UNIVERSIDAD TÉCNICA DE COTOPAXI
FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS
CARRERA DE SISTEMAS DE INFORMACIÓN

Asignatura: CONTROL Y AUDITORIA INFORMÁTICA
Alumno: Anthony Steeven Monta Chiliquinga
Ciclo: SÉPTIMO
Actividad: Taller #1

1. **¿Qué elementos integran un sistema informático según el documento?**
   a) Hardware, software, datos y redes
   b) Hardware, software, datos y usuarios
   c) Software, datos, usuarios y protocolos
   d) Hardware, redes, usuarios y datos

   Justificación: Como nos explicó los sistemas informaticos solo estan integrados por el hardware, software, datos y usuarios, ya que si alguno de estos falta no se puede llegar a nada

2. **El principio de seguridad informática que garantiza la privacidad de la información es:**
   a) Integridad
   b) Disponibilidad
   c) Confidencialidad
   d) Autenticación

   Justificación: la confidencialidad es que la información sea privada, que no cualquiera pueda verla

3. **¿Qué característica define a un virus informático?**
   a) Solo afecta hardware
   b) Se replica sin consentimiento del usuario
   c) Es inofensivo hasta que se elimina
   d) Solo se propaga por correo electrónico

   Justificación: Un virus se copia solo, sin que uno le diga y afecta el equipo

4. **Un virus que se aloja en el sector de arranque del disco y se carga en memoria al iniciar el sistema se llama:**
   a) Virus de macro
   b) Virus mutante
   c) Virus de sector de arranque
   d) Virus de Internet

   Justificación: Este tipo de virus se mete en la parte que se carga primero cuando prendes la pc

Ing. Jorge Bladimir Rubio Peñaherrera, Mgs.
jorge.rubio@utc.edu.ec
0995220308 (WhatsApp)

5. **¿Qué tipo de virus está diseñado para atacar un producto antivirus específico?**
   a) Virus genérico
   b) Bounty Hunter
   c) Virus recombinable
   d) Virus de red

   Justificación: Estos son virus que atacan directamente a los programas antivirus

6. **Según el documento, los crackers buscan principalmente:**
   a) Mejorar la seguridad del sistema
   b) Obtener beneficio personal o destruir el sistema
   c) Reportar fallas a los administradores
   d) Crear software libre

   Justificación: Los crackers buscan sacar provecho o dañar los sistemas

7. **¿Cuál es un mecanismo de seguridad orientado a fortalecer la disponibilidad?**
   a) Encripción de datos
   b) Planes de recuperación
   c) Firewall
   d) Software anti-virus

   Justificación: Estos si algo falla, puedas recuperar el sistema rápido

8. **La técnica que enmascara datos para proteger su confidencialidad se llama:**
   a) Sincronización
   b) Cifrado de datos
   c) Respaldo incremental
   d) Autenticación biométrica

   Justificación: Cifrar es como ponerle un candado a los datos para que nadie los pueda ver

9. **¿Qué factor de riesgo incluye fallas en el servicio eléctrico y ataques de virus?**
   a) Ambientales
   b) Humanos
   c) Tecnológicos
   d) Impredecibles

   Justificación: Son problemas tecnológicos, porque tienen que ver con las máquinas y programas

10. **Para proteger físicamente los dispositivos, se recomienda:**
    a) Colocarlos cerca de ventanas
    b) Instalar detectores de humo y pararrayos

Ing. Jorge Bladimir Rubio Peñaherrera, Mgs.
jorge.rubio@utc.edu.ec
0995220308 (WhatsApp)

c) Permitir acceso libre a las áreas de computadoras
d) Ubicarlos directamente en el piso

Justificación: Poner detectores y pararrayos ayuda a proteger el hardware de incendios o tormentas

Ing. Jorge Bladimir Rubio Peñaherrera, Mgs.
jorge.rubio@utc.edu.ec
0995220308 (WhatsApp)