MORINI COMPUTERS

MORINI COMPUTERS SL

Service Catalog

Pruebas de penetración y evaluación de seguridad

EDICIÓN 2026

MORINICOMPUTERS.COM

SERVICE CATALOG

Índice

Por qué una prueba de penetración 3

Cómo trabajamos 3

01 INFRAESTRUCTURA

EPT External Penetration Test 4

IPT Internal Penetration Test 6

AD Active Directory Assessment 8

VA Vulnerability Assessment 10

02 APLICACIONES

WAPT Web Application Penetration Test 12

API API Penetration Test 14

MAPT Mobile Application Penetration Test 16

03 INALÁMBRICAS Y COMUNICACIONES

WIFI Wi-Fi Penetration Test 18

VOIP VoIP Penetration Test 20

04 DISPOSITIVOS E INDUSTRIA

IOT IoT Penetration Test 22

OT OT Penetration Test 24

05 NUBE E IA

CLOUD Cloud Penetration Test 26

AI Agentic AI & LLM Penetration Test 28

06 SEGUIMIENTO

RETEST Remediation Retest 30

Qué pedimos al cliente 32

Hablemos 32

© Morini Computers SL · morinicomputers.com · Edición 2026

MORINI COMPUTERS SL

Por qué una prueba de penetración

Una prueba de penetración es un ataque controlado a tus sistemas. Intentamos entrar como lo haría un atacante real, pero con reglas precisas y sin causar daños, para descubrir los puntos débiles antes de que los encuentre otro. Al final sabes qué está expuesto, cómo de grave es y qué hacer para solucionarlo.

No nos limitamos al escaneo automático. Una herramienta encuentra los fallos conocidos; una persona entiende cómo encadenarlos para llegar al dato o al control que realmente importa. Cada resultado lo verificamos a mano, con una prueba concreta, y lo explicamos para que tanto el técnico como quien decide entiendan qué implica.

Este catálogo reúne nuestros servicios de seguridad ofensiva. Cada ficha dice qué es el servicio, cuándo tiene sentido, qué entra y qué queda fuera del alcance, cómo trabajamos y qué recibes. Si no sabes por dónde empezar, normalmente se empieza por una prueba externa o por un análisis de vulnerabilidades: a partir de ahí se ve dónde hace falta profundizar.

CÓMO TRABAJAMOS

01 **Recopilación de requisitos**

Partimos de una conversación: qué quieres proteger, qué te preocupa, qué sistemas están en juego y qué restricciones tienes (ventanas de mantenimiento, sistemas delicados, terceros). De ahí sacamos una lista clara de objetivos y de lo que hay que probar.

02 **Propuesta y reglas de enfrentamiento**

Ponemos por escrito el alcance, los plazos y la forma de trabajar en una propuesta y en un documento de autorización firmado por ambas partes. Ahí están las direcciones dentro del alcance, las ventanas acordadas, los contactos de emergencia y lo que nunca tocamos. Sin autorización firmada no empieza nada.

03 **Ejecución**

Ejecutamos la prueba siguiendo la metodología del servicio. Mantenemos el contacto durante el trabajo: si encontramos algo grave que expone a la empresa de inmediato, te avisamos mientras aún estamos probando, no al final del encargo.

04 **Informe**

Escribimos un informe con un resumen para quien decide y el detalle técnico para quien corrige. Cada vulnerabilidad tiene una descripción, la prueba, la gravedad con puntuación CVSS y una recomendación concreta de cómo solucionarla, ordenada por prioridad.

05 **Presentación de resultados**

Repasamos juntos el informe en una reunión: qué encontramos, qué importa de verdad, por dónde conviene empezar. Respondemos a las preguntas del equipo técnico y aclaramos las dudas sobre las correcciones.

06 **Retest**

Después de que hayas corregido los problemas, volvemos a verificar las vulnerabilidades del informe para confirmar que están cerradas de verdad. Es un servicio aparte (ver Remediation Retest) y cierra el ciclo.

© Morini Computers SL · morinicomputers.com · Edición 2026

01 INFRAESTRUCTURA

EPT INFRAESTRUCTURA

External Penetration Test

Comprueba qué puede hacer un atacante partiendo de Internet, sin credenciales.

QUÉ ES

Simulamos un ataque desde fuera, como alguien que no tiene ningún acceso e intenta entrar desde la red pública. Buscamos tus sistemas expuestos en Internet — sitios web, portales, VPN, correo, servicios accesibles — e intentamos aprovechar sus debilidades para entrar o acceder a datos sensibles. El objetivo es medir cómo de sólido es el perímetro visto por quien lo ataca cada día.

CUÁNDO LO NECESITAS

- Tienes servicios publicados en Internet (web, webmail, VPN, portales) y quieres saber cómo aguantan.
- Nunca has hecho una prueba desde fuera o ha pasado más de un año desde la última.
- Has abierto nuevos puertos, cambiado de proveedor o publicado un nuevo servicio.
- Un cliente, una aseguradora o una normativa te piden una verificación del perímetro externo.
- Quieres un punto de partida antes de invertir en nuevas defensas.

+ DENTRO DEL ALCANCE

- Direcciones IP y nombres de dominio públicos acordados.
- Servicios expuestos: web, correo, VPN, accesos remotos, DNS, servicios de transferencia de archivos.
- Búsqueda de información y credenciales ya filtradas al exterior (OSINT).
- Intentos de explotación controlada de las vulnerabilidades encontradas.

− FUERA DEL ALCANCE

- Red interna y puestos de trabajo (ver Internal Penetration Test).
- Ataques de ingeniería social al personal, salvo petición explícita.
- Ataques dirigidos a tumbar los servicios (denegación de servicio).
- Sistemas de terceros sin autorización escrita del propietario.

ENFOQUES

Black box

Partimos sin información, como un atacante cualquiera: reconstruimos por nuestra cuenta qué está expuesto.

Grey box

Nos das de antemano la lista de activos en el alcance: menos tiempo mapeando, más tiempo probando en profundidad.

© Morini Computers SL · morinicomputers.com · Edición 2026

EPT · External Penetration Test

METODOLOGÍA

01	**Reconocimiento**	Recopilamos todo lo visible desde fuera: dominios, subdominios, direcciones, tecnologías, datos expuestos en línea.
02	**Enumeración**	Mapeamos puertos y servicios abiertos, versiones y configuraciones, para saber dónde están las superficies de ataque.
03	**Análisis de vulnerabilidades**	Cruzamos servicios y versiones con debilidades conocidas y configuraciones débiles, filtrando los falsos positivos.
04	**Explotación**	Intentamos explotar de verdad las debilidades encontradas, de forma controlada, para demostrar el impacto real.
05	**Post-explotación**	Si entramos, comprobamos hasta dónde se puede llegar: datos alcanzables, movimiento hacia dentro, persistencia.
06	**Informe**	Documentamos cada resultado con prueba, gravedad y recomendación de corrección.

ESTÁNDARES DE REFERENCIA

- **PTES** — estructura general de las fases de la prueba.
- **OSSTMM** — criterios de medición para los controles expuestos.
- **CVSS v3.1/v4.0** — para asignar la gravedad a cada vulnerabilidad.
- **NIST SP 800-115** — guía técnica sobre cómo realizar y documentar la prueba.
- **MITRE ATT&CK** — para describir técnicas de ataque y movimiento.

QUÉ RECIBES

- Informe con resumen para la dirección y detalle técnico.
- Lista de vulnerabilidades con prueba, puntuación CVSS y prioridad.
- Recomendaciones de corrección concretas para cada resultado.
- Reunión de presentación de resultados.
- Aviso inmediato en caso de riesgos críticos durante la prueba.

© Morini Computers SL · morinicomputers.com · Edición 2026

IPT INFRAESTRUCTURA

Internal Penetration Test

Qué puede hacer quien ya está dentro de la red: un empleado, un proveedor, un PC comprometido.

QUÉ ES

Probamos la red interna desde el punto de vista de quien ya tiene un pie dentro: un colaborador, un invitado en la red, o un atacante que ha comprometido un puesto. Partimos de un acceso limitado y vemos hasta dónde se puede llegar — servidores, datos, control del dominio. Sirve para saber cuánto daño puede causar una amenaza interna o un ataque que ya ha superado el perímetro.

CUÁNDO LO NECESITAS

- Quieres saber qué pasa si un atacante supera el perímetro o infecta un PC.
- Tienes una red plana donde todo habla con todo y temes el movimiento lateral.
- Gestionas datos sensibles en servidores internos y quieres verificar su aislamiento.
- Quieres medir la eficacia de la segmentación de red y de los controles internos.
- Un requisito de cumplimiento exige una verificación desde dentro.

+ DENTRO DEL ALCANCE

- Segmentos de red internos acordados y sus servidores y servicios.
- Servicios de red y protocolos internos (recursos compartidos, autenticación, impresión, gestión).
- Escalada de privilegios en las máquinas alcanzadas.
- Movimiento lateral entre sistemas y verificación de la segmentación.

− FUERA DEL ALCANCE

- Perímetro expuesto en Internet (ver External Penetration Test).
- Análisis específico de Active Directory (ver Active Directory Assessment) salvo inclusión explícita.
- Ataques destructivos o que comprometen la disponibilidad de los servicios.
- Ingeniería social, salvo acuerdo específico.

ENFOQUES

Estándar

Partimos de un puesto típico con un usuario de dominio normal, como un empleado cualquiera.

Assumed breach

Partimos de la hipótesis de que un atacante ya está dentro con un acceso básico: nos centramos en qué puede hacer desde ahí.

Sin credenciales

Nos conectamos solo a la red, sin cuenta, para ver qué se obtiene desde cero (poisoning, servicios abiertos, datos expuestos).

© Morini Computers SL · morinicomputers.com · Edición 2026

IPT · Internal Penetration Test

METODOLOGÍA

01	**Reconocimiento interno**	Mapeamos la red alcanzable: hosts activos, servicios, recursos compartidos, sistemas de autenticación.
02	**Recopilación de credenciales**	Intentamos interceptar o recuperar credenciales con técnicas de red (envenenamiento de protocolos, relay, datos expuestos).
03	**Escalada de privilegios**	Desde un usuario normal intentamos obtener derechos de administrador local y luego de dominio.
04	**Movimiento lateral**	Nos movemos de un sistema a otro para alcanzar los objetivos de valor y verificar la segmentación.
05	**Acceso a los datos**	Demostramos qué podría leer o sustraer un atacante, sin tocar los datos reales.
06	**Informe**	Reconstruimos las rutas de ataque e indicamos dónde romperlas.

ESTÁNDARES DE REFERENCIA

- **PTES** — estructura de las fases de la prueba interna.
- **OSSTMM** — medición de los controles de red internos.
- **CVSS v3.1/v4.0** — gravedad de las vulnerabilidades.
- **NIST SP 800-115** — método técnico de prueba y documentación.
- **MITRE ATT&CK** — catálogo de las técnicas de escalada y movimiento lateral.

QUÉ RECIBES

- Informe con rutas de ataque reconstruidas paso a paso.
- Lista de vulnerabilidades con prueba, CVSS y prioridad.
- Evaluación de la segmentación y de los controles internos.
- Recomendaciones de corrección específicas.
- Reunión de presentación de resultados.

© Morini Computers SL · morinicomputers.com · Edición 2026

AD INFRAESTRUCTURA

Active Directory Assessment

La salud del dominio Windows: quién puede convertirse en administrador y cómo.

QUÉ ES

Active Directory es el corazón de casi toda red Windows: si cae eso, cae todo. Analizamos el dominio para encontrar los caminos que llevan a un usuario cualquiera a convertirse en administrador: delegaciones mal hechas, contraseñas débiles, configuraciones peligrosas, cuentas olvidadas, permisos demasiado amplios. Reconstruimos las rutas de ataque reales e indicamos dónde intervenir para cerrarlas, por orden de gravedad.

CUÁNDO LO NECESITAS

- Tu red funciona sobre dominio Windows y nunca la has hecho analizar.
- Después de un incidente o la sospecha de un acceso no autorizado.
- Antes o después de una migración, una consolidación o una limpieza del dominio.
- Quieres reducir la superficie de ataque frente al ransomware, que a menudo pasa por el dominio.
- Tienes muchas cuentas administrativas y ya no sabes quién puede hacer qué.

+ DENTRO DEL ALCANCE

- Estructura del dominio: usuarios, grupos, delegaciones, unidades organizativas.
- Rutas de escalada hacia Domain Admin y cuentas privilegiadas.
- Políticas de contraseñas, cuentas kerberoastable y credenciales débiles.
- Configuraciones peligrosas (ACL, GPO, trusts, servicios mal configurados).

− FUERA DEL ALCANCE

- Pruebas de la infraestructura de red no ligada al dominio.
- Cambios en la configuración: entregamos el análisis, no aplicamos los cambios.
- Ataques que degradan el servicio del controlador de dominio.
- Entornos cloud de identidad externos al dominio, salvo inclusión explícita.

ENFOQUES

Desde usuario estándar

Partimos de una cuenta de dominio normal, como la de un empleado, para ver qué es alcanzable desde ahí.

Con credenciales privilegiadas

Si la enumeración desde usuario básico es limitada, usamos credenciales facilitadas para completar el análisis en profundidad.

© Morini Computers SL · morinicomputers.com · Edición 2026

AD · Active Directory Assessment

METODOLOGÍA

01	**Recopilación de la estructura**	Extraemos la fotografía del dominio: objetos, relaciones, permisos, delegaciones.
02	**Análisis de rutas**	Identificamos las cadenas que llevan de un usuario común a derechos elevados.
03	**Verificación de credenciales**	Buscamos contraseñas débiles, cuentas kerberoastable y secretos expuestos.
04	**Configuraciones de riesgo**	Examinamos ACL, GPO, trusts y servicios mal configurados explotables.
05	**Demostración**	Probamos de forma controlada las rutas más graves hasta derechos elevados.
06	**Informe**	Ordenamos las intervenciones por impacto y facilidad de corrección.

ESTÁNDARES DE REFERENCIA

- **MITRE ATT&CK** técnicas de ataque a credenciales e identidad.
- **PTES** estructura de las fases de análisis.
- **CIS Benchmarks** referencia para el hardening del dominio Windows.
- **CVSS v3.1/v4.0** gravedad de los problemas identificados.

QUÉ RECIBES

- Informe con las rutas de ataque hacia el dominio.
- Lista de configuraciones de riesgo con prioridad.
- Indicaciones de hardening alineadas con las buenas prácticas.
- Recomendaciones sobre cuentas privilegiadas e higiene de credenciales.
- Reunión de presentación de resultados.

© Morini Computers SL · morinicomputers.com · Edición 2026

VA INFRAESTRUCTURA

Vulnerability Assessment

Fotografía amplia de las vulnerabilidades, ordenadas por prioridad. Sin explotarlas.

QUÉ ES

El análisis de vulnerabilidades identifica, clasifica y ordena por prioridad las vulnerabilidades en redes, sistemas y servicios. Es más amplio que una prueba de penetración pero menos profundo: cubre muchos sistemas rápidamente con escaneos exhaustivos y verificación manual, sin explotar los fallos. Sirve para hacerse una idea completa de qué es vulnerable y por dónde empezar, a menudo como primer paso o como control periódico recurrente.

CUÁNDO LO NECESITAS

- Quieres una visión de conjunto de qué es vulnerable, en muchos sistemas.
- Necesitas un control periódico y repetible de la postura de seguridad.
- Quieres una base antes de decidir dónde hacer una prueba de penetración específica.
- Tienes un parque de máquinas heterogéneo y no sabes cómo de actualizado está.
- Una política interna o un requisito exige escaneos regulares.

+ DENTRO DEL ALCANCE

- Redes, servidores y servicios acordados, internos y/o externos.
- Identificación de software desactualizado y configuraciones débiles.
- Clasificación de las vulnerabilidades por gravedad.
- Verificación manual para reducir los falsos positivos.

– FUERA DEL ALCANCE

- La explotación activa de las vulnerabilidades (eso es la prueba de penetración).
- Movimiento lateral y post-explotación.
- Análisis manual en profundidad de la lógica de la aplicación.
- Ingeniería social.

ENFOQUES

Autenticado

Con credenciales en los sistemas: fotografía más precisa de parches y configuraciones.

No autenticado

Sin credenciales: qué es visible y vulnerable desde fuera del sistema.

© Morini Computers SL · morinicomputers.com · Edición 2026

VA · Vulnerability Assessment

METODOLOGÍA

01	**Identificación de activos**	Mapeamos hosts y servicios activos dentro del alcance acordado.
02	**Escaneo**	Analizamos los sistemas con escáneres exhaustivos, autenticados cuando es posible.
03	**Verificación**	Comprobamos a mano los resultados para descartar los falsos positivos.
04	**Clasificación**	Asignamos gravedad y prioridad según impacto y exposición.
05	**Informe**	Entregamos la lista ordenada con las indicaciones de corrección.

ESTÁNDARES DE REFERENCIA

- **NIST SP 800-115** método de escaneo y evaluación.
- **CIS Benchmarks** referencia para las configuraciones seguras.
- **CVSS v3.1/v4.0** clasificación de la gravedad.

QUÉ RECIBES

- Informe con la lista de vulnerabilidades ordenadas por prioridad.
- Distinción entre confirmadas y por profundizar, con falsos positivos filtrados.
- Puntuación CVSS para cada entrada.
- Indicaciones de corrección y actualización.
- Formato adecuado para comparaciones periódicas en el tiempo.

© Morini Computers SL · morinicomputers.com · Edición 2026

02 APLICACIONES

WAPT APLICACIONES

Web Application Penetration Test

Atacamos tu aplicación web como lo haría quien quiere vulnerarla.

QUÉ ES

Probamos una aplicación web — un ERP, un portal de clientes, un e-commerce, un área privada — intentando saltarnos su lógica y sus controles. Buscamos los fallos que permiten acceder a datos ajenos, saltarse la autenticación, alterar los permisos o ejecutar comandos. Vamos más allá del escáner: entendemos cómo funciona la aplicación y la usamos de formas no previstas para demostrar qué podría conseguir realmente un atacante.

CUÁNDO LO NECESITAS

- Publicas una nueva aplicación o una versión importante.
- La aplicación trata datos personales, pagos o información confidencial.
- Un cliente o una normativa exige una verificación de seguridad de la aplicación.
- Has integrado inicios de sesión externos, pagos o funciones sensibles.
- Nunca la ha probado nadie fuera de quien la desarrolló.

+ DENTRO DEL ALCANCE

- La aplicación web y sus funciones, con los distintos roles de usuario.
- Autenticación, gestión de sesión y control de accesos.
- Validación de entradas y fallos típicos (injection, XSS, IDOR y similares).
- Lógica de la aplicación y flujos de negocio sensibles.

− FUERA DEL ALCANCE

- Las API subyacentes como prueba dedicada (ver API Penetration Test) salvo inclusión.
- Infraestructura y servidores que alojan la aplicación, salvo acuerdo.
- Pruebas de carga o ataques a la disponibilidad del servicio.
- Código fuente completo, salvo elección del enfoque white box.

ENFOQUES

Black box
Probamos sin credenciales ni documentación, como un usuario externo.

Grey box
Con cuentas de prueba para cada rol: cubrimos también las funciones privadas y los controles entre roles.

White box
Con documentación y, donde sea útil, acceso al código: la cobertura más completa.

© Morini Computers SL · morinicomputers.com · Edición 2026

WAPT · Web Application Penetration Test

METODOLOGÍA

01	**Reconocimiento**	Mapeamos funciones, páginas, puntos de entrada, tecnologías y roles.
02	**Análisis de la configuración**	Verificamos cabeceras, gestión de errores, protecciones y ajustes débiles.
03	**Autenticación y sesión**	Intentamos saltarnos el inicio de sesión, la gestión de contraseñas y las sesiones.
04	**Control de accesos**	Verificamos que un usuario no pueda ver o hacer lo que no le corresponde (IDOR, escalada).
05	**Entradas y lógica**	Buscamos injection, XSS y fallos en la lógica de negocio.
06	**Explotación e impacto**	Encadenamos los fallos para demostrar el impacto real.
07	**Informe**	Documentamos cada fallo con prueba, gravedad y corrección.

ESTÁNDARES DE REFERENCIA

- **OWASP WSTG** — guía de referencia para las pruebas web.
- **OWASP Top 10** — las categorías de riesgo más comunes.
- **CVSS v3.1/v4.0** — gravedad de las vulnerabilidades.
- **OWASP ASVS** — niveles de verificación de los requisitos de seguridad.
- **PTES** — estructura de las fases.

QUÉ RECIBES

- Informe con resumen y detalle técnico de cada fallo.
- Prueba de explotación (capturas, peticiones, pasos para reproducirlo).
- Puntuación CVSS y prioridad de intervención.
- Recomendaciones de corrección utilizables por el equipo de desarrollo.
- Reunión de presentación de resultados.

© Morini Computers SL · morinicomputers.com · Edición 2026

API APLICACIONES

API Penetration Test

Las API son la puerta trasera de las apps: comprobamos que no esté abierta de par en par.

QUÉ ES

Las API mueven los datos entre apps, servicios y socios, y a menudo tienen menos controles que la interfaz de usuario. Probamos REST, GraphQL y servicios similares intentando saltarnos autorizaciones, leer datos de otros usuarios, abusar de la lógica y ejecutar acciones no permitidas. El fallo más común es la autorización: un usuario que, cambiando un identificador en la petición, accede a los datos de otro. Lo buscamos a fondo.

CUÁNDO LO NECESITAS

- Expones API a clientes, apps móviles o socios externos.
- Una app web o móvil se apoya en un backend de API.
- Has publicado nuevos endpoints o cambiado el modelo de autorización.
- Tratas datos sensibles o pagos a través de API.
- Quieres verificar los controles entre roles y tenants distintos.

+ DENTRO DEL ALCANCE

- Los endpoints de API acordados y sus métodos.
- Autenticación, gestión de tokens y autorización entre roles.
- Referencias directas a objetos (IDOR) y acceso a datos ajenos.
- Validación de entradas, límites de frecuencia y abuso de la lógica.

– FUERA DEL ALCANCE

- Interfaz web que consume las API (ver Web Application Penetration Test).
- Infraestructura del backend, salvo acuerdo.
- Pruebas de carga o ataques a la disponibilidad.
- API de terceros sin autorización del propietario.

ENFOQUES

Grey box

Con documentación (p. ej., especificación OpenAPI) y cuentas de prueba por rol: cobertura más completa de los controles de autorización.

Black box

Sin documentación: enumeramos endpoints y comportamientos por nuestra cuenta.

© Morini Computers SL · morinicomputers.com · Edición 2026

API · API Penetration Test

METODOLOGÍA

01	**Enumeración**	Mapeamos endpoints, métodos, parámetros y roles previstos.
02	**Autenticación y tokens**	Verificamos emisión, caducidad y robustez de tokens y sesiones.
03	**Autorización**	Probamos controles por función, por objeto y entre tenants (IDOR, escalada).
04	**Entradas y lógica**	Buscamos injection, validaciones débiles y abusos de la lógica de negocio.
05	**Encadenamiento**	Unimos los fallos hasta un impacto concreto en el negocio.
06	**Informe**	Documentamos cada fallo con peticiones, prueba y corrección.

ESTÁNDARES DE REFERENCIA

- **OWASP API Security Top 10** las categorías de riesgo específicas de las API.
- **OWASP WSTG** técnicas de prueba aplicables a las API.
- **PTES** estructura de las fases.
- **CVSS v3.1/v4.0** gravedad de las vulnerabilidades.

QUÉ RECIBES

- Informe con resumen y detalle de cada endpoint problemático.
- Prueba con peticiones y respuestas para reproducir el fallo.
- Puntuación CVSS y prioridad.
- Recomendaciones de corrección para el equipo de desarrollo.
- Reunión de presentación de resultados.

© Morini Computers SL · morinicomputers.com · Edición 2026

MAPT APLICACIONES

Mobile Application Penetration Test

La app iOS o Android bajo examen: en el dispositivo, en tránsito y en el backend.

QUÉ ES

Probamos una app móvil (iOS y/o Android) en todos los frentes: cómo trata y guarda los datos en el dispositivo, cómo se comunica con el servidor, y cómo resiste a quien la analiza o la modifica. Combinamos análisis estático (estudio de la app parada y del código) y dinámico (la app en ejecución en un dispositivo controlado). Buscamos datos guardados en claro, comunicaciones débiles, controles evitables y secretos mal escondidos dentro de la app.

CUÁNDO LO NECESITAS

- Publicas una app que gestiona inicio de sesión, datos personales o pagos.
- Lanzas una nueva app o una versión importante.
- Un cliente o una normativa exige una verificación de la app.
- La app guarda datos sensibles en el móvil o se comunica con un backend privado.
- Quieres saber cómo de fácil es extraer secretos o saltarse los controles de la app.

+ DENTRO DEL ALCANCE

- La app móvil (iOS y/o Android) en las versiones acordadas.
- Almacenamiento de datos en el dispositivo y gestión de secretos.
- Comunicación con el backend y robustez del canal.
- Resistencia a la ingeniería inversa y a la manipulación.

− FUERA DEL ALCANCE

- El backend y las API como prueba dedicada (ver API Penetration Test) salvo inclusión.
- Sistema operativo o dispositivo del fabricante fuera del control de la app.
- Apps de terceros integradas sin autorización.
- Pruebas de carga o de disponibilidad.

ENFOQUES

Análisis estático
Estudiamos la app parada: paquete, recursos, código, secretos escondidos.

Análisis dinámico
Ejecutamos la app en un dispositivo controlado y observamos su comportamiento en tiempo real.

Grey box
Con cuentas de prueba y documentación: cobertura más completa de los flujos.

© Morini Computers SL · morinicomputers.com · Edición 2026

MAPT · Mobile Application Penetration Test

METODOLOGÍA

01	**Reconocimiento**	Analizamos paquete, permisos, componentes y tecnologías de la app.
02	**Análisis estático**	Buscamos secretos, claves y lógica sensible en el código y en los recursos.
03	**Almacenamiento de datos**	Verificamos qué guarda la app en el dispositivo y cómo lo protege.
04	**Comunicación**	Probamos el canal con el servidor: cifrado, validación de certificados, datos en tránsito.
05	**Análisis dinámico**	Intentamos saltarnos controles y manipular la app en ejecución.
06	**Informe**	Documentamos cada fallo con prueba y corrección.

ESTÁNDARES DE REFERENCIA

- **OWASP MASVS** — requisitos de seguridad para apps móviles.
- **OWASP MASTG** — guía técnica para las pruebas móviles.
- **OWASP Mobile Top 10** — las categorías de riesgo más comunes.
- **PTES** — estructura de las fases.
- **CVSS v3.1/v4.0** — gravedad de las vulnerabilidades.

QUÉ RECIBES

- Informe con resumen y detalle técnico para iOS y/o Android.
- Prueba de cada fallo y pasos para reproducirlo.
- Puntuación CVSS y prioridad.
- Recomendaciones de corrección para el equipo de desarrollo.
- Reunión de presentación de resultados.

© Morini Computers SL · morinicomputers.com · Edición 2026

03 INALÁMBRICAS Y COMUNICACIONES

WIFI INALÁMBRICAS Y COMUNICACIONES

Wi-Fi Penetration Test

Cómo de sólida es tu red inalámbrica, vista por quien está dentro del alcance de la señal.

QUÉ ES

Probamos las redes Wi-Fi corporativas desde el punto de vista de quien está dentro del alcance de la señal, dentro o fuera del edificio. Verificamos cifrado y autenticación, intentamos acceder a las redes privadas, buscamos puntos de acceso no autorizados y comprobamos que la red de invitados esté realmente aislada de la corporativa. Incluye intentos de atraer a los usuarios hacia redes falsas para robar credenciales. Requiere presencia en la sede o cerca de ella.

CUÁNDO LO NECESITAS

- Tienes Wi-Fi corporativa y de invitados y quieres verificar su resistencia.
- Usas autenticación corporativa (802.1X/RADIUS) y quieres comprobar su robustez.
- Temes puntos de acceso no autorizados o redes falsas dentro del alcance de la oficina.
- Quieres confirmar que la red de invitados está aislada de la interna.
- Has renovado o ampliado la cobertura inalámbrica.

+ DENTRO DEL ALCANCE

- Las redes Wi-Fi (SSID) corporativas y de invitados acordadas.
- Cifrado y autenticación (WPA2/WPA3, 802.1X/RADIUS).
- Identificación de puntos de acceso no autorizados y redes falsas.
- Aislamiento entre la red de invitados y la red interna.

− FUERA DEL ALCANCE

- La red cableada interna más allá del punto de entrada inalámbrico (ver Internal Penetration Test).
- Redes Wi-Fi que no son propiedad del cliente.
- Ataques de interferencia de señal (jamming) que degradan el servicio.
- Dispositivos personales de los empleados sin autorización.

ENFOQUES

Red personal (PSK)
Verificamos la robustez de la clave compartida y la posibilidad de recuperarla.

Red corporativa (802.1X)
Probamos la autenticación RADIUS, la validación de certificados y los ataques a las credenciales.

Ingeniería social inalámbrica
Redes falsas y portales trampa para inducir a los usuarios a ceder sus credenciales, donde se acuerde.

© Morini Computers SL · morinicomputers.com · Edición 2026

WIFI · Wi-Fi Penetration Test

METODOLOGÍA

01	**Reconocimiento radio**	Detectamos las redes presentes, sus parámetros y los dispositivos conectados.
02	**Análisis de cifrado/autenticación**	Evaluamos protocolos y configuraciones de cada SSID.
03	**Ataque al acceso**	Intentamos acceder a las redes privadas (claves débiles, RADIUS, certificados).
04	**Puntos de acceso no autorizados y redes falsas**	Buscamos AP no autorizados y verificamos la reacción de los usuarios (si está en el alcance).
05	**Verificación del aislamiento**	Comprobamos que desde la red de invitados no se alcance la interna.
06	**Informe**	Documentamos cada debilidad con prueba y corrección.

ESTÁNDARES DE REFERENCIA

- **PTES** — estructura de las fases.
- **NIST SP 800-115** — método de prueba técnico, sección inalámbrica.
- **OSSTMM** — medición de los controles inalámbricos.
- **CVSS v3.1/v4.0** — gravedad de las vulnerabilidades.

QUÉ RECIBES

- Informe con el estado de cada red Wi-Fi examinada.
- Prueba de los accesos obtenidos y de las debilidades encontradas.
- Verificación del aislamiento entre invitados y red interna.
- Recomendaciones de corrección sobre cifrado, autenticación y configuración.
- Reunión de presentación de resultados.

© Morini Computers SL · morinicomputers.com · Edición 2026

VOIP INALÁMBRICAS Y COMUNICACIONES

VoIP Penetration Test

La centralita IP y los teléfonos: interceptación, fraudes y accesos no autorizados.

QUÉ ES

El teléfono de empresa hoy funciona sobre red IP, y eso abre nuevos riesgos: llamadas interceptables, fraudes de tráfico, centralitas alcanzables desde fuera, cuentas débiles. Probamos la infraestructura VoIP — centralita, teléfonos, gateway, protocolos de señalización — para encontrar posibles interceptaciones, accesos no autorizados, abusos de llamada y configuraciones débiles. Verificamos también que el tráfico de voz esté aislado del resto de la red como debería.

CUÁNDO LO NECESITAS

- Tienes una centralita VoIP, sobre todo si es alcanzable desde fuera.
- Temes fraudes telefónicos o llamadas a tarifas especiales a tu cargo.
- Quieres verificar que las conversaciones no sean interceptables.
- Tienes teléfonos remotos o teletrabajo que se conectan a la centralita.
- Has renovado o migrado el sistema de telefonía.

+ DENTRO DEL ALCANCE

- Centralita, gateway y teléfonos IP acordados.
- Protocolos de señalización y transporte de la voz.
- Autenticación de las extensiones y de las cuentas SIP.
- Aislamiento de la VLAN de voz respecto a la red de datos.

− FUERA DEL ALCANCE

- Red de datos general más allá de la infraestructura de voz (ver Internal Penetration Test).
- Servicios del operador telefónico fuera del control del cliente.
- Ataques que interrumpen el servicio telefónico.
- Equipos de terceros sin autorización.

ENFOQUES

Desde dentro

Conectados a la red, verificamos interceptación, acceso a las extensiones y aislamiento de la VLAN de voz.

Desde fuera

Si la centralita está expuesta, probamos accesos no autorizados y abusos de llamada desde Internet.

© Morini Computers SL · morinicomputers.com · Edición 2026

VOIP · VoIP Penetration Test

METODOLOGÍA

01	**Reconocimiento**	Identificamos centralita, teléfonos, gateway y servicios de voz activos.
02	**Enumeración de extensiones**	Buscamos cuentas SIP, extensiones y credenciales débiles.
03	**Interceptación**	Verificamos si la voz viaja en claro y si es capturable.
04	**Abuso y fraude**	Probamos accesos no autorizados y llamadas no permitidas, de forma controlada.
05	**Aislamiento de la VLAN de voz**	Comprobamos si desde la red de datos se alcanza el tráfico de voz y viceversa.
06	**Informe**	Documentamos cada debilidad con prueba y corrección.

ESTÁNDARES DE REFERENCIA

- **PTES** — estructura de las fases.
- **NIST SP 800-115** — método de prueba técnico.
- **OSSTMM** — medición de los controles sobre las comunicaciones.
- **CVSS v3.1/v4.0** — gravedad de las vulnerabilidades.

QUÉ RECIBES

- Informe sobre el estado de la infraestructura VoIP.
- Prueba de interceptaciones, accesos o abusos posibles.
- Verificación del aislamiento de la VLAN de voz.
- Recomendaciones de corrección sobre configuración y autenticación.
- Reunión de presentación de resultados.

© Morini Computers SL · morinicomputers.com · Edición 2026

04 DISPOSITIVOS E INDUSTRIA

IOT DISPOSITIVOS E INDUSTRIA

IoT Penetration Test

El dispositivo conectado al completo: hardware, firmware, comunicaciones, app y nube.

QUÉ ES

Los dispositivos conectados — cerraduras inteligentes, cámaras, sensores, equipos de gestión de edificios — son pequeños ordenadores, a menudo con defensas débiles. Probamos todo el ecosistema del dispositivo: el hardware y sus interfaces, el firmware, las comunicaciones radio y de red, la app y las API de gestión, hasta la nube del fabricante. Buscamos credenciales de fábrica, firmware extraíble, comunicaciones en claro e interfaces de depuración dejadas abiertas.

CUÁNDO LO NECESITAS

- Fabricas, integras o usas dispositivos conectados en la empresa.
- Quieres evaluar un dispositivo antes de adoptarlo a gran escala.
- Los dispositivos tratan datos sensibles o controlan accesos físicos.
- Debes cumplir requisitos de seguridad sobre productos conectados.
- Temes que un dispositivo pueda hacer de puente hacia la red corporativa.

+ DENTRO DEL ALCANCE

- Hardware del dispositivo e interfaces físicas (puertos de depuración, memorias).
- Firmware: extracción, análisis, credenciales y secretos.
- Comunicaciones radio y de red del dispositivo.
- App, API de gestión y, con autorización del fabricante, la nube.

− FUERA DEL ALCANCE

- Nube y servicios del fabricante sin autorización escrita del propietario.
- Red corporativa general más allá del dispositivo (ver Internal Penetration Test).
- Componentes hardware cuya apertura destruye el dispositivo, salvo acuerdo.
- Certificaciones formales de producto (no las emitimos).

ENFOQUES

Local
Sin la autorización del fabricante nos quedamos en el dispositivo, la app y las consolas de gestión locales, sin tocar la nube.

Completo
Con la autorización del fabricante incluimos también nube, API y app hasta el backend.

© Morini Computers SL · morinicomputers.com · Edición 2026

IOT · IoT Penetration Test

METODOLOGÍA

01	**Análisis de hardware**	Identificamos interfaces, puertos de depuración y memorias en el dispositivo.
02	**Análisis de firmware**	Extraemos y estudiamos el firmware: credenciales, claves, servicios, fallos.
03	**Comunicaciones**	Capturamos y analizamos el tráfico radio y de red, buscando datos en claro y manipulaciones.
04	**App y API de gestión**	Probamos las interfaces web y móvil que controlan el dispositivo.
05	**Nube (si está autorizada)**	Ampliamos la prueba al backend del fabricante.
06	**Informe**	Documentamos cada fallo a lo largo de toda la cadena con prueba y corrección.

ESTÁNDARES DE REFERENCIA

- **OWASP IoT Top 10** — las categorías de riesgo de los dispositivos conectados.
- **OWASP FSTM** — metodología de prueba del firmware.
- **PTES** — estructura de las fases.
- **CVSS v3.1/v4.0** — gravedad de las vulnerabilidades.

QUÉ RECIBES

- Informe sobre todo el ecosistema del dispositivo.
- Prueba de los fallos en hardware, firmware, comunicaciones y app.
- Puntuación CVSS y prioridad.
- Recomendaciones de corrección para el fabricante o el integrador.
- Reunión de presentación de resultados.

© Morini Computers SL · morinicomputers.com · Edición 2026

OT DISPOSITIVOS E INDUSTRIA

OT Penetration Test

Entornos industriales (PLC, SCADA, líneas de producción), probados con la máxima cautela.

QUÉ ES

En los entornos industriales la prioridad es la continuidad: una planta no se puede parar, y muchos equipos son frágiles y antiguos. Probamos las redes OT — PLC, SCADA, sistemas de control, protocolos industriales — con un enfoque prudente, priorizando el análisis pasivo y las pruebas acordadas, a menudo en entornos de pruebas. El objetivo es entender hasta dónde puede llegar un ataque a afectar la producción, sin ponerla nunca en riesgo durante la prueba.

CUÁNDO LO NECESITAS

- Tienes una red industrial (producción, energía, logística, automatización de edificios).
- Quieres verificar la separación entre la red de oficina (IT) y la red de planta (OT).
- Debes cumplir requisitos de seguridad para infraestructuras o instalaciones.
- Has conectado la OT a Internet o a proveedores externos para el mantenimiento.
- Temes que un ataque IT pueda propagarse hasta las instalaciones.

+ DENTRO DEL ALCANCE

- Red OT y equipos de control acordados (PLC, SCADA, HMI).
- Protocolos industriales en uso (p. ej., Modbus, OPC).
- Separación y puntos de contacto entre la red IT y la red OT.
- Accesos remotos de los proveedores hacia la instalación.

– FUERA DEL ALCANCE

- Pruebas intrusivas en equipos en producción sin entorno de pruebas.
- Cualquier acción que pueda parar o alterar la producción.
- Nube del fabricante sin autorización escrita del propietario.
- Cambios en la configuración de las instalaciones.

ENFOQUES

Pasivo

Escuchamos el tráfico sin interferir: el modo más seguro para instalaciones en producción.

Activo en pruebas

Pruebas más profundas en un entorno de test o en equipos fuera de línea, acordadas caso por caso.

Verificación de la segmentación

Nos centramos en los límites IT/OT y en los accesos remotos, donde está el mayor riesgo.

© Morini Computers SL · morinicomputers.com · Edición 2026

OT · OT Penetration Test

METODOLOGÍA

01	**Estudio del entorno**	Entendemos arquitectura, equipos críticos y restricciones de continuidad junto con el cliente.
02	**Análisis pasivo**	Observamos el tráfico industrial para mapear equipos, protocolos y flujos.
03	**Verificación de los límites**	Probamos la separación entre IT y OT y los accesos remotos de los proveedores.
04	**Pruebas acordadas**	Solo donde es seguro (pruebas o equipos fuera de línea) probamos la explotación controlada.
05	**Evaluación del impacto**	Estimamos hasta dónde podría llegar un ataque hacia la producción.
06	**Informe**	Documentamos los riesgos con prioridad y correcciones compatibles con la operativa.

ESTÁNDARES DE REFERENCIA

- **IEC 62443** — referencia para la seguridad de los sistemas de automatización industrial.
- **NIST SP 800-82** — directrices de seguridad para los sistemas de control industrial.
- **MITRE ATT&CK for ICS** — técnicas de ataque específicas de los entornos industriales.
- **CVSS v3.1/v4.0** — gravedad de las vulnerabilidades.

QUÉ RECIBES

- Informe sobre los riesgos del entorno OT, calibrado según la continuidad.
- Evaluación de la separación IT/OT y de los accesos remotos.
- Prioridad de intervención compatible con la operativa.
- Recomendaciones de corrección alineadas con los estándares industriales.
- Reunión de presentación de resultados.

© Morini Computers SL · morinicomputers.com · Edición 2026

CLOUD NUBE E IA

Cloud Penetration Test

El entorno cloud donde de verdad importa: permisos, configuraciones e identidades.

QUÉ ES

En la nube, la mayoría de los problemas no están en el software sino en la configuración: permisos demasiado amplios, almacenes expuestos, identidades y claves mal gestionadas. Analizamos tu entorno cloud — máquinas, almacenes, bases de datos, funciones, roles y permisos — para encontrar los caminos que llevan a un atacante a acceder a los datos o a tomar el control. Trabajamos dentro de las reglas del proveedor de cloud y nos centramos en lo que depende de ti.

CUÁNDO LO NECESITAS

- Has trasladado sistemas o datos a la nube y nunca los has hecho verificar.
- Gestionas muchas cuentas, roles y permisos y temes errores de configuración.
- Tienes almacenes, bases de datos o funciones potencialmente expuestos.
- Quieres verificar identidades, claves y accesos privilegiados en la nube.
- Un cliente o una normativa exige una verificación del entorno cloud.

+ DENTRO DEL ALCANCE

- Configuración de los servicios cloud acordados (cómputo, almacenamiento, bases de datos, funciones).
- Identidades, roles y permisos (quién puede hacer qué).
- Almacenes y datos potencialmente expuestos.
- Rutas de escalada de privilegios dentro del entorno.

− FUERA DEL ALCANCE

- La infraestructura del proveedor de cloud (fuera de tu control y de sus reglas).
- Aplicaciones alojadas como prueba dedicada (ver Web/API Penetration Test) salvo inclusión.
- Ataques que degradan los servicios.
- Tenants o cuentas de terceros sin autorización.

ENFOQUES

Revisión de la configuración
Con acceso de lectura al entorno, examinamos permisos y ajustes para encontrar los errores.

Assumed breach
Partimos de una identidad o una clave comprometida y vemos hasta dónde se llega.

Desde fuera
Buscamos recursos cloud expuestos y alcanzables desde Internet.

© Morini Computers SL · morinicomputers.com · Edición 2026

CLOUD · Cloud Penetration Test

METODOLOGÍA

01	**Inventario**	Mapeamos servicios, recursos, identidades y roles en uso en el entorno.
02	**Análisis de la configuración**	Comparamos los ajustes con las buenas prácticas para encontrar los errores.
03	**Identidad y permisos**	Verificamos roles, claves y permisos excesivos.
04	**Datos expuestos**	Buscamos almacenes y bases de datos accesibles más de lo debido.
05	**Escalada**	Probamos de forma controlada a pasar de un acceso limitado al control del entorno.
06	**Informe**	Documentamos cada fallo con prueba y corrección.

ESTÁNDARES DE REFERENCIA

- **CSA** — guía de la Cloud Security Alliance para las pruebas en cloud.
- **CIS Benchmarks** — referencia para las configuraciones seguras de los servicios cloud.
- **CVSS v3.1/v4.0** — gravedad de las vulnerabilidades.
- **MITRE ATT&CK** — técnicas de ataque para entornos cloud.
- **NIST SP 800-115** — método de prueba técnico.

QUÉ RECIBES

- Informe sobre la postura del entorno cloud.
- Lista de los errores de configuración y de los permisos de riesgo.
- Prueba de las rutas de acceso a los datos o de escalada.
- Recomendaciones de corrección alineadas con las buenas prácticas.
- Reunión de presentación de resultados.

© Morini Computers SL · morinicomputers.com · Edición 2026

AI NUBE E IA

Agentic AI & LLM Penetration Test

Asistentes y agentes basados en modelos de lenguaje: prompt injection, abuso de herramientas, fugas de datos.

QUÉ ES

Los chatbots, asistentes y agentes basados en modelos de lenguaje (LLM) introducen riesgos nuevos: el lenguaje natural se convierte en un canal de entrada no confiable, y un agente con herramientas y memoria puede realizar acciones reales en la empresa. Probamos toda la cadena — prompts y guardrails, recuperación de documentos (RAG), herramientas y plugins conectados, memoria, permisos — para demostrar impactos concretos: fugas de datos, acciones no autorizadas, escalada. No buscamos solo respuestas incorrectas del modelo.

CUÁNDO LO NECESITAS

- Has puesto en producción un chatbot o un asistente basado en LLM.
- El agente puede realizar acciones: enviar correos, abrir tickets, llamar a API, acceder a datos.
- Conectas el modelo a documentos internos mediante recuperación (RAG).
- Usas herramientas, plugins o servidores MCP que amplían el agente.
- Quieres saber qué puede hacer un usuario malintencionado que escribe al asistente.

+ DENTRO DEL ALCANCE

- Prompt de sistema, guardrails y filtros de entrada y de respuesta.
- Pipeline de recuperación de documentos (RAG) y sus fuentes de datos.
- Herramientas, plugins y servidores MCP conectados al agente.
- Memoria, modelo de identidad y permisos detrás de las acciones del agente.

− FUERA DEL ALCANCE

- El entrenamiento del modelo base y sus pesos (fuera de tu control).
- Infraestructura subyacente como prueba dedicada (ver Cloud Penetration Test) salvo inclusión.
- Servicios de modelos de terceros sin autorización.
- Evaluación de la calidad de las respuestas no relacionada con la seguridad.

ENFOQUES

Black box
Interactuamos con el asistente como un usuario cualquiera, sin conocer los detalles internos.

Grey box
Con documentación sobre prompts, herramientas y flujos: cobertura más completa de la cadena.

© Morini Computers SL · morinicomputers.com · Edición 2026

AI · Agentic AI & LLM Penetration Test

METODOLOGÍA

01	**Análisis del stack**	Reconstruimos prompts, guardrails, herramientas, memoria, RAG y permisos del agente.
02	**Prompt injection y jailbreak**	Intentamos saltarnos las instrucciones y los filtros con entradas construidas a propósito.
03	**Abuso de herramientas**	Verificamos si se puede inducir al agente a realizar acciones no autorizadas.
04	**RAG y memoria**	Buscamos fugas de datos y envenenamiento a través de documentos y memoria.
05	**Encadenamiento**	Unimos los fallos hasta un impacto concreto: fuga de datos, acción o escalada.
06	**Informe**	Documentamos cada cadena de ataque con prueba y corrección.

ESTÁNDARES DE REFERENCIA

- **OWASP Top 10 for LLM Applications** — las categorías de riesgo de las aplicaciones LLM.
- **MITRE ATLAS** — técnicas de ataque a los sistemas de inteligencia artificial.
- **OWASP Agentic AI** — amenazas y mitigaciones específicas de los agentes.
- **NIST AI RMF** — marco de gestión del riesgo para la IA.
- **PTES** — estructura de las fases de la prueba.

QUÉ RECIBES

- Informe sobre las cadenas de ataque al asistente o al agente.
- Prueba de fugas de datos, acciones no autorizadas o escaladas.
- Evaluación de guardrails, RAG, herramientas y permisos.
- Recomendaciones de corrección sobre prompts, controles y límites del agente.
- Reunión de presentación de resultados.

© Morini Computers SL · morinicomputers.com · Edición 2026

06 SEGUIMIENTO

RETEST SEGUIMIENTO

Remediation Retest

Verifica que las correcciones hayan cerrado de verdad las vulnerabilidades encontradas.

QUÉ ES

Después de una prueba, recibes una lista de vulnerabilidades y las corriges. El remediation retest vuelve a verificar, una por una, que las correcciones hayan cerrado de verdad el problema y no hayan abierto otros. Repasamos los resultados del informe original con el mismo método con el que los encontramos y actualizamos el estado de cada uno: cerrado, aún abierto o parcialmente resuelto. Cierra el ciclo y te da una prueba documentada de los avances.

CUÁNDO LO NECESITAS

- Has corregido las vulnerabilidades de una prueba anterior y quieres confirmación de que están cerradas.
- Debes demostrar a un cliente, a un auditor o a una aseguradora que los problemas están resueltos.
- Quieres una prueba documentada de la mejora de la postura de seguridad.
- Antes de volver a poner en producción un sistema corregido.
- Como paso final de un ciclo de prueba y corrección.

+ DENTRO DEL ALCANCE

- Las vulnerabilidades enumeradas en un informe de prueba anterior.
- Verificación de la eficacia de cada corrección aplicada.
- Comprobación de que la corrección no haya introducido nuevos problemas evidentes en el mismo punto.
- Actualización del estado de cada resultado.

– FUERA DEL ALCANCE

- Una nueva prueba completa o el análisis de áreas no cubiertas por el informe original.
- Vulnerabilidades en sistemas añadidos después de la prueba inicial.
- Corrección de las vulnerabilidades (sigue a cargo del cliente).
- Búsqueda exploratoria de fallos nuevos no relacionados con los anteriores.

ENFOQUES

Dirigido
Reverificamos solo las vulnerabilidades del informe original, con el mismo método con el que fueron encontradas.

© Morini Computers SL · morinicomputers.com · Edición 2026

RETEST · Remediation Retest

METODOLOGÍA

01	**Revisión del informe**	Retomamos la lista de vulnerabilidades y de las correcciones declaradas.
02	**Reverificación**	Volvemos a ejecutar la prueba sobre cada resultado para confirmar su estado actual.
03	**Actualización de estado**	Marcamos cada entrada como cerrada, abierta o parcialmente resuelta.
04	**Informe actualizado**	Entregamos la comparación entre el estado inicial y el estado tras las correcciones.

ESTÁNDARES DE REFERENCIA

CVSS v3.1/v4.0 recálculo de la gravedad residual tras la corrección.

PTES mismo método de la prueba original para la reverificación.

QUÉ RECIBES

- Informe de retest con el estado actualizado de cada vulnerabilidad.
- Comparación entre la situación inicial y la situación tras las correcciones.
- Prueba actualizada para las entradas aún abiertas.
- Indicación de las correcciones aún por completar.
- Documento utilizable frente a clientes o auditores.

© Morini Computers SL · morinicomputers.com · Edición 2026

MORINI COMPUTERS SL

Qué pedimos al cliente

01 Un interlocutor localizable durante toda la duración de la prueba, para las decisiones y las emergencias.

02 Autorización firmada antes de empezar: sin el documento de contratación no tocamos nada.

03 Sistemas y equipos dentro del alcance encendidos y operativos en la ventana acordada.

04 Accesos, credenciales de prueba, documentación o cuentas que el tipo de prueba requiera, entregados en los plazos establecidos.

05 Cuando un sistema dentro del alcance está gestionado o alojado por terceros, la autorización escrita del propietario antes de probarlo.

06 Una copia de seguridad reciente y verificada de los sistemas delicados, antes de pruebas que puedan afectar a la disponibilidad.

07 Respuesta y confirmación sobre los documentos entregados en plazos razonables, para poder planificar el eventual retest.

08 La corrección de las vulnerabilidades sigue a cargo del cliente o de sus proveedores: nosotros las identificamos, las explicamos y luego las reverificamos.

HABLEMOS

Habla con nosotros sobre tu proyecto

Cuéntanos qué quieres proteger y cuáles son tus preocupaciones. Definimos juntos el alcance adecuado y te proponemos el camino más adecuado, sin vender más de lo que necesitas.

E-MAIL
info@morinicomputers.com

TEL.
+34 612 491 394

WEB
morinicomputers.com

© Morini Computers SL · morinicomputers.com · Edición 2026