

Reporte Mensual de Ciberseguridad

Inteligencia de Amenazas

Estimados clientes, estar actualizados frente a las nuevas amenazas digitales es un componente esencial de cualquier estrategia de continuidad empresarial. Desde **Hinforcom** seguimos analizando la evolución del panorama de ciberseguridad para ayudar a nuestros clientes a reducir su exposición, anticipar vulnerabilidades y proteger sus sistemas críticos.

Contexto Estratégico de Ciberseguridad

Septiembre ha confirmado que el **perímetro corporativo** sigue siendo la puerta de entrada favorita de los atacantes. En un solo mes se han explotado activamente vulnerabilidades en gateways VPN y plataformas de acceso de Citrix, Check Point, F5, Fortinet y Cisco, varias de ellas como *zero-day*, antes de que existiera un parche.

Al mismo tiempo, el robo de identidad ha dado un salto cualitativo: ya no hacen falta malware ni contraseñas. Basta una **llamada haciéndose pasar por el soporte IT** o un código introducido en una página legítima de Microsoft para obtener una sesión válida que supera el MFA.

La seguridad ya no es un producto que se instala, sino una capacidad que se mantiene. Este reporte reúne los cinco acontecimientos de mayor impacto del mes y el marco defensivo con el que **Hinforcom** protege tu continuidad operativa.

5

fabricantes de VPN, firewall y acceso remoto con fallos explotados activamente

+12.000

buzones corporativos comprometidos por el kit EvilTokens

1,44 M

archivos de la administración de Berlín publicados por ransomware



Hinforcom

— Infraestructura IT y Ciberseguridad —



LAS 5 NOTICIAS E INCIDENTES DE CIBERSEGURIDAD MÁS IMPORTANTES DEL MES

1 Citrix NetScaler: dos nuevos zero-day críticos explotados a escala global

QUÉ OCURRIÓ

Citrix publicó ocho nuevas vulnerabilidades en **NetScaler ADC** y **NetScaler Gateway** (CVE-2026-88771 a CVE-2026-88778). Dos de ellas, **CVE-2026-88771** y **CVE-2026-88772**, son críticas, permiten por sí solas la ejecución remota de código y ya se explotaban como *zero-day* antes de su publicación.

CISA las añadió a su catálogo de vulnerabilidades explotadas y confirmó ataques a nivel global. Su recomendación es poco habitual: revisar indicios de compromiso **antes** de parchear y preservar las evidencias forenses, porque la actualización puede borrar el rastro del atacante.

Es el segundo mes consecutivo en que NetScaler aparece en este reporte (en agosto fue CVE-2026-8452).

POR QUÉ IMPORTA A TU EMPRESA

Si tu acceso remoto depende de un gateway expuesto a Internet, un fallo así permite entrar en la red interna sin credenciales. Actualizar no basta: hay que comprobar si ya entraron.

QUÉ HACER AHORA

- Inventariar todos los NetScaler expuestos a Internet
- Revisar indicadores de compromiso antes de actualizar
- Aplicar el boletín de seguridad de Citrix
- Renovar credenciales y sesiones si hay sospecha

Fuente: CISA · Critical Zero-Day Vulnerabilities Exploited in Citrix NetScaler ADC, Gateway (27/09/2026)

2 Check Point y F5: VPN y consolas de seguridad atacadas sin autenticación

QUÉ OCURRIÓ

CVE-2026-85102 (Check Point VPN): fallo en la negociación VPN que permite a un atacante no autenticado saltarse controles y ejecutar código en el gateway. El NCSC de Países Bajos ya había alertado de su explotación inminente.

CVE-2026-93616 (Check Point Security Management): permite subir y ejecutar scripts sin iniciar sesión en el servidor que controla políticas, logs y administración. Check Point confirmó clientes ya atacados.

CVE-2026-94127 (F5 BIG-IP APM): ejecución de código sin autenticación en configuraciones OAuth, explotada desde el mismo día de su divulgación. CISA sumó además fallos explotados en Fortinet, Cisco FMC, Cisco ISE y Cisco SD-WAN.

POR QUÉ IMPORTA A TU EMPRESA

El propio equipo que debe protegerte puede convertirse en la puerta de entrada si no se mantiene actualizado y vigilado.

QUÉ HACER AHORA

- Aplicar los hotfix publicados por Check Point y F5
- No exponer nunca las consolas de gestión a Internet
- Contrastar logs con los IOCs del fabricante
- Priorizar fallos del catálogo KEV de CISA

Fuente: Security Affairs · CISA adds Check Point, Arista VeloCloud and F5 BIG-IP APM flaws to KEV (23/09/2026)

3 Falsas llamadas del soporte IT: el vishing abre la puerta a Microsoft 365

QUÉ OCURRIÓ

Microsoft documentó una campaña activa desde mayo en la que los atacantes **llaman o escriben al móvil personal** de los empleados haciéndose pasar por el help desk. Con la excusa de una actualización urgente de passkey o MFA, los llevan a un inicio de sesión falso (AiTM) o a un flujo de código de dispositivo y capturan una sesión ya autenticada.

Después registran sus propios métodos de autenticación y descargan de forma masiva SharePoint, OneDrive y correo. Arctic Wolf detectó un grupo similar centrado en **directores y altos cargos**.

Caso del mes: **McKesson**. Una llamada de vishing obtuvo credenciales de su sistema de identidad Okta; desde ahí los atacantes accedieron a Salesforce y Snowflake y exfiltraron cerca de 1 TB en cuatro días.

POR QUÉ IMPORTA A TU EMPRESA

Una sola llamada convincente a la persona adecuada puede abrir el correo, los documentos y las aplicaciones cloud de toda la empresa. El MFA tradicional no lo detiene.

QUÉ HACER AHORA

- Protocolo de verificación: el soporte nunca pide códigos por teléfono
- MFA resistente al phishing (FIDO / passkeys)
- Alertas al registrar nuevos métodos de autenticación
- Formación específica para dirección y administración

Fuente: Microsoft Security · Passkey-themed social engineering leads to identity and cloud compromise (09/09/2026)

4 EvilTokens: phishing con IA por suscripción que comprometió +12.000 buzones

QUÉ OCURRIÓ

Microsoft publicó el análisis de **EvilTokens**, una plataforma de phishing como servicio que desde febrero ha comprometido **más de 12.000 buzones en más de 10.000 organizaciones**, con Francia y Reino Unido entre los países europeos afectados. Su Unidad de Delitos Digitales coordinó la desarticulación de parte de la infraestructura.

La víctima recibe una factura, una RFP o un aviso de contraseña y acaba introduciendo un código en la página **legítima** de Microsoft, autorizando sin saberlo la sesión del atacante.

Una vez dentro, la IA del kit analiza el buzón, localiza perfiles financieros y facturas pendientes y redacta correos de fraude creíbles. Precio: 1.500 dólares más 500 al mes.

POR QUÉ IMPORTA A TU EMPRESA

El fraude del CEO y las facturas falsas ya no requieren atacantes sofisticados: se alquilan por suscripción.

QUÉ HACER AHORA

- Bloquear el flujo de código de dispositivo si no se usa
- Activar políticas anti-phishing y Safe Links
- Alertar sobre reglas de buzón sospechosas
- Verificar por otro canal cualquier cambio de cuenta bancaria

Fuente: Microsoft Security · Unmasking EvilTokens: getting to the root of device code phishing (22/09/2026)

5 Ransomware en Europa: Rhysida publica 1,4 millones de archivos de Berlín

QUÉ OCURRIÓ

El grupo **Rhysida** atacó la red del Estado de Berlín, robó **5,79 TB** de dos departamentos (Obras Públicas y Transporte) y los subastó desde 30 bitcoins, unos 2 millones de euros.

Ante la negativa a pagar, el 4 de septiembre publicó en la dark web cerca de **1,44 millones de archivos**: expedientes de empleados, nóminas, contratos, documentos de identidad escaneados y direcciones particulares, a menos de un mes de las elecciones regionales.

Berlín activó una unidad de crisis con la BSI y la autoridad de protección de datos para revisar el material e informar a ciudadanos y empresas afectados.

POR QUÉ IMPORTA A TU EMPRESA

Con la doble extorsión, aunque tengas copias de seguridad, el atacante puede publicar tus datos. Prevenir y detectar a tiempo vale más que cualquier recuperación.

QUÉ HACER AHORA

- Backups automáticos, aislados y probados
- Segmentar la red para frenar el movimiento lateral
- Monitorizar exfiltración de datos 24/7
- Plan de respuesta y notificación RGPD en 72 horas

Fuente: Reuters (28/08/2026) • DW: Cyberattack in Berlin, 1.4 million files on the dark web (10/09/2026)

NIS2 en España: la obligación llega antes que la ley

A cierre de septiembre, España sigue sin transponer la Directiva NIS2. El plazo venció el **17 de octubre de 2024** y en julio de 2026 la Comisión Europea llevó a España ante el **Tribunal de Justicia de la UE**. El Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad continúa en tramitación parlamentaria.

Mientras tanto, las exigencias de NIS2 ya llegan a las empresas por la vía de los contratos: grandes clientes y cadenas de suministro piden evidencias de gestión de riesgos, notificación de incidentes y continuidad de negocio.

Lo que se trabaje hoy sobre esa base no se pierde cuando llegue el texto definitivo: se aprovecha.

LA LECTURA PARA DIRECCIÓN

Esperar al BOE es la estrategia más cara. La seguridad ya es un criterio para ganar y conservar contratos.

CÓMO AYUDA HINFORCOM

- Diagnóstico de madurez NIS2
- Mapa de brechas y roadmap priorizado
- Evidencias operativas con SOC, EDR y backups

Fuentes: Comisión Europea · Transposición de la Directiva NIS2 · Pumpun · NIS2 en España: el TJUE llega antes que la ley (22/09/2026)



Hinform

— Infraestructura IT y Ciberseguridad —



FORMAS CLAVE EN QUE HINFORCOM PROTEGE E IMPULSA LA SEGURIDAD CORPORATIVA

Gestión de Vulnerabilidades y Perímetro

1. Gestión proactiva de vulnerabilidades y parcheo prioritario

Citrix, Check Point, F5, Fortinet y Cisco en un solo mes demuestran que la ventana entre la publicación de un fallo y su explotación ya es de horas, o incluso negativa. **Hinforcom** mantiene la infraestructura bajo control con soporte y mantenimiento continuo, auditorías de seguridad y actualización priorizada de los servicios expuestos a Internet, incluyendo la revisión de indicios de compromiso antes de parchear.

2. Cloud Firewall, VPN y protección del perímetro

Hinforcom diseña e implementa **Cloud Firewall Fortinet** (IDS/IPS, antivirus, filtrado URL y control de más de 3.500 aplicaciones), redes seguras y **VPN para acceso remoto**, con segmentación y controles de acceso para que gateways, consolas de gestión, servidores y NAS no queden innecesariamente expuestos a Internet.

Identidad, Zero Trust y Endpoint

3. Protección de Identidad y Zero Trust frente al vishing y el device code phishing

Las falsas llamadas de soporte y EvilTokens demuestran que una buena contraseña y el MFA tradicional ya no bastan. La estrategia de **Protección de Identidad y Zero Trust** evalúa dispositivo, contexto y riesgo de cada sesión. En línea con Microsoft: MFA resistente al phishing, acceso condicional, bloqueo del flujo de código de dispositivo y alertas ante nuevos métodos de autenticación.

4. Protección avanzada de endpoints y servidores con EDR

Cuando el atacante supera las primeras capas, detectar lo que hace después es decisivo. **EDR CrowdStrike** aporta análisis conductual continuo sobre endpoints y servidores para identificar ejecución anómala, movimiento lateral, escalada de privilegios e instalación de herramientas de acceso remoto no autorizadas.

Monitorización Continua y Recuperación

5. SOC gestionado 24/7, copias de seguridad y capacidad de recuperación

Casos como el de Berlín muestran que el objetivo final del atacante es el dato: documentación, bases de datos, servidores y NAS. El **SOC Gestionado 24/7** de **Hinforcom** detecta comportamientos anómalos, como descargas masivas en SharePoint u OneDrive o accesos desde ubicaciones inusuales, y responde antes de que la exfiltración se complete.

Una estrategia de **backups automáticos y almacenamiento NAS** reduce el impacto del ransomware, los errores humanos y los fallos de infraestructura. Todo ello, unido a la **consultoría NIS2**, convierte la seguridad en resiliencia demostrable ante clientes, partners y auditores.

¿Sabes cuánto de tu infraestructura está expuesta hoy?

Habla con nuestro equipo y revisamos tu perímetro, identidad y copias de seguridad.

hinforcom.com/contacto

Fuentes consultadas

1. **CISA** · Critical Zero-Day Vulnerabilities Exploited in Citrix NetScaler ADC, Gateway, 27 sept. 2026. <https://www.cisa.gov/news-events/alerts/2026/09/27/critical-zero-day-vulnerabilities-exploited-citrix-netscaler-adc-gateway>
2. **Security Affairs** · CISA adds Check Point, Arista VeloCloud Orchestrator, and F5 BIG-IP APM flaws to KEV, 23 sept. 2026. <https://securityaffairs.com/199631/hacking/u-s-cisa-adds-check-point-arista-velocloud-orchestrator-and-f5-big-ip-apm-flaws-to-its-known-exploited-vulnerabilities-catalog.html>
3. **Microsoft Security** · Passkey-themed social engineering leads to identity and cloud compromise, 9 sept. 2026. <https://www.microsoft.com/en-us/security/blog/2026/09/09/passkey-themed-social-engineering-leads-identity-cloud-compromise/>
4. **Microsoft Security** · Unmasking EvilTokens: getting to the root of device code phishing, 22 sept. 2026. <https://www.microsoft.com/en-us/security/blog/2026/09/22/unmasking-eviltokens-getting-to-the-root-of-device-code-phishing/>
5. **DW** · Cyberattack in Berlin: 1.4 million files on the dark web, 10 sept. 2026. <https://www.dw.com/en/cyberattack-in-berlin-14-million-files-on-the-dark-web/a-79220829>
6. **Pumpun** · NIS2 en España: el TJUE llega antes que la ley, 22 sept. 2026. <https://pumpun.com/nis2-espana-tjue-contrato/>