|  |  |  |  |
| --- | --- | --- | --- |
| 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 Fundamentos del ciberespacio, la ciberseguridad y los delitos informáticos.*  *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* | |
| 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 | | **El *phishing* es una técnica de ataque que consiste en engañar a las personas para que revelen información personal mediante correos electrónicos o sitios *web* falsos.** | Rta(s) correcta(s) (x) |
| Opción a) | Verdadero | | X |
| Opción b) | Falso | |  |
| Comentario respuesta correcta | | Excelente trabajo. El *phishing* es una técnica comúnmente utilizada para robar información personal. | |
| Comentario respuesta incorrecta | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| Pregunta 2 | | **El *software* antivirus debe ser desinstalado después de realizar un escaneo completo en el equipo.** | |
| Opción a) | Verdadero | |  |
| Opción b) | Falso | | X |
| Comentario respuesta correcta | | Excelente trabajo. El *software* antivirus debe mantenerse instalado y actualizado para proteger el equipo de amenazas continuas. | |
| Comentario respuesta incorrecta | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| Pregunta 3 | | **La ciberseguridad solo se refiere a la protección de los sistemas informáticos de las grandes empresas.** | |
| Opción a) | Verdadero | |  |
| Opción b) | Falso | | X |
| Comentario respuesta correcta | | Excelente trabajo. La ciberseguridad es importante tanto para individuos como para empresas. | |
| Comentario respuesta incorrecta | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| Pregunta 4 | | **El “*ransomware*” es un tipo de virus que permite a los hackers acceder a tus archivos y robar información personal.** | |
| Opción a) | Verdadero | |  |
| Opción b) | Falso | | X |
| Comentario respuesta correcta | | Excelente trabajo. El *ransomware* cifra los archivos de la víctima y exige un rescate para su desbloqueo. | |
| Comentario respuesta incorrecta | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| Pregunta 5 | | **El uso de contraseñas fuertes es una buena práctica para mejorar la ciberseguridad personal.** | |
| Opción a) | Verdadero | | X |
| Opción b) | Falso | |  |
| Comentario respuesta correcta | | Excelente trabajo. Las contraseñas fuertes protegen mejor las cuentas y sistemas personales. | |
| Comentario respuesta incorrecta | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| Pregunta 6 | | **El derecho a la privacidad en Internet no está protegido por ninguna ley internacional.** | |
| Opción a) | Verdadero | |  |
| Opción b) | Falso | | X |
| Comentario respuesta correcta | | Excelente trabajo. El derecho a la privacidad en Internet sí está protegido por leyes internacionales. | |
| Comentario respuesta incorrecta | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| Pregunta 7 | | **El fraude electrónico se refiere a la manipulación ilegal de información o transacciones a través de internet para obtener beneficios económicos.** | |
| Opción a) | Verdadero | | X |
| Opción b) | Falso | |  |
| Comentario respuesta correcta | | Excelente trabajo. El fraude electrónico incluye el uso ilícito de la tecnología para cometer fraudes financieros. | |
| Comentario respuesta incorrecta | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| Pregunta 8 | | **El *hacking* ético es la práctica de realizar pruebas de seguridad en sistemas con el permiso de los propietarios, con el objetivo de identificar y corregir vulnerabilidades.** | |
| Opción a) | Verdadero | | X |
| Opción b) | Falso | |  |
| Comentario respuesta correcta | | Excelente trabajo. El *hacking* ético tiene como objetivo mejorar la seguridad al encontrar vulnerabilidades. | |
| Comentario respuesta incorrecta | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| Pregunta 9 | | **Una persona recibe un correo electrónico aparentemente de su banco pidiéndole que actualice su contraseña haciendo clic en un enlace. Ingresa sus datos y luego descubre movimientos sospechosos en su cuenta. Este es un ejemplo de *phishing*.** | |
| Opción a) | Verdadero | | X |
| Opción b) | Falso | |  |
| Comentario respuesta correcta | | Excelente trabajo. Esto es un ejemplo típico de *phishing*, un delito informático común. | |
| Comentario respuesta incorrecta | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| Pregunta 10 | | **Instalar una aplicación en el celular que promete funciones útiles, pero sin revisar los permisos que solicita no representa ningún riesgo.** | |
| Opción a) | Verdadero | |  |
| Opción b) | Falso | | X |
| Comentario respuesta correcta | | Excelente trabajo. Algunas *apps* pueden robar información personal o espiar al usuario, lo que es una forma de delito informático. | |
| Comentario respuesta incorrecta | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Pregunta 11** | | **Publicar fotos comprometedoras de otra persona sin su consentimiento puede ser considerado un delito informático.** | |
| **Opción a)** | Verdadero | | X |
| **Opción b)** | Falso | |  |
| **Comentario respuesta correcta** | | Excelente trabajo. Difundir contenido íntimo sin autorización, especialmente en medios digitales, puede constituir un delito, como la violación de la privacidad. | |
| **Comentario respuesta incorrecta** | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| **Pregunta 12** | | **Utilizar la misma contraseña para todas tus cuentas en línea es una práctica segura si nadie más la conoce.** | |
| **Opción a)** | Verdadero | |  |
| **Opción b)** | Falso | | X |
| **Comentario respuesta correcta** | | Excelente trabajo. Reutilizar contraseñas aumenta el riesgo en caso de una filtración. | |
| **Comentario respuesta incorrecta** | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| **Pregunta 13** | | **El uso de la autenticación de dos factores (2FA) mejora significativamente la seguridad de una cuenta.** | |
| **Opción a)** | Verdadero | | X |
| **Opción b)** | Falso | |  |
| **Comentario respuesta correcta** | | Excelente trabajo. 2FA añade una capa adicional de protección, incluso si la contraseña es robada. | |
| **Comentario respuesta incorrecta** | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| **Pregunta 14** | | **Es seguro conectarse a redes Wi-Fi públicas para hacer transacciones bancarias, siempre que se use el navegador en modo incógnito.** | |
| **Opción a)** | Verdadero | |  |
| **Opción b)** | Falso | | X |
| **Comentario respuesta correcta** | | Excelente trabajo. Las redes públicas pueden ser peligrosas, y el modo incógnito no protege la conexión. | |
| **Comentario respuesta incorrecta** | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| **Pregunta 15** | | **Los ataques de ingeniería social explotan la confianza o desconocimiento de las personas, no las fallas técnicas.** | |
| **Opción a)** | Verdadero | | X |
| **Opción b)** | Falso | |  |
| **Comentario respuesta correcta** | | Excelente trabajo. Se basan en manipulación psicológica para obtener acceso o información. | |
| **Comentario respuesta incorrecta** | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| **Pregunta 16** | | **Actualizar frecuentemente el sistema operativo y las aplicaciones ayuda a protegerse contra vulnerabilidades.** | |
| **Opción a)** | Verdadero | | X |
| **Opción b)** | Falso | |  |
| **Comentario respuesta correcta** | | Excelente trabajo. Las actualizaciones suelen corregir fallas de seguridad explotadas por atacantes. | |
| **Comentario respuesta incorrecta** | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| **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** | | Excelente trabajo. Las copias de seguridad y soluciones especializadas pueden ayudar a recuperarse sin pagar. | |
| **Comentario respuesta incorrecta** | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
|  | |  | |
| **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** | | Excelente trabajo. Los *smartphones* también pueden infectarse con *malware* o ser atacados. | |
| **Comentario respuesta incorrecta** | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| **Pregunta 19** | | **Hacer clic en enlaces desconocidos o sospechosos en redes sociales puede comprometer la seguridad de tu dispositivo.** | |
| **Opción a)** | Verdadero | | X |
| **Opción b)** | Falso | |  |
| **Comentario respuesta correcta** | | Excelente trabajo. Estos enlaces pueden llevar a sitios maliciosos o descargar *software* dañino. | |
| **Comentario respuesta incorrecta** | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |
| **Pregunta 20** | | **Es seguro compartir tu contraseña con un amigo si confías en él completamente.** | |
| **Opción a)** | Verdadero | |  |
| **Opción b)** | Falso | | X |
| **Comentario respuesta correcta** | | Excelente trabajo. Compartir contraseñas siempre representa un riesgo, sin importar la confianza. | |
| **Comentario respuesta incorrecta** | | Respuesta incorrecta, revise nuevamente el contenido del componente formativo. | |

|  |  |
| --- | --- |
| MENSAJE FINAL ACTIVIDAD | |
| Mensaje cuando supera el 70 % de respuestas correctas | ¡Excelente! Lo felicito, 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** |