Hinforcom
— Infraestructura IT y Ciberseguridad —

Octubre de 2026

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.

www.hinforcom.com | info@hinforcom.com

Contexto Estratégico de Ciberseguridad

Octubre ha dejado el **mayor robo de criptomonedas de la historia** y una lección que va mucho más allá de ese sector: a Binance no le rompieron el cifrado, **engañaron a sus ingenieros**. Un instalador manipulado, una entrevista de trabajo falsa y una herramienta interna de IA bastaron para sacar unos 6.300 millones de dólares en cuestión de minutos.

A la vez, la base de Internet ha estado bajo presión. Dos fallos críticos en **PHP**, el lenguaje que mueve buena parte de las webs, y otro en la librería de compresión **Brotli** pasaron en pocos días al catálogo de vulnerabilidades explotadas de CISA. Y los ataques a los frigoríficos de supermercados en Francia, repetidos ya en noviembre en otros siete países europeos, demostraron que un equipo conectado mal protegido puede parar una tienda.

El denominador común: los atacantes buscan a las personas y los sistemas que nadie vigila. Este reporte reúne los cinco acontecimientos de mayor impacto del mes, una mirada a lo que se espera para la próxima década y el marco defensivo con el que **Hinforcom** protege tu continuidad operativa.

6.300 M$
robados a Binance el 29 de octubre, el mayor robo cripto registrado

2
fallos críticos de PHP (PHP2Shell) ya explotados según CISA

7
países europeos con frigoríficos de supermercados atacados el 2 de noviembre

Hinforcom

Infraestructura IT y Ciberseguridad

LAS 5 NOTICIAS E INCIDENTES DE CIBERSEGURIDAD MÁS IMPORTANTES DEL MES

1 Binance: 6.300 millones robados tras una entrevista de trabajo falsa

QUÉ OCURRIÓ

El 29 de octubre, atacantes vaciaron *hot wallets* de **Binance**, el mayor exchange de criptomonedas del mundo, en unas diez blockchains. La mayor parte de los fondos salió en unos 20 minutos. El impacto ronda los **6.300 millones de dólares**, más de cuatro veces el récord anterior (Bybit, 1.500 millones en 2025). El FBI atribuye el ataque a **Corea del Norte** (grupo TraderTraitor).

Según el análisis publicado por Binance el 3 de noviembre, la campaña duró meses. En **junio**, un ingeniero instaló una versión manipulada de una herramienta de desarrollo que encontró en un buscador. En **septiembre**, otro ingeniero recibió una oferta de empleo falsa: tras dos entrevistas le pidieron descargar una «prueba técnica» que era malware y que no detectó la protección de su equipo. El **20 de octubre**, los atacantes usaron ese portátil y una **herramienta interna de IA** para tomar el control de los equipos de otros dos ingenieros, y el 29 lanzaron el robo con un token de despliegue robado.

Binance asegura que no se filtraron claves privadas, que cubrirá todas las pérdidas con su fondo de emergencia y fondos propios, y que unos 3.000 millones quedaron congelados. Los retiros estuvieron suspendidos hasta el 1 de noviembre.

Fuentes: Binance · Security Incident Update (30/10/2026) · The Hacker News (03/11/2026) · BBC News (03/11/2026)

POR QUÉ IMPORTA A TU EMPRESA

No hace falta tener criptomonedas para sufrir este ataque. Falsas ofertas de empleo, software descargado de anuncios y permisos de producción guardados en un portátil existen en cualquier empresa con equipo técnico.

QUÉ HACER AHORA

- Instalar software solo desde fuentes oficiales y controlar las instalaciones
- Prohibir ejecutar «pruebas técnicas» o archivos de terceros en equipos de trabajo
- Retirar tokens y credenciales de despliegue de los portátiles
- Doble aprobación para pagos, despliegues y operaciones críticas
- Limitar qué pueden hacer las herramientas internas de IA

2 PHP2Shell y HTTP2Shell: la base de la web, bajo ataque

QUÉ OCURRIÓ

El 21 de octubre, PHP publicó parches para **CVE-2026-109618** y **CVE-2026-109619** (CVSS 9,2), conocidos como **PHP2Shell**. Permiten ejecutar código en remoto sin autenticación en configuraciones muy extendidas: PHP-FPM, Apache con mod_php, php-cgi, FrankenPHP y LiteSpeed. El 24 de octubre se confirmó la primera explotación con éxito y el **26 de octubre CISA los añadió a su catálogo de vulnerabilidades explotadas**, con tres días de plazo para las agencias federales de EE. UU.

En paralelo, **CVE-2026-111497**, apodado **HTTP2Shell**, afecta al decodificador de la librería de compresión **Brotli**, integrado en Node.js, .NET, paquetes de Python y proxies. Permite corromper la memoria del proceso y, en algunos casos, ejecutar código. Microsoft publicó parches de emergencia para .NET y CISA también lo incluyó en su catálogo el 27 de octubre.

Versiones corregidas: PHP 8.5.12, 8.4.27, 8.3.36 y 8.2.35 · Brotli 1.0.10, 1.1.1 y 1.2.1 · Node.js 22.23.4, 24.22.1 y 26.12.1.

POR QUÉ IMPORTA A TU EMPRESA

Tener el CMS y los plugins al día no basta. El fallo está en la capa del servidor o en librerías empaquetadas dentro de otras aplicaciones, que nadie suele revisar.

QUÉ HACER AHORA

- Inventariar servidores con PHP y su versión, incluido el hosting
- Actualizar, reiniciar servicios y reconstruir contenedores
- Revisar aplicaciones Node.js y .NET que descompriman datos
- WAF como medida temporal: no sustituye el parche
- Revisar registros y procesos anómalos en servidores expuestos

Fuentes: CISA (21/10/2026) · The Hacker News (27/10/2026) · BleepingComputer (26/10/2026) · Microsoft MSRC (30/10/2026)

3 Frigoríficos hackeados: de Francia a siete países europeos

QUÉ OCURRIÓ

En octubre, atacantes tomaron el control de los sistemas de refrigeración de hasta **700 supermercados en Francia**. Las temperaturas llegaron a **50 °C** y las pérdidas de alimentos se estiman en decenas de millones de euros. Esos mismos días, **Ahold Delhaize** desconectó webs, aplicaciones y sistemas logísticos por actividad maliciosa en su infraestructura, sin relación demostrada con el primer caso.

El **2 de noviembre** el ataque se repitió en **Bélgica, Luxemburgo, Suecia, Irlanda, Países Bajos, Estonia y Finlandia**. Según el fabricante Sabcobel, los evaporadores se pusieron en modo descongelación para que los equipos se calentaran. Los atacantes se apoyaron en software de gestión de los equipos **expuesto a Internet**. La Comisión Europea lo calificó de «intento deliberado de perturbar nuestra cadena de suministro alimentaria». Nadie lo ha reivindicado.

POR QUÉ IMPORTA A TU EMPRESA

Refrigeración, climatización, cámaras o control de accesos también son superficie de ataque. Aquí el daño es físico, inmediato y no se arregla restaurando una copia.

QUÉ HACER AHORA

- Inventariar los equipos conectados y quién los gestiona
- Sacar de Internet los paneles de gestión y acceder solo por VPN
- Separar la red de operación de la red corporativa
- Actualizar firmware y eliminar contraseñas por defecto
- Alarmas independientes y plan manual si un sistema falla

Fuentes: AP News (10/2026 y 03/11/2026) · BBC News (02/11/2026) · The Guardian (02/11/2026) · Ahold Delhaize (19/10/2026)

4 Falso soporte IT en Microsoft Teams: del spam al ransomware en minutos

QUÉ OCURRIÓ

Arctic Wolf documentó el 26 de octubre **más de 400 incidentes** con el mismo patrón. Primero, el empleado recibe cientos de correos de suscripciones en pocos minutos (*mail bombing*). Después le escribe por el chat externo de Teams un supuesto **«IT Support (Internal)»** que se ofrece a arreglarlo, le llama por Teams y le pide instalar una herramienta de acceso remoto legítima como Quick Assist o AnyDesk.

Con acceso al equipo, el atacante ejecuta su código en **menos de 15 minutos**, instala puertas traseras, se mueve hacia los controladores de dominio, roba datos y despliega **ransomware**. No explota ninguna vulnerabilidad: abusa del acceso externo de Teams, que viene activado por defecto en Microsoft 365.

Fuentes: Arctic Wolf Labs (26/10/2026) · The Hacker News (26/10/2026) · Help Net Security (27/10/2026)

POR QUÉ IMPORTA A TU EMPRESA

Es la misma lógica que en Binance: el atacante se gana la confianza de una persona. Cualquier empresa con Microsoft 365 tiene esta puerta abierta si no la ha cerrado.

QUÉ HACER AHORA

- Limitar el acceso externo de Teams a dominios de confianza
- Bloquear Quick Assist y herramientas remotas no aprobadas
- Alertas ante la instalación de software de acceso remoto
- Protocolo claro: el soporte real nunca escribe por chat externo
- Formar al personal frente a la saturación de correo

5 SafePay: ransomware que va primero a por las copias de seguridad

QUÉ OCURRIÓ

CISA, el FBI y socios internacionales publicaron una alerta conjunta sobre **SafePay**, grupo que ha afectado a **al menos 600 organizaciones** desde agosto de 2024 en América, Europa y Australia. Entra con credenciales robadas, fuerza bruta, phishing y vulnerabilidades en **VPN y otros equipos expuestos**.

Una vez dentro, se mueve con herramientas legítimas, roba datos, cifra sistemas e intenta **borrar o desactivar las copias de seguridad**, incluidos los almacenamientos en red (NAS). Después aplica doble extorsión: pide rescate por descifrar y por no publicar la información robada.

Fuentes: CISA y FBI · Aviso conjunto AA26-293A sobre SafePay (10/2026)

POR QUÉ IMPORTA A TU EMPRESA

Tener copias no garantiza recuperarse si el atacante puede alcanzarlas desde la red corporativa. Y restaurar no evita la exposición de los datos ya robados.

QUÉ HACER AHORA

- Parchear VPN, firewalls y equipos expuestos con prioridad
- MFA obligatorio y menos cuentas con privilegios
- Copias aisladas, con credenciales distintas a las del dominio
- Probar una restauración real y medir cuánto tarda
- Detección y respuesta en endpoints y servidores

También en octubre: lo que conviene revisar

CISCO SECURE EMAIL GATEWAY

CVE-2026-76519 (CVSS 9,8), con explotación activa confirmada por Cisco. Permite ejecutar comandos como root mediante un adjunto manipulado si se cumplen condiciones concretas (File Reputation de AMP y versiones vulnerables).

GITLAB AUTOGESTIONADO

CVE-2026-110264 (CVSS 10) permite ejecutar código sin autenticación. CERT-EU pide actualizar con prioridad las instancias accesibles desde Internet y revisar tokens y secretos de CI/CD.

ADOBE COMMERCE Y MAGENTO

CISA añadió el 27 de octubre CVE-2026-48356 (CVSS 9,3) a su catálogo de fallos explotados. El parche existe desde julio: las tiendas online sin actualizar son objetivo directo.

PROVEEDOR CLOUD EN JAPÓN (GMO)

Una intrusión en Onamae Desktop Cloud pudo instalar malware en hasta 26.739 servidores de clientes. El atacante publicó datos y pidió 50 millones de dólares. Recordatorio: el riesgo también llega por el proveedor.

Fuentes: Cisco (14/10/2026) · CERT-EU 2026-019 (21/10/2026) · CISA KEV vía IntelFusions (27/10/2026) · BleepingComputer (27/10/2026)

La próxima década: más ataques, más rápidos y más baratos

El caso Binance resume hacia dónde va la ciberdelincuencia: campañas pacientes, ingeniería social muy elaborada y herramientas de IA dentro de la cadena de ataque. Estas son las tendencias que anticipan los principales organismos y analistas.

122.223
incidentes gestionó INCIBE en España en 2025, un 26 % más que en 2024

12,2 bill. $
coste anual estimado del cibercrimen en 2031 (Cybersecurity Ventures)

94 %
de los líderes cree que la IA será el factor que más cambiará la ciberseguridad (WEF)

LA IA ABARATA Y ACELERA EL ATAQUE

MITRE lo resume así: la IA no cambia lo que consiguen los atacantes, cambia lo rápido y lo barato que lo consiguen, y baja la barrera de entrada. Fortinet prevé agentes de IA capaces de ejecutar fases completas de un ataque y de reducir de días a minutos el tiempo entre la intrusión y el impacto.

MÁS FRAUDE Y MÁS ATAQUES A PERSONAS

Según el Global Cybersecurity Outlook 2026 del Foro Económico Mundial, el 77 % de los encuestados vio crecer el fraude y el phishing, y los CEO ya lo sitúan por delante del ransomware entre sus preocupaciones. Llamadas, chats y entrevistas falsas seguirán siendo la vía de entrada principal.

EL PROVEEDOR COMO PUERTA DE ENTRADA

El 65 % de las grandes empresas cita el riesgo de terceros y de la cadena de suministro como su mayor barrera de resiliencia (WEF). Hosting, software, mantenimiento remoto o equipos conectados: cada proveedor amplía la superficie de ataque.

LA CUENTA ATRÁS CUÁNTICA

Gartner estima que la computación cuántica hará insegura la criptografía asimétrica actual hacia 2029 y que podrá romperla hacia 2034. El riesgo ya existe: hay atacantes que roban hoy datos cifrados para descifrarlos más adelante.

Las cifras de coste varían mucho según la metodología: un estudio académico de 2026 sitúa los daños cuantificables en unos 500.000 millones de dólares al año. Todas las fuentes coinciden en la tendencia: más ataques, más rápidos y más baratos de lanzar.
Fuentes: INCIBE · Balance de Ciberseguridad 2025 · Cybersecurity Ventures · WEF Global Cybersecurity Outlook 2026 · MITRE (22/10/2026) · Fortinet 2026 Cyberthreat Predictions · Gartner

NIS2 en España: las elecciones retrasan la ley hasta 2027

España sigue sin transponer la Directiva NIS2, cuyo plazo venció el **17 de octubre de 2024**. Desde julio de 2026 la Comisión Europea tiene a España ante el **Tribunal de Justicia de la UE**.

El **6 de octubre** el Real Decreto 806/2026 disolvió las Cortes y convocó elecciones generales para el **29 de noviembre**. Con las cámaras disueltas, el anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad tendrá que esperar al nuevo Gobierno: **no habrá ley NIS2 española antes de 2027**.

Mientras tanto, las exigencias de NIS2 siguen llegando por la vía de los contratos: grandes clientes, aseguradoras y cadenas de suministro piden evidencias de gestión de riesgos, notificación de incidentes y continuidad.

Fuentes: Comisión Europea · Transposición de NIS2 · Dazr: NIS2 en España (19/10/2026) · QuantumSec: estado de la ley (08/10/2026)

LA LECTURA PARA DIRECCIÓN

Cada mes de espera es un mes menos de preparación. Las empresas que lleguen a 2027 con su diagnóstico hecho tendrán ventaja frente a clientes y auditores.

CÓMO AYUDA HINFORCOM

- Diagnóstico de madurez NIS2
- Mapa de riesgos y proveedores críticos
- Plan de respuesta y notificación de incidentes
- Evidencias operativas con SOC, EDR y backups

Hinforcom

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

PHP2Shell pasó de parche a explotación confirmada en cinco días. **Hinforcom** mantiene la infraestructura bajo control con soporte y mantenimiento continuo, auditorías de seguridad y actualización priorizada de los servidores, librerías y servicios expuestos a Internet, empezando por los fallos que CISA confirma como explotados.

2. Cloud Firewall, VPN y segmentación de redes

Los frigoríficos atacados tenían su gestión expuesta a Internet. **Hinforcom** implementa **Cloud Firewall Fortinet** (IDS/IPS, antivirus, filtrado URL, control de más de 3.500 aplicaciones), **VPN para acceso remoto** y segmentación para que paneles de gestión, equipos conectados, servidores y NAS no queden al alcance de cualquiera.

Identidad, Zero Trust y Endpoint

3. Identidad, Zero Trust y mínimo privilegio

Binance y las falsas llamadas de soporte en Teams tienen algo en común: un atacante que se hace pasar por alguien de confianza. La estrategia de **Protección de Identidad y Zero Trust** combina MFA resistente al phishing, acceso condicional, permisos temporales en lugar de tokens permanentes y restricción del acceso externo de Teams y de las herramientas de soporte remoto.

4. Protección avanzada de endpoints y servidores con EDR

Cuando el engaño funciona, lo decisivo es detectar lo que pasa después. **EDR CrowdStrike** aporta análisis de comportamiento continuo para identificar malware disfrazado de prueba técnica, instalación de herramientas remotas no autorizadas, robo de credenciales y movimiento lateral.

Monitorización Continua y Recuperación

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

SafePay demuestra que el atacante busca primero las copias. El **SOC gestionado 24/7** de **Hinforcom** detecta comportamientos anómalos y responde antes de que el daño se complete, mientras que una estrategia de **backups automáticos y almacenamiento NAS** aislado permite recuperarse sin pagar rescates. Todo ello alineado con la **consultoría NIS2** para convertir la seguridad en resiliencia demostrable ante clientes y auditores.

¿Sabes cuánto de tu infraestructura está expuesta hoy?

Habla con nuestro equipo y revisamos contigo tu perímetro, tus accesos y tus copias de seguridad.

hinforcom.com/contacto

Fuentes consultadas

1. **Binance** · Security Incident Update, 30 oct. 2026. https://www.binance.com/en/support/announcement/detail/c5a8729a97ac486d963784d96c5642d7

2. **The Hacker News** · Binance Reveals How Fake Job Interviews and AI Tool Abuse Led to $6.43 Billion Theft, 3 nov. 2026. https://thehackernews.com/2026/11/binance-reveals-how-fake-job-interviews.html

3. **BBC News** · Binance says fake job interviews used as part of $6.3bn crypto hack, 3 nov. 2026. https://www.bbc.com/news/articles/ck5ynwz9gy67o

4. **CISA** · Critical Vulnerabilities in PHP Require Immediate Patching, 21 oct. 2026. https://www.cisa.gov/news-events/alerts/2026/10/21/critical-vulnerabilities-php-require-immediate-patching

5. **The Hacker News** · CISA Confirms Active Exploitation of Two PHP2Shell Flaws, 27 oct. 2026. https://thehackernews.com/2026/10/cisa-confirms-active-exploitation-of.html

6. **BleepingComputer** · Critical 'HTTP2Shell' Brotli vulnerability triggers emergency patches, 26 oct. 2026. https://www.bleepingcomputer.com/news/security/critical-http2shell-brotli-vulnerability-triggers-emergency-patches/

7. **Microsoft MSRC** · Patch now: PHP2Shell, Brotli, and eMudhra guidance for customers, 30 oct. 2026. https://www.microsoft.com/en-us/msrc/blog/2026/10/patch-now-php2shell-brotli-emudhra-guidance-for-customers

8. **AP News** · European supermarkets face spoiled food losses after fridge cyberattacks, 3 nov. 2026. https://apnews.com/article/supermarkets-europe-internet-cyberattack-food-fridges-hacked-b6abfab3f5cdd65c19476b9032eb7a9d

9. **BBC News** · Shop freezers in seven European countries hit by cyber-attack, 2 nov. 2026. https://www.bbc.com/news/articles/cq1kd1nee80eo

10. **Ahold Delhaize** · Update on status of cybersecurity incident, 19 oct. 2026. https://newsroom.aholddelhaize.com/ahold-delhaize-update-on-status-of-cybersecurity-incident/

11. **Arctic Wolf Labs** · How Threat Actors Abuse Microsoft Teams External Chat for Initial Access, 26 oct. 2026. https://arcticwolf.com/resources/blog/threat-actors-abuse-microsoft-teams-external-chat-for-initial-access/

12. **CISA y FBI** · Aviso conjunto AA26-293A sobre SafePay, oct. 2026. https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-293a

13. **Cisco** · Security Advisory CVE-2026-76519, Secure Email Gateway, 14 oct. 2026. https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-esa-afw-zqYJkjxp.html

14. **CERT-EU** · Critical vulnerability in GitLab CE/EE (2026-019), 21 oct. 2026. https://cert.europa.eu/publications/security-advisories/2026-019/

15. **BleepingComputer** · Japan's GMO urges customers to shut down PCs amid ransomware threat, 27 oct. 2026. https://www.bleepingcomputer.com/news/security/japans-gmo-urges-customers-to-shut-down-pcs-amid-ransomware-threat/

16. **INCIBE** · Balance de Ciberseguridad 2025, feb. 2026. https://www.incibe.es/incibe/sala-de-prensa/incibe-detecto-mas-de-122000-incidentes-de-ciberseguridad-en-2025

17. **World Economic Forum** · Global Cybersecurity Outlook 2026, ene. 2026. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf

18. **Cybersecurity Ventures** · Cybercrime To Cost The World $12.2 Trillion Annually By 2031. https://cybersecurityventures.com/official-cybercrime-report-2025/

19. **MITRE** · The New Economics of Cyber Risk in the Age of Frontier AI, 22 oct. 2026. https://www.mitre.org/news-insights/publication/new-economics-cyber-risk-age-frontier-ai

20. **Dazr** · NIS2 en España: estado de la ley y qué hacer ya, 19 oct. 2026. https://compliance.dazr.eu/es/nis2/espana

21. **Gartner** · Postquantum Cryptography: The Time to Prepare Is Now!, 2024. https://www.gartner.com/en/documents/5550295

22. **Fortinet (vía SME Magazine)** · Fortinet Forecasts Faster, More Organised Cyberattacks in 2026, dic. 2025. https://sme.asia/fortinet-forecasts-faster-more-organised-cyberattacks-in-2026/