INSTRUMENTO DE EVALUACION SOLUCION DE PREGUNTAS

CRITERIO	**DESCRIPCIÓN**	**PUNTAJE**
Concepto de ciberseguridad	Define correctamente el concepto	5
Identificación de riesgos	Propone acciones frente a riesgos	5
Factor humano	Explica su importancia	5
Errores humanos	Identifica mínimo dos correctamente	5
Verdadero/Falso	Responde correctamente	5
Análisis institucional	Argumenta consecuencias claras	15

INSTRUMENTO DE EVALUACIÓN - CASO PRÁCTICO RANSOMWARE

Programa
Tratamiento de Riesgos de Ciberseguridad

Caso
Ataque de Ransomware en Tecnored S.A.S.

Resultado de Aprendizaje
Analizar incidentes de ciberseguridad, identificar amenazas, vulnerabilidades y proponer medidas de mitigación.

Criterios de Evaluación (100 puntos)

Criterio	Descripción	Puntaje
Identificación del ataque	Reconoce correctamente el ransomware	15
Análisis de amenaza	Describe la amenaza correctamente	15
Identificación de vulnerabilidad	Explica la causa del incidente	15
Análisis de riesgos	Identifica impactos y riesgos	15
Propuesta de soluciones	Plantea medidas preventivas	20
Argumentación	Claridad y coherencia en respuestas	10
Reflexión	Análisis crítico del caso	10

Lista de Chequeo

Nombre del aprendiz: _____

Fecha: _____

✅ CRITERIOS DE EVALUACIÓN

ÍTEM	CRITERIO A EVALUAR	CUMPLE ✔	NO CUMPLE ✖	OBSERVACIONES
1	Identifica correctamente el tipo de ataque (ransomware)	☐	☐	
2	Reconoce la amenaza (malware)	☐	☐	
3	Identifica la vulnerabilidad (error humano / correo)	☐	☐	
4	Analiza los riesgos (pérdida de información, impacto)	☐	☐	
5	Describe las consecuencias del ataque	☐	☐	
6	Propone medidas de prevención (ej. capacitación, antivirus)	☐	☐	
7	Propone soluciones ante el incidente	☐	☐	
8	Aplica conceptos de ciberseguridad correctamente	☐	☐	
9	Argumenta de forma clara y coherente	☐	☐	
10	Realiza reflexión crítica del caso	☐	☐	

📊 VALORACIÓN

- ✔ Cumple (1 punto por ítem)
- ✖ No cumple (0 puntos)

📌 **Puntaje total:** _____ / 10

📄 **INTERPRETACIÓN**

- 9 – 10 → 🌟 Superior
- 7 – 8 → ✅ Alto
- 5 – 6 → ⚠️ Básico
- 0 – 4 → ❌ Bajo

📝 **OBSERVACIONES DEL INSTRUCTOR**
