

# ADiestramiento sobre conciencia en la seguridad informática y reglas de comportamiento – Año fiscal 2016

## EXAMEN 3- PAPEL

1. La meta de la Seguridad de los Sistemas de Información (o ISS por sus siglas en inglés) es:
  - a. Animar a los hackers
  - b. Proteger los sistemas de información contra el acceso no autorizado
  - c. Disminuir la disponibilidad de los sistemas
  - d. Ambos: animar a los hackers y disminuir la disponibilidad de los sistemas
  
2. El Manejo de Seguridad de la Información Federal (o FISMA por sus siglas en inglés):
  - a. Define la seguridad nacional de los sistemas
  - b. Todas las respuestas son correctas
  - c. Requiere un alto nivel de protección para la información de los sistemas de gobierno que contienen el Acta de Información Privada
  - d. Exige un programa de seguridad informática en todas las agencias federales
  
3. ¿Cuál de los siguientes no es información de identificación personal (PII por sus siglas en inglés)?
  - a. Historial de empleo
  - b. Información sobre o asociada a un individuo
  - c. Lugar de nacimiento
  - d. Código postal
  
4. ¿Cuál de los siguientes es un ejemplo de un incidente de seguridad?
  - a. Intento de enviar correo electrónico basura en forma de anuncio comercial
  - b. Todos son incidentes de seguridad
  - c. Pérdida de una computadora portátil (laptop) que contiene información personal
  - d. Intento de las personas no identificadas o no autorizadas a obtener información sensible personal o de negocios

5. Lauren recibe un correo electrónico con un documento adjunto enviado por el director de su agencia. Este documento tiene una extensión de archivo que no es familiar. Lauren debe hacer todas las siguientes excepto:
  - a. Llamar al personal de ayuda al cliente (help desk) y pedir direcciones sobre cómo manejar la situación
  - b. Verificar que el remitente haya enviado el correo electrónico y el documento adjunto
  - c. Sospechar del correo electrónico y el documento adjunto
  - d. Abrir el documento adjunto
  
6. Thomas visita un sitio web que sin él saberlo ha transmitido un código malicioso a su computadora. Este código malicioso puede hacer todo lo siguiente a su equipo, excepto:
  - a. Corromper los archivos
  - b. Causar que su computadora se prenda en fuego
  - c. Borrar su disco duro
  - d. Permitir que otros ganen acceso a su computadora
  
7. Diana tiene su cheque de pago depositado directamente de la cuenta de su empleador a su cuenta de cheques. Esto es un ejemplo de:
  - a. Fraude electrónico (Phishing)
  - b. Comercio electrónico
  - c. Cookies
  - d. Teletrabajo
  
8. Nancy acaba de leer en su periódico local que el FBI ha determinado que este crimen está creciendo más rápido que otros. ¿Cuál es?
  - a. Apropiación
  - b. Robo de identidad
  - c. Fraude
  - d. Asesinato
  
9. Los cookies contienen información sobre usted. La información si no está cifrada (encrypted) puede ser vista por terceras partes. La mejor practica para evitar que esto suceda es:
  - a. Asegurarse que su navegador este programado para no aceptar cookies.
  - b. Visitar sólo sitios web que utilicen códigos ActiveX o JavaScript
  - c. No visitar sitios web no gubernamentales
  - d. Instalar software espía (spyware)

10. Jacob colecciona películas. Él ha encontrado la forma de obtener las películas sin ningún costo utilizando un servicio donde comparte el contenido de su computadora con otros usuarios. Él ha programado su computadora para este servicio. Esto es un ejemplo de la siguiente vulnerabilidad:
- Código móvil
  - Tecnología peer-to-peer
  - Ingeniería social
  - Falla en el software
11. Para Uso Oficial Solamente (FOUO por sus siglas en inglés) o Información No Clasificada Controlada (CUI por sus siglas en inglés) pueden incluir todas las siguientes excepto:
- Información de pago
  - Información de personal
  - Información secreta
  - Información sensitiva
12. Todas las siguientes son procedimientos aceptables para copias de respaldo (backup) de información clasificada excepto:
- Copiar (backup) información clasificada diariamente
  - Almacenar las copias de respaldo en la gaveta de su computadora
  - Rotular las copias de respaldo con etiquetas de sensibilidad
  - Almacenar las copias de respaldo en una localización segura aprobada