Su calificación final en este cuestionario es 10,00/10,00.
Promedio de calificaciones: 10,00 / 10,00.

1. Por defecto y atendiéndonos a los principios de seguridad el CDROM debería estar desactivado en la BIOS. ¿Verdadero o falso?
   a. Verdadero
   b. Falso

2. ¿Cuál de los siguiente no es un riesgo de tener los USB activados?
   a. Eleva el riesgo de fuega de información y de infección
   b. Aumenta la concienciaciónd de los usuarios
   c. Permite conecar dispositivos "rogue" para captura de información, lineas de conexión no controladas, despliegue de malware,...

3. Desde el punto de vista de la seguridad, el particionado del disco duro nos permite
   a. No será necesario actualizar el sistema tan frecuentemente
   b. Tener más organizado el disco duro
   c. Proteger la información más sensible

4. Cual de lo siguientes es el puerto que menos riesgo tiene dejar habilitado en un equipo a través de la BIOS:
   a. Bluetooth
   b. Audio
   c. USB

5. En los sistema linux, ¿qué mecanismo nos permite proteger la secuencia de arranque?:
   a. Ansible
   b. Network Deception
   c. GRUB

6. ¿Qué parámetro de la configuración de particiones de Linux en /etc/fstab permite protege al sistema de la ejecución de ficheros en dicha partición?.
   a. nodev
   b. default
   c. noexec

7. ¿Es seguro habilitar por defecto las nuevas funcionalidades de actualización remota de la UEFI? ¿Verdadero o falso?
   a. Verdadero
   b. Falso

8. Qué tecnología nos proporciona el acceso más segura al sistema de manera remota sin que la información tenga que almacenarse en el dispositivo desde el que nos conectamos.
   a. Telnet
   b. VDI/VGI
   c. RDP

9. ¿Qué mecanismo de seguridad permite proteger el acceso la BIOS?
   a. Cambiar la secuencia de arranque
   b. Contraseña
   c. Actualizarla

10. La comprobación de integridad de la nuevar versión de la BIOS nos asegura:
    a. **Autenticidad del software por parte del fabricante**
    b. Que no tiene vulnerabilidades
    c. La correcta funcionalidad

Segundo intento:
1. ¿Cómo se denomina el modo de arranque del sistema que nos permite realizar un diagnóstico de un problema?
    a. Arranque antihacking
    b. Arranque TOR
    c. **Arranque seguro**

2. El método de intercambio de ficheros entre dos equipos a través de un dispositivo externo se denomina:
    a. **Air Gap**
    b. Hand Disk
    c. USB transportting

3. El Bluetooth activado contituye un riesgo para la fuga de información del sistema. ¿Verdadero o falso?
    a. **Verdadero**
    b. Falso

4. Qué herramienta de Windows permite el cifrado de la información del sistema de archivos:
    a. CipherWin
    b. **BitLocker**
    c. AppLocker

5. Por qué se ha tenido en consideración la utilización de productos ciberseguros acreditados
    a. Por el continuo negocio de las blockchain
    b. El alto coste que tienen los productos de software libre
    c. **Ataques a la cadena de suministros**

6. ¿Qué debemos monitorizar en el arranque del sistema?
    a. Consumo de disco
    b. Número de usuarios
    c. **Jerarquía de procesos**

7. Que tipo de malware se instala en el arranque del sistema:
    a. **rootkit**
    b. adware
    c. spoofing

8. La descarga de la actualización firware de BIOS/UEFI se debe hacer desde:
    a. La página que aglutina más software relativo a BIOS/UEFI.
    b. **Página oficial del fabricante.**
    c. Página web del Ministerio de Industria.

9. ¿Qué herramienta permite cifrar archivos en Linux?

a. **gpg**
b. ppp
c. man

10. ¿Es considerada segura la UEFI de un fabricante que no publica actualizaciones de seguridad de su firmware?. ¿Verdadero o falso?

a. Verdadero
b. **Falso**