**Control y monitoreo de la información**

Instrucción: Es tiempo de validar el conocimiento y poner a prueba lo aprendido.

Pregunta 1: **¿Cuál de estos no es un dispositivo de control de seguridad?**

1. Teclado.
2. *Firewall*.
3. IPS.
4. *Antispam*.

**Retroalimentación positiva:** Muy bien, has acertado. Recuerda que los dispositivos de control son aquellos que permiten evitar los incidentes de seguridad en una organización.

**Retroalimentación negativa:** Lastimosamente, no has acertado. Te invitamos a repasar el componente formativo en la temática relacionada con los dispositivos de control de seguridad.

Pregunta 2: **Un *software* de *antimalware* permite prevenir ataques informáticos variados, los cuales son:**

1. Troyanos, gusanos, *spyware*.
2. Troyanos, gusanos, daños de *hardware*.
3. *Spyware*, troyanos, velocidad de la red.
4. Solamente troyanos y *spyware*.

**Retroalimentación positiva:** Muy bien, has acertado. Recuerda que los *antimalware* son implementados para contrarrestar ataques de diversos virus, entre ellos troyanos, gusanos y *spyware.*

**Retroalimentación negativa:** Lastimosamente, no has acertado. Te invitamos a repasar el componente formativo en los conceptos de tecnologías de protección.

Pregunta 3: **¿Qué es el parchado virtual?**

1. Es un proceso que permite mantener actualizados los dispositivos de seguridad y *software* de control conectados con los proveedores de productos.
2. Descargar de Internet las actualizaciones de seguridad e instalarlas en los equipos de la organización.
3. Comprar las actualizaciones en páginas de proveedores e instalarlas en los dispositivos de seguridad.
4. Pedir prestados los archivos de parches de seguridad a un amigo e instalarlos en los dispositivos de seguridad de la organización.

**Retroalimentación positiva:** Muy bien, has acertado. Recuerda que el parchado virtual es una ventaja para las organizaciones, ya que les permite estar conectados con las actualizaciones de manera oportuna.

**Retroalimentación negativa:** Lastimosamente, no has acertado. Te invitamos a repasar el componente formativo en los conceptos de seguridad y controles de seguridad.

Pregunta 4: **¿Cuál es la ley que regula los delitos informáticos en Colombia?**

1. Ley 1273 de 2009
2. Ley 1279 de 2009
3. Ley 1273 de 2012
4. Ley 1279 de 2012

**Retroalimentación positiva:** Muy bien, has acertado. Recuerda que la normatividad en Colombia, con respecto a los delitos informáticos, es la Ley 1273 del 5 de enero de 2009.

**Retroalimentación negativa:** Lastimosamente, no has acertado. Te invitamos a repasar el componente formativo CF04 en la temática relacionada con la normatividad.

Pregunta 5: **¿Cuáles son las características de las evidencias forenses?**

1. Duplicar, verificar autenticidad, recuperación, almacenamiento.
2. Duplicar y almacenar.
3. Verificar autenticidad y recuperación.
4. Almacenamiento y duplicación.

**Retroalimentación positiva:** Muy bien, has acertado. Recuerda que las evidencias forenses tienen cuatro características principales: duplicar, verificar la autenticidad, recuperar y almacenar.

**Retroalimentación negativa:** Lastimosamente, no has acertado. Te invitamos a repasar el componente formativo en los conceptos del proceso forense.

Pregunta 6: **Los procesos de mejora continua para el trabajo de manejo de incidentes proponen cuatro aspectos fundamentales, los cuales son:**

1. Preparación, detección del incidente, plan de contingencia, procesos a realizar luego del incidente.
2. Detección del incidente, realizar una reunión con el equipo de contingencia, contratar una empresa experta, contratación.
3. Detección del incidente, eliminar el incidente, reunión equipo de trabajo, desplegar plan de contingencia.
4. Desplegar plan de contingencia, eliminar incidente, eliminar incidente.

**Retroalimentación positiva:** Muy bien, has acertado. Recuerda que los procesos de mejora continua son fundamentales en la mejora de la respuesta y recuperación de desastres; ellos proponen los siguientes pasos: preparación del plan, detectar el incidente, definir el plan de contingencia a aplicar, y luego las acciones a realizar cuando se supera la emergencia.

**Retroalimentación negativa:** Desafortunadamente, no has contestado de manera correcta. Te invitamos a repasar los conceptos de planes de contingencia que encontrarás en el componente formativo.

Pregunta 7: Un *firewall* es un dispositivo de seguridad, que puede encontrarse como *hardware* o *software,* que se encarga de controlar el acceso a la infraestructura y por ende a la información de una compañía.

1. Verdadero
2. Falso

**Retroalimentación positiva:** Muy bien, has contestado de manera correcta. Recuerda que el *firewall* es un dispositivo de *hardware* o *software* que se dedica a permitir el acceso a la información y los dispositivos que estén previamente autorizados.

**Retroalimentación negativa:** Lastimosamente, no has contestado de manera correcta. Te invitamos a realizar un repaso al componente en la temática de tecnologías de protección.

Pregunta 8: **¿Qué es un IPS?**

1. Es un dispositivo que se encarga de vigilar el tráfico de la red, detectar anomalías y enviar alertas de seguridad.
2. Es un dispositivo que se encarga del bloqueo de todos los dispositivos de la red en caso de detectar un intruso.
3. Es un dispositivo que se encarga de realizar copias de seguridad de la información en un lugar seguro.
4. Es un dispositivo de seguridad que se encarga de gestionar el tamaño de los archivos en la red de datos.

**Retroalimentación positiva:** Muy bien, has acertado. Recuerda que los IPS son dispositivos que realizan un escaneo de la red para ver problemas de vulnerabilidad y generar alertas de seguridad.

**Retroalimentación negativa:** Lastimosamente, has contestado de manera errada. Te invitamos a realizar un repaso al componente formativo en la temática de tecnologías de protección.

Pregunta 9: **Según la Ley 1273 del 5 de enero de 2009, en el Artículo 269ª, cuando se refiere a “Acceso abusivo a un sistema informático”, hace referencia a:**

1. Utilizar mecanismos para violar un sistema de seguridad con el fin de sustraer o dañar información del mismo.
2. Probar la seguridad del sistema.
3. Establecer si el sistema es seguro o no.
4. Medir la eficacia de las contraseñas utilizadas.

**Retroalimentación positiva:** Muy bien, has acertado. Tenga en cuenta que la Ley 1273 de 2009 permite sancionar los comportamientos delictivos en el ámbito informático. El Artículo 269A se refiere al comportamiento de utilizar mecanismos para ingresar a sistemas de información protegidos o no por medida de seguridad para fines delictivos.

**Retroalimentación negativa:** Lastimosamente, no has contestado de manera correcta. Te invitamos a realizar un repaso del componente formativo en el tema relacionado con la normatividad.

Pregunta 10: **¿A qué marco de referencia está asociada la certificación CCNA Security?**

1. A los pilares de la seguridad de la información: integridad, confidencialidad, disponibilidad.
2. A que un profesional debe ser competente en la instalación de dispositivos de seguridad de última tecnología.
3. Los pilares de la seguridad de la información son: integridad y disponibilidad.
4. A la implementación de *hardware* de manera correcta.

**Retroalimentación positiva:** Muy bien, has contestado de manera correcta la pregunta. Recuerda que la certificación en CCNA Security es para profesionales que se están adentrando en el mundo de la seguridad de la información, y tiene como propósito conocer y hacer cumplir los tres pilares de la seguridad de la información, los cuales son: integridad, disponibilidad y confidencialidad.

**Retroalimentación negativa:** Lastimosamente, no has contestado de manera correcta. Te invitamos a realizar un repaso del componente formativo CF04 en la temática de certificaciones.