|  |  |  |  |
| --- | --- | --- | --- |
| ACTIVIDAD DIDÁCTICA CUESTIONARIO | | | |
| Generalidades de la actividad   * Las indicaciones, el mensaje de correcto e incorrecto debe estar la redacción en segunda persona. * Diligenciar solo los espacios en blanco. * El aprendiz recibe una retroalimentación cuando responde de manera correcta o incorrecta cada pregunta. * Señale en la columna Rta. Correcta con una (x) de acuerdo con las opciones presentadas. * Al final de la actividad se muestra una retroalimentación de felicitación si logra el 70 % de respuestas correctas o retroalimentación de mejora si es inferior a este porcentaje.   Para sugerir este tipo de actividad tener presente equipo de Diseño Instruccional, que solo debe haber máximo doce opciones de pregunta y que cada campo tiene un límite de palabras permitidas para garantizar el responsive web. | | | |
| Instrucciones para el aprendiz | | Esta actividad le permitirá determinar el grado de apropiación de los contenidos del componente formativo **Análisis forense y profesionalización en ciberseguridad.**  Antes de su realización, se recomienda la lectura del componente formativo mencionado. Es opcional (no es calificable), y puede realizarse todas las veces que se desee.  Lea la afirmación de cada ítem y luego señale verdadero o falso según corresponda. | |
| Nombre de la Actividad | | Gestión del riesgo y seguridad digital. | |
| Objetivo de la actividad | | Evaluar y reforzar el conocimiento adquirido sobre el análisis forense y profesionalización, teniendo en cuenta los procesos en ciberseguridad. | |
| Texto descriptivo | | Lea cada enunciado referente a los temas desarrollados en el componente formativo y elija entre verdadero y falso según corresponda. | |
| PREGUNTAS | | | |
| Pregunta 1 | | **La ciberseguridad solo protege computadoras y no datos ni redes.** | Rta(s) correcta(s) (x) |
| Opción a) | Verdadero | |  |
| Opción b) | Falso | | X |
| Comentario respuesta correcta | | Correcto. La ciberseguridad protege computadoras, datos, redes y otros dispositivos frente a amenazas digitales | |
| Comentario respuesta incorrecta | | Incorrecto. La ciberseguridad abarca la protección de computadoras, datos y redes. | |
| Pregunta 2 | | **El origen de la ciberseguridad está ligado a la conexión de computadoras y el nacimiento de las redes.** | |
| Opción a) | Verdadero | | X |
| Opción b) | Falso | |  |
| Comentario respuesta correcta | | Correcto. La ciberseguridad surge a partir del desarrollo de redes informáticas entre los años 50 y 60. | |
| Comentario respuesta incorrecta | | Incorrecto. La ciberseguridad surgió con las primeras redes y conexiones de computadoras. | |
| Pregunta 3 | | **Una de las características clave de la ciberseguridad es la confidencialidad de la información.** | |
| Opción a) | Verdadero | | X |
| Opción b) | Falso | |  |
| Comentario respuesta correcta | | Correcto. La confidencialidad es una característica básica de la ciberseguridad, junto con la integridad y la disponibilidad | |
| Comentario respuesta incorrecta | | Incorrecto. La confidencialidad, junto con integridad y disponibilidad, son pilares de la ciberseguridad. | |
| Pregunta 4 | | **Las empresas no necesitan ciberseguridad si no manejan datos confidenciales.** | |
| Opción a) | Verdadero | |  |
| Opción b) | Falso | | X |
| Comentario respuesta correcta | | Correcto. Todas las empresas, independientemente del tipo de datos, están expuestas a riesgos y deben proteger su información y sistemas | |
| Comentario respuesta incorrecta | | Incorrecto. Todas las empresas deben proteger su información y sistemas, sin importar el tipo de dato. | |
| Pregunta 5 | | **La Ley 1273 de 2009 regula delitos informáticos en Colombia.** | |
| Opción a) | Verdadero | | X |
| Opción b) | Falso | |  |
| Comentario respuesta correcta | | Correcto. La Ley 1273 es un marco legal clave para la protección frente a delitos informáticos en Colombia. | |
| Comentario respuesta incorrecta | | Incorrecto. Esta ley regula y sanciona delitos informáticos en el país. | |
| Pregunta 6 | | **Los delitos informáticos solo incluyen el robo de información.** | |
| Opción a) | Verdadero | |  |
| Opción b) | Falso | | X |
| Comentario respuesta correcta | | Correcto. Incluyen una variedad de actos como fraude, sabotaje, acceso no autorizado y malware | |
| Comentario respuesta incorrecta | | Incorrecto. Involucran varios delitos como fraude, sabotaje, hacking, etc. | |
| Pregunta 7 | | **Los ciberdelincuentes siempre actúan de manera aislada, sin formar grupos.** | |
| Opción a) | Verdadero | |  |
| Opción b) | Falso | | X |
| Comentario respuesta correcta | | Correcto. Los actores pueden ser individuos o grupos organizados (cibercriminales, hacktivistas, etc.) | |
| Comentario respuesta incorrecta | | Incorrecto. Existen tanto individuos como grupos organizados en el cibercrimen. | |
| Pregunta 8 | | **El *phishing* es una técnica común para engañar a usuarios y robar datos.** | |
| Opción a) | Verdadero | | X |
| Opción b) | Falso | |  |
| Comentario respuesta correcta | | Correcto. Es una técnica ampliamente utilizada para obtener información mediante el engaño. | |
| Comentario respuesta incorrecta | | Incorrecto. El *phishing* es una de las técnicas más comunes en ciberataques. | |
| Pregunta 9 | | **La infraestructura tecnológica de una empresa solo comprende computadoras.** | |
| Opción a) | Verdadero | |  |
| Opción b) | Falso | | X |
| Comentario respuesta correcta | | Correcto. Incluye *hardware, software*, redes, almacenamiento y procesos de gestión | |
| Comentario respuesta incorrecta | | Incorrecto. Comprende *hardware*, *software*, redes, almacenamiento y más. | |
| Pregunta 10 | | **El 5G y la inteligencia artificial son tendencias emergentes en tecnologías de la información en la actualidad.** | |
| Opción a) | Verdadero | | X |
| Opción b) | Falso | |  |
| Comentario respuesta correcta | | Correcto. Ambas figuran están entre las tendencias líderes para el entorno digital actual. | |
| Comentario respuesta incorrecta | | Incorrecto. Son tendencias clave para el futuro de las TI. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Pregunta 11** | | **Una adecuada gestión de incidentes implica solo identificar amenazas, sin necesidad de responder a ellas.** | |
| **Opción a)** | Verdadero | |  |
| **Opción b)** | Falso | | X |
| **Comentario respuesta correcta** | | Correcto. La gestión de incidentes incluye la identificación, respuesta y recuperación frente a amenazas | |
| **Comentario respuesta incorrecta** | | Incorrecto. Se requiere identificar, responder y recuperarse de incidentes. | |
| **Pregunta 12** | | **El SOC es responsable de monitorear y responder a incidentes de seguridad en tiempo real.** | |
| **Opción a)** | Verdadero | | X |
| **Opción b)** | Falso | |  |
| **Comentario respuesta correcta** | | Correcto. El Centro de Operaciones de Seguridad, se encarga del monitoreo y respuesta a incidentes en la organización. | |
| **Comentario respuesta incorrecta** | | Incorrecto. El SOC sí cumple esta función en la ciberseguridad organizacional. | |
| **Pregunta 13** | | **El análisis forense digital se limita a la recuperación de datos perdidos, sin investigar incidentes.** | |
| **Opción a)** | Verdadero | |  |
| **Opción b)** | Falso | | X |
| **Comentario respuesta correcta** | | Correcto. Abarca recuperación, investigación y análisis de incidentes de seguridad. | |
| **Comentario respuesta incorrecta** | | Incorrecto. El análisis forense también investiga e identifica evidencias e incidentes. | |
| **Pregunta 14** | | **El marco NIST y la norma ISO/IEC 27005 son herramientas para la gestión de riesgos en seguridad de la información.** | |
| **Opción a)** | Verdadero | | X |
| **Opción b)** | Falso | |  |
| **Comentario respuesta correcta** | | Correcto. Ambos son marcos de referencia ampliamente utilizados en gestión de riesgos | |
| **Comentario respuesta incorrecta** | | Incorrecto. Son estándares internacionales para la gestión de riesgos. | |
| **Pregunta 15** | | **La educación y capacitación en ciberseguridad no es necesaria para trabajar en el área.** | |
| **Opción a)** | Verdadero | |  |
| **Opción b)** | Falso | | X |
| **Comentario respuesta correcta** | | Correcto. Es esencial estar en constante capacitación y formación para adaptarse a las nuevas amenazas y tecnologías. | |
| **Comentario respuesta incorrecta** | | Incorrecto. La formación es clave para desempeñarse en ciberseguridad. | |
| **Pregunta 16** | | **Las certificaciones como CISSP o CEH ayudan a demostrar competencias en ciberseguridad.** | |
| **Opción a)** | Verdadero | | X |
| **Opción b)** | Falso | |  |
| **Comentario respuesta correcta** | | Correcto. Certificaciones internacionales validan conocimientos y habilidades profesionales. | |
| **Comentario respuesta incorrecta** | | Incorrecto. Estas certificaciones son reconocidas en el ámbito profesional. | |
| **Pregunta 17** | | **El análisis de evidencia digital debe cumplir con normativas legales específicas en cada país.** | |
| **Opción a)** | Verdadero | | X |
| **Opción b)** | Falso | |  |
| **Comentario respuesta correcta** | | Correcto. Es necesario cumplir la normativa local o internacional para validar la evidencia. | |
| **Comentario respuesta incorrecta** | | Incorrecto. El cumplimiento legal es obligatorio en el análisis forense. | |
| **Pregunta 18** | | **El *ransomware* es un tipo de *malware* que bloquea el acceso a los datos hasta que se paga un rescate.** | |
| **Opción a)** | Verdadero | | X |
| **Opción b)** | Falso | |  |
| **Comentario respuesta correcta** | | Correcto. Es una de las formas más comunes y peligrosas de cibercrimen hoy día. | |
| **Comentario respuesta incorrecta** | | Incorrecto. El *ransomware* funciona cifrando datos y pidiendo rescate por ellos. | |
| **Pregunta 19** | | **Solo las grandes empresas pueden ser víctimas de ciberataques.** | |
| **Opción a)** | Verdadero | |  |
| **Opción b)** | Falso | | X |
| **Comentario respuesta correcta** | | Correcto. Personas, pymes y grandes empresas pueden ser blanco de ataques cibernéticos. | |
| **Comentario respuesta incorrecta** | | Incorrecto. Todas las organizaciones y usuarios pueden ser víctimas. | |
| **Pregunta 20** | | **La gestión de riesgos de seguridad de la información ayuda a identificar, evaluar y tratar posibles amenazas.** | |
| **Opción a)** | Verdadero | | X |
| **Opción b)** | Falso | |  |
| **Comentario respuesta correcta** | | Correcto. Es un proceso central para prevenir daños en las organizaciones. | |
| **Comentario respuesta incorrecta** | | Incorrecto. Ayuda precisamente a identificar y gestionar amenazas a la información. | |

|  |  |
| --- | --- |
| MENSAJE FINAL ACTIVIDAD | |
| Mensaje cuando supera el 70 % de respuestas correctas | ¡Excelente! Felicitaciones, ha superado la actividad, demostrando sólidos conocimientos sobre el componente formativo. |
| Mensaje cuando el porcentaje de respuestas correctas es inferior al 70 % | No ha superado la actividad. Le recomendamos volver a revisar el componente formativo e intentar nuevamente la actividad didáctica. |

|  |  |  |
| --- | --- | --- |
| **CONTROL DE REVISIÓN** | | |
|  | **Responsable** | **Fecha** |
| **Revisión Experta temática** | **Javier Eduardo Díaz Machuca** | **Julio de 2025** |
| **Revisión Evaluador instruccional** | **Andrés Felipe Velandia Espitia** | **Agosto de 2025** |