INSTRUMENTO DE EVALUACIÓN - CIBERSEGURIDAD

Datos Generales

Programa: Tratamiento de Riesgos de Ciberseguridad

Caso Práctico: Ataque de Ransomware

🎓 **Programa:**

Tratamiento de Riesgos de Ciberseguridad

🎯 **Resultado de Aprendizaje:**

Analizar incidentes de ciberseguridad, identificar amenazas, vulnerabilidades y proponer soluciones efectivas.

📋 **CRITERIOS Y NIVELES DE DESEMPEÑO**

CRITERIO	🌟 SUPERIOR (4.6–5.0)	✅ ALTO (4.0–4.5)	⚠️ BÁSICO (3.0–3.9)	❌ BAJO (0–2.9)
Identificación del ataque	Identifica correctamente el ransomware y lo explica con claridad	Identifica el ataque pero con poca explicación	Presenta confusión en el tipo de ataque	No identifica el ataque
Análisis de la amenaza	Describe claramente el malware y su funcionamiento	Describe la amenaza de forma general	Presenta descripción incompleta	No reconoce la amenaza
Identificación de vulnerabilidad	Explica claramente la causa (error humano, correo)	Identifica la vulnerabilidad parcialmente	Presenta dificultad para identificarla	No identifica vulnerabilidad
Análisis de riesgos	Analiza impactos técnicos, económicos y operativos	Identifica algunos riesgos	Menciona riesgos de forma superficial	No identifica riesgos
Propuesta de soluciones	Propone soluciones claras, viables y	Propone soluciones básicas	Propone pocas o poco claras	No propone soluciones

	completas			
Argumentación	Respuestas claras, coherentes y bien estructuradas	Presenta coherencia con leves errores	Presenta desorden en ideas	No hay coherencia
Reflexión crítica	Reflexiona con profundidad y sentido crítico	Reflexión adecuada	Reflexión básica	No reflexiona

Observaciones

Espacio para comentarios del instructor.