

VISTA PREVIA · DATOS FICTICIOS

Informe técnico

Prueba de intrusión interna

Cliente Ejemplo, S.A. (cliente ficticio)

Cliente / Organización	Cliente Ejemplo, S.A. (ficticio)
Evaluación	Prueba de intrusión interna
Periodo de ejecución	1 al 19 de septiembre de 2026 (fechas de ejemplo)
Versión	Muestra 1.0
Elaborado por	SoluProTec
Fecha de emisión	12 de octubre de 2026

CONFIDENCIAL. Un informe real lleva este aviso en la portada y se distribuye de forma restringida. Esta vista previa es pública y **todos sus datos son ficticios**: ningún cliente, activo, dirección ni resultado es real.

Acerca de esta muestra

Esta vista previa reúne 6 de las 25 páginas del informe técnico de muestra de SoluProTec, con datos inventados: la portada, estas aclaraciones, el resumen ejecutivo con la cadena de ataque y un hallazgo completo. Muestra cómo presentamos lo que se encontró, qué tan grave es y qué hacer primero.

Qué es ficticio

Todo. El cliente, las personas y los cargos, los nombres de equipos y dominios (.test), las direcciones IP (rangos de documentación 192.0.2.0/24 , 198.51.100.0/24 y 203.0.113.0/24 , reservados para ejemplos), las fechas, las cifras y los hallazgos. Las puntuaciones CVSS sí se calculan con la fórmula oficial a partir de cada vector.

Qué cambia en un informe real

- Es una versión condensada: un informe real incluye el inventario completo de activos, la evidencia (capturas y salidas) en anexos y más hallazgos.
- Los secretos (contraseñas, hashes, tokens) siguen apareciendo redactados, salvo que el cliente pida otra cosa por escrito.
- El cierre incluye una reunión de resultados y, si se contrata, la validación de las correcciones.

¿Quieres un informe como este para tu organización? Escríbenos a info@soluprotec.org y cuéntanos qué quieres proteger.

Control del documento

Esta copia	Vista previa pública: 6 de las 25 páginas del informe de muestra
Versión	Muestra 1.0
Fecha	12 de octubre de 2026
Estado	Final (muestra)
Revisión de calidad (QA / peer review)	Realizada por un segundo evaluador antes de la emisión (en un informe real)
Distribución	Dirección general, dirección de TI y responsable de seguridad de Cliente Ejemplo, S.A. (cargos ficticios)

1 Resumen ejecutivo

1.1 Visión general

SoluProTec realizó una prueba de intrusión interna a Cliente Ejemplo, S.A. entre el 1 y el 19 de septiembre de 2026 (fechas de ejemplo). La prueba partió de un puesto de usuario conectado a la red corporativa y sin credenciales, y buscó responder una pregunta: **¿qué lograría alguien que consiga ese primer punto de apoyo?** Por ejemplo, llegar a información crítica, tomar el control de la identidad corporativa o impedir la recuperación tras un incidente.

Se identificaron **6 hallazgos**: 1 crítico, 3 altos, 1 medio y 1 bajo. Tres de ellos (H-03, H-02 y H-01) forman una cadena: desde un puesto sin credenciales se obtuvo una cuenta de dominio, luego una cuenta con privilegios de administración sobre servidores y, además, acceso a la consola de respaldos. **El nivel de riesgo global es ALTO.**

También se verificaron controles que funcionan bien (sección 5.4 del informe completo): la VPN exige autenticación multifactor, la detección en estaciones de trabajo reaccionó ante herramientas ofensivas y la red de invitados está aislada.

1.2 Distribución por severidad

La severidad se deriva estrictamente de la puntuación base CVSS v3.1 de cada hallazgo (sección 4 del informe completo).

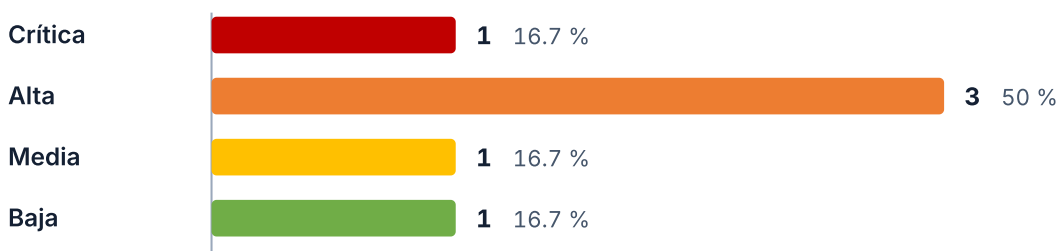


Figura 1. Hallazgos por severidad (total: 6).

Severidad	Cantidad	%	Lectura ejecutiva	Prioridad
Crítica	1	16.7 %	Compromete sistemas críticos sin esfuerzo técnico relevante. Corregir de inmediato.	P0
Alta	3	50 %	Permite escalar privilegios o acceder a información sensible con pocas condiciones previas.	P1
Media	1	16.7 %	Requiere condiciones adicionales para aprovecharse; debilita la postura general.	P2
Baja	1	16.7 %	Impacto limitado; mejora de higiene y de defensa en profundidad.	P3
Total	6	100 %		

1.3 Cadena de ataque principal

Los hallazgos no son aislados: **H-03** entrega la primera cuenta de dominio, **H-02** la convierte en control administrativo de servidores y **H-01** deja sin recuperación posible a la organización. **H-01** además se alcanza directamente desde la red de usuarios, sin pasar por los otros dos.

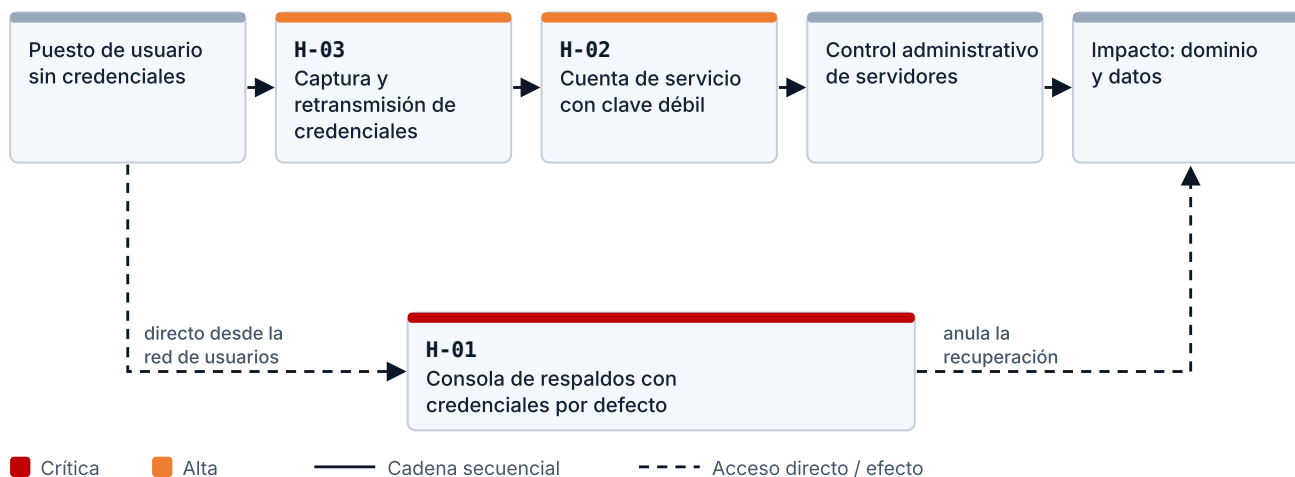


Figura 2. Cadena de ataque principal. El color superior de cada recuadro indica la severidad.

1.4 Indicadores positivos identificados

Control	Qué se verificó
VPN con MFA obligatorio	No fue posible eludirlo con las técnicas autorizadas.
Detección en estaciones de trabajo (EDR)	Detectó y alertó 2 de 3 intentos de ejecución de herramientas ofensivas habituales.
Aislamiento de la red de invitados	Sin ruta hacia la red corporativa desde la Wi-Fi de invitados.

1.5 Mensaje para la dirección

El riesgo no está en el perímetro, que resistió, sino en la red interna: protocolos heredados, cuentas de servicio con contraseñas débiles y una consola de respaldos sin protección. Son problemas conocidos y de solución acotada.

Tres acciones concentran la mayor reducción de riesgo y pueden completarse en 15 días: cambiar las credenciales de la consola de respaldos y restringir su acceso (**H-01**); deshabilitar LLMNR/NBT-NS y exigir la firma SMB (**H-03**); y rotar la contraseña de la cuenta de servicio y quitarle privilegios (**H-02**). Con ellas, la cadena principal deja de ser posible.

Un hallazgo completo

De los 6 hallazgos del informe de muestra, esta es la ficha del de mayor severidad (H-01), tal como se entrega: datos de riesgo, cadena de ataque, descripción, justificación, contramedidas, referencias, pasos para reproducirlo y evidencia.

H-01 Consola de respaldos accesible con credenciales por defecto

Calificación de riesgo	Crítica Crítica · P0
Estado	Abierto — respuesta inmediata requerida
CVSS v3.1 base / vector	9.8 — CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE / MITRE ATT&CK	CWE-1392: Uso de credenciales por defecto · MITRE ATT&CK T1078.001
Herramientas utilizadas	Nmap; navegador web (validación manual)
Categoría	Credenciales por defecto
Activos afectados	bkp01 · 198.51.100.20 · 8443/tcp (consola web de administración de respaldos)
Identificado por / método	Enumeración de consolas web en el segmento de servidores y validación manual del acceso.

Continuidad y cadena de ataque

- **Vulnerabilidad precursora (origen):** Ninguna. Es un vector independiente: solo requiere conectividad de red hasta la consola.
- **Vulnerabilidad secuencial (impacto continuo):** Permite borrar o alterar copias de seguridad y sus políticas de retención, y copiar los datos respaldados de todos los sistemas.
- **Vector de conexión:** Último eslabón de la cadena de impacto: sin respaldos íntegros, un incidente de ransomware no se puede recuperar. Se alcanza directamente desde la red de usuarios y también desde el control de servidores obtenido con H-02.

Descripción de la vulnerabilidad

La consola web del sistema de respaldos aceptó la cuenta de administrador con la credencial de fábrica que el fabricante publica en su documentación (no se reproduce aquí). Con esa sesión se listaron los trabajos, los repositorios y las políticas de retención. No se modificó, descargó ni eliminó ningún respaldo: la validación se limitó a lectura. La consola es accesible desde la red de usuarios porque no hay filtrado entre ese segmento y la red de servidores para este puerto.

Justificación de riesgo

Confidencialidad, integridad y disponibilidad: impacto alto. Quien llegue a la consola puede eliminar o cifrar los repositorios y las políticas de retención, o copiar de una vez los datos respaldados de todos los sistemas. Es el hallazgo de mayor prioridad porque su aprovechamiento no requiere conocimientos técnicos y anula la capacidad de recuperación de la organización.

Contramedidas y mitigación (paso a paso)

1. Cambiar de inmediato la credencial por defecto y rotar las demás credenciales de la consola (cuentas locales, de servicio y de integración).
2. Restringir el acceso a la consola a una red de administración y a un bastión, con lista de direcciones permitidas.
3. Administrar los respaldos con cuentas nominales y autenticación multifactor (MFA); deshabilitar la cuenta genérica.
4. Activar repositorios inmutables y una copia fuera de línea o en otro dominio de identidad, para que una cuenta comprometida no pueda borrar todos los puntos de recuperación.
5. Registrar los inicios de sesión y los cambios de retención, y alertar ante cualquier acceso administrativo fuera de la ventana habitual.

Referencias externas

- **CWE-1392** · <https://cwe.mitre.org/data/definitions/1392.html>
- **MITRE ATT&CK T1078.001** · <https://attack.mitre.org/techniques/T1078/001/>
- Guía de endurecimiento del fabricante del sistema de respaldos.

Prueba de concepto (PoC) y pasos para reproducir

```
$ nmap -sV -p 8443 198.51.100.20
8443/tcp open  ssl/https  (consola web de administración de respaldos)
```

Validación manual (solo lectura):

1. Inicio de sesión en <https://bkp01.corp.ejemplo.test:8443> con el usuario de fábrica y su credencial por defecto [REDACTADA].
2. Resultado: sesión de administrador válida.
3. Acciones realizadas: listar trabajos y repositorios. Ninguna modificación.

Resumen de lo que se hizo, sin secretos. Los comandos y las salidas completas van en el anexo de evidencia de un informe real.

Evidencia digital

- [EV-H01-01] Captura de pantalla: consola con sesión administrativa (no incluida en la muestra).
- [EV-H01-02] Salida del escaneo de puertos: 198.51.100.20:8443.

¿Quieres ver el informe completo?

Esta vista previa muestra 6 de las 25 páginas. El informe completo añade el alcance y las reglas de compromiso, la metodología, la escala de severidad, los 6 hallazgos con su evidencia, las observaciones técnicas, la hoja de ruta de remediación priorizada, las conclusiones y los anexos.

Pídalo con el botón «Solicitar el informe completo» de www.soluprotec.org/servicios/pentesting o escribe a info@soluprotec.org. Cada solicitud la revisa nuestro equipo y respondemos en un día hábil; el informe se envía por correo electrónico.