

Lista de cotejo para la presentación de los equipos

Sesión: "Ciberdetectives de Javier Heraud" | **Fases:** Controlar y Evaluar | I.E. Javier Heraud, San Juan de Miraflores

Datos de la evaluación

Equipo	_____
Caso analizado	☐ Caso 1: La cuenta de Camila ☐ Caso 2: El premio de Yape ☐ Caso 3: La memoria USB ☐ Caso 4: Archivos secuestrados
Grado y sección	5.º _____
Fecha	____ / ____ / 2026
Evaluador	☐ Equipo (autoverificación) ☐ Otro equipo (coevaluación) ☐ Docente

Indicación: marca **Sí** si el indicador se cumple y **No** si aún falta mejorar. Cada "Sí" vale 1 punto.

1. Carátula

N.º	Indicador	Sí	No
1	Incluye el nombre de la I.E., el grado y la sección	☐	☐
2	Muestra el título del trabajo y el nombre del equipo	☐	☐
3	Escribe los nombres de todos los integrantes y la fecha	☐	☐
4	El diseño es limpio y legible (colores, letra y una imagen alusiva a ciberseguridad)	☐	☐

Subtotal: ____ / 4

2. Organización del grupo

N.º	Indicador	Sí	No
5	Presenta los roles (coordinador, investigador, diseñador, redactor) con el nombre de cada responsable	☐	☐
6	Explica qué tarea realizó cada integrante	☐	☐
7	Muestra el plan de trabajo o el cronograma que siguió el equipo	☐	☐
8	Todos los integrantes participan en la exposición	☐	☐

Subtotal: ____ / 4

3. Análisis del caso

Criterio de evaluación: reconoce los tipos de malware y sus formas de propagación.

N.º	Indicador	Sí	No
9	Resume el caso con sus palabras (qué pasó, a quién y dónde)	☐	☐
10	Identifica correctamente la amenaza (malware, phishing, acceso no autorizado o ransomware)	☐	☐
11	Explica cómo llegó la amenaza (USB, correo, enlace, contraseña débil, sesión abierta)	☐	☐
12	Reconoce el tipo de malware y su forma de propagación, cuando el caso lo requiere	☐	☐
13	Señala qué se puso en riesgo (equipos, red, datos o personas)	☐	☐
14	Indica los errores o señales de alerta que aparecen en el caso	☐	☐

Subtotal: ____ / 6

4. Desarrollo de las preguntas

Criterio de evaluación: identifica señales de phishing y describe los riesgos de los accesos no autorizados.

N.º	Indicador	Sí	No
15	Responde todas las preguntas de análisis del caso	☐	☐
16	Sus respuestas son correctas y coherentes con el caso	☐	☐
17	Sustenta sus respuestas con datos o ejemplos del texto	☐	☐
18	Identifica señales de phishing o describe los riesgos del acceso no autorizado	☐	☐
19	Propone medidas de prevención realistas (copias de seguridad, antivirus, contraseñas distintas, verificación en dos pasos, no abrir enlaces dudosos)	☐	☐
20	Indica qué hacer si ocurre la amenaza (desconectar el equipo, cambiar contraseñas, reportar)	☐	☐

Subtotal: ____ / 6

5. Exposición (aspectos generales)

N.º	Indicador	Sí	No
21	Se expresa con claridad y volumen adecuado	☐	☐

N.º	Indicador	Sí	No
22	Usa un lenguaje sencillo y los términos técnicos correctos	☐	☐
23	Respeto el tiempo asignado (3 min por equipo)	☐	☐
24	Responde con seguridad las preguntas del público	☐	☐

Subtotal: ____ / 4

Resumen de resultados

Sección	Puntaje obtenido	Puntaje máximo
1. Carátula		4
2. Organización del grupo		4
3. Análisis del caso		6
4. Desarrollo de las preguntas		6
5. Exposición		4
Total		24

Escala de valoración

Puntaje	Nivel de logro
21 a 24	Logro destacado (AD)
17 a 20	Logro esperado (A)
12 a 16	En proceso (B)
0 a 11	En inicio (C)

Retroalimentación

Aciertos del equipo (2):

1.

2.

Aspecto por mejorar (1):

1.

Observaciones del docente: _____

Notas para el uso docente

- Las secciones 3 y 4 miden directamente los dos criterios de evaluación de la sesión, por eso conviene que el docente les preste más atención.
- La lista tiene 24 indicadores y la exposición dura 3 minutos por equipo; para la coevaluación, cada equipo puede revisar solo las secciones 3 y 4 (12 indicadores) y dejar las demás para el docente.
- La escala de 24 puntos se adapta a los niveles del Currículo Nacional (AD, A, B, C), pero los rangos son sugeridos: ajústalos a lo que indique tu institución.