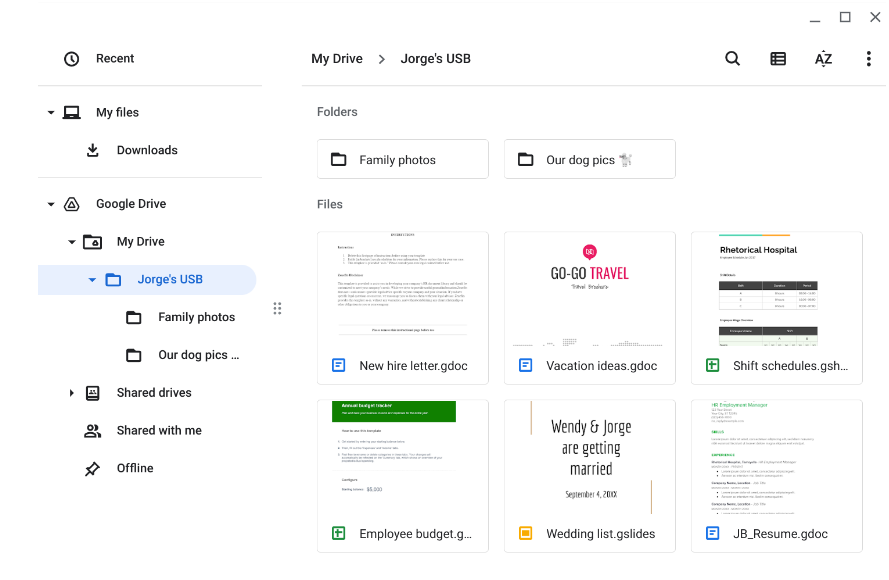
Revisa el siguiente escenario. Luego, completa las instrucciones paso a paso.

Formas parte del equipo de seguridad del Rhetorical Hospital y llegas al trabajo una mañana. En el suelo del estacionamiento, te encuentras una memoria USB con el logotipo del hospital impreso en ella. No hay nadie más alrededor que pueda haberla dejado caer, así que decides recogerla por curiosidad.

Llevas la unidad USB a tu oficina, donde el equipo tiene instalado un software de virtualización en una estación de trabajo. El software de virtualización se puede usar para este mismo propósito, ya que es una de las únicas maneras de investigar con seguridad el contenido de una memoria USB desconocida. El software funciona ejecutando una instancia simulada de la computadora en la misma estación de trabajo. Esta simulación no está conectada a otros archivos o redes, por lo que la unidad USB no puede afectar a otros sistemas si está infectada con software malicioso.

### Paso 2: Inspecciona el contenido de la memoria USB

Creas un entorno virtual y conectas la unidad USB a la estación de trabajo. El contenido del dispositivo parece pertenecer a Jorge Bailey, gerente de recursos humanos del Rhetorical Hospital.



La unidad de Jorge contiene una mezcla de archivos personales y de archivos relacionados con el trabajo. Por ejemplo, contiene carpetas que parecen almacenar fotos de familiares y de mascotas. También hay una carta de una nueva contratación y un horario de los turnos de los empleados.

Revisa los tipos de información que Jorge almacenó en este dispositivo. Luego, en la fila **Contenido** de la plantilla de actividad, escribe **2-3 frases** (40-60 palabras) sobre el tipo de información que se encuentra almacenada en la unidad USB.

***Nota:*** Las memorias USB suelen contener  información de identificación personal (PII, por sus siglas en inglés). Los atacantes pueden usar fácilmente esta información confidencial para atacar al propietario de los datos o a otras personas de su entorno.

### Paso 3: Aplica una mentalidad de atacante al contenido de la unidad USB

La unidad flash parece contener una mezcla de archivos personales y de archivos relacionados con el trabajo. Considera cómo podría utilizar esta información un atacante si la obtuviera. Ten en cuenta también si todo este evento ha sido un montaje.

Por ejemplo, un atacante podría haber colocado estos archivos en la unidad USB como distracción. Podrían haber apuntado a Jorge o a alguien que él conoce, esperando que encontraran el dispositivo y lo conectaran a su estación de trabajo. Al hacerlo, el atacante podría establecer una puerta trasera en los sistemas de la empresa mientras el objetivo desprevenido examinaba los archivos.

En la fila **Mentalidad del atacante** de la plantilla de la actividad, escribe **2-3 frases** (40-60 palabras) sobre cómo se podría usar esta información contra Jorge o el hospital.

***Consejo profesional:*** La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) ofrece algunos  [consejos de seguridad para tener cuidado con las unidades USB](https://www.cisa.gov/news-events/news/using-caution-usb-drives), como mantener separadas las unidades personales de las laborales.

### Paso 4: Analiza los riesgos de encontrar una memoria USB en un estacionamiento

No has abierto ninguno de los archivos del dispositivo, lo cual es una buena práctica.

Los atacantes a veces realizan ataques de cebo USB para distribuir código malicioso que han creado.

Sin embargo, esta unidad USB seguía siendo un riesgo para la seguridad aunque no contuviera código malicioso. Podría haber sido encontrada fácilmente por un atacante que podría haber utilizado su contenido para planificar diversos ataques.

Considera algunos de los riesgos asociados a los ataques de cebo USB:

* ¿Qué tipos de software malicioso podrían estar ocultos en estos dispositivos? ¿Qué podría haber sucedido si el dispositivo hubiera estado infectado y lo hubiera descubierto otro empleado?
* ¿Qué información confidencial podría encontrar un agente de amenaza en un dispositivo como este?
* ¿Cómo se podría utilizar esa información contra un individuo o una organización?

En la fila **Análisis de riesgos** de la plantilla de la actividad, escribe **3 o 4 frases** (60-80 palabras) que describan los controles técnicos, operativos o de gestión que podrían mitigar los ataques de cebo USB.

## Qué debes incluir en tu respuesta

Asegúrate de abordar los siguientes criterios en la actividad terminada:

* 2-3 frases sobre los tipos de información almacenada en la unidad USB.
* 2-3 frases sobre cómo se podría usar la información contra el propietario y/o la organización.
* 3-4 frases que analizan los riesgos de los ataques de cebo USB.