Examen: Seguridad Informática

11. Un Cracker es:
    a) Un delincuente informático que solo se plantea retos intelectuales.
    b) Un pirata informático que intenta atentar contra la seguridad de la red.
    c) Es una persona que elabora aplicaciones para usar programas sin licencia.
12. El pharming es:
    a) Una cadena de correo iniciada por empresas para recopilar direcciones de emails.
    b) Es una práctica para suplantar páginas webs
    c) Es una mensaje de correo electrónico que inunda la red
13. Una vulnerabilidad crítica:
    a) Puede poner en peligro la integridad o disponibilidad de los recursos de procesamiento
    b) Puede permitir la propagación de un gusano de internet sin la acción del usuario.
    c) Se puede reducir en gran medida a partir de configuraciones predeterminadas
14. Un antivirus:
    a) Es un sistema de defensa que controla y filtra el tráfico de entrada y salida a una red.
    b) Es un software que funciona como puerta de entrada para limitar el tráfico de la red.
    c) Es un programa que revisa el código de los archivos y analiza las distintas unidades y dispositivos.
15. Un certificado digital
    a) Es un documento en formato analógico que contiene datos de una persona.
    b) Se diferencia de la firma electrónica en que solo sirve para validar la firma manuscrita.
    c) Contiene datos identificativos de una persona validados de forma electrónica.
16. La seguridad pasiva:
    a) Trata de evitar el impacto de un posible daño informático
    b) Utiliza el SAI y el backup o copia de seguridad como mecanismos de actuación
    c) Trata de evitar en los equipos los ataques de piratas informáticos.
17. La huella digital es:
    a) El rastro que dejamos cuando utilizamos los servicios de internet.
    b) Un tipo de certificado digital que nos identifica ante terceros por internet.
    c) La configuración que presenta nuestro equipo informático para navegar por internet.
18. Un CAPTCHA es:
    a) Una clave que introducimos para darnos de alta en un servicio de internet.
    b) Es una clave que demuestra que quién maneja el ordenador es administrador de la red
    c) Es una prueba de que quién intenta acceder a una cuenta con contraseña es un ser humano.
19. Los protocolos HTTPS e IPV6:
    a) Son evoluciones de los protocolos HTTP y TCP/IP para ganar rapidez en la conexión.
    b) Son protocolos seguros de los protocolos HTTP e IPV4
    c) No tienen relación con los protocolos de internet, sino con las páginas web.
20. Los protocolos IPV4 e IPV6:
    a) Se diferencian en que el segundo permite más direcciones de memoria que el primero
    b) Se parecen en que ambos son protocolos pocos seguros porque trabajan de manera cifrada.
    c) Se diferencian en que el primero utiliza direcciones con dígitos hexadecimales y el segundo no.

TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA COMUNICACIÓN II

Examen: Seguridad Informática

Nombre estudiante:

En las siguientes cuestiones, señaliza la respuesta válida. Obtendrás 1 punto por cada acierto y -0.5 por cada error. Las preguntas no contestadas no puntúan en ningún sentido.

1. El big data es:
   a) Es la gestión y análisis de enormes cantidades de redes tratadas de manera digital.
   b) Es la gestión y análisis de los datos que tenemos guardados en el ordenador.
   c) Es la gestión y análisis de grandes cantidades de datos.
2. Un cortafuegos o firewall es:
   a) Es un sistema de defensa para cortar el fuego en las redes de ordenadores.
   b) Es un sistema que controla el trafico de datos entre el ordenador y el disco duro.
   c) Es un sistema de defensa que controla y filtra el trafico de datos a una red.
3. La criptografía es:
   a) Un sistema de cifrado para ocultar los archivos en las carpetas donde están ubicados.
   b) El cifrado de información para proteger la red de virus y software espía.
   c) Un sistema cifrado para la protección de claves, archivos y comunicaciones
4. Internet de las cosas es:
   a) La conexión de objetos de uso cotidiano a una red para dotarlos de energía.
   b) La conexión de objetos a internet para dotarlos de interactividad.
   c) La conexión de objetos a internet para que se protejan de infecciones por virus.
5. La seguridad informática es:
   a) El conjunto de medidas para proteger a las personas de los ordenadores.
   b) Las medidas que nos permiten proteger los equipos frente el hardware y el software.
   c) Las medidas para proteger el hardware, el software, la información y las personas.
6. La seguridad lógica:
   a) Es alternativa de la seguridad física y protege el hardware de los virus.
   b) Complementa la seguridad física y protege la información y el software.
   c) Protege el hardware ante posible desastres naturales.
7. La seguridad activa es:
   a) Es la que pretende minimizar el impacto de un posible daño informático
   b) Es la que pretende proteger al ordenador y su contenido.
   c) Es la que pretende minimizar el impacto de las pérdidas de las copias de seguridad.
8. La seguridad en la persona:
   a) Trata de proteger ante amenazas, fraudes y daños materiales a nuestros ordenadores.
   b) Protege a las personas de amenazas y fraudes.
   c) Trata de defender los derechos de los usuarios de internet.
9. Se denomina Adware:
   a) A un programa que se instala en el ordenador para infectarlo más tarde.
   b) A un tipo de virus en el que se han introducido instrucciones de copia de archivos.
   c) A un programa que muestran publicidad después de ser instalados.
10. Un Keylogger es:
    a) Es un tipo de programa que recoge información sobre la navegación del usuario por la red.
    b) Es un programa que destruye información en el disco duro del usuario cuando se instala.
    c) Es un programa que obtiene y memoriza las pulsaciones de un teclado.