1. **¿Por qué proteger?**

   - Nuestras conversaciones son personales;
   - Nuestros mensajes son privados;
   - Una compra solo interesa al vendedor y al comprador;
   - La información pública de Internet debe estar al alcance de todos;
   - Las empresas deben cuidar su imagen;
   - Los contratos de las empresas son privados en muchos casos.

2. **¿Qué hace la Seguridad Informática?**

   La seguridad informática intenta proteger la transmisión, procesamiento y el almacenamiento de la información digital

3. **¿Cómo se protege el almacenamiento, procesamiento y transmisión de información digital?**

   - **Las conversaciones** por teléfono móvil deben ir cifradas;
   - **Los mensajes** se almacenan en el servidor de correo y, opcionalmente, en el cliente de correo que ejecuta un ordenador. Debemos proteger esos equipos, así como la comunicación entre ambos.
   - **La navegación** por la web del vendedor puede ser una conexión no cifrada, pero cuando se utiliza el carrito debemos pasar a un servidor seguro. La web del vendedor debe estar disponible a todas horas: hay que protegerla frente a caídas de tensión, cortes de red, accidentes o sabotajes de sus instalaciones;
   - **Los servidores** de información de una red mundial deben estar disponibles a todas horas;
   - Las empresas deben restringir **el acceso a las partes protegidas de su web;**
   - **Los contratos** deben llevar la firma digital de las empresas interesadas y deben almacenarse en discos cifrados.

4. **¿Cómo desplegar la máxima seguridad?**

   - Con más dinero podríamos replicar los servidores, conexiones, el suministro eléctrico o todo a la vez;
   - Con más formación en los técnicos podríamos desplegar sistemas avanzados de protección
   - Con más formación en los usuarios podríamos estar tranquilos porque no compartirían su contraseña con otros usuarios, no entrarían en páginas peligrosas, etc.

5. **¿Qué es una auditoría de seguridad?**

   Una auditoría de seguridad es un procedimiento que evalúa el nivel de seguridad de una empresa o entidad.

6. **¿Qué es un Sistema de Prevención de Intrusos (NIPS)?**

   Es un software que protege a los sistemas de ataques o intrusiones.

7. **¿Qué es un Tiger Team?**

   Es un equipo de crackers profesionales que se ocupan de hacer inspecciones o pruebas para estudiar los problemas de seguridad de una empresa.

8. **¿Cuál es el mayor activo a proteger?**

   El mayor activo a proteger es la información contenida en los equipos.

9. **¿Cuáles son los activos?**

   Equipos, aplicaciones, datos y comunicaciones.

10. **Equipos:**

- No se pueda sustraer, ni un equipo ni sus piezas, principalmente el disco duro.
- Vigilar los portátiles de la empresa y aplicar un cifrado en el disco duro.
- Prohibir la introducción de equipos no autorizados en la red.
- Mantenimiento preventivo.

11. **Aplicaciones:**

    - Evitar instalar software extra, incluir únicamente lo necesario
    - Instalar antivirus.
    - Desactivar los mecanismos de autoarranque o deshabilitar las unidades lectoras.

    Objetivos:

    - Ahorrar al usuario la tarea de instalar y configurar las aplicaciones.
    - Asegurar que el software instalado responde a las licencias.
    - Homogenizar el equipamiento.

12. **Datos:**

Motivos:

- Si desaparecen, la empresa no puede funcionar con normalidad.
- Si llegan a manos de la competencia, la estrategia y el futuro de la compañía está en riesgo.

Existen el esquema de las oficinas sin papeles, es decir, todos los datos están informatizados.

- Facturación electrónica;
- Tramitación electrónica.

La infraestructura necesaria es amplia y compleja porque los niveles de seguridad son elevados

- Todos los equipos deben estar protegidos contra software malicioso que pueda robar datos o alterarlos
- El almacenamiento debe ser redundante
- El almacenamiento debe ser cifrado

13. **Comunicaciones:**

- Se deben cifrar los canales de comunicación
- Controlar las conexiones de red en la empresa
- Nadie debe de poder conectarse a nuestra red sin permiso
- Evitar el spam y la publicidad en general

14. **¿Qué es la seguridad física?**

La seguridad física cubre toda la seguridad referida a los equipos informáticos; ordenadores, servidores, equipamiento de red, etc.

15. **Amenazas contra la seguridad física:**

- Desastres naturales.
- Robos
- Fallos de suministro

16. **¿Qué es la seguridad lógica?**

La seguridad lógica se refiere a la seguridad en el uso de software y los sistemas, protección de datos programas, etc.

17. **Amenazas conta la seguridad lógica:**

- Virus, troyanos y malware en general.
- Pérdida de datos.
- Ataques a las aplicaciones de los servidores.

18. **¿Qué es la seguridad pasiva?**

    La seguridad pasiva son todos los mecanismos que, cuando sufrimos un ataque, nos permiten recuperarnos de buena manera.

19. **¿Qué es la seguridad activa?**

    La seguridad activa intenta protegernos de los ataques mediante la adopción de medidas preventivas que protejan a los activos de la empresa.

20. **¿Qué es la confidencialidad? Define sus tipos:**

    La confidencialidad intenta que la información solo sea utilizada por las personas o máquinas debidamente autorizadas.

    - Autenticación
    - Autorización
    - Cifrado

21. **¿Qué es la disponibilidad?**

    La disponibilidad intenta que los usuarios puedan acceder a los servicios con normalidad en el horario establecido.

22. **¿Qué es el no repudio?**

    Ante una relación entre dos partes, intentaremos evitar que cualquiera de ellas pueda negar participar en esa relación

23. **¿Cuál es el objetivo de la integridad?**

    Es que los datos queden almacenados tal y como espera el usuario; que no sean alterados sin su consentimiento.

24. **¿Cuál es el esquema utilizado para analizar la autenticación? Define sus tipos:**

    - Algo que sabes: Contraseñas/claves
    - Algo que tienes: tarjetas de seguridad
    - Algo que eres: biometría

25. **¿Qué es AAA? Define Accounting**

    La sigla AAA se refiere a autenticación, autorización y accounting.
    Accounting es el proceso de rastrear la actividad del usuario mientras accede a los recursos de la red, incluso la cantidad de tiempo que permanece conectado, los servicios a los que accede, así como los datos transferidos durante la sesión.

26. ¿Qué es una vulnerabilidad? Dicta sus tipos:

Una vulnerabilidad es el defecto de una aplicación que puede ser aprovechado por un atacante. Hay tres tipos de vulnerabilidades:

- Vulnerabilidades reconocidas
- Vulnerabilidades reconocidas, pero que todavía no hay un parche
- Vulnerabilidad no reconocida

27. ¿Qué es e2e?

e2e significa extremo a extremo: la seguridad debe controlar el canal de comunicación utilizado entre el origen y el destino de los datos.

28. Principales tipos de malware:

- Virus: dejan inservible el ordenador infectado.
- Gusanos: Van acaparando todos los recursos del ordenador.
- Troyanos: habilitan puertas traseras en los equipos.

29. ¿Qué es un LiveCD?

Un LiveCD es un sistema operativo almacenado en un medio extraíble, tradicionalmente un CD o un DVD, que puede ejecutarse directamente en una computadora sin necesidad de ser instalado.

30. Formas de ataque:

- **Interrupción:** consigue provocar un corte en un servicio.
- **Interceptación:** accede a nuestras comunicaciones y copia la información.
- **Modificación:** Consigue acceder y modifica la información.
- **Fabricación:** El atacante se hace pasar por el destino de la transmisión, por lo que puede tranquilamente conocer el objeto de nuestra comunicación y engañarnos para obtener información valiosa

31. Técnicas de ataque:

- Ingeniería Social:
- Phising:
- Keyloggers:
- Fuerza Bruta:
- Spoofing:
- Sniffing:
- DoS
- DDoS

32. Tipos de atacantes:

- Hacker
- Cracker
- Script kiddie
- Programadores de malware
- Sniffers
- Ciberterroristas

33. Buenas prácticas:

- Localizar los activos que hay que proteger
- Redactar y revisar los planes de actuación ante catástrofes
- No instalar nada que no sea necesario y revisar los permisos
- Estar al día de los informes de seguridad
- Activar los mecanismos de actualización automática
- Dar formación a los usuarios
- Revisar los logs de los sistemas
- Considerar la opción de contratar una auditoría externa
- Revisar la lista de quipos conectados
- Revisar la lista de usuarios activos
- Avisar de cualquier problema por correo o SMS

34. ¿Qué es LOPD? Define sus niveles:

Es la Ley Órganica de Protección de Datos de Carácter Personal: establece las bases para proteger el tratamiento de los datos de carácter personal de las personas físicas.

- Nivel Básico
- Nivel Medio
- Nivel alto

35. ¿Qué es LSSI-CE?

Es la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico: intenta cubrir el hueco legal que había con las empresas que prestan servicios de la sociedad de la información

36. ¿Qué es LPI?

La Ley de Propiedad Intelectual: establece los derechos de autor en los entornos digitales.