Actividad 2 - Preguntas. **Angie Daniela Ruiz Alfonso.**

1. ¿Qué estudios (formación, capacitación) y cualidades debería tener el:

- Oficial del caso (Case Manager / Case Officer):

Responde a las consultas sobre los incidentes de seguridad que impacten de forma inmediata y es el responsable del modelo de gestión de incidentes y deberá poder revisar todos los incidentes de seguridad, al igual que revisar y evaluar los indicadores de gestión correspondientes al grado de preocupación por incidentes de seguridad para poder ser presentados a los directivos.

El Líder Grupo de Atención de Incidentes estará en la capacidad de convocar la participación de otros funcionarios de la organización cuando el incidente lo amerita (Prensa y Comunicaciones, Gestión de Talento Humano, Gestión Jurídica, Tecnología, Representante de las Directivas para el SGSI).

También debe estar al tanto del cumplimiento de las actividades y de revisión de los procedimientos y mejores prácticas, así como también de los indicadores de gestión, y ser capaz de desencadenar planes de contingencia y/o continuidad cuando sea necesario.

- Examinador/Analista del caso (Case Examiner/Analyst):

Es un experto forense, quien debe estar disponible en caso de que un incidente ocurra y requiera una investigación completa para solucionarlo y determinar los siguientes ítems:

- Qué sucedió.
- Dónde sucedió.
- Cuándo sucedió.
- Quién fue el responsable.
- Cómo sucedió.

Este actor debe ser un apoyo para los demás actores en caso de dudas sobre los procedimientos y debe ejercer un liderazgo técnico en el proceso de atención de Incidentes de seguridad de la información.

- Investigador de la escena del crimen (Crime Scene Investigator):

Se encargan de investigar los escenarios donde se han producido incidentes en busca de pruebas forenses, en los cuales registran y reúnen pruebas, como por ejemplo huellas digitales o fotografías de la escena del crimen, que después pueden presentar a los tribunales.

Para ser investigador de escenarios del crimen se necesita:

- Ser paciente, comprensivo y amable en el trato con las víctimas de delitos. **(APLICA PARA LOS 3 CARGOS)**
- Mantener la calma y ser seguro de si mismo. **(APLICA PARA LOS 3 CARGOS)**
- Estar preparado para asistir a incidentes de todo tipo.
- Ser capaz de trabajar en condiciones desagradables.

- Ser observador y capaz de seguir procedimientos al detalle. **(APLICA PARA LOS 3 CARGOS)**
- Ser capaz de trabajar en solitario y también formando parte de un equipo. **(APLICA PARA LOS 3 CARGOS)**
- Ser flexible; por ejemplo, para seguir métodos de trabajo poco usuales. **(APLICA PARA LOS 3 CARGOS)**
- Ser habilidoso en la realización de tareas de detalle con las manos.

Recomiendan poseer:

- Buenas habilidades de comunicación verbal y escrita. **(APLICA PARA LOS 3 CARGOS)**
- Una visión cromática excelente.
- Buenas habilidades para la fotografía digital.
- Cierto dominio de las TIC.

Y tener estudios que permitan ejercer la labor, afines a los siguientes:

- Formación en Criminología
- Grado en Criminalística: Ciencias y Tecnologías Forenses
- Grado en Criminología y Química
- Máster Oficial en Criminalística

Pero estos dependen estrechamente del ámbito de especialización, el sector y resaltando que la formación continua es un aspecto clave para la mejora profesional. **(APLICA PARA LOS 3 CARGOS)**

Fuentes: https://mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf y https://www.educaweb.com/profesion/investigador-escenarios-crimen-853/

2.- Investigar qué es un HASH y cómo ayuda a distinguir que dos elementos digitales son iguales.

Un hash es un algoritmo matemático que transforma cualquier bloque de datos en una nueva serie de caracteres únicos con una longitud fija, en el cual, sin importar la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud y no existen dos entradas que produzcan el mismo hash de salida.

Se utilizan también para asegurar la “integridad de los mensajes”, por ende, ayuda a distinguir que dos elementos digitales son iguales, esto sí y solo si ese mismo bloque de datos nunca ha sido alterado, a penas sufra cualquier modificación el valor del hash cambiará, y al no ser el mismo de antes, ambos los elementos digitales ya no serán idénticos.

Fuente: https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/

3.- De los siguientes elementos de evidencia online, determinar cuáles son del ámbito privado (requieren de autorización para poder ser investigados) y cuales no:

- Post de una cuenta de Facebook: PRIVADO.

“Estas normas operativas están pensadas para **los miembros de las fuerzas del orden que solicitan información a Facebook e Instagram. Para solicitudes de particulares,**

incluidas las solicitudes de litigantes en materia civil y acusados en materia penal ..."

"Solo divulgamos los datos de las cuentas de acuerdo con lo dispuesto en nuestras Condiciones del servicio y en las leyes aplicables. **Para exigir la divulgación del contenido de una cuenta, es posible que se deba presentar un exhorto o una solicitud en virtud del acuerdo de asistencia judicial mutua** ..."

"Si los miembros de las fuerzas del orden buscan información sobre un usuario de Facebook que **les dio su consentimiento para acceder a la información de su cuenta o para obtenerla**, se debe indicar al usuario en cuestión que obtenga esa información por sus propios medios, desde su cuenta."

"En respuesta a una situación que implique un daño inminente a un menor o el riesgo de muerte o lesiones físicas graves a cualquier persona, y que requiera la divulgación de información con inmediatez, **los miembros de las fuerzas del orden pueden presentar una solicitud a través del sistema de solicitudes por internet para fuerzas del orden** ..."

"Nuestra política es notificar a las personas que usan nuestro servicio cuando alguien solicita su información antes de divulgarla, **a menos que lo prohíba la ley o en circunstancias excepcionales, como casos de explotación infantil, emergencias o cuando una notificación previa podría resultar contraproducente** ..."

- Información en un blog del investigado: DEPENDE de la política de privacidad del sitio.

"... **el usuario deberá someterse a las condiciones de uso y a la política de privacidad de la página web** ..."

- Datos personales en una cuenta de Google: PRIVADO.

"Primero, como se explicará en detalle, Google no trata datos personales **sin el consentimiento de los Titulares de los datos**. Segundo, Google recolecta datos personales de personas que pueden estar ubicadas en diferentes partes del mundo, incluido Colombia. "

- Conversaciones de WhatsApp: PRIVADO.

"Almacenamos información durante el tiempo que sea necesario para los fines que se identifican en esta Política de privacidad, incluida la provisión de nuestros Servicios, o para otros fines legítimos, **como el cumplimiento de las obligaciones legales** ..."

"Accedemos a tu información descrita anteriormente en la sección "Información que recopilamos" de esta Política de privacidad, la preservamos y la compartimos si, de buena fe, consideramos que es necesario para: **(a) responder en virtud de la normativa aplicable a un procedimiento legal o a solicitudes de autoridades competentes;** ..."

Fuentes: https://www.whatsapp.com/legal/updates/privacy-policy/?lang=es_pe, https://mintic.gov.co/portal/inicio/2627:Pol-ticas-de-Privacidad-y-Condiciones-de-Uso, https://www.sic.gov.co/sites/default/files/boletin-juridico/ORDEN%20GOOGLE%281%29.pd y https://es-la.facebook.com/safety/groups/law/guidelines/

4.-Investigue e identifique dos herramientas de software de investigación forense que permita analizar teléfonos móviles inteligentes. Establezca un cuadro comparativo de referencia.

En mi caso seleccioné dos herramientas de investigación forense en teléfonos móviles de uso gratuito para Android: AFLogical OSE - Open source Android Forensics App and Framework y Andriller.

	AFLogical OSE	**Andriller**
Legalidad	La edición de código abierto fue lanzada para uso por parte de personal ajeno a la ley, aficionados a Android y gurús forenses. El software completo de AFLogical está disponible de forma gratuita para el personal encargado de hacer cumplir la ley.	Es una edición comunitaria, la cual está en un repositorio de código en la plataforma GitHub, donde claramente expresan en la Licencia MIT (licencia de software que se origina en el Instituto Tecnológico de Massachusetts, la cual permite reutilizar software dentro de Software propietario) que el software se entrega sin algún tipo de garantía y responsabilidad.
Compatibilidad con Sistemas Operativos	Solo la puede usar Android, ya sea descargando la última apk o usando Santoku Linux porque esta distribución tiene la herramienta preinstalada.	Se puede usar tanto en Windows como en Ubuntu Linux, y es recomendable configurar un entorno virtual para su instalación.
Formato	Es una aplicación que viene en formato APK (Android Application Package), este formato tiene los datos que permiten la ejecución de la aplicación en el sistema operativo Android, estos archivos pueden enviarse entre móviles Android y se abren al pulsar en ellos como cualquier otra aplicación móvil.	Es una aplicación multiplataforma que cuenta con una colección de herramientas forenses para teléfonos inteligentes, la cual realiza adquisiciones de solo lectura, forenses y no destructivas desde dispositivos Android.
Requisitos de instalación	N/A	Windows requiere tener instalado el paquete redistribuible de Microsoft Visual C ++ 2010 (x86), los controladores USB para su dispositivo Android y un navegador web para ver los resultados,

		mientras que Ubuntu necesita el paquete "android-tools-adb" instalado. Python 3.6+ (se recomienda la versión de 64 bits)
Caracteristicas de uso	La aplicación debe ser previamente instalada en el terminal Android para poder extraer información variada a la tarjeta SD (como lo son el registro de llamadas, listado de contactos y de aplicaciones instaladas, mensajes de texto y multimedia)	Permite obtener información de interés relacionada con redes sociales como con programas de mensajería (Skype, Tinder, WhatsApp, etc). Cuenta con descifrado de la pantalla de bloqueo para patrón, código PIN o contraseña, decodificadores personalizados para datos de aplicaciones de bases de datos de Android (algunos Apple iOS y Windows).
Extracción de la Información	Puede conectar la tarjeta a un dispositivo externo o mediante el ADB (Android Debug Bridge), esta es una herramienta mediante la cual la consola de comandos de nuestro computador hará puente de comunicación con el móvil, el cual nos permite enviar ordenes al dispositivo, así como cargar archivos entre una y otra plataforma.	Toda la extracción y los decodificadores producen informes en formatos HTML y Excel.

Fuentes: https://www.incibe-cert.es/blog/herramientas-forense-moviles, http://www.disoftin.com/2019/07/andriller-herramientas-forenses-de.html, https://www.xatakandroid.com/aplicaciones-android/que-apk-android-como-se-instala-diferencias-apps-normales, https://www.xatakandroid.com/tutoriales/adb-android-que-puedes-utilizarlo, https://www.nowsecure.com/blog/2017/07/29/aflogical-trade-open-source-edition-now-available-for-download/, https://github.com/nowsecure/android-forensics, https://es.wikipedia.org/wiki/Licencia_MIT#:~:text=La%20licencia%20MIT%20es%20una,%2C%20Massachusetts%20Institute%20of%20Technology).&text=La%20licencia%20MIT%20permite%20reutilizar%20software%20dentro%20de%20Software%20propietario y https://github.com/den4uk/andriller