|  |  |  |  |
| --- | --- | --- | --- |
| 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 **Ciberseguridad y gestión del riesgo organizacional.**  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 | | Desafío cibernético | |
| Objetivo de la actividad | | Evaluar y reforzar el conocimiento adquirido sobre la ciberseguridad y los delitos informáticos, con el fin de lograr ajustar los procesos organizacionales. | |
| 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 busca proteger la confidencialidad, integridad y disponibilidad de la información.** | Rta(s) correcta(s) (x) |
| Opción a) | Verdadero | | X |
| Opción b) | Falso | |  |
| Comentario respuesta correcta | | Correcto, estos son los pilares fundamentales de la ciberseguridad. | |
| Comentario respuesta incorrecta | | Incorrecto, la ciberseguridad se basa en asegurar confidencialidad, integridad y disponibilidad. | |
| Pregunta 2 | | **Un Centro de Operaciones de Seguridad (SOC) monitorea continuamente las redes para detectar amenazas.** | |
| Opción a) | Verdadero | | X |
| Opción b) | Falso | |  |
| Comentario respuesta correcta | | Correcto, el SOC realiza monitoreo 24/7 para proteger la infraestructura tecnológica. | |
| Comentario respuesta incorrecta | | Incorrecto, el SOC sí monitorea continuamente para detectar y responder a incidentes. | |
| Pregunta 3 | | **Las políticas de seguridad son documentos que establecen normas para proteger los activos de información.** | |
| Opción a) | Verdadero | | X |
| Opción b) | Falso | |  |
| Comentario respuesta correcta | | Correcto, las políticas oficializan las normas y responsabilidades en seguridad. | |
| Comentario respuesta incorrecta | | Incorrecto, las políticas definen formalmente las reglas para proteger información. | |
| Pregunta 4 | | **El NIST SP 800-61 es un marco internacional para la gestión de incidentes de ciberseguridad.** | |
| Opción a) | Verdadero | | X |
| Opción b) | Falso | |  |
| Comentario respuesta correcta | | Correcto, es uno de los marcos más reconocidos para la respuesta a incidentes. | |
| Comentario respuesta incorrecta | | Incorrecto, este es un estándar internacional para la gestión de incidentes. | |
| Pregunta 5 | | **La gestión de incidentes solo consiste en detectar ataques, sin importar la respuesta o mitigación.** | |
| Opción a) | Verdadero | |  |
| Opción b) | Falso | | X |
| Comentario respuesta correcta | | Correcto, la gestión de incidentes incluye detección, respuesta, mitigación y recuperación. | |
| Comentario respuesta incorrecta | | Incorrecto, la gestión cubre todo el ciclo de vida del incidente, no solo la detección. | |
| Pregunta 6 | | **La autenticación multifactor (MFA) es una medida que aumenta la seguridad en el acceso a sistemas.** | |
| Opción a) | Verdadero | | X |
| Opción b) | Falso | |  |
| Comentario respuesta correcta | | Correcto, MFA añade capas adicionales para verificar identidades. | |
| Comentario respuesta incorrecta | | Incorrecto, usar MFA es un método eficaz para mejorar la seguridad de accesos. | |
| Pregunta 7 | | **Los SOC solo funcionan durante horas laborales, no operan las 24 horas del día.** | |
| Opción a) | Verdadero | |  |
| Opción b) | Falso | | X |
| Comentario respuesta correcta | | Correcto, los SOC operan 24/7 para una vigilancia continua. | |
| Comentario respuesta incorrecta | | Incorrecto, la vigilancia continuada es esencial para detectar amenazas a cualquier hora. | |
| Pregunta 8 | | **ISO/IEC 27035 es una norma que guía la gestión de incidentes de seguridad de la información.** | |
| Opción a) | Verdadero | | X |
| Opción b) | Falso | |  |
| Comentario respuesta correcta | | Correcto, es un estándar internacional para la gestión de incidentes. | |
| Comentario respuesta incorrecta | | Incorrecto, esta norma realmente orienta sobre la gestión de incidentes. | |
| Pregunta 9 | | **El *phishing* es un tipo de ataque que busca engañar para obtener información confidencial.** | |
| Opción a) | Verdadero | | X |
| Opción b) | Falso | |  |
| Comentario respuesta correcta | | Correcto, el phishing busca engañar a usuarios para robar datos. | |
| Comentario respuesta incorrecta | | Incorrecto, el phishing es un ataque de ingeniería social para obtener información. | |
| Pregunta 10 | | **Las políticas de seguridad solo deben aplicarse al personal del área de tecnología.** | |
| Opción a) | Verdadero | |  |
| Opción b) | Falso | | X |
| Comentario respuesta correcta | | Correcto, la etapa de lecciones aprendidas es fundamental para prevenir futuros incidentes. | |
| Comentario respuesta incorrecta | | Incorrecto, la mejora continua es clave en la gestión de incidentes. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Pregunta 11** | | **Un buen programa antivirus puede proteger completamente contra todos los tipos de ataques cibernéticos.** | |
| **Opción a)** | Verdadero | |  |
| **Opción b)** | Falso | | X |
| **Comentario respuesta correcta** | | Correcto, el antivirus es una herramienta, pero no garantiza protección total. | |
| **Comentario respuesta incorrecta** | | Incorrecto, la seguridad debe ser integral y no depender solo de antivirus. | |
| **Pregunta 12** | | **La respuesta rápida y coordinada ante un incidente puede reducir el impacto en la organización.** | |
| **Opción a)** | Verdadero | | X |
| **Opción b)** | Falso | |  |
| **Comentario respuesta correcta** | | Correcto, actuar rápido limita daños y permite recuperación eficaz. | |
| **Comentario respuesta incorrecta** | | Incorrecto, la rapidez y coordinación son esenciales en la respuesta a incidentes. | |
| **Pregunta 13** | | **El SOC es responsable de monitorear solo los sistemas físicos, no los servicios en la nube.** | |
| **Opción a)** | Verdadero | |  |
| **Opción b)** | Falso | | X |
| **Comentario respuesta correcta** | | Correcto, el SOC también monitorea servicios en la nube y otros recursos digitales. | |
| **Comentario respuesta incorrecta** | | Incorrecto, el SOC cubre toda la infraestructura tecnológica, incluyendo nube. | |
| **Pregunta 14** | | **Las políticas de seguridad deben actualizarse regularmente para mantenerse efectivas.** | |
| **Opción a)** | Verdadero | | X |
| **Opción b)** | Falso | |  |
| **Comentario respuesta correcta** | | Correcto, los incidentes pueden ser causados también por errores humanos o fallas internas. | |
| **Comentario respuesta incorrecta** | | Incorrecto, no todos los incidentes tienen origen externo. | |
| **Pregunta 15** | | **La inteligencia artificial es una tendencia emergente que ayuda a mejorar la ciberseguridad.** | |
| **Opción a)** | Verdadero | | X |
| **Opción b)** | Falso | |  |
| **Comentario respuesta correcta** | | Correcto, la IA se usa para detección avanzada y respuesta automatizada. | |
| **Comentario respuesta incorrecta** | | Incorrecto, la IA es una herramienta emergente clave en ciberseguridad. | |
| **Pregunta 16** | | **Una política de seguridad debe definir claramente roles y responsabilidades.** | |
| **Opción a)** | Verdadero | | X |
| **Opción b)** | Falso | |  |
| **Comentario respuesta correcta** | | Correcto, para que las políticas se apliquen correctamente, se deben asignar responsabilidades. | |
| **Comentario respuesta incorrecta** | | Incorrecto, los roles bien definidos son esenciales para la eficacia de una política. | |
| **Pregunta 17** | | **No hay forma de protegerse contra los ataques de *ransomware* una vez que el *malware* ha cifrado los archivos.** | |
| **Opción a)** | Verdadero | |  |
| **Opción b)** | Falso | | X |
| **Comentario respuesta correcta** | | Correcto, las copias de seguridad y soluciones especializadas pueden ayudar a recuperarse sin pagar. | |
| **Comentario respuesta incorrecta** | | Incorrecto, aunque el *ransomware* haya cifrado los archivos, aún es posible recuperarse si se cuenta con copias de seguridad o se utilizan soluciones especializadas. | |
| **Pregunta 18** | | **Los dispositivos móviles no necesitan protección contra virus porque solo las computadoras son vulnerables.** | |
| **Opción a)** | Verdadero | |  |
| **Opción b)** | Falso | | X |
| **Comentario respuesta correcta** | | Correcto, los *smartphones* también pueden infectarse con *malware* o ser atacados. | |
| **Comentario respuesta incorrecta** | | Incorrecto, los dispositivos móviles sí pueden ser vulnerables. Al igual que las computadoras, los *smartphones* pueden infectarse con *malware* o sufrir ataques de seguridad. | |
| **Pregunta 19** | | **Hacer clic en enlaces desconocidos o sospechosos en redes sociales puede comprometer la seguridad de un dispositivo.** | |
| **Opción a)** | Verdadero | | X |
| **Opción b)** | Falso | |  |
| **Comentario respuesta correcta** | | Correcto, estos enlaces pueden llevar a sitios maliciosos o descargar *software* dañino. | |
| **Comentario respuesta incorrecta** | | Incorrecto, estos enlaces pueden dirigir a sitios maliciosos o descargar *software* dañino sin que el usuario lo note. | |
| **Pregunta 20** | | **Es seguro compartir la contraseña con un amigo si se confías en él completamente.** | |
| **Opción a)** | Verdadero | |  |
| **Opción b)** | Falso | | X |
| **Comentario respuesta correcta** | | Correcto, compartir contraseñas siempre representa un riesgo, sin importar la confianza. | |
| **Comentario respuesta incorrecta** | | Incorrecto, la seguridad digital se basa en mantener las credenciales de acceso personales y confidenciales. | |

|  |  |
| --- | --- |
| 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. Se recomienda 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 Evaluadora instruccional** | **Andrés Felipe Velandia Espitia** | **Julio de 2025** |