BIBLIOTECA
ACCCF

09
VOLUMEN

ACCCF / CONOCIMIENTO APLICADO

Manual de pentest con evidencia: validación, remediación y retest para empresas

Reglas de enfrentamiento, hallazgos, impacto delimitado, corrección y comprobación

Convertir una prueba de seguridad en un proceso autorizado y revisable, donde cada hallazgo tenga evidencia proporcionada y cada corrección pueda comprobarse sin crear otro incidente.

Coordinación editorial · Jocsan Laguna

Consejo Americano de Ciberseguridad y Cómputo Forense · 2026

Guía técnica general. Ejemplos y cifras de demostración son ficticios.

Contenido

Índice navegable. Los títulos enlazan a su ubicación dentro del documento.

Presentación: un escaneo no demuestra todo lo que importa . . . 4

Capítulo 1. Autorización y reglas . . . 4

1.1 Alcance que pueda ejecutarse sin interpretación . . . 4

1.2 Riesgo operativo y plan de salida . . . 5

Capítulo 2. Preparación técnica y validación . . . 6

2.1 Arquitectura y preguntas de seguridad . . . 6

2.2 Herramientas y datos de control . . . 6

2.3 Registros y sincronización . . . 6

Capítulo 3. Ejecución segura y bitácora . . . 6

3.1 Bitácora por acción . . . 6

3.2 Paro, escalamiento y comunicación . . . 7

3.3 Manejo de información obtenida . . . 7

Capítulo 4. Evidencia por hallazgo . . . 7

4.1 Ficha reproducible . . . 8

4.2 Falsos positivos y duplicados . . . 8

4.3 Impacto y prioridad . . . 8

Capítulo 5. Remediación y gestión del riesgo . . . 9

5.1 Corrección que responde a la causa . . . 9

5.2 Plan por impacto y dependencia . . . 9

5.3 Evidencia de la corrección . . . 10

Capítulo 6. Retest y cierre . . . 10

6.1 Repetir condiciones comparables . . . 10

6.2 Estados de cierre . . . 10

6.3 Informe final y lecciones . . . 10

Anexo A. Reglas de enfrentamiento y ficha . . . 11

A.1 Reglas de enfrentamiento . . . 12

A.2 Ficha de hallazgo 12

A.3 Informe de retest 12

Anexo B. Marco jurídico y control de salida 12

Presentación: un escaneo no demuestra todo lo que importa

Un informe con cientos de alertas puede dejar sin respuesta las preguntas esenciales: qué riesgo es real, en qué activo, bajo qué condiciones, con qué impacto y cómo se comprueba que la corrección funcionó. La prueba de penetración no es una carrera para obtener acceso a cualquier precio. Es una evaluación autorizada que produce evidencia para reducir riesgo sin dañar personas, datos ni continuidad.

NIST SP 800-115 distingue técnicas de revisión, identificación, análisis y validación de vulnerabilidades. Un escáner puede formar parte, pero no sustituye la planificación, el análisis ni la evaluación posterior. El valor del especialista no está en ejecutar más herramientas, sino en decidir cuál es necesaria, con qué alcance y cuándo detenerse.[1]

La evidencia se diseña antes de la prueba. Debe permitir revisar activo, configuración, condiciones, procedimiento, resultado, impacto y límite. No se capturan secretos reales para probar que existían si puede demostrarse con datos ficticios, respuestas parciales o un entorno controlado. La remediación y el retest pertenecen al encargo desde el inicio, no se improvisan cuando el informe ya fue entregado.

> **Regla rectora**
>
> Poder probar algo no significa estar autorizado a probarlo. La autorización define activos, técnicas, ventana, datos, contactos y criterios de paro; el método conserva esa frontera.

Capítulo 1. Autorización y reglas

1.1 Alcance que pueda ejecutarse sin interpretación

El documento de autorización incluye activos por dominio, dirección, aplicación, cuenta, entorno y propietario; técnicas permitidas y prohibidas; fechas y zonas; datos de prueba; manejo de información; contactos; comunicación; condiciones de paro y entrega. “Puedes auditar todo” no indica si permite ingeniería social, denegación de servicio, explotación, fuerza bruta, acceso físico o revisión de datos reales.

Se identifican terceros y dependencias: nube, CDN, proveedores de correo, pasarelas de pago, servicios compartidos, API externas y redes de clientes. Un dominio autorizado puede resolver a infraestructura de un tercero que exige otra autorización. La prueba no se extiende por descubrimiento: si aparece un activo nuevo, se registra y se pide ampliación antes de tocarlo.

Elemento	Contenido que debe quedar escrito	Ejemplo ficticio
Objetivo	Riesgo de negocio y pregunta de evaluación.	Validar controles de acceso a portal de clientes.
Activos	Dominios, rangos, aplicaciones, cuentas y entorno.	demo.empresa.invalid y dos cuentas ficticias.
Técnicas	Permitidas, limitadas y excluidas.	Sin denegación, sin fuerza bruta productiva, sin spam.

Elemento	Contenido que debe quedar escrito	Ejemplo ficticio
Ventana	Inicio, fin, zona y horarios de contacto.	10–12 nov, 22:00–02:00 −06.
Datos	Ficticios, máscara, manejo y eliminación.	No descargar base real ni exportar secretos.
Paro	Condición, responsable y forma de aviso.	Degradación, acceso inesperado a terceros o alcance dudoso.
Entrega	Formato, destinatarios, canal y borrado.	Informe cifrado al responsable autorizado.

1.2 Riesgo operativo y plan de salida

Se revisan posibles bloqueos, consumo de recursos, registros, alertas, cambios de estado, datos residuales y efectos en usuarios. El plan incluye respaldo cuando proceda, contacto técnico, reversa de configuración, suspensión de tareas y comunicación. No se inicia una acción irreversible para demostrar un riesgo que puede probarse de otra manera.

La prueba se realiza preferentemente con cuentas, registros y objetos ficticios. Si el objetivo es demostrar acceso indebido, se define una condición de paro antes de ver contenido real. La captura conserva lo mínimo: respuesta, código, estructura y referencia, sin difundir datos de clientes. La evidencia del hallazgo no debe ser una segunda vulneración.

Criterio de inicio

Si no puedes responder quién autoriza, qué activos incluye, qué acciones están permitidas, a quién llamar y cuándo parar, todavía no hay una prueba lista para ejecutar.



Figura 1. La autorización es parte del método. Antes de probar se delimitan acciones y salida Reconstrucción editorial; no constituye evidencia real.

Capítulo 2. Preparación técnica y validación

2.1 Arquitectura y preguntas de seguridad

Se reúne arquitectura, inventario, flujos de autenticación, roles, registros, dependencias, cambios recientes y requisitos de negocio. La revisión de documentos puede responder debilidades sin tocar el servicio. La arquitectura orienta pruebas de autorización, configuración, manejo de sesiones, exposición de datos y controles de integración. No todas las preguntas requieren explotación.

El plan asigna prioridad por impacto y probabilidad, no por facilidad de explotación. Una alerta en un servicio sin datos puede tener menos prioridad que una función que permite cambiar beneficiarios. La evaluación distingue riesgo técnico, condición de entorno y consecuencia empresarial. Si no se conoce la función del activo, el impacto se limita.

2.2 Herramientas y datos de control

Las herramientas se validan con objetivos conocidos y datos ficticios: identificación, salida, límites, tasa, reintentos, formato y efecto en registros. Se anota nombre, versión, configuración y resultado. Un escáner puede producir falsos positivos o perder una condición por interpretar una respuesta genérica. La salida no se copia al informe sin revisión.

Los datos de control permiten comparar comportamiento esperado y observado: usuario sin permiso, usuario con rol limitado, recurso propio, recurso ajeno ficticio, solicitud válida y solicitud alterada. La diferencia de respuesta puede probar una condición sin leer contenido sensible. Si el sistema solo permite pruebas en producción, se acuerdan umbrales más estrictos y un responsable disponible.

2.3 Registros y sincronización

Antes de probar se revisa qué registros genera el sistema, quién puede consultarlos y si la hora está sincronizada. Se registran valores literales y zona de cada fuente. Una alerta del WAF, un evento de aplicación y una petición del evaluador pueden tener relojes distintos. La correlación se explica con identificadores, no solo por aproximación temporal.

> **Control de calidad**
>
> Si la prueba no deja registros comprensibles, se limita lo que puede afirmarse sobre ella. La solución no es inventar una secuencia completa: es habilitar fuentes adecuadas o declarar la ausencia.

Capítulo 3. Ejecución segura y bitácora

3.1 Bitácora por acción

Cada acción registra fecha y zona, operador, activo, herramienta y versión, configuración, objetivo, solicitud o procedimiento autorizado, respuesta, artefactos y efectos. No se guardan credenciales reales ni tokens en la bitácora. Los archivos de salida se relacionan con un manifiesto y se restringe el acceso. La captura se utiliza para mostrar lo necesario, no para acumular imágenes.

La bitácora también conserva lo que no funcionó. Un resultado negativo en una condición documentada puede evitar una afirmación de riesgo falsa, pero no prueba inexistencia universal. Si una herramienta falla, se anota versión, error y alcance. Repetir una prueba crea una nueva ejecución relacionada, no elimina el intento anterior.

Campo	Ejemplo ficticio	Revisión
Acción	Solicitud autorizada a recurso DEMO-02 con rol limitado.	Dentro de alcance y datos ficticios.
Hora y zona	2026-11-10T22:14:03−06:00.	Coincide con registro del servidor.
Resultado	Respuesta 200 con estructura de recurso ajeno de prueba.	Acceso indebido sin leer datos reales.
Evidencia	Petición, respuesta parcial, identificador y captura mínima.	Sin tokens ni datos personales.
Efecto	Sin cambios de estado ni impacto visible en servicio.	Monitoreo y contacto confirmados.
Decisión	Detener la ruta y documentar hallazgo.	No ampliar a otros registros reales.

3.2 Paro, escalamiento y comunicación

Se detiene si hay degradación, efecto no previsto, alcance incierto, datos reales fuera del plan, alerta de seguridad que requiere respuesta o instrucción del contacto autorizado. El aviso incluye activo, acción, estado, evidencia disponible y decisión pendiente. No se continúa para aprovechar una oportunidad que la autorización no contemplaba.

El incidente real se separa de la prueba. Si el equipo descubre una actividad que no generó, se registra como hallazgo independiente y se comunica por canal seguro. No se atribuye automáticamente al pentest ni se eliminan sus huellas. La cronología debe distinguir quién ejecutó cada acción y qué ocurrió al mismo tiempo.

3.3 Manejo de información obtenida

Si la prueba accede a datos inesperados, se detiene la exploración, se registra la condición sin copiar contenido adicional y se consulta cómo tratar lo obtenido. La entrega se realiza por canal cifrado y con destinatarios limitados. Las llaves viajan por separado. La eliminación de archivos de prueba se documenta con alcance y límites; no se borra evidencia de la acción sin acuerdo.

> **Principio de mínima demostración**
>
> Si una respuesta parcial y un identificador ficticio demuestran el problema, no descargues la base completa. La fuerza de la evidencia no se mide por la cantidad de datos expuestos.

Capítulo 4. Evidencia por hallazgo

4.1 Ficha reproducible

La ficha contiene identificador, título, activo, versión, condición, fuentes, procedimiento, resultado, impacto, alcance, limitaciones, severidad acordada, recomendación y criterio de retest. La prueba se describe con suficiente detalle para que una persona autorizada pueda repetirla, pero el informe general evita publicar secretos o rutas que amplíen riesgo fuera del destinatario.

La evidencia debe relacionar petición y respuesta con el activo correcto. Una captura sin URL ni fecha no identifica el objeto. Un mensaje de error no prueba explotación. Un escáner etiquetado “crítico” no demuestra impacto empresarial. El especialista revisa y explica qué se hizo y qué efecto fue realmente demostrado.

4.2 Falsos positivos y duplicados

Un falso positivo puede deberse a versión inferida, respuesta personalizada, proxy, configuración o una firma de escáner incorrecta. Se contrasta con revisión manual, registros y comportamiento esperado. Si no se puede confirmar, se marca como no confirmado y no se suma al total de hallazgos. Los duplicados con la misma causa se relacionan sin ocultar activos afectados.

Situación	Tratamiento metodológico	No hacer
Alerta sin confirmar	Revisar fuente, versión y comportamiento; declarar límite.	Presentarla como vulnerabilidad probada.
Misma causa en varios activos	Agrupar causa y listar cada cobertura.	Ocultar activos o inflar cantidad.
Resultado intermitente	Documentar condiciones, reintentos y entorno.	Escoger solo la ejecución favorable.
Impacto no demostrado	Separar condición técnica de consecuencia potencial.	Asumir control total del sistema.
Activo fuera de alcance	Detener y solicitar ampliación.	Probar porque parece relacionado.

4.3 Impacto y prioridad

La severidad técnica se complementa con exposición, privilegios, datos, explotabilidad, controles compensadores y efecto en el negocio. Una vulnerabilidad difícil de explotar en un activo crítico puede requerir prioridad distinta a una fácil en un entorno aislado. Se evita tanto minimizar por relaciones comerciales como exagerar para impresionar.

El resumen ejecutivo explica qué puede ocurrir, a qué activos, bajo qué condiciones y qué decisión se necesita. No incluye una lista interminable de términos sin contexto. El anexo técnico conserva la prueba, los logs y las limitaciones. Dirección recibe decisiones; seguridad recibe ruta de reproducción; cumplimiento recibe evidencia de seguimiento.

Caso ficticio

Una función permite consultar un documento de prueba de otro usuario cambiando un identificador. Se detiene antes de consultar documentos reales. El hallazgo demuestra una falla de autorización en el objeto ficticio. No afirma que todos los documentos sean accesibles ni que el atacante haya descargado la base: el impacto se delimita con pruebas adicionales autorizadas.

Una ficha de hallazgo permite revisar sin repetir daño
ACCCF · RECONSTRUCCIÓN EDITORIAL · DATOS FICTICIOS

Prueba mínima, impacto delimitado y ruta de corrección

Campo	Contenido	Control
Activo y versión	Servicio DEMO y configuración observada.	Objeto inequívoco y dentro de alcance.
Procedimiento	Pasos en entorno controlado y datos ficticios.	Repetibilidad sin credenciales reales.
Resultado	Respuesta técnica y evidencia asociada.	No confundir advertencia con explotación.
Impacto	Activo, condición y consecuencia demostrada.	No extrapolar a toda la empresa.
Remediación	Cambio propuesto y prioridad.	Responsable, fecha y criterio de retest.

La figura explica decisiones y relaciones; no representa evidencia de un caso real.

Figura 2. Una ficha de hallazgo permite revisar sin repetir daño. Prueba mínima, impacto delimitado y ruta de corrección
Reconstrucción editorial; no constituye evidencia real.

Capítulo 5. Remediación y gestión del riesgo

5.1 Corrección que responde a la causa

La recomendación identifica la condición que debe cambiar, no solamente una actualización genérica. Si el problema es autorización, se revisa validación en servidor y relación con el recurso; ocultar el enlace no resuelve. Si el problema es configuración, se revisa efecto en otros entornos y componentes. La corrección incluye propietario, fecha objetivo, dependencia, prueba y posible regresión.

Cuando no se corrige de inmediato, se documenta riesgo aceptado, mitigación temporal, responsable y fecha de revisión. La aceptación no se presenta como remediación. Un WAF puede limitar una ruta pero no eliminar la causa; se conserva evidencia de ambos estados y se comprueba si la regla afecta funciones legítimas.

5.2 Plan por impacto y dependencia

Acción	Responsable y fecha	Criterio de aceptación
Mitigación temporal	[Propietario, implementación y vigencia]	[Reduce exposición sin romper operación]
Corrección definitiva	[Cambio, versión y despliegue]	[Causa eliminada en el alcance]
Revisión de otros activos	[Mismo patrón y cobertura]	[Sin duplicados ocultos]
Prueba de regresión	[Funciones críticas y roles]	[Sin daño a usuarios legítimos]
Actualización documental	[Diagrama, configuración y procedimiento]	[Realidad y documentos coinciden]
Aceptación residual	[Quién, motivo y vencimiento]	[No confundir con cierre técnico]

5.3 Evidencia de la corrección

Se conserva cambio de configuración, versión, fecha, responsable, despliegue, pruebas y efectos. Una captura del panel con “actualizado” no demuestra que la ruta quedó corregida. Si existen múltiples entornos, se registra dónde se aplicó. El informe inicial no se modifica para borrar el hallazgo: se añade una nueva evaluación relacionada.

> **Regla de honestidad**
>
> “El proveedor dice que ya está corregido” es una declaración, no un retest. La evidencia de cierre exige una comprobación técnica o una decisión explícita de riesgo residual con su alcance.

Capítulo 6. Retest y cierre

6.1 Repetir condiciones comparables

El retest utiliza el mismo objeto, rol, condiciones y procedimiento cuando sea posible, con nueva versión y fecha. Se compara con el hallazgo original sin alterar la evidencia anterior. Si cambió la aplicación o el entorno, se registra porque puede explicar un resultado diferente. Un resultado negativo solo se refiere a la prueba y cobertura actuales.

Se prueba también la regresión: el usuario legítimo puede trabajar y la función no expone otros datos. Si se bloqueó la petición maliciosa pero se rompió el acceso normal, el estado puede ser parcial. Si la corrección solo funciona para una ruta y existen equivalentes, se revisan dentro del alcance. La prueba de cierre no se limita a una captura del error deseado.

6.2 Estados de cierre

Estado	Criterio	Evidencia
Corregido	La condición no se reproduce en el alcance y no hay regresión observada.	Retest, fecha, versión y funciones legítimas.
Parcial	Algunos activos o rutas mejoraron; otras mantienen la condición.	Cobertura y pendientes por activo.
Mitigado	Existe control temporal que reduce exposición sin eliminar causa.	Regla, prueba, vigencia y límite.
Aceptado	Responsable acepta riesgo residual con motivo y vencimiento.	Decisión, alcance y revisión.
Abierto	La condición se reproduce o no existe evidencia suficiente.	Hallazgo original y acciones pendientes.

6.3 Informe final y lecciones

El informe final vincula hallazgo inicial, cambio, retest y estado, sin borrar lo anterior. Incluye riesgo residual, limitaciones y fecha de siguiente revisión. El resumen directivo no promete “sistema seguro”; informa qué riesgos fueron evaluados y qué evidencia existe de mejora. Si una prueba no fue posible, se declara en lugar de marcarla como superada.

La lección puede exigir autenticación resistente al phishing, revisión de autorizaciones, pruebas de regresión, inventario de terceros o registros mejores. NIST SP 800-63B-4 ofrece guía de autenticación y niveles de garantía; no reemplaza la evaluación del flujo de recuperación, que suele ser la ruta real de compromiso.[2]

Cierre real

La prueba termina cuando la organización puede mostrar qué encontró, qué cambió, qué comprobó y qué riesgo queda. No cuando el PDF recibe el nombre “final”.

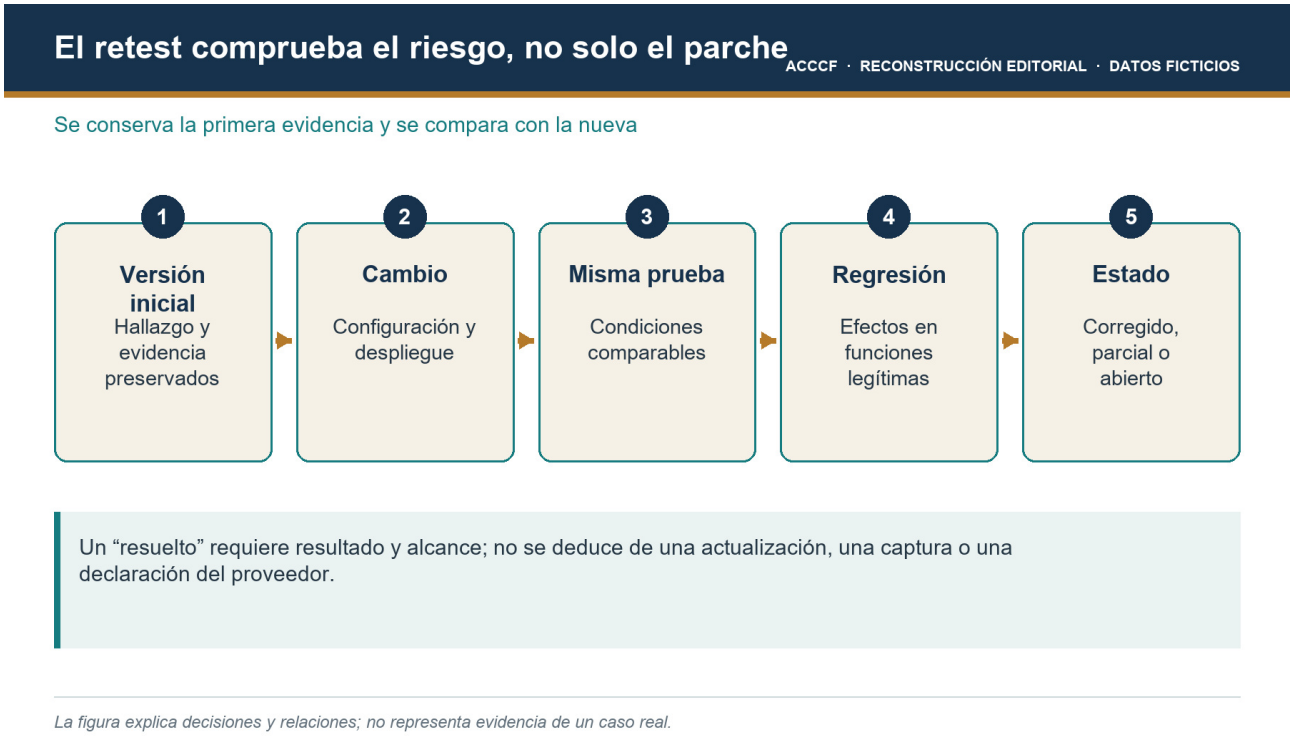


Figura 3. El retest comprueba el riesgo, no solo el parche. Se conserva la primera evidencia y se compara con la nueva Reconstrucción editorial; no constituye evidencia real.

Anexo A. Reglas de enfrentamiento y ficha

A.1 Reglas de enfrentamiento

Plantilla ficticia para aprobación

```
Proyecto: DEMO-PENTEST-2026-009
Objetivo y riesgo empresarial: [pregunta concreta]
Activos incluidos: [dominios, rangos, aplicaciones, cuentas]
Exclusiones: [activos, terceros, datos y técnicas]
Ventana y zona: [inicio, fin, contactos]
Datos permitidos: [ficticios, máscara, tratamiento]
Acciones permitidas: [revisión, validación, condiciones]
Acciones prohibidas: [DoS, fuerza bruta, ingeniería social, otras]
Umbrales de paro: [degradación, datos, alcance, alerta]
Contacto de emergencia y suplencia: [canal seguro]
Evidencia: [formatos, minimización y custodia]
Entrega: [destinatarios, cifrado y fecha]
Eliminación: [objetos, respaldo y límites]
Retest: [fecha, alcance y aceptación]
Autorizaciones: [titular, terceros y versión]
```

A.2 Ficha de hallazgo

Campo	Contenido requerido	Ejemplo ficticio
Identificador	Código estable relacionado con bitácora.	DEMO-AUTH-003.
Activo y versión	Aplicación, entorno y configuración.	Portal DEMO v2.4, pruebas.
Condición	Qué control falla y bajo qué rol.	Recurso de otro usuario ficticio accesible.
Procedimiento	Pasos autorizados, solicitudes y parámetros.	Rol limitado y recurso de control.
Resultado	Respuesta y artefactos sin secretos.	Código 200 y estructura parcial.
Impacto	Consecuencia demostrada y alcance.	Acceso al objeto ficticio; no extrapolación.
Limitaciones	Qué no se probó y por qué.	Sin consulta de documentos reales.
Remediación	Cambio, propietario y prioridad.	Validación de autorización en servidor.
Retest	Condiciones, fecha y resultado.	Misma ruta y rol, más regresión.

A.3 Informe de retest

Registro de comparación

```
Hallazgo original: [ID, evidencia y fecha]
Cambio aplicado: [configuración, versión, responsable]
Fecha y zona del retest: [literal]
Condiciones equivalentes: [rol, objeto, parámetros]
Resultado de la prueba original repetida: [observado]
Pruebas de regresión: [funciones legítimas]
Cobertura adicional: [rutas o activos]
Estado: [corregido, parcial, mitigado, aceptado, abierto]
Riesgo residual y límites: [declaración]
Próxima revisión: [fecha y responsable]
Anexos: [salida, registros y manifiesto]
```

Anexo B. Marco jurídico y control de salida

La autorización es el primer requisito; la evidencia electrónica requiere método, atribución, integridad y accesibilidad. En México, las instituciones de crédito tienen revisiones de seguridad y registros

específicos en las disposiciones CNBV aplicables, incluida revisión al menos anual del artículo 316 Bis 17 en su ámbito. En Perú y Argentina existen requisitos de gestión y respuesta sectorial; España distingue pagos y riesgos. No se exportan obligaciones a toda empresa.[345678]

Colombia, Ecuador, Chile y España cuentan con reglas de documento electrónico, firma y conservación que ayudan a estructurar evidencia; no autorizan por sí mismas pruebas de intrusión. La protección de datos limita qué puede capturarse y compartirse, incluso si el objetivo es demostrar una vulnerabilidad.[91011121314]

Control	Pregunta de aceptación
Autoridad	¿Activos, técnicas, datos, ventana y paro aprobados?
Seguridad	¿La prueba evita daño y exposición innecesaria?
Método	¿Herramientas, versiones y salidas fueron validadas?
Hallazgo	¿Activo, procedimiento, resultado e impacto son trazables?
Corrección	¿Cambio y cobertura están documentados?
Retest	¿Misma condición y regresión comprobadas?
Conclusión	¿Riesgo residual y límites no fueron escondidos?

Cierre

La mejor prueba no es la que demuestra mayor acceso, sino la que permite reducir un riesgo con evidencia suficiente y sin producir otro incidente.

Referencias citadas

Cada número remite a la fuente consultada en el cuerpo. La fecha general de revisión documental es el 10 de noviembre de 2026; el uso en un expediente exige comprobar la versión aplicable al hecho, materia, sujeto y jurisdicción.

[1] NIST SP 800-115. Guía técnica para pruebas y evaluación de seguridad: planificación, ejecución y análisis posterior. Un escaneo automatizado no equivale por sí solo a una prueba de penetración ni a una validación completa. Fuente oficial en línea

[2] NIST SP 800-63B-4 (julio de 2025). Directrices de autenticación y gestión de autenticadores, incluidos niveles de garantía y autenticación resistente al phishing. La recuperación de cuentas forma parte del riesgo y no debe reducirse a contraseñas. Fuente oficial en línea

[3] Disposiciones de carácter general aplicables a las instituciones de crédito, artículos 316 Bis, 316 Bis 1, 316 Bis 10 a 17: comprobantes, cifrado, acceso, incidentes, incidencias, bitácoras y revisiones. Fuente oficial en línea

[4] Perú. SBS 504-2021, artículos 12.6.g, 15 y 17.3–17.4: preservación, reporte y análisis forense, registros de enrolamiento, autenticación y operaciones. Fuente oficial en línea

[5] Argentina. BCRA Comunicación A 8280: respuesta y recuperación ante ciberincidentes; reporte final dentro de cinco días corridos posteriormente a contención, recuperación y resolución. Fuente oficial en línea

[6] España. Real Decreto-ley 19/2018, artículos 45, 66 y 67: restitución por operaciones no autorizadas, gestión de riesgos y notificación inmediata de incidentes graves. Fuente oficial en línea

[7] Código de Comercio de México, artículos 89–94 y 1205: neutralidad, atribución, escrito, original, integridad, accesibilidad y admisión de mensajes de datos. Compilación oficial. Fuente oficial en línea

[8] Código Nacional de Procedimientos Civiles y Familiares, artículos 348–350. Compilación con reforma del 15-01-2026. La aplicación es gradual y depende de declaratorias. Fuente oficial en línea

[9] Chile. Ley 19.799 sobre documentos electrónicos y firma electrónica, artículos 1–5: equivalencia, escrito, firma simple/avanzada, fecha y valor probatorio. Fuente oficial en línea

[10] Colombia. Ley 527 de 1999, artículos 5–13, 16–25 y 28: mensajes de datos, escrito, original, integridad, admisibilidad, conservación, envío, recepción y firma digital. Fuente oficial en línea

[11] Ecuador. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Ley 67, artículos 2, 6–8, 10–16: equivalencia, escrito, original, conservación, procedencia, envío, recepción y firma electrónica. Fuente oficial en línea

[12] Reglamento (UE) 910/2014 eIDAS, artículos 25–26 y 46: no discriminación de firmas electrónicas y documentos por su formato, firma avanzada y efectos de firma cualificada. Fuente oficial en línea

[13] México. Ley Federal de Protección de Datos Personales en Posesión de los Particulares, texto publicado el 20-03-2025 y reforma del 14-11-2025. Artículos 5–9, 18–20 y 31: principios, seguridad, confidencialidad, vulneraciones y atención de derechos. La autoridad federal actual es la Secretaría Anticorrupción y Buen Gobierno. Fuente oficial en línea

[14] Unión Europea. Reglamento (UE) 2016/679, artículos 5, 25, 28 y 32–34: principios, protección desde el diseño, encargados, seguridad y notificación/comunicación de violaciones de seguridad. España exige revisar además la legislación nacional y sectorial aplicable. Fuente oficial en línea

Aviso editorial: guía técnica general y material educativo. No constituye asesoría legal, dictamen pericial ni autorización para acceder a sistemas o información. Los ejemplos y cifras de demostración son ficticios; las figuras son reconstrucciones editoriales.