|  |  |  |  |
| --- | --- | --- | --- |
| 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* **Amenazas digitales, ingeniería social y ética 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 | | Descubre la verdad detrás de las amenazas y ataques de ciberseguridad. | |
| Objetivo de la actividad | | Evaluar y fortalecer la comprensión sobre las amenazas y ataques de ciberseguridad mediante la identificación de afirmaciones verdaderas y falsas, promoviendo el análisis crítico. | |
| 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 | | **Una amenaza informática es cualquier circunstancia o evento con el potencial de causar daño a un sistema, red o datos.** | Rta(s) correcta(s) (x) |
| Opción a) | Verdadero | | X |
| Opción b) | Falso | |  |
| Comentario respuesta correcta | | Excelente trabajo. Tiene un claro entendimiento sobre las amenazas y ataques de ciberseguridad. | |
| Comentario respuesta incorrecta | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| Pregunta 2 | | **Un ataque de *phishing* consiste en el uso de *software* malicioso para explotar vulnerabilidades en el sistema operativo.** | |
| Opción a) | Verdadero | |  |
| Opción b) | Falso | | X |
| Comentario respuesta correcta | | Excelente trabajo. Tiene un claro entendimiento sobre las amenazas y ataques de ciberseguridad. | |
| Comentario respuesta incorrecta | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| Pregunta 3 | | **Un ataque de denegación de servicio (DoS) busca hacer que un sistema o red sea inaccesible para los usuarios legítimos.** | |
| Opción a) | Verdadero | | X |
| Opción b) | Falso | |  |
| Comentario respuesta correcta | | Excelente trabajo. Tiene un claro entendimiento sobre las amenazas y ataques de ciberseguridad. | |
| Comentario respuesta incorrecta | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| Pregunta 4 | | **Un *ransomware* cifra los archivos de un sistema y exige un pago para recuperarlos.** | |
| Opción a) | Verdadero | | X |
| Opción b) | Falso | |  |
| Comentario respuesta correcta | | Excelente trabajo. Tiene un claro entendimiento sobre las amenazas y ataques de ciberseguridad. | |
| Comentario respuesta incorrecta | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| Pregunta 5 | | **El *malware* es cualquier tipo de *software* diseñado para dañar o explotar dispositivos, redes o datos.** | |
| Opción a) | Verdadero | | X |
| Opción b) | Falso | |  |
| Comentario respuesta correcta | | Excelente trabajo. Tiene un claro entendimiento sobre las amenazas y ataques de ciberseguridad. | |
| Comentario respuesta incorrecta | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| Pregunta 6 | | **Una vulnerabilidad es una debilidad en un sistema que puede ser explotada por un atacante.** | |
| Opción a) | Verdadero | | X |
| Opción b) | Falso | |  |
| Comentario respuesta correcta | | Excelente trabajo. Tiene un claro entendimiento sobre las amenazas y ataques de ciberseguridad. | |
| Comentario respuesta incorrecta | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| Pregunta 7 | | **Mantener el *software* actualizado ayuda a reducir el riesgo de explotación de vulnerabilidades.** | |
| Opción a) | Verdadero | | X |
| Opción b) | Falso | |  |
| Comentario respuesta correcta | | Excelente trabajo. Tiene un claro entendimiento sobre las amenazas y ataques de ciberseguridad. | |
| Comentario respuesta incorrecta | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| Pregunta 8 | | **Todas las vulnerabilidades son detectadas antes de que los atacantes puedan explotarlas.** | |
| Opción a) | Verdadero | |  |
| Opción b) | Falso | | X |
| Comentario respuesta correcta | | Excelente trabajo. Tiene un claro entendimiento sobre las amenazas y ataques de ciberseguridad. | |
| Comentario respuesta incorrecta | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| Pregunta 9 | | **Un sistema sin antivirus está completamente protegido si el *firewall* está activado.** | |
| Opción a) | Verdadero | |  |
| Opción b) | Falso | | X |
| Comentario respuesta correcta | | Excelente trabajo. Tiene un claro entendimiento sobre las amenazas y ataques de ciberseguridad. | |
| Comentario respuesta incorrecta | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| Pregunta 10 | | **La ingeniería social se basa en la manipulación psicológica para obtener información confidencial.** | |
| Opción a) | Verdadero | | X |
| Opción b) | Falso | |  |
| Comentario respuesta correcta | | Excelente trabajo. Tiene un claro entendimiento sobre las amenazas y ataques de ciberseguridad. | |
| Comentario respuesta incorrecta | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Pregunta 11** | | **Una contraseña segura evita completamente los ataques de ingeniería social.** | |
| **Opción a)** | Verdadero | |  |
| **Opción b)** | Falso | | X |
| **Comentario respuesta correcta** | | Excelente trabajo. Tiene un claro entendimiento sobre las amenazas y ataques de ciberseguridad. | |
| **Comentario respuesta incorrecta** | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| **Pregunta 12** | | **La mejor forma de prevenir ataques de ingeniería social es educar a los usuarios sobre posibles engaños.** | |
| **Opción a)** | Verdadero | | X |
| **Opción b)** | Falso | |  |
| **Comentario respuesta correcta** | | Excelente trabajo. Tiene un claro entendimiento sobre las amenazas y ataques de ciberseguridad. | |
| **Comentario respuesta incorrecta** | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| **Pregunta 13** | | **El *adware* es un tipo de *software* malicioso que muestra publicidad no deseada y, en algunos casos, puede recopilar información del usuario sin su consentimiento.** | |
| **Opción a)** | Verdadero | | X |
| **Opción b)** | Falso | |  |
| **Comentario respuesta correcta** | | Excelente trabajo. Tiene un claro entendimiento sobre las amenazas y ataques de ciberseguridad. | |
| **Comentario respuesta incorrecta** | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| **Pregunta 14** | | **Usar contraseñas largas y únicas en cada servicio en línea, reduce el riesgo de ataques de fuerza bruta.** | |
| **Opción a)** | Verdadero | | X |
| **Opción b)** | Falso | |  |
| **Comentario respuesta correcta** | | Excelente trabajo. Tiene un claro entendimiento sobre las amenazas y ataques de ciberseguridad. | |
| **Comentario respuesta incorrecta** | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| **Pregunta 15** | | **La autenticación de dos factores (2FA) proporciona una capa adicional de seguridad a las cuentas.** | |
| **Opción a)** | Verdadero | | X |
| **Opción b)** | Falso | |  |
| **Comentario respuesta correcta** | | Excelente trabajo. Tiene un claro entendimiento sobre las amenazas y ataques de ciberseguridad. | |
| **Comentario respuesta incorrecta** | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| **Pregunta 16** | | **Un *firewall* protege contra todos los tipos de ataques cibernéticos.** | |
| **Opción a)** | Verdadero | |  |
| **Opción b)** | Falso | | X |
| **Comentario respuesta correcta** | | Excelente trabajo. Tiene un claro entendimiento sobre las amenazas y ataques de ciberseguridad. | |
| **Comentario respuesta incorrecta** | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| **Pregunta 17** | | **Es seguro hacer clic en enlaces de correos electrónicos si provienen de una fuente conocida.** | |
| **Opción a)** | Verdadero | |  |
| **Opción b)** | Falso | | X |
| **Comentario respuesta correcta** | | Excelente trabajo. Tiene un claro entendimiento sobre las amenazas y ataques de ciberseguridad. | |
| **Comentario respuesta incorrecta** | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| **Pregunta 18** | | **La ética en ciberseguridad implica proteger la privacidad y los datos de las personas de manera responsable.** | |
| **Opción a)** | Verdadero | | X |
| **Opción b)** | Falso | |  |
| **Comentario respuesta correcta** | | Excelente trabajo. Tiene un claro entendimiento sobre las amenazas y ataques de ciberseguridad. | |
| **Comentario respuesta incorrecta** | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| **Pregunta 19** | | **Es aceptable *hackear* un sistema sin autorización si se hace con buenas intenciones.** | |
| **Opción a)** | Verdadero | |  |
| **Opción b)** | Falso | | X |
| **Comentario respuesta correcta** | | Excelente trabajo. Tiene un claro entendimiento sobre las amenazas y ataques de ciberseguridad. | |
| **Comentario respuesta incorrecta** | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| **Pregunta 20** | | **Los reportes de ciberseguridad deben ser detallados y contener información sobre la amenaza, su impacto y posibles soluciones.** | |
| **Opción a)** | Verdadero | | X |
| **Opción b)** | Falso | |  |
| **Comentario respuesta correcta** | | Excelente trabajo. Tiene un claro entendimiento sobre las amenazas y ataques de ciberseguridad. | |
| **Comentario respuesta incorrecta** | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |

|  |  |
| --- | --- |
| MENSAJE FINAL ACTIVIDAD | |
| Mensaje cuando supera el 70 % de respuestas correctas | ¡Excelente! Felicitaciones, ha superado la actividad y demuestra 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 Experto temático** | **Javier Eduardo Díaz Machuca** | **Marzo de 2025** |
| **Revisión Evaluadora instruccional** | **Viviana Herrera Quiñonez** | **Abril de 2025** |