1. Explique los motivos por los que el software es vulnerable.

R: Una vulnerabilidad es un fallo en la programación de un software, uno dentro de la seguridad del mismo. Existen 5 factores por los que se puede conocer la magnitud de dicha vulnerabilidad:

* **Producto:** Debe conocerse cuál producto o versión del producto está afectada, puede ser a una sola versión, varias o incluso a programas totalmente diferentes que compartan el mismo fallo.
* **Dónde:** Por lo general, la vulnerabilidad se localiza dentro de un componente o modulo del programa. Por ejemplo, una vulnerabilidad en el módulo de interpretación de ficheros de formato RTF en Word no afectaría a los módulos que procesan otros tipos de ficheros. Por el contrario, si el fallo se encuentra en un componente intrínseco del programa, esto afectaría a todo el mismo en sí. Por ejemplo, un fallo en el explorador de Windows.
* **Causa y consecuencia:** Se refiere a una falla técnica al momento de la programación, una falta de comprobación que permite que se den consecuencias indeseadas. Por ejemplo: Una falta de comprobación de caracteres en una aplicación web (causa), lleve a una posible SQL Injection (consecuencia).
* **Impacto:** Es lo que un atacante puede conseguir al aprovechar una vulnerabilidad. Define la gravedad del fallo. Por ejemplo: La ejecución de código arbitrario es muy grave, ya que significa que el atacante podrá realizar cualquier acción en el sistema de la víctima.
* **Vector:** Es la FORMA en la que el atacante aprovecha la vulnerabilidad. Por ejemplo, en un caso de *Phishing,* el vector seria el enlace malintencionado dentro de un correo electrónico.

2) ¿Que solución de seguridad implementaría para interconectar dos oficinas remotas? Indique de qué depende la seguridad de dicha solución.

R: Para interconectar dos oficinas usaría una red VPN para las terminales de dichas oficinas dentro de la red, aprovechando además el firewall proporcionado por el punto de enlace de la red para filtrar información no deseada a toda la subred. También implementaría un NIDS justo después de entrar a la subred para detectar ataques dentro de la subred, y de ser necesario, un HIDS para las terminales importantes dentro de las oficinas.  
La solución solo dependería de que no se envíen ficheros maliciosos dentro de la red VPN.

3) ¿En que se basa un IDS para detectar intrusiones? ¿Qué parámetros tendría en cuenta para la compra de un equipo de IDS en una empresa?

R: Un IDS analiza el tráfico de red que pasa por él, tanto en comportamiento como en contenido. Una de sus características es que puede ir mutando en su análisis a lo largo de su tiempo operativo.  
Para comprar un IDS en la empresa tendría en cuenta si la información que se debe cuidar está concentrada en una sola terminal, en ese caso utilizaría un HIDS en ese host, si por lo contrario la información esta diseminada por varios puntos de la subred utilizaría un NIDS cerca del punto de enlace de la red.

4) Indique los beneficios que obtiene una organización al certificar la norma ISO 27.000.

R: Al certificar la norma ISO 27000 una organización:

* Asegura la seguridad de la información, lo que aumenta la confianza del cliente.
* Permite destacar sobre la competencia
* Cuenta con un ciclo PDCA, garantiza una mejora seguida en los controles de seguridad establecidos en la organización.

5) ¿En qué fases o etapas del ciclo de vida del desarrollo de software incluiría la seguridad?

R: La seguridad se debe incluir en todas las partes del ciclo del desarrollo de software, siendo estas:

* **Inicio del proceso:** analizando riesgos, haciendo un modelado de las amenazas o teniendo una estandarización sobre prácticas de un diseño seguro.
* **Implementación de código:** Implementando prácticas de programación segura o realizando auditorias de código fuente (White box).
* **Al momento de la utilización:** realizando Penetration Testing (Black box).
* **A lo largo de la vida útil del software:** PDCA.

6) ¿Cómo podría identificar vulnerabilidades en una aplicación?

R: Para identificar vulnerabilidades en una aplicación se realizan Vulnerability Research, realizadas por Vulnerability Researchers, quienes son profesionales o entusiastas de la seguridad impulsados por diferentes motivos: Diversión, curiosidad, dinero, trabajo, etc.

7) Explique el proceso completo de un ataque de Phishing.

R: Pasos de Phishing:

* El atacante (phisher) envía un mail masivo o dirigido para inducir al usuario a acceder a un website.
* El servidor es un sitio falso controlado por el phisher.
* El usuario ingresa y se loguea, todos sus datos son robados.

8) Explique qué métodos de autenticación utilizaría en el acceso a un datacenter, a un edificio de oficinas, y a un sistema de software. Tenga en cuenta la minimización de los costos.

R: Probablemente utilizaría sistema de Huella digital como método de autenticación en cualquiera de los casos planteados, por su fiabilidad, bajo costo y aceptación. Adicionalmente se puede también implementar otro sistema en el caso del datacenter, como el de Geometría fácil por ejemplo, para tener más seguridad.

9) Explique qué es Nmap y para qué se lo utiliza.

R: Nmap (Network Mapear) es una utilidad de software libre para explorar, administrar y auditar la seguridad de redes de ordenadores. Detecta hosts online, sus puertos abiertos, servicios y aplicaciones corriendo en ellos, su SO, que filtros corren en una red y de qué tipo son.  
Se lo utiliza básicamente para 3 cosas:

* Auditorias de seguridad.
* Pruebas rutinarias de redes.
* Recolector de información para futuros ataques.

10) Explique cómo conseguiría que un software sea más seguro.

R: Se deben garantizar la seguridad en la información en los aspectos físicos, técnicos y administrativos.   
Para el aspecto físico, una red segura, con la implementación de sniffers.  
En cuanto a técnico, realizar pruebas metódicas y repetibles o documentar todo.  
Y desde administración, contratar personal especializado y entrenar al ya contratado.

11) Explique las 2 técnicas que utiliza un antivirus para detectar que un ejecutable es malicioso.

R: Las 2 técnicas que utilizan los antivirus para detectar que un ejecutable es malicioso son:

* **Detección por firmas:** Determina las características que lleva a un archivo a ser considerado o no un malware. No es muy eficiente, ya que no admite que un nuevo malware, que aún no esté incluido en la base de datos del antivirus sea detectado.
* **Detección heurística:** Anticipa el descubrimiento de un malware, basándose en la base de datos donde guarda sus firmas. El gran problema que tiene es que genera un gran número de falsos positivos. Los falsos positivos son aquellas detecciones de archivos que parecen malware por sus características pero que en realidad no lo son.  
  Además es más lento en su verificación y también sufre la característica de no poder identificar malware diferentes a los ya conocidos.

12) Defina qué es un Penetration Test y explique cuáles son las principales metodologías existentes.

R: Un Penetration Test es un método de evaluación de la seguridad de un sistema u organización, simulando un ataque tal y como la llevaría a cabo cualquier hacker que pretendiera hacerse con el sistema, manipular información o robarla, sobre todo aquella considerada “sensible”. Las principales metodologías existentes son:

* **ISSAF:** Está diseñada para evaluar una red, los sistemas y la aplicación de controles. No se actualiza desde el 2006. Su objetivo es proporcionar procedimientos muy detallados para el Testing de sistemas de información que reflejan situaciones reales.
* **PTES:** Pretende unir esfuerzos de analistas y expertos en seguridad para hacer un estándar que pueda completar una auditoria en todos sus procesos más habituales. Divide la ejecución de un test de intrusión en 7 fases.
* **OWASP:** Método de test para aplicaciones web basado en dos fases: pasiva y activa. Su enfoque es “black box” preferentemente, se sabe poco o nada de la aplicación que vamos a probar, incluso del contexto en el que se van a hacer las pruebas.
* **OSSTMM:** En constante actualización conceptual y estratégica. Está diseñada para ser consistente y repetible y ofrece al mismo tiempo una estrategia, test de evaluación y medida de riesgos, una valoración intrínseca en función de los resultados arrojados por los tests.

13) Explique qué diferencia existe entre las certificaciones profesionales de seguridad CISSP, CISA, y CEH.

R: Teniendo en cuenta que todos los certificados son orientados a la seguridad de la información, estos se diferencian en pequeños aspectos. Si bien los profesionales certificados en CISSP y CISA los podemos juntar en un grupo de auditoria, el CISSP es un perfil más técnico que funcional y en el otro caso esta exclusivamente orientado a un perfil de auditor. El caso de CEH lo podemos orientar más al perfil de Hacker Ético, los cuales entran más en detalle sobre tipos de ataques y metodologías.  
Otra diferencia es que tanto en CISA como en CISSP se requiere tener 5 años de experiencia como auditor de seguridad para obtener la licencia, por otro lado, no es necesario ese requisito para un perfil de CEH, en su lugar debe presentar gran conocimiento sobre técnicas de hacking y pentesting.

14) Explique en qué se basa la seguridad de los siguientes algoritmos criptográficos: RSA, El Gamal y AES.

R:

* **AES:** Sistema de cifrado simétrico y más utilizado hoy en día. La longitud de su clave puede variar entre 128, 192 y 256 bits. El cifrado se basa en sustituciones, permutaciones y transformaciones lineales ejecutadas varias veces en bloques de 16 bytes. El cambio de un solo bit, sea en la clave o en los bloques texto, resulta en un bloque de texto cifrado completamente diferente.
* **El Gamal:** Sistema de cifrado asimétrico que trabajo con 2 claves, una “publica” y otra “privada”, está libre de patentes y es utilizado tanto para generar firmas digitales como para cifrar/descifrar. Se basa en cálculos sobre “logaritmos discretos”, factorizando números muy grandes, de 150 dígitos o más. Usa para ello un número primo y dos enteros. Al cifrar o firmar es más lento que RSA.
* **RSA:** Sistema de cifrado asimétrico, que trabaja con dos claves diferentes: una clave “pública”, y otra “privada”. Ambas son complementarias entre sí, así que un mensaje cifrado con una de ellas sólo puede ser descifrado por su contraparte. La longitud de clave va desde los 128 bits a los 4096.

15) Explique técnicamente el funcionamiento de un Ransomware.

R: Un Ransomware se “camufla” dentro de otro archivo o programa, que a priori parece inofensivo, e invita al usuario a hacer click, por ejemplo: archivos adjuntos o actualizaciones de sistema.  
Una vez que el malware ha penetrado en el ordenador, el malware se activa y provoca el bloqueo de todo el sistema operativo y lanza el mensaje de advertencia con la amenaza y el importe de “rescate” que se debe pagar para recuperar la información.  
Para potenciar la incertidumbre y miedo de la víctima, en ocasiones se incluyen en la amenaza la dirección IP, la compañía proveedora de internet y hasta fotografías captada desde la propia webcam.

16) Explique el funcionamiento de una Botnet y sus usos.

R: Una Botnet es una red de robots, llamados “bots” o “zombies” para lograr la infección de otros equipos. Primero el atacante suelta un gusano en un servidor, este se reproduce a sí mismo, auto duplicándose.  
Estas copias son enviadas a una o varias red/es de computadoras para que se repliquen y se expandan sobre esa red mediante el uso de diferentes protocolos o servicios (SMTP, IRC, P2P), todo esto de manera automática sin que el usuario se dé cuenta. Su uso, por lo general, puede variar entre:

* **Ataques DDoS:** Utilizan la potencia del ordenador y el ancho de banda de ciento o miles de equipos para enviar gran cantidad de tráfico a una página web específica y sobrecargar dicha site. Existen varios tipos pero siempre es el mismo objetivo: colapsar una web.
* **Envío masivo de spam:** La idea es enviar spam a diferentes correos electrónicos.
* **Fraude de tarjeta de crédito a gran escala:** Básicamente irrumpen contra el sitio web de una tienda para obtener datos de las tarjetas de créditos de millones de usuarios.

17) Explique el funcionamiento de la Deep Web.

R: La Deep web es una gran parte del total de internet, el cual existe porque esa gran parte de contenido de la internet no puede ser indexado con los navegadores usuales (Google Chrome, Mozilla Firefox, Opera, etc.) por diferentes motivos, ya sea porque el contenido no se encuentre el formato HTML o las paginas estén intencionalmente restringidas u otras razones.  
Para ingresar a estar páginas se pueden utilizar navegadores específicamente creados para esta función, como por ejemplo Tor (The Onion Router).

18) Explique el funcionamiento de la Blockchain.

R: Blockchain llegó para registrar la veracidad de las transacciones sin necesidad de un tercero. Para esto, combina la tecnología P2P de intercambio entre pares con la criptografía.  
Cuando una transacción es realizada por un usuario del sistema, ésta es registrada y transmitida a todos los nodos de la red, así todos los integrantes tienen la información actualizada.  
Un nodo es un ordenador conectado que distribuye información actualizada a la red. Esto hace que con que haya un nodo funcionando la red funciona y se pueda recuperar ante cualquier eventualidad.  
Las transacciones se realizan desde monederos electrónicos, wallets, que son archivos encriptados que funcionan de manera similar a una cuenta bancaria. Así, de manera asimétrica, para que alguien te envíe datos previamente debes darle la clave pública.  
De esta manera fluyen las transacciones por la red, luego se añaden a un pool temporal de transacciones sin verificar. Luego por otra entidad (mineros), las transacciones sin confirmar crearan un nuevo bloque de transacciones.

19) Explique qué es la metodología Magerit, y para que se la utiliza.

R: Magerit es una metodología de análisis y gestión de riesgos, que ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones.  
**Se basa en analizar el impacto que puede tener para la empresa la violación de la seguridad**, buscando **identificar las amenazas** que pueden llegar a afectar la compañía**y las vulnerabilidades**que pueden ser utilizadas por estas amenazas. De esta forma, la compañía podrá **implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados**.

20) Indique cuáles son las principales herramientas comerciales de explotación de vulnerabilidades.

R: Hay muchas herramientas utilizadas para la explotación de vulnerabilidades, entre ellas se encuentran: Nmap, Nessus, Metasploit, w3af, Nikto, Wireshark, Putty, Core Impact, sqlmap, Canvas, NetStmbler, etc…