

Servicios de ciberseguridad

Pentesting como servicio, seguridad ofensiva, inteligencia, respuesta ante incidentes y protección de entornos cloud, gestionados desde nuestras propias plataformas: DARKFORGE y TORO.



Anticiparse a las amenazas es la mejor defensa.

Jaquers Ciberseguridad es una empresa especializada en la protección de sistemas de información y la mitigación de riesgos digitales. Trabajamos desde la perspectiva del atacante para encontrar antes que nadie las debilidades que un adversario real explotaría, y acompañamos a nuestros clientes en la respuesta ante incidentes, el análisis forense y el cumplimiento normativo.

Perspectiva ofensiva

Simulamos ataques reales, con técnicas actuales y explotación controlada, no solo escaneos automáticos.

Evidencias que resisten

Cada hallazgo se documenta con evidencia reproducible y, cuando procede, con validez legal.

Visibilidad continua

DARKFORGE sigue cada proyecto en tiempo real; TORO vigila su superficie de ataque y las amenazas que le afectan.

Proyectos

Trabajos con un alcance, un calendario y un informe final, pensados para responder a una pregunta concreta.

- Pentesting externo e interno
- Auditorías de código, nube y Microsoft 365
- Simulacros y análisis forense

OF-01 a OF-05 · IR-01 a IR-04 · CL-01 y CL-02

Servicios continuos

Vigilancia y entrenamiento recurrentes, con resultados siempre disponibles en DARKFORGE y TORO.

- PTaaS: pentesting como servicio, nuestro servicio estrella
- Descubrimiento continuo de superficie de ataque
- Campañas periódicas de simulación de phishing

PT-01 · OF-06 · OF-05 · Programas combinados (pág. 17)



Dos plataformas propias. DARKFORGE es el espacio privado de cada cliente para seguir sus proyectos en tiempo real, consultar evidencias y descargar los informes (pág. 18). TORO, Threat Observation & Risk Operations, es la plataforma sobre la que prestamos la ciberinteligencia y la vigilancia de la superficie de ataque (pág. 19).

Mapa de servicios

Un servicio estrella, doce servicios en tres familias y las dos plataformas que los sostienen. Cada servicio tiene un código para referenciarlo en propuestas y programas.

Servicio estrella

Páginas 4–8

PT-01	PTaaS · Pentesting como servicio	Pentesting continuo desde DARKFORGE, con retest ilimitado y cuota fija.	4
-------	----------------------------------	---	---

Seguridad ofensiva

Páginas 9–12

OF-01	Pentesting externo	Ataques reales simulados desde Internet.	9
OF-02	Pentesting interno	Qué ocurre cuando el atacante ya está dentro de la red corporativa.	10
OF-03	Auditoría de código	Revisión de seguridad del código antes de producción.	10
OF-04	Simulacro Man in the Middle	Interceptación y suplantación de comunicaciones.	11
OF-05	Simulación de phishing	Campañas simuladas para medir y entrenar al factor humano.	11
OF-06	Descubrimiento continuo de superficie de ataque	Vigilancia permanente de los activos expuestos a Internet.	12

Inteligencia y respuesta

Páginas 13–15

IR-01	Análisis forense digital	Investigación del origen, la naturaleza y el impacto de un ataque.	13
IR-02	Análisis forense de correo y phishing	Correos fraudulentos y postura antisuplantación del dominio.	14
IR-03	Ciberinteligencia OSINT	Exposición digital de la empresa y de sus directivos.	14
IR-04	Respuesta ante incidentes y retirada de fraudes	Contención del incidente y takedown de dominios fraudulentos.	15

Nube y puesto de trabajo digital

Páginas 16–17

CL-01	Seguridad en la nube	Auditoría y configuración segura de AWS, Azure y Google Cloud.	16
CL-02	Seguridad en Microsoft 365	Correo, SharePoint, OneDrive y Teams protegidos.	17

Plataforma y método

Páginas 18–22

DF	Plataforma DARKFORGE	Portal privado: hallazgos, evidencias, informes y remediación.	18
TO	Plataforma TORO	Ciberinteligencia y superficie de ataque: observación continua y riesgos priorizados.	19
—	Cómo trabajamos	Metodología paso a paso y escala de severidad.	20
—	Marcos, cumplimiento y garantías	Estándares, normativa y qué recibe al final de cada proyecto.	21
—	Glosario	Los términos técnicos del catálogo, explicados en una línea.	22

PTaaS

Pentesting como servicio

Un pentesting no debería ser la foto de un solo día al año. PTaaS convierte las pruebas de intrusión en un servicio continuo: su infraestructura y sus aplicaciones se prueban de forma recurrente, cada hallazgo llega al portal en cuanto se valida y cada corrección se verifica sin esperar al siguiente proyecto.

Pensado para organizaciones que despliegan cambios con frecuencia, que necesitan evidencia continua para auditorías (ISO 27001, ENS, NIS2, DORA) o que no cuentan con un equipo de seguridad ofensiva propio.

Pruebas continuas

Ciclos programados y pruebas bajo demanda ante cada versión, migración o cambio relevante.

Hallazgos en tiempo real

Cada vulnerabilidad aparece en DARKFORGE en cuanto se confirma, con evidencia y recomendación.

Retest ilimitado

Verificamos cada corrección cuando su equipo la tiene lista, tantas veces como haga falta.

Coste predecible

Cuota mensual fija y alcance revisable cada trimestre, sin presupuestos proyecto a proyecto.

Pentesting puntual frente a PTaaS

	Pentesting puntual	PTaaS
Frecuencia	Una vez al año, o después de un incidente	■ Continua: ciclos programados y pruebas bajo demanda
Resultados	Un informe al cerrar el proyecto	■ En el portal, en cuanto cada hallazgo se valida
Retest	Uno, al final del proyecto	■ Ilimitado, cuando su equipo tiene lista la corrección
Cambios y nuevas versiones	Sin probar hasta el siguiente pentesting	■ Se prueban como parte del servicio
Conocimiento del entorno	Se parte de cero en cada proyecto	■ Equipo estable que conoce su infraestructura
Evidencia para auditorías	Puntual; envejece en pocos meses	■ Continua, con histórico y trazabilidad
Presupuesto	Por proyecto, cada vez	■ Cuota mensual fija, alcance revisable

Cómo funciona

Un arranque rápido, una línea de base clara y, a partir de ahí, un ciclo que no se detiene.

- 1 Onboarding** *Semanas 1-2*
Definimos el alcance, los activos, las ventanas horarias y las reglas de compromiso. Damos de alta su espacio en DARKFORGE y, si hay alcance interno, conectamos la sonda.
- 2 Pentest base** *Semanas 3-6*
Pentesting completo de todo el alcance para fijar la línea de base: inventario de activos, hallazgos iniciales y primer valor del Cyber Security Risk Meter.
- 3 Ciclos continuos** *Desde el mes 2*
Pruebas programadas según el plan, descubrimiento continuo de la superficie de ataque en TORO y pruebas bajo demanda ante cada versión, migración o cambio relevante.
- 4 Retest y seguimiento** *En cualquier momento*
Cada corrección se verifica cuando su equipo la tiene lista, sin límite de veces. El estado de cada hallazgo se actualiza en el portal.
- 5 Revisión trimestral** *Cada tres meses*
Informe ejecutivo, reunión con dirección y ajuste del alcance: se incorporan los activos nuevos y se retiran los que ya no existen.
- 6 Cierre anual** *Mes 12*
Informe anual con la evolución completa, comparación con la línea de base y plan para el siguiente ejercicio.

Qué puede entrar en el alcance

El alcance se define en el onboarding y se revisa cada trimestre. Puede combinar cualquiera de estos activos:

- Aplicaciones web y APIs
- Infraestructura expuesta a Internet
- Red interna y Directorio Activo
- Entornos cloud (AWS, Azure, Google Cloud)
- Microsoft 365
- Aplicaciones móviles
- Redes WiFi
- Código fuente

Qué incluye y planes

Pruebas

- Pentest base completo al inicio del servicio
- Ciclos de pentesting externo según el plan
- Pruebas bajo demanda ante cambios y nuevas versiones
- Descubrimiento continuo de superficie de ataque en TORO
- Pentesting interno, phishing, nube y M365 según el plan

Plataforma y seguimiento

- Espacio privado en DARKFORGE con app móvil
- Hallazgos en tiempo real con evidencia y recomendación
- Estado de cada hallazgo y retest ilimitado
- Interlocutor técnico asignado y canal directo
- Reuniones de seguimiento periódicas

Informes y evidencias

- Informe por hallazgo, exportable en PDF y Word
- Informe ejecutivo periódico para dirección
- Informe anual con evolución y línea de base
- Evidencias con histórico para auditorías
- Notificación prioritaria de hallazgos críticos

Tres planes, una misma base

Todos incluyen el pentest inicial, el portal DARKFORGE, el retest ilimitado y la notificación de críticos en menos de 24 horas. La diferencia está en la cadencia y en los servicios que se incorporan.

	Esencial	Avanzado Recomendado	Integral
Incluye	Cobertura externa continua	Perímetro, red interna y factor humano	Toda la organización, cada mes
Ciclos de pentesting externo	Semestral	Trimestral	Mensual
Descubrimiento continuo de superficie de ataque (TORO)	Mensual	Semanal	Semanal
Pruebas bajo demanda ante cambios y versiones	2 al año	6 al año	Sin límite*
Pentesting interno con sonda	—	Anual	Semestral
Simulación de phishing	—	Semestral	Trimestral
Auditoría de nube y Microsoft 365	—	Anual	Semestral
Auditoría de código	—	—	Por versión mayor
Retest de hallazgos	Ilimitado	Ilimitado	Ilimitado
Notificación de hallazgos críticos	≤ 24 h	≤ 24 h	≤ 24 h
Informe ejecutivo	Semestral	Trimestral	Mensual
Reunión de seguimiento	Trimestral	Mensual	Quincenal

* Dentro del alcance contratado y con planificación previa. Todos los planes se contratan por suscripción anual con facturación mensual o trimestral; el alcance se revisa cada trimestre y los cambios se reflejan en la cuota del periodo siguiente.

Compromisos y calendario

Compromisos de servicio

Lo que puede exigirnos por contrato, en todos los planes.

Hallazgos críticos	Notificación en menos de 24 horas desde su confirmación: portal, correo y llamada al contacto designado.	Hallazgos altos	Notificación en menos de 72 horas, con evidencia y recomendación provisional.
Retest	Inicio en un máximo de 5 días laborables desde la solicitud en el portal.	Pruebas bajo demanda	Planificación en un máximo de 10 días laborables desde la solicitud.
Informes	Informe ejecutivo en los 10 primeros días del periodo siguiente; informe anual en el mes 12.	Consultas	Respuesta del interlocutor técnico en menos de un día laborable.
Pausa de las pruebas	Puede detener cualquier prueba en curso con un simple aviso, sin coste ni penalización.		

Un año de PTaaS

Ejemplo de calendario para el plan Avanzado. El calendario real se acuerda en el onboarding y se ajusta en cada revisión trimestral.

	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
Onboarding	●											
Pentest base	■	■										
Ciclos de pentesting externo					●			●			●	
Descubrimiento continuo de superficie		■	■	■	■	■	■	■	■	■	■	■
Pruebas bajo demanda y retest		■	■	■	■	■	■	■	■	■	■	■
Pentesting interno con sonda				●								
Simulación de phishing			●						●			
Auditoría de nube y Microsoft 365						●						
Informe ejecutivo y revisión de alcance			●			●			●			●
Informe anual												●

Empezar con PTaaS

1. Sesión de alcance

Una reunión de 60 minutos para inventariar activos, entender su ritmo de cambios y elegir el plan.

2. Propuesta con plan y cuota

Alcance detallado, calendario del primer año y cuota mensual cerrada, sin sorpresas.

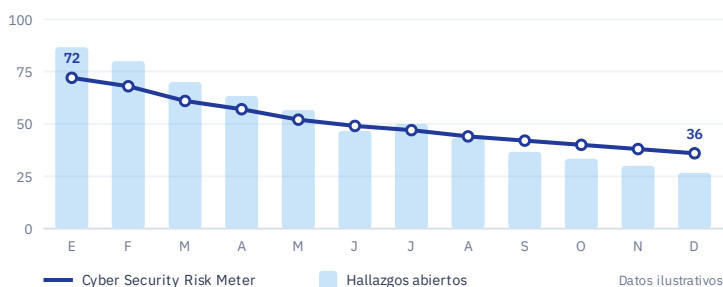
3. Onboarding en dos semanas

Alta en DARKFORGE, reglas de compromiso firmadas y arranque del pentest base.

Métricas y preguntas frecuentes

Lo que verá cada mes

El informe periódico y los paneles de DARKFORGE y TORO responden a la misma pregunta desde dos ángulos: ¿estamos mejor que el mes pasado y dónde no?



Hallazgos abiertos

Por severidad y antigüedad.

Tiempo medio de remediación

Cuánto tarda su equipo en corregir, por severidad.

Cobertura

Activos en alcance frente a activos descubiertos.

Risk Meter

Evolución mensual frente a la línea de base.

Regresiones

Hallazgos que reaparecen tras un retest.

Superficie de ataque

Altas y bajas de activos detectadas por TORO.

Para quién es PTaaS

Desarrollo continuo

Empresas con software propio y despliegues frecuentes que no pueden esperar al pentesting anual.

Entornos regulados

Organizaciones bajo ISO 27001, ENS, NIS2 o DORA que necesitan evidencia continua y trazable.

Sin equipo ofensivo propio

Organizaciones que quieren un equipo estable que conozca su infraestructura, a coste fijo.

Proveedores y cadena de suministro

Empresas que deben demostrar su seguridad a clientes y auditores de terceros.

Preguntas frecuentes

¿Sustituye al pentesting anual?

Sí. El pentest base equivale a un pentesting completo y los ciclos posteriores mantienen viva esa cobertura. El informe anual documenta todo el ejercicio.

¿Sirven los resultados para ISO 27001, NIS2 o DORA?

Sí. Cada hallazgo conserva evidencia, fechas, responsable y estado, y tanto los informes como cada hallazgo se exportan en PDF y Word como evidencia de control o para su gestor de tickets.

¿Afecta a la operativa?

Igual que en cualquier pentesting: ventanas acordadas, sin denegación de servicio, contacto de emergencia y posibilidad de pausar las pruebas en cualquier momento.

¿Quién realiza las pruebas?

Un equipo estable asignado a su cuenta, con un interlocutor técnico fijo. Los mismos analistas ciclo tras ciclo, para no perder el conocimiento del entorno.

¿Qué ocurre cuando desplegamos una versión nueva?

Se solicita una prueba bajo demanda desde el portal o por el canal directo. Se planifica dentro del plazo comprometido y los resultados se incorporan al histórico.

¿Se puede ampliar o reducir el alcance?

Sí, en cada revisión trimestral. Los cambios se reflejan en la cuota del periodo siguiente.

¿Y si ya tenemos un pentesting reciente?

Lo incorporamos como línea de base: importamos sus hallazgos a DARKFORGE y el servicio arranca directamente con los ciclos continuos y el retest.

¿Cómo se gestionan las credenciales de prueba?

Se crean específicamente para el servicio, se custodian cifradas y se revocan al terminar cada ciclo. Nunca se reutilizan credenciales reales de usuarios.

Seguridad ofensiva

Pensamos y actuamos como lo haría un atacante real, con reglas de compromiso claras y explotación controlada. El objetivo no es un listado de vulnerabilidades, sino saber qué podría pasar de verdad en su organización y qué hay que corregir primero.

Servicios de esta familia

- OF-01 Pentesting externo
- OF-02 Pentesting interno
- OF-03 Auditoría de código
- OF-04 Simulacro Man in the Middle
- OF-05 Simulación de phishing
- OF-06 Descubrimiento continuo de superficie de ataque

OF-01

Pentesting externo



Lo que un atacante vería —y conseguiría— desde Internet.

Evaluación de seguridad que simula ataques reales desde el exterior de la organización. Analizamos redes, aplicaciones web, APIs y servidores expuestos a Internet, identificando debilidades en firewalls, configuraciones erróneas y vulnerabilidades explotables que podrían ser utilizadas por atacantes.

Cada hallazgo se valida manualmente y se documenta con evidencia reproducible, acompañado de recomendaciones concretas para mejorar la postura de seguridad de la empresa.

Qué incluye

- Reconocimiento y mapeo de la superficie expuesta
- Análisis de vulnerabilidades con validación manual
- Explotación controlada, sin denegación de servicio
- Revisión de aplicaciones web y APIs (OWASP Top 10)
- Plan de remediación priorizado por riesgo

Entregables

- Informe ejecutivo
- Informe técnico
- Sesión de presentación de resultados
- Retest de hallazgos

Datos clave

Modalidad
Remoto

Enfoque
Caja negra o caja gris

Marco
OWASP WSTG, PTES

Recomendado
Anual

Caja negra, caja gris o caja blanca

El enfoque determina cuánta información recibe el equipo antes de empezar. Recomendamos caja gris para la mayoría de los pentestings web e internos: más profundidad en menos tiempo.

Caja negra

Sin información previa. Reproduce fielmente a un atacante externo que parte de cero.

Caja gris

Con credenciales o información parcial. Permite llegar más lejos y evaluar el riesgo de un usuario legítimo.

Caja blanca

Con acceso completo a código, arquitectura y configuraciones. Máxima cobertura para sistemas críticos.

OF-02

Pentesting interno



Qué ocurre cuando el atacante ya está dentro.

Simula un ataque desde dentro de la red corporativa, asumiendo que un atacante ha logrado acceso a la infraestructura interna: un portátil comprometido, un empleado malintencionado o un dispositivo conectado sin control. Evaluamos servidores, estaciones de trabajo, dispositivos de red, Directorio Activo y permisos de acceso, además de la segmentación de la red y la efectividad del control de privilegios, para minimizar el riesgo de movimientos laterales.

Se realiza íntegramente en remoto, mediante conexión a un equipo de la organización o con nuestro hardware propio, que nos ofrece visibilidad completa de la infraestructura interna.

Qué incluye

- Enumeración de la red interna y del Directorio Activo
- Escalada de privilegios y movimiento lateral controlado
- Revisión de segmentación y políticas de control de acceso
- Análisis de puestos, servidores y dispositivos de red
- Recomendaciones para reforzar la seguridad interna

Entregables

- Informe ejecutivo
- Informe técnico
- Sesión de presentación de resultados
- Retest de hallazgos

Datos clave

Modalidad
100 % remoto, con sonda propia o equipo del cliente

Marco
PTES, MITRE ATT&CK

Recomendado
Anual

OF-03

Auditoría de código



Vulnerabilidades detectadas antes de llegar a producción.

Revisión de seguridad del código fuente de aplicaciones y servicios, combinando análisis automatizado con revisión manual de las partes críticas: autenticación, gestión de sesiones, tratamiento de datos de entrada, criptografía y control de acceso.

Detectamos secretos y credenciales embebidas, dependencias vulnerables y patrones inseguros, con recomendaciones específicas y ejemplos de corrección para el equipo de desarrollo.

Qué incluye

- Análisis estático del código y de sus dependencias
- Detección de secretos, claves y credenciales embebidas
- Revisión manual de los flujos críticos
- Recomendación de corrección por hallazgo, con ejemplos

Entregables

- Informe técnico con hallazgos por fichero y línea
- Sesión con el equipo de desarrollo
- Retest sobre la versión corregida

Datos clave

Modalidad
Remoto

Ámbito
Aplicaciones web, backend, móvil

Marco
OWASP ASVS, CWE Top 25

Recomendado
Antes de cada versión mayor

OF-04

Simulacro Man in the Middle



¿Puede alguien escuchar —o alterar— las comunicaciones de su empresa?

Los ataques Man in the Middle (MitM) siguen siendo una de las amenazas más comunes en las redes empresariales. Realizamos simulaciones controladas para evaluar la vulnerabilidad de las comunicaciones ante este tipo de ataques: seguridad de las conexiones WiFi, protocolos de autenticación y cifrado de datos.

El informe incluye soluciones concretas para mitigar los riesgos, como la implementación de VPN, el uso de certificados digitales y el refuerzo de las políticas de seguridad.

Qué incluye

- Auditoría de redes WiFi corporativas y de invitados
- Pruebas de interceptación de tráfico y suplantación de servicios
- Revisión de protocolos de autenticación y cifrado
- Medidas de mitigación: VPN, certificados y políticas

Entregables

- Informe técnico
- Guía de mitigación
- Sesión de presentación de resultados

Datos clave

Modalidad
On-site o remoto con sonda

Marco
PTES, buenas prácticas del fabricante

Recomendado
Anual o tras cambios en la red

OF-05

Simulación de phishing



El factor humano, medido y entrenado.

El phishing sigue siendo una de las principales amenazas para las empresas porque explota el factor humano. Diseñamos campañas de phishing simuladas para evaluar la concienciación y la preparación de los empleados: enviamos correos y mensajes que replican las técnicas reales de los ciberdelincuentes y analizamos la tasa de apertura, de clic y de entrega de credenciales.

Después, proporcionamos formación y capacitación para mejorar la cultura de seguridad, reducir los riesgos y evitar incidentes reales.

Qué incluye

- Diseño de escenarios adaptados a la empresa
- Campañas por correo electrónico y mensajería
- Métricas por departamento: apertura, clic y credenciales
- Formación de concienciación posterior

Entregables

- Informe de resultados con métricas
- Sesión de concienciación
- Material formativo

Datos clave

Modalidad
Remoto

Opcional
Vishing y smishing

Recomendado
Trimestral o semestral

OF-06



Descubrimiento continuo de superficie de ataque

Su exposición cambia cada semana. Nosotros la vigilamos.

Un pentesting es una fotografía; la superficie de ataque es una película. Este servicio recurrente identifica de forma periódica todos los recursos expuestos de la organización —dominios, subdominios, direcciones IP, servicios, certificados y aplicaciones—, tanto los proporcionados por la organización como los descubiertos durante la fase de reconocimiento.

Cada nuevo activo o cambio relevante se analiza y se notifica, y el estado completo puede consultarse en cualquier momento en TORO, nuestra plataforma de observación de amenazas y superficie de ataque.

Qué incluye

- Inventario de activos expuestos y shadow IT
- Detección de nuevos dominios, servicios y puertos
- Vigilancia de certificados, tecnologías y versiones vulnerables
- Alertas ante cambios y exposiciones críticas

Entregables

- Panel de superficie de ataque en TORO
- Alertas ante cambios
- Informe periódico de exposición

Datos clave

Modalidad
Servicio continuo

Plataforma
TORO

Frecuencia
Semanal o mensual

Complementa
OF-01 Pentesting externo

Un ciclo que no se detiene

Cada iteración descubre los activos expuestos, analiza los cambios frente a la iteración anterior, notifica lo relevante —un subdominio nuevo, un puerto abierto, un certificado caducado— y verifica que lo notificado se ha atendido.

El inventario completo, con su histórico, está siempre disponible en TORO, y sirve de punto de partida para el siguiente pentesting externo.



Qué vigilamos

Dominios y subdominios

Registros nuevos, olvidados o caducados, y subdominios que apuntan a servicios ya retirados.

Direcciones IP y servicios

Rangos propios y de proveedores, puertos abiertos y servicios expuestos con su versión.

Certificados y tecnologías

Certificados a punto de caducar, configuraciones TLS débiles y componentes con vulnerabilidades conocidas.

Inteligencia y respuesta

Cuando algo ya ha ocurrido —o podría estar ocurriendo— lo importante es entenderlo con rigor: qué pasó, cómo, qué impacto tiene y cómo evitar que se repita. Trabajamos con evidencias trazables y, cuando se requiere, con validez legal.

Servicios de esta familia

- IR-01 Análisis forense digital
- IR-02 Análisis forense de correo y phishing
- IR-03 Ciberinteligencia OSINT
- IR-04 Respuesta ante incidentes y retirada de fraudes

IR-01

Análisis forense digital



Qué pasó, cómo y con qué impacto, con evidencias que resisten.

El análisis forense digital es clave en la respuesta ante incidentes. Realizamos investigaciones exhaustivas para identificar el origen, la naturaleza y el impacto de un ataque informático, utilizando herramientas avanzadas para recuperar datos eliminados, analizar registros del sistema y extraer evidencias digitales con validez legal.

Determinamos si ha existido acceso no autorizado, robo de información o alteraciones en los sistemas, y entregamos informes detallados con recomendaciones para fortalecer la seguridad.

Qué incluye

- Adquisición de evidencias con cadena de custodia
- Análisis de discos, memoria, registros y artefactos
- Reconstrucción de la línea temporal del incidente
- Recuperación de información eliminada

Entregables

- Informe pericial
- Línea temporal del incidente
- Recomendaciones de refuerzo

Datos clave

Modalidad
Remoto u on-site

Ámbito
Servidores, puestos, móviles y nube

Disponibilidad
Bajo demanda

Cuándo activar un análisis forense

Señales habituales

- Sospecha de acceso no autorizado a sistemas o cuentas
- Fuga, robo o cifrado de información
- Fraude interno o uso indebido de los sistemas
- Necesidad de evidencias para un procedimiento legal o un seguro

Mientras nos avisa

- No apague ni reinicie el equipo afectado
- No lo formatee, reinstale ni ejecute limpiezas
- Limite el acceso al mínimo imprescindible
- Anote quién ha hecho qué y cuándo

IR-02



Análisis forense de correo y phishing

Cada correo sospechoso, analizado hasta el último encabezado.

Analizamos en profundidad los correos electrónicos sospechosos o fraudulentos recibidos por la organización: cabeceras completas, autenticación SPF, DKIM y DMARC, dominios, direcciones IP y servidores implicados, enlaces y adjuntos.

Verificamos también la postura del propio dominio de la empresa frente a la suplantación y entregamos un informe útil tanto para tomar decisiones técnicas como para documentar el incidente ante terceros.

Qué incluye

- Análisis de cabeceras y verificación SPF, DKIM y DMARC
- Investigación de dominios, IP y servidores implicados
- Análisis de enlaces y adjuntos maliciosos
- Auditoría antissuplantación del dominio propio

Entregables

- Informe forense en PDF o Word
- Indicadores de compromiso
- Recomendaciones

Datos clave

Modalidad
Remoto

Plataforma
Módulo forense de DARKFORGE

Complementa
IR-04 y CL-02

IR-03



Ciberinteligencia OSINT

Lo que Internet ya sabe de su empresa, antes de que lo use un atacante.

La ciberinteligencia basada en fuentes abiertas (OSINT) nos permite recolectar y analizar información pública relevante sobre organizaciones, personas y posibles amenazas. Con técnicas especializadas y herramientas avanzadas identificamos vulnerabilidades expuestas, fugas de datos, credenciales filtradas y riesgos reputacionales.

Es el servicio ideal para prevenir ataques dirigidos, monitorizar amenazas emergentes y evaluar la exposición digital de una empresa o de sus directivos. Todo el proceso se apoya en TORO (Threat Observation & Risk Operations), nuestra plataforma de ciberinteligencia, que mantiene la vigilancia activa entre un informe y el siguiente.

Qué incluye

- Huella digital de la organización y de personas clave
- Credenciales y datos filtrados en brechas y foros
- Dominios similares y suplantaciones de marca
- Riesgos reputacionales y de ingeniería social

Entregables

- Informe de exposición
- Acceso al panel de inteligencia en TORO
- Recomendaciones de reducción de huella

Datos clave

Modalidad
Remoto

Plataforma
TORO

Recomendado
Anual o previo a un pentesting

IR-04

Respuesta ante incidentes y retirada de fraudes



Contención rápida, comunicación clara y cierre documentado.

Acompañamos a la organización durante un incidente de seguridad: contención, erradicación y recuperación, con criterios claros de priorización y una comunicación comprensible para la dirección.

Gestionamos además la retirada (takedown) de dominios, webs y perfiles fraudulentos que suplantan a la empresa, coordinándonos con registradores, proveedores de alojamiento y organismos como INCIBE-CERT, y elaboramos la documentación necesaria para las notificaciones obligatorias.

Qué incluye

- Triage, contención y erradicación
- Takedown de dominios y sitios fraudulentos
- Coordinación con INCIBE-CERT, proveedores y registradores
- Apoyo en las notificaciones regulatorias (RGPD, NIS2, DORA)

Entregables

- Informe de incidente
- Dossier de evidencias
- Informe de cierre

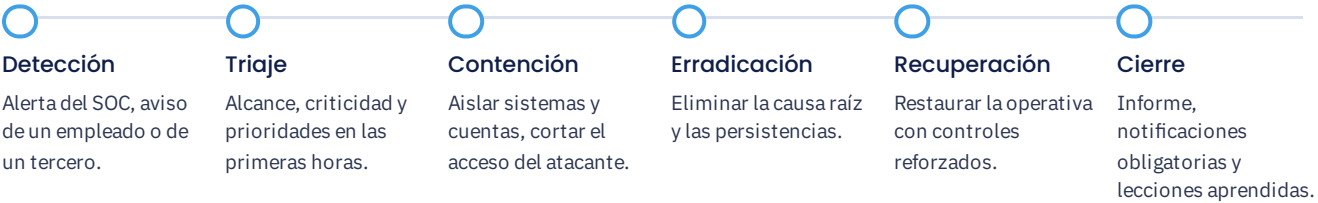
Datos clave

Modalidad
Remoto u on-site

Disponibilidad
Bajo demanda

Complementa
IR-01 e IR-02

Las fases de un incidente



Plazos de notificación que ayudamos a cumplir

Durante un incidente, el reloj regulatorio corre en paralelo al técnico. Preparamos la documentación para que las notificaciones lleguen a tiempo y con el contenido exigido.

RGPD	Brechas de datos personales: notificación a la AEPD en un máximo de 72 horas desde que se tiene constancia, y comunicación a los afectados sin dilación indebida cuando el riesgo sea alto.
NIS2	Entidades esenciales e importantes: alerta temprana en 24 horas , notificación del incidente en 72 horas e informe final en el plazo de un mes .
DORA	Entidades financieras: notificación inicial en 4 horas desde la clasificación del incidente como grave, informe intermedio en 72 horas e informe final en un mes .

Plazos orientativos. La obligación concreta depende del tipo de entidad, del incidente y de la normativa aplicable en cada caso.

Nube y puesto de trabajo digital

La infraestructura ya no termina en el perímetro. Auditamos los entornos cloud y las plataformas de colaboración donde hoy vive la información de la empresa, y decimos exactamente qué cambiar y cómo.

Servicios de esta familia

- CL-01 Seguridad en la nube
- CL-02 Seguridad en Microsoft 365

CL-01



Seguridad en la nube

AWS, Azure y Google Cloud, configurados como deben estar.

Cada vez más empresas migran sus infraestructuras a la nube, lo que introduce nuevos desafíos de seguridad. Realizamos auditorías de seguridad de entornos AWS, Azure y Google Cloud: identidades y permisos, cifrado de datos, configuración de red y servicios, registro de actividad y cumplimiento normativo.

El resultado es la configuración recomendada para su entorno —autenticación multifactor (MFA), segmentación de redes, monitorización de actividades sospechosas— con instrucciones concretas para que su equipo o su proveedor la apliquen.

Qué incluye

- Revisión de identidades, roles y permisos (IAM)
- Auditoría de configuraciones frente a CIS Benchmarks
- Cifrado, copias de seguridad y exposición del almacenamiento
- Registro, alertas y detección de actividad sospechosa

Entregables

- Informe de auditoría
- Configuración recomendada, paso a paso
- Retest tras los cambios

Datos clave

Modalidad Remoto
Marco CIS Benchmarks, buenas prácticas del proveedor
Recomendado Anual

Responsabilidad compartida

El proveedor protege la nube; el cliente protege lo que pone en ella. La mayoría de los incidentes en entornos cloud tiene su origen en errores de configuración y credenciales expuestas, no en fallos del proveedor.

Protege el proveedor

- Centros de datos, hardware y red física
- Hipervisores y servicios gestionados
- Disponibilidad de la plataforma

Protege el cliente

- Identidades, permisos y MFA
- Configuración de servicios, red y almacenamiento
- Datos, copias de seguridad y registro de actividad

CL-02

Seguridad en Microsoft 365



Correo, SharePoint, OneDrive y Teams, protegidos frente al phishing y el robo de cuentas.

Las plataformas de colaboración como Microsoft 365 (Office 365) son objetivos frecuentes de ataques de phishing y de compromiso de cuentas empresariales. Auditamos la protección del correo electrónico, la configuración de SharePoint, OneDrive y Teams, y la capacidad de detectar actividades sospechosas.

Definimos las políticas de seguridad, las reglas de filtrado y las configuraciones necesarias para evitar accesos no autorizados a la información corporativa, y las documentamos paso a paso para que su equipo o su proveedor las apliquen.

Qué incluye

- Revisión de acceso condicional y MFA
- Correo: SPF, DKIM, DMARC y reglas de filtrado
- Configuración de SharePoint, OneDrive y Teams
- Registro y alertas de actividad sospechosa

Entregables

- Informe de auditoría
- Políticas y configuraciones recomendadas
- Guía de aplicación paso a paso

Datos clave

Modalidad
Remoto

Recomendado
Anual y tras cambios de licenciamiento

Programas combinados

Los servicios se combinan en programas anuales con un único interlocutor, un calendario compartido y todos los resultados en DARKFORGE. Tres combinaciones habituales:

Exposición externa

Para saber qué ve un atacante desde Internet y mantenerlo vigilado desde TORO.

OF-01

OF-06

IR-03

Factor humano y correo

Para reducir el riesgo del phishing y del robo de cuentas.

OF-05

CL-02

IR-02

Infraestructura completa

Para evaluar el perímetro, la red interna y la nube de una vez.

OF-01

OF-02

OF-04

CL-01



Incluido en todos los programas. Un único interlocutor técnico, un informe de estado trimestral para dirección, acceso permanente a DARKFORGE y una revisión anual del alcance. Cualquier programa puede contratarse en modalidad PTaaS (pág. 4), con pruebas continuas y retest ilimitado.

DARKFORGE

El centro de operaciones de cada proyecto.

DARKFORGE es la plataforma desarrollada por Jaquers Ciberseguridad para gestionar de principio a fin cada proyecto de seguridad. Cada cliente accede a un espacio privado, aislado del resto, desde el que puede seguir el trabajo en tiempo real, consultar las evidencias, descargar los informes y marcar lo que su equipo va corrigiendo. Es también la base sobre la que se presta PTaaS (pág. 4); para la inteligencia de amenazas y la superficie de ataque se complementa con TORO (pág. 19).



Hallazgos en tiempo real

Cada vulnerabilidad aparece en el portal en cuanto se valida, con su severidad, evidencia y recomendación.



Informes ejecutivo y técnico

Generados desde la plataforma en PDF, con exportación a Word para integrarlos en su documentación.



Cyber Security Risk Meter

Una puntuación global y un cuadro de mando que resumen la postura de seguridad de un vistazo.



Evidencias trazables

Capturas, tarjetas de evidencia y sesiones documentadas para reproducir cada hallazgo.



Seguimiento y retest

Estado de cada hallazgo —abierto, en corrección o corregido— y verificación en el retest.



Módulo forense de phishing

Análisis de correos sospechosos con verificación SPF, DKIM y DMARC y exportación del informe.



Escáner e importación

Los resultados de escáneres y de auditorías anteriores se incorporan para partir de una línea de base.



Acceso móvil

Consulte el estado de sus proyectos desde el móvil, en cualquier momento.



Aislamiento por cliente, cifrado TLS en todas las comunicaciones y acceso protegido: la plataforma se somete a los mismos criterios de auditoría que aplicamos a nuestros clientes.

TORO

Threat Observation & Risk Operations

TORO es la plataforma de Jaquers Ciberseguridad para la ciberinteligencia de amenazas (CTI) y la gestión de la superficie de ataque (ASM). Observa de forma continua lo que la organización expone a Internet y lo que se dice, se filtra o se suplanta de ella, y convierte esa observación en riesgos priorizados sobre los que actuar. Sobre TORO se prestan el descubrimiento continuo de superficie de ataque (OF-06) y la ciberinteligencia OSINT (IR-03).



Descubrimiento continuo

Dominios, subdominios, direcciones IP, servicios, certificados y tecnologías, con histórico de altas y bajas.



Alertas de exposición

Puertos abiertos, servicios nuevos, certificados a punto de caducar y versiones con vulnerabilidades conocidas.



Credenciales filtradas

Cuentas corporativas presentes en brechas y volcados, con aviso en cuanto aparecen nuevas.



Dominios similares y suplantación

Registros parecidos a los suyos y sitios que imitan su marca, con paso directo al takedown (IR-04).



Huella de personas clave

Exposición digital de directivos y perfiles sensibles, para prevenir la ingeniería social y los ataques dirigidos.



Riesgo priorizado

Cada observación se convierte en un riesgo con prioridad, responsable y estado, no en una lista interminable de datos.



Informes de exposición

Informe periódico de superficie de ataque y de inteligencia, exportable como evidencia para auditorías.



Alimenta los pentestings

Los activos que TORO descubre se incorporan al alcance de PTaaS y de los pentestings en cada revisión.



TORO trabaja únicamente sobre activos y fuentes públicas: no requiere instalar nada en su infraestructura ni acceder a sus sistemas, y los datos de cada organización se mantienen aislados del resto.

Cómo trabajamos

El mismo método en todos los proyectos, para que los resultados sean comparables entre sí y a lo largo del tiempo.

- 1 Alcance y reglas de compromiso**
Definimos objetivos, activos, ventanas horarias, contactos de emergencia y la autorización formal.
- 2 Reconocimiento**
Mapeamos la superficie de ataque e inventariamos los activos, conocidos y descubiertos.
- 3 Análisis y explotación controlada**
Validamos manualmente cada hallazgo, sin denegación de servicio ni extracción innecesaria de datos.
- 4 Informe y presentación**
Informe ejecutivo para dirección e informe técnico para el equipo, con un plan de remediación priorizado.
- 5 Retest y seguimiento**
Verificamos las correcciones y actualizamos el estado de cada hallazgo en DARKFORGE.

Escala de severidad

Cada hallazgo se clasifica con CVSS y se contextualiza según el activo afectado, la facilidad de explotación y el impacto real en el negocio. El plan de remediación ordena las acciones por ese riesgo contextualizado, no solo por la puntuación.

Crítica CVSS 9,0 – 10,0	Alta CVSS 7,0 – 8,9	Media CVSS 4,0 – 6,9	Baja CVSS 0,1 – 3,9
-----------------------------------	-------------------------------	--------------------------------	-------------------------------

Durante el proyecto

Hallazgos críticos, de inmediato

Una vulnerabilidad crítica se comunica en cuanto se confirma, con su evidencia y una recomendación provisional, sin esperar al informe final.

Un único interlocutor

Un responsable técnico acompaña el proyecto de principio a fin y resuelve dudas por el canal que prefiera el cliente.

Sin sorpresas en el informe

Todo lo que aparece en el informe se ha comentado antes. El documento final confirma; no revela.

Marcos, cumplimiento y garantías

Marcos de referencia

Metodologías y estándares que guían las pruebas y la clasificación de los hallazgos.

OWASP WSTG

OWASP Top 10

OWASP ASVS

PTES

MITRE ATT&CK

CVSS

NIST SP 800-115

CIS Benchmarks

Cumplimiento normativo

Nuestros informes aportan la evidencia técnica que exigen los principales marcos regulatorios y de certificación.

ENS

ISO/IEC 27001

NIS2

DORA

RGPD

Qué recibe al final de cada proyecto

Cada entregable tiene un destinatario claro, para que la dirección y el equipo técnico trabajen sobre la misma información sin necesidad de traducirla.

Informe ejecutivo

Para dirección: postura global, riesgos principales y decisiones recomendadas, en lenguaje de negocio.

Informe técnico

Para el equipo: cada hallazgo con evidencia, puntuación CVSS, pasos de reproducción y corrección.

Plan de remediación

Acciones priorizadas por riesgo y esfuerzo, con plazos sugeridos, para que su equipo o su proveedor las ejecuten.

Sesión de resultados

Presentación de los hallazgos y resolución de dudas con ambos perfiles.

Retest

Verificación de las correcciones aplicadas por su equipo y actualización del estado de cada hallazgo.

Acceso a DARKFORGE

Todo lo anterior, disponible en su espacio privado de la plataforma.

Garantías en todos los servicios



Autorización y contrato
Ninguna prueba comienza sin autorización expresa por escrito y un alcance firmado.



Sin impacto en la operativa
Ventanas acordadas, sin denegación de servicio y con un contacto de emergencia permanente.



Confidencialidad
Acuerdo de confidencialidad, custodia de la información y borrado seguro al cierre.



Evidencias que resisten
Hallazgos reproducibles y, cuando procede, evidencias con validez legal.

Cómo empezar

1. Cuéntenos su situación

Una primera conversación de 30 minutos para entender su organización, sus sistemas y lo que le preocupa.

2. Alcance y propuesta

Definimos juntos el servicio o el programa, los activos incluidos y el calendario, y se lo enviamos por escrito.

3. Kick-off y acceso a DARKFORGE

Formalizamos la autorización, creamos su espacio en la plataforma y empezamos.

Glosario

Los términos técnicos que aparecen en este catálogo, explicados en una línea para que dirección y equipo técnico hablen el mismo idioma.

Pentesting

Prueba de intrusión: simulación controlada de un ataque para encontrar y explotar vulnerabilidades antes que un atacante real.

TORO

Threat Observation & Risk Operations: nuestra plataforma de ciberinteligencia y gestión de la superficie de ataque.

Caja negra, gris y blanca

Grado de información que recibe el equipo antes de la prueba: ninguna, parcial o completa.

Hallazgo

Vulnerabilidad o debilidad confirmada, documentada con evidencia, severidad y recomendación de corrección.

Retest

Verificación de que un hallazgo ha quedado realmente corregido.

Risk Meter

Puntuación global de DARKFORGE que resume la postura de seguridad de una organización.

Escalada de privilegios

Obtención de permisos superiores a los conseguidos inicialmente.

Sonda

Equipo que conectamos en la red del cliente para realizar el pentesting interno en remoto.

Phishing, vishing y smishing

Engaños por correo, llamada o SMS para robar credenciales o provocar acciones perjudiciales.

SPF, DKIM y DMARC

Mecanismos que permiten verificar que un correo procede realmente del dominio que dice.

Cadena de custodia

Registro que garantiza que una evidencia no se ha alterado desde su obtención.

MFA

Autenticación multifactor: verificar la identidad con más de un elemento, como contraseña y código o llave.

PTaaS

Pentesting como servicio: pruebas continuas por suscripción, con portal, retest ilimitado y cuota fija.

CTI y ASM

Ciberinteligencia de amenazas y gestión de la superficie de ataque: las dos disciplinas que cubre TORO.

Superficie de ataque

Conjunto de activos y puntos de entrada que un atacante puede ver y probar, desde fuera o desde dentro.

CVSS

Sistema estándar para puntuar la gravedad de una vulnerabilidad de 0 a 10.

Evidencia

Prueba reproducible (capturas, peticiones, registros) que demuestra la existencia de un hallazgo.

Movimiento lateral

Desplazamiento de un atacante entre sistemas de una red tras comprometer el primero.

Directorio Activo

Servicio de Microsoft que gestiona usuarios, equipos y permisos en las redes corporativas.

Man in the Middle

Ataque en el que un tercero se interpone en una comunicación para leerla o alterarla.

OSINT

Inteligencia obtenida a partir de fuentes de acceso público.

Takedown

Retirada de un dominio, web o perfil fraudulento a través de proveedores y organismos competentes.

Indicadores de compromiso

Datos (direcciones IP, dominios, hashes) que permiten detectar un ataque concreto.

Shadow IT

Sistemas y servicios que usa la organización sin conocimiento ni control del departamento de TI.



Hablemos de su seguridad.

Solicite una evaluación inicial sin compromiso y le propondremos el servicio —o el programa— que mejor encaje con su organización.

Correo	hola@jaquers.es
Web	jaquers.es
Plataforma	darkforge.jaquers.es