Rúbrica Analítica para Evaluar Seguridad Digital y Protección de Datos

Rúbrica Analítica | Tecnología e Informática | Informática | 4 niveles

Descripción

Esta rúbrica está diseñada para evaluar el conocimiento y aplicación de prácticas de seguridad digital y protección de datos en estudiantes de educación media (15-17 años). Cada criterio se evalúa de forma individual para identificar fortalezas y áreas de mejora.

Rúbrica

Rúbrica Analítica para Evaluar Seguridad Digital y Protección de Datos

Esta rúbrica está diseñada para evaluar el conocimiento y aplicación de prácticas de seguridad digital y protección de datos en estudiantes de educación media (15-17 años). Cada criterio se evalúa de forma individual para identificar fortalezas y áreas de mejora.

Criterios	Excelente (4 puntos)	Bueno (3 puntos)	Aceptable (2 puntos)	Bajo (1 punto)
Comprensión de conceptos básicos de seguridad digital	Demuestra un dominio completo y preciso de los conceptos clave de seguridad digital.	Comprende correctamente la mayoría de los conceptos básicos con pocas imprecisiones.	Entiende algunos conceptos pero presenta confusiones importantes.	No comprende los conceptos básicos o muestra información errónea.
Aplicación de contraseñas seguras	Utiliza contraseñas complejas, únicas y maneja su almacenamiento de forma segura.	Usa contraseñas seguras pero con cierta repetición o almacenamiento poco adecuado.	Emplea contraseñas poco seguras o repetidas con manejo inconsistente.	No utiliza contraseñas seguras ni sigue buenas prácticas para su manejo.
Manejo adecuado de datos personales en línea	Protege rigurosamente sus datos personales y evita compartir información innecesaria.	Generalmente cuida sus datos personales, aunque a veces comparte información no esencial.	Comparte datos personales de forma poco cuidadosa o sin considerar riesgos.	No protege sus datos personales y los expone sin precaución.

Criterios	Excelente (4 puntos)	Bueno (3 puntos)	Aceptable (2 puntos)	Bajo (1 punto)
Identificación y prevención de amenazas digitales	Reconoce claramente diferentes tipos de amenazas y aplica medidas efectivas para evitarlas.	Identifica amenazas comunes y toma algunas precauciones adecuadas.	Reconoce pocas amenazas y sus acciones preventivas son limitadas o ineficaces.	No identifica amenazas digitales ni toma medidas preventivas.
Uso responsable de redes sociales y privacidad	Administra configuración de privacidad y contenido compartido con pleno control y responsabilidad.	Configura privacidad adecuadamente con algunas omisiones en el contenido compartido.	Usa redes sociales sin configurar privacidad correctamente y comparte contenido inapropiado.	No controla la privacidad ni el contenido compartido en redes sociales.
Reconocimiento y respuesta ante intentos de phishing o fraude digital	Detecta con precisión mensajes sospechosos y sabe cómo responder correctamente.	Identifica la mayoría de intentos de phishing, pero puede dudar en la respuesta adecuada.	Reconoce algunos casos de phishing, pero su respuesta es inadecuada o incierta.	No reconoce ni actúa frente a intentos de phishing o fraude digital.
Actualización y mantenimiento de software de seguridad	Mantiene actualizado todo software de seguridad y realiza mantenimiento preventivo regularmente.	Actualiza software de seguridad con frecuencia, pero ocasionalmente omite algún mantenimiento.	Actualiza software solo cuando hay problemas o no mantiene adecuadamente la seguridad.	No actualiza ni mantiene software de seguridad, exponiéndose a riesgos.
Capacidad para explicar y justificar prácticas seguras	Explica con claridad y fundamento las razones de sus prácticas seguras y su importancia.	Justifica la mayoría de sus prácticas con explicaciones claras aunque simples.	Ofrece explicaciones poco claras o incompletas sobre sus prácticas de seguridad.	No puede explicar ni justificar sus prácticas relacionadas con la seguridad digital.