ALERTA TÉCNICA DE CIBERSEGURIDAD

INSTEL & SEGURIDAD

ANÁLISIS FORENSE - AUDITORÍA - PENTESTING

VULNERABILIDADES CRÍTICAS, PARCHES E INCIDENTES DE SEGURIDAD

Microsoft 365 · CISA KEV · Fortinet · SAP · Navegadores · WordPress

DESTINATARIOS	Empresas, organismos públicos, hospitales y equipos de TI
ELABORADO POR	Pedro Matías Cacivio · Instel & Seguridad
PERÍODO	7 al 12 de noviembre de 2026 · hora argentina
CRITERIO	Explotación activa, gravedad, exposición y continuidad operativa

DOCUMENTO TÉCNICO DE DIFUSIÓN INSTITUCIONAL · FUENTES CITADAS

Alerta preventiva. La afectación requiere verificar producto, versión y exposición.
La publicación de una CVE no demuestra por sí misma una intrusión ni explotación local.

ACTUALIZACIÓN COMPLEMENTARIA · 13/11/2026

1. Resumen ejecutivo

Entre el **sábado 7 y el jueves 12 de noviembre de 2026** se registraron publicaciones de alto impacto en seguridad informática y un incidente significativo de disponibilidad de Microsoft 365. La situación exige una respuesta coordinada que incluya gestión acelerada de parches, búsqueda de indicios de compromiso y continuidad operativa.

CISA incorporó **diez vulnerabilidades explotadas** a su catálogo KEV los días 9 y 10 de noviembre. El ciclo de parches de Microsoft del 10 de noviembre incluyó una falla de Outlook con explotación confirmada. Fortinet publicó un grupo extenso de avisos, SAP difundió cuatro CVE con puntuación CVSS 10,0 y Mozilla, Google y Apple actualizaron productos de uso cotidiano. [F01-F10]

El **12 de noviembre** Microsoft reconoció problemas de conexión en Exchange Online y otros servicios Microsoft 365 bajo los identificadores **EX1550543** y **MO1550821**. A la hora de corte, la hipótesis técnica pública se relacionaba con infraestructura, sobrecarga y comprobaciones de salud fallidas; **no se había acreditado una vinculación causal con ciberataques ni con los parches de noviembre**. [F11-F12]

Decisiones que requieren instrucción de autoridades

- Ordenar la identificación y corrección prioritaria de equipos efectivamente afectados por las diez CVE incorporadas a KEV.
- Autorizar ventanas de mantenimiento urgentes para sistemas Microsoft, Fortinet, SAP y navegadores, con verificación posterior.
- Activar un plan alternativo de comunicaciones, acceso a documentos y coordinación administrativa frente a caídas del proveedor de nube.
- Exigir evidencia de respaldo recuperable, segmentación, control de privilegios y revisión de los sitios públicos WordPress.
- Designar responsables técnicos y de comunicación institucional, con un reporte de estado y pendientes a las 24, 72 horas y 7 días.

2. Alcance, criterio y niveles de prioridad

La ventana del presente documento es del 07/11/2026 al 12/11/2026, conforme a las publicaciones disponibles al cierre. Se distingue la fecha de **incorporación a KEV** de la fecha en la que una CVE fue publicada originalmente. Los antecedentes previos al 7 de noviembre se identifican expresamente cuando mantienen valor preventivo.

Explotación activa significa que existen reportes confiables de uso de la vulnerabilidad en entornos reales; no significa que cada institución esté comprometida. El CVSS cuantifica la severidad técnica, pero la prioridad operativa también depende de versión, exposición, función de negocio y capacidad de contención.

Prioridad	Criterio institucional	Acción mínima
P0 / inmediata	KEV con activo afectado, infraestructura expuesta o indicio de intrusión	Contener, corregir, preservar registros e investigar compromiso.
P1 / 24-72 h	CVSS crítico o sistema de identidad, perímetro o producción muy expuesto	Aplicar actualización validada y comprobar funcionamiento.
P2 / 7 días	Otros avisos relevantes, equipos internos o sin explotación confirmada	Gestionar cambios, verificar versiones y completar inventario.

3. Microsoft 365: análisis de la interrupción del 12 de noviembre

El evento afectó el acceso a buzones de **Exchange Online** mediante Outlook Web, MAPI, ActiveSync y API, con comunicaciones adicionales sobre posibles interrupciones en Teams, SharePoint, Copilot y otros servicios. La empresa reconoció el incidente mediante **EX1550543 / MO1550821**. [F11-F12]

Secuencia técnica informada

- Errores de conectividad en una parte de los servidores que procesaban solicitudes de Exchange Online.
- Incremento de carga de infraestructura y comprobaciones automáticas de salud que retiraban servidores del servicio.
- Medidas de mitigación: redirección de tráfico, reinicio de equipos afectados y pruebas de ajustes en la verificación de salud.
- Investigación de cambios recientes de configuración como factores posibles, sin establecer todavía una causa raíz definitiva.

> **Conclusión técnica:** se trató de un incidente de **disponibilidad de servicios de nube**. No es correcto presentarlo como una caída generalizada de computadoras Windows, como una filtración de datos ni como un ataque informático confirmado.

Riesgos para empresas y organismos públicos

La pérdida de acceso al correo, sistemas colaborativos, archivos y herramientas administrativas puede interrumpir trámites, atención ciudadana, coordinación hospitalaria, facturación y la gestión de emergencias. La criticidad aumenta cuando el proveedor de correo también concentra identidades, documentación y canales internos de emergencia.

Medidas de continuidad concretas

- Mantener un **canal alternativo independiente de Microsoft 365** para crisis y coordinación ejecutiva.
- Conservar fuera del servicio afectado los contactos de guardia, procedimientos críticos, actas y manuales de contingencia.
- Ensayar el acceso a copias recuperables de la documentación esencial y a los sistemas de expedientes en modo degradado.
- Publicar comunicaciones institucionales claras sin atribuir la caída a causas no confirmadas.
- No cambiar DNS, federación de identidad, correo o configuración de seguridad de forma improvisada durante un incidente del proveedor.

4. Vulnerabilidades explotadas: nuevas incorporaciones a CISA KEV

Los días 9 y 10 de noviembre, CISA añadió **diez CVE** al catálogo Known Exploited Vulnerabilities. Su inclusión justifica priorización extraordinaria sobre los productos y versiones realmente afectados. [F01]

CVE	Producto	Impacto principal	Prior.
CVE-2026-116606	Barracuda ESG	Evasión de autenticación, potencial cadena con inyección de comandos	P0
CVE-2026-111560	Barracuda (varios)	Inyección de comandos del sistema	P0
CVE-2026-102895	GPUStack	Obtención de acceso administrativo sin autenticación	P0
CVE-2026-116779	FreeSWITCH	Ejecución de comandos mediante mensaje SIP manipulado	P0
CVE-2026-123218	IBM Aspera Faspex	Elusión de controles de autorización y escalada administrativa	P0
CVE-2026-123158	OpenSSH en musl	Evasión de autenticación solo en configuraciones específicas	P0
CVE-2026-125350	Chromium	Use-after-free en XML; posible ejecución de código	P0
CVE-2026-124194	Microsoft Outlook	Exposición de credenciales NTLMv2 al abrir mensaje preparado	P0
CVE-2026-20320	Cisco BroadWorks	XXE; posible lectura de información sensible	P1
CVE-2026-111793	Openwave Messaging	Procesamiento indebido de archivos multimedia	P1

4.1 Barracuda ESG y otras plataformas

Barracuda confirmó problemas que, combinados, pueden permitir modificar configuración global y ejecutar comandos en dispositivos vulnerables. **Acción:** comprobar versión y firmware, aplicar los parches específicos del fabricante, restringir interfaces de administración, comparar configuraciones anteriores y actuales, auditar accesos y conservar evidencias de modificaciones. [F01-F02]

4.2 GPUStack y sistemas de IA

La CVE-2026-102895 afecta la validación de confianza en la procedencia de solicitudes, que puede derivar en acceso administrativo no autenticado. **Acción:** actualizar al menos a GPUStack 2.2.0 según aviso, revisar cabeceras de proxy inverso, validar autenticación en origen, auditar claves API y secretos de trabajadores y servicios de nube. [F01-F03]

4.3 FreeSWITCH: comunicaciones institucionales

La CVE-2026-116779 permite abusar del tratamiento de mensajes SIP para ejecutar funciones del servidor. **Acción:** actualizar a FreeSWITCH 1.11.3 o versión corregida de la distribución, restringir SIP a operadores confiables cuando sea posible, revisar llamadas anómalas, registros y credenciales. [F01]

4.4 IBM Aspera Faspex

La CVE-2026-123218 permite a un usuario autenticado evadir verificaciones de autorización y elevar privilegios. Afecta versiones 5.0.0 a 5.0.19. **Acción:** actualizar a **5.0.19 PL1**, revisar cuentas administrativas, cambios de permisos y transferencias sensibles. [F04]

4.5 OpenSSH en Linux: condición precisa

La CVE-2026-123158 afecta a OpenSSH anterior a 10.6p2 **cuando se utiliza musl libc sin PAM** y concurren configuraciones particulares de autenticación. No implica exposición automática de sistemas Linux con glibc/PAM. **Acción:** verificar la biblioteca, el uso de PAM, las cuentas configuradas y el parche provisto por el distribuidor; actualizar, deshabilitar autenticación por contraseña cuando sea viable y vigilar accesos. [F05]

4.6 Cisco BroadWorks y Openwave Messaging

Revisar las versiones y aplicar correcciones específicas en BroadWorks y Webtop Media Transcoder. Para BroadWorks reforzar el control de entrada de XML y limitar servicios expuestos; para Openwave, restringir procesamientos multimedia y verificar permisos y registros. No sustituir parches con reglas genéricas de firewall. [F01]

5. Microsoft: Patch Tuesday del 10 de noviembre

El ciclo de actualizaciones de noviembre incluyó más de mil correcciones contabilizadas por reportes especializados bajo diferentes criterios. La medida operativa no depende del total, sino de identificar los CVE aplicables a las versiones instaladas. Es fundamental revisar Windows Server, Active Directory, Microsoft 365 Apps, Office, SQL Server, SharePoint, RDP y componentes de administración. [F06]

5.1 Outlook CVE-2026-124194: explotación activa

La CVE-2026-124194 tiene CVSS 6,5 y explotación confirmada. Al abrir un archivo de mensaje diseñado por un atacante, Outlook puede intentar conectarse a una ubicación remota sin la advertencia habitual y divulgar un **hash NTLMv2**. La vista previa **no** constituye un vector de explotación según Microsoft. [F07]

- Actualizar Microsoft Outlook y Office/Microsoft 365 Apps en los canales de despliegue utilizados.
- Bloquear el tráfico SMB saliente a Internet (TCP 445), salvo excepciones documentadas.
- Reducir NTLM donde sea compatible, proteger cuentas privilegiadas y revisar conexiones de autenticación inusuales.
- Recordar que MFA no neutraliza por sí solo todas las formas de retransmisión NTLM ni sustituye la corrección.

5.2 Active Directory, LDAP y SMB

Entre los CVE que merecen revisión sobre servidores Windows se encuentran **CVE-2026-119958 (LDAP, CVSS 9,8)**, **CVE-2026-118146 (Active Directory, CVSS 8,8)** y **CVE-2026-113825 (SMB Server, CVSS 7,7)**. La corrección depende del producto y la versión concreta. Para esas tres fallas no se presenta aquí explotación activa confirmada. [F06]

- Priorizar controladores de dominio y servidores de archivos; probar autenticación y replicación luego de parchear.
- Desactivar SMBv1; usar SMB 3.x con firma/cifrado cuando corresponda y segmentar acceso a SMB.
- No deshabilitar indiscriminadamente SMB2: en Windows las implementaciones SMB2/SMB3 comparten componentes y podrían afectarse servicios.
- Evitar exposición de RDP, LDAP y SMB a redes no autorizadas; auditar cuentas de servicio y privilegios excesivos.

5.3 Fin de soporte de Windows 11 23H2 Enterprise y Education

El 10 de noviembre finalizó el soporte de seguridad regular para esas ediciones de Windows 11 23H2. Debe completarse la migración hacia una versión con mantenimiento vigente, verificando compatibilidad de aplicaciones críticas y planes de reversión. [F06]

6. Fortinet: alertas publicadas en noviembre

El 11 de noviembre, NHS England comunicó un conjunto amplio de avisos Fortinet: **98 vulnerabilidades**, entre ellas 19 críticas. Su publicación no equivale a explotación activa confirmada de todas ellas; se debe revisar producto, rama y exposición. [F08]

CVE	CVSS	Tipo de falla
CVE-2026-126170	9,8	Tratamiento inseguro de salida; posible ejecución de comandos en ciertos productos de gestión.
CVE-2026-126262	9,3	Inyección SQL.
CVE-2026-126253	9,3	Evasión de autenticación.
CVE-2026-126261	9,0	Autorización incorrecta.
CVE-2026-126259	9,0	Ausencia de autenticación en función crítica.

Acción específica: inventariar FortiOS, FortiManager, FortiAnalyzer y demás productos Fortinet; consultar FortiGuard PSIRT para la **rama instalada**; aplicar las compilaciones corregidas siguiendo la ruta de actualización soportada; restringir la administración remota y revisar accesos, políticas, cuentas y cambios de configuración. Hacer respaldos y documentar la situación previa. [F08-F09]

> **Importante:** las fallas nuevas de Fortinet no deben confundirse con los casos previamente explotados de otros meses. No existe sustento para declarar explotación activa de todas las CVE de esta publicación.

7. SAP: cuatro fallas con CVSS 10,0

SAP publicó su Security Patch Day del 10 de noviembre, con **35 notas nuevas, cuatro avisos de GitHub y tres actualizaciones de notas anteriores**. Cuatro CVE obtuvieron CVSS 10,0; deben verificarse en NetWeaver, Web Dispatcher, Gateway y autenticación SAML2. [F10]

CVE	Plataforma	Tipo de falla
CVE-2026-76964	NetWeaver AS ABAP - ICM	Corrupción de memoria; riesgo de ejecución remota.

CVE	Plataforma	Tipo de falla
CVE-2026-89126	SAP Web Dispatcher	Corrupción de memoria en el tratamiento de tráfico.
CVE-2026-89103	SAP Gateway	Control de acceso incorrecto.
CVE-2026-120017	NetWeaver / SAML2	Falta de autenticación en función crítica.

También se notificaron otros fallos graves en componentes ABAP. **Acción:** aplicar SAP Security Notes según productos y versiones, proteger los servicios expuestos, revisar SAML y cuentas privilegiadas y realizar pruebas de negocio después de actualizar. La identificación de una CVE crítica **no demuestra** que esté siendo explotada en el entorno. [F10]

8. Navegadores, correo y dispositivos personales

8.1 Chrome y Chromium

Google corrigió la **CVE-2026-125350**, un fallo de memoria *use-after-free* en el componente XML de Chromium, incorporado a KEV el 10 de noviembre. Deben actualizarse Chrome, Edge y otros navegadores derivados de Chromium de acuerdo con los avisos de cada fabricante; **cerrar y reabrir** el navegador es necesario para completar la instalación cuando así lo indique. [F01]

La actualización del 9 de noviembre corrige Chrome para Windows/macOS a **157.0.8103.50/.51** y Linux a **157.0.8103.50**. Instalar versiones posteriores cuando existan y comprobar que el navegador se haya reiniciado. [F18]

8.2 Firefox y Thunderbird

Mozilla publicó correcciones el 10 de noviembre para **Firefox 160**, versiones ESR y **Thunderbird 160/ESR**. Entre ellas figuran errores de aislamiento, memoria y escenarios de divulgación de información, incluyendo las CVE-2026-124853, CVE-2026-124855, CVE-2026-126132 y CVE-2026-126134. Actualizar por la rama institucional y revisar extensiones y complementos. [F13]

8.3 Apple

Apple publicó actualizaciones de seguridad el **9 de noviembre**, entre ellas iOS/iPadOS 27.2.1 y actualizaciones de otras plataformas. Los equipos móviles utilizados por directivos y personal de guardia deben estar incluidos en el inventario, con una política de actualización y copias de seguridad. [F14]

9. WordPress y portales gubernamentales

WordPress continúa siendo una superficie sensible por sus plugins, temas, permisos de administración y servidores subyacentes. La versión **7.1.4** fue publicada como actualización de seguridad el **28 de octubre de 2026**, antes de la ventana de este informe, pero sigue siendo imprescindible para sitios rezagados. La CVE-2026-119977 se incorporó a KEV el 3 de noviembre como antecedente relevante. [F15-F16]

Para las instituciones que administran portales sin actualizaciones periódicas, no corresponde asumir que están comprometidos ni que todos comparten las mismas fallas. Es indispensable relevar cada instalación, su versión, plugins y exposición.

Plugins: vulnerabilidades notificadas durante la ventana

Plugin / CVE	Falla	Versión corregida
WP w3all phpBB / CVE-2026-121769	Inyección SQL; CVSS 8,5	3.2.0 o superior
WP2LEADS / CVE-2026-120834	Elevación de privilegios; CVSS 7,3	3.5.18 o superior
WP Activity Log / CVE-2026-121573	XSS almacenado; CVSS 6,5	5.6.8 o superior
JetFormBuilder / CVE-2026-123482	XSS almacenado; CVSS 7,1	3.6.8.1 o superior

Las cuatro entradas poseen **correcciones disponibles** según los avisos consultados. Su inclusión no significa explotación activa confirmada. [F19]

- Realizar un inventario nominal de los sitios, responsables, hosting, WordPress, PHP, plugins y temas.
- Actualizar núcleo y extensiones con copia de seguridad verificada y prueba funcional.
- Retirar plugins sin mantenimiento, con vulnerabilidades conocidas sin parche o que ya no sean necesarios.
- Exigir MFA, mínimos privilegios, registro de accesos y control de cambios a archivos.
- Revisar formularios, expedientes y cualquier integración que procese datos personales; utilizar WAF como defensa complementaria.

10. Infraestructura industrial, edificios y servicios esenciales

CISA publicó avisos de seguridad industrial el 12 de noviembre sobre diversos productos de automatización y redes industriales. Los hospitales, centros de operación, plantas de servicios y edificios gubernamentales deben revisar específicamente dispositivos de control, redes OT, consolas y plataformas de acceso remoto, sin aplicar cambios no probados que afecten operaciones físicas. [F17]

Las medidas incluyen segmentación entre IT y OT, inventario de versiones, coordinación con mantenedores, planificación de ventanas y monitoreo de accesos. En instalaciones críticas, el procedimiento de cambio debe contemplar seguridad operacional y posibilidad de reversión.

11. Plan de intervención por plazos

Plazo	Acciones exigibles	Evidencia de cierre
0-24 horas	Relevar activos KEV; validar exposición de Outlook, Barracuda, FreeSWITCH, GPUStack, Aspera y OpenSSH; verificar comunicación alternativa y backups.	Inventario firmado, responsable designado y lista de sistemas P0.
24-72 horas	Desplegar parches Microsoft, Fortinet y SAP aplicables; actualizar navegadores y clientes; auditar accesos y credenciales; revisar WordPress.	Versiones antes/después, bitácora de cambio, pruebas y registros preservados.
Dentro de 7 días	Probar restauración; revisar segmentación, cuentas administrativas, SMB, continuidad de Microsoft 365 y entornos OT; cerrar excepciones.	Acta de restauración, reporte de pendientes, riesgos aceptados y plan de acción.

Controles mínimos de ciberseguridad

- **Respaldo:** estrategia 3-2-1, al menos una copia inmutable o aislada y restauraciones probadas.
- **Antirransomware:** EDR, segmentación, MFA resistente al phishing cuando sea viable y privilegio mínimo.
- **SMB:** eliminar SMBv1, restringir TCP 445 y aplicar firma/cifrado de SMB3 donde sea compatible.

- **Comunicación:** responsable de prensa y protocolo de avisos a autoridades, personal y ciudadanía.
- **Auditoría:** identificar hallazgo, activo, CVE, versión, cambio, responsable, evidencia y fecha de verificación.
- **Preservación:** ante indicios de intrusión, asegurar registros, hashes y trazabilidad antes de realizar cambios que borren evidencia.

12. Recomendación final para organismos y empresas

Se recomienda dictar una **revisión extraordinaria del estado de seguridad** durante esta semana, con relevamiento, aplicación priorizada de parches, validación de la recuperación y una comunicación centralizada. Las decisiones deben sustentarse en activos realmente afectados y fuentes oficiales, no en titulares ni en la gravedad nominal de una CVE aislada.

La caída de Microsoft 365 demuestra que incluso sin un ataque confirmado puede existir una interrupción operativa de alto impacto. Por eso, junto con las correcciones, las autoridades deberían aprobar un **plan verificable de continuidad institucional**, incluyendo responsables alternativos, documentación offline, respaldos recuperables y protocolos de atención al público.

El presente documento tiene carácter técnico y preventivo. No implica que un organismo específico posea los productos afectados o haya sido vulnerado; esa condición debe establecerse mediante inventario, auditoría y revisión de evidencias.

13. Fuentes oficiales y de referencia

Las referencias siguientes permiten comprobar el estado de las alertas al corte. Las versiones corregidas deben reconfirmarse en el aviso vigente de cada fabricante antes de intervenir.

[F01] CISA - Known Exploited Vulnerabilities Catalog
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[F02] Barracuda - Security Updates
https://www.barracuda.com/support/security

[F03] GPUStack - Advisory GHSA-gj9m-f8ph-pmhr
https://github.com/gpustack/gpustack/security/advisories/GHSA-gj9m-f8ph-pmhr

[F04] IBM - Security bulletin Aspera Faspex CVE-2026-123218
https://www.ibm.com/support/pages/security-bulletin-ibm-aspera-faspex-has-addressed-vulnerability-could-allow-authorization-bypass

[F05] NVD - OpenSSH CVE-2026-123158
https://nvd.nist.gov/vuln/detail/CVE-2026-123158

[F06] Microsoft - Security Update Guide, noviembre 2026
https://msrc.microsoft.com/update-guide/releaseNote/2026-Nov

[F07] Microsoft - CVE-2026-124194 Outlook
https://msrc.microsoft.com/security-guidance/advisory/CVE-2026-124194

[F08] NHS England - Fortinet multiple vulnerabilities, CC-4888
https://digital.nhs.uk/cyber-alerts/2026/cc-4888

[F09] FortiGuard - Fortinet PSIRT
https://fortiguard.fortinet.com/psirt

[F10] SAP - November 2026 Security Patch Day
https://support.sap.com/en/my-support/knowledge-base/security-notes-news/november-2026.html

[F11] Microsoft 365 status - incidente EX1550543 / MO1550821 (resumen público)
https://isdown.app/status/microsoft365/incidents/685663-users-may-be-unable-to-connect-to-their-mailboxes-in-exchange-online-through-multiple-connection-methods

[F12] BleepingComputer - Microsoft 365 outage, 12/11/2026
https://www.bleepingcomputer.com/news/microsoft/massive-microsoft-365-outage-disrupts-outlook-teams-copilot-worldwide/

[F13] Mozilla - Foundation Security Advisories
https://www.mozilla.org/en-US/security/advisories/

[F14] Apple - Security content iOS 27.2.1
https://support.apple.com/en-us/149715

[F15] WordPress - 7.1.4 security release
https://wordpress.org/news/2026/10/wordpress-7-1-4/

[F16] NVD - WordPress CVE-2026-119977
https://nvd.nist.gov/vuln/detail/CVE-2026-119977

[F17] CISA - ICS Advisories
https://www.cisa.gov/news-events/ics-advisories

[F18] Centro Canadiense de Ciberseguridad - Chrome AV26-1140
https://www.cyber.gc.ca/en/alerts-advisories/google-security-advisory-av26-1140

[F19] Patchstack - WordPress plugin vulnerability database
https://patchstack.com/database/wordpress/

14. Anexo ejecutivo: instrucciones para autoridades

Hoja de lectura rápida para distribuir a ministerios, dependencias, hospitales y organismos descentralizados. Cada responsable debe marcar cumplimiento, informar excepciones y remitir evidencia técnica.

Instrucción operativa	Área responsable	Plazo
Actualizar navegadores, Outlook y los equipos alcanzados por KEV.	TI / Soporte	24 h
Revisar controladores de dominio, LDAP, SMB, acceso remoto y credenciales.	Infraestructura	24-72 h
Verificar actualizaciones Fortinet, SAP y dispositivos perimetrales.	Redes / Sistemas	72 h
Auditar WordPress y sus plugins; retirar componentes abandonados.	Web / Aplicaciones	72 h
Probar respaldos, restauración y comunicación alternativa a Microsoft 365.	Continuidad / TI	7 días
Designar vocero y protocolo de aviso para personal y ciudadanía.	Dirección / Prensa	24 h
Conservar registros e investigar signos de compromiso cuando corresponda.	Seguridad / Forense	Inmediato
Elevar informe con activos corregidos, pendientes y responsables.	Dirección de TI	7 días

Constancia de gestión: la decisión de no aplicar una corrección dentro del plazo recomendado debe documentarse, con motivo, riesgo remanente, medidas compensatorias y autoridad responsable.

Elaborado por: Pedro Matías Cacivio
Instel & Seguridad · Análisis forense, auditoría y pentesting
Fecha de emisión: 12 de noviembre de 2026

14. Adenda de actualización - últimas 12 horas

Período de revisión: del 12/11/2026 a las 23:04 al 13/11/2026 a las 11:04 (hora de Argentina, UTC-3). **Edición:** ampliación del informe emitido con corte al 12/11/2026. Se mantiene íntegro el análisis original y se identifican aquí las novedades verificadas y su fecha real de publicación.

En esta ventana se registraron **nuevas publicaciones formales de CVE** sobre productos de gestión de datos y sitios web, y una confirmación periodística de un problema operativo de activación de Windows documentado por Microsoft. No se identificaron **nuevas incorporaciones al catálogo CISA KEV** posteriores al 10/11 en las fuentes consultadas al corte [A01-A03].

> **Criterio de rigurosidad:** las CVE registradas el 13/11 remiten a avisos GitHub de octubre. Por tanto, la novedad es su **formalización CVE**, no el descubrimiento del problema ni un parche liberado necesariamente en las últimas doce horas. Los incidentes de disponibilidad no se clasifican como vulnerabilidades explotables.

14.1 Matriz de novedades publicadas el 13 de noviembre

Identificador / activo	Vulnerabilidad / efecto	Versión / solución	Prioridad
CVE-2026-126269 NocoDB	XSS persistente por tipo MIME de adjuntos; requiere Editor autenticado y puede exponer sesiones.	Afecta **< 2026.09.0**; corregido en **2026.09.0**.	P1
CVE-2026-126274 NocoDB	XSS persistente en diálogo de eliminación de tabla, con rol Creator autenticado y acción de la víctima.	Afecta **< 2026.08.0**; corregido en **2026.08.0**.	P1
CVE-2026-126286 NocoDB	XSS reflejado por URL de salida manipulada; riesgo de robo de sesión al acceder al enlace.	Afecta **< 2026.08.0**; corregido en **2026.08.0**.	P1
CVE-2026-126370 Vvveb	RCE con rol administrativo limitado mediante editor de código; se requiere autenticación.	Afecta **≤ 1.0.8.6**; **sin versión corregida** en el aviso.	P0/P1
Microsoft Windows licencias/KMS	Operaciones de activación fallan con **0x80041008** tras parches de noviembre. No es CVE.	Solución definitiva pendiente en el corte; soporte empresarial para mitigación.	Operativa

Fuente y estado: registros CVE del 13/11; avisos de los proyectos y notas de Microsoft [A02-A08]. P0/P1 representa prioridad contextual, según exposición y privilegios existentes. **No se ha confirmado explotación activa** de las cuatro CVE anteriores en los avisos revisados.

15. Recomendaciones técnicas para nuevas publicaciones

15.1 NocoDB: actualización y control de sesiones

La combinación de CVE-2026-126269, CVE-2026-126274 y CVE-2026-126286 afecta al tratamiento de adjuntos y enlaces o a vistas de interfaz. Su consecuencia relevante es la posibilidad de ejecutar JavaScript con el origen de la aplicación, con exposición de tokens y suplantación de sesiones en escenarios específicos. Las fichas CVE se publicaron el **13/11**; los avisos de GitHub datan del **27/10** [A02-A05].

- **Acción:** actualizar a **NocoDB 2026.09.0 o posterior**, que cubre los rangos señalados; comprobar la rama efectivamente desplegada antes de intervenir.
- Examinar cuentas Editor/Creator, privilegios, tokens, sesiones y registros de API; invalidar sesiones solo cuando exista evidencia o sospecha razonable de exposición.
- Aplicar CSP apropiada, restricciones de carga de adjuntos y control de acceso; estas medidas no sustituyen la actualización.

15.2 Vvveb: ejecución de código desde cuenta de privilegio limitado

La CVE-2026-126370, formalizada el 13/11, describe ejecución de código en **Vvveb 1.0.8.6 o anteriores** mediante controles insuficientes del editor para un rol *site_admin*. La vulnerabilidad ya había sido divulgada en GitHub el **29/10**. En el aviso consultado no figura una versión corregida [A06].

- Identificar instalaciones Vvveb; impedir el acceso al editor administrativo desde redes no autorizadas y revisar usuarios con roles de edición.
- Restringir o deshabilitar temporalmente funciones de edición de código que no sean indispensables, mediante controles de acceso documentados; revisar archivos modificados y logs.
- Solicitar al proveedor la corrección y validar la versión reparada antes de reabrir funcionalidades. Si existen indicios de intrusión, preservar evidencia antes de la intervención.

16. Microsoft: confirmación del 13/11 y consideraciones operativas

El **13/11 a las 04:36**, BleepingComputer informó que Microsoft reconoce fallas de activación y gestión de licencias tras parches de noviembre. Las páginas oficiales de KB habían incorporado la incidencia el 11/11, por lo que **la novedad en esta ventana es la publicación de seguimiento**, no un parche nuevo. Afecta operaciones con comandos **slmgr.vbs /skms-domain** o **/ipk**, que pueden arrojar **0x80041008** [A07-A08].

> **Importante:** no equivale a la interrupción de Microsoft 365 del 12/11 ni implica que las estaciones Windows ya activadas queden desactivadas. Microsoft indica que los dispositivos previamente activados y sin cambios de KMS normalmente no resultan afectados.

- Relevar scripts de despliegue, imágenes corporativas, tareas KMS y procedimientos automatizados de instalación de claves.
- No revertir masivamente actualizaciones de seguridad por este inconveniente. Si hay impacto real, abrir caso de soporte empresarial Microsoft y seguir las instrucciones oficiales.
- Antes de actualizar de manera masiva, validar parches en un grupo piloto y conservar evidencia de activación y resultados operativos.

16.1 CISA KEV: estado al nuevo corte

Los datos públicos consultados el 13/11 muestran como última incorporación el lote del **10/11/2026**. No corresponde informar nuevos zero-days KEV en estas doce horas. Permanecen vigentes obligaciones de corrección de equipos afectados, y el **13/11** coincide con fechas de remediación para **CVE-2026-111560** y **CVE-2026-116606** (Barracuda) y **CVE-2026-118527** (Ivanti) según el catálogo consultado. Las fechas aplican a organismos federales de EE. UU.; en Argentina son señales de prioridad técnica, no plazos legales locales [A01].

17. Seguimiento adicional: alertas del 12/11 sin hora certificada

Se identificaron también dos avisos de fabricante fechados el **12/11** que no estaban desarrollados en el cuerpo principal. Las fuentes no aportan una hora pública concluyente que permita asegurar que se emitieron dentro de las doce horas estrictas de esta adenda. Se incluyen expresamente como **seguimiento complementario**, no como novedades horarias verificadas.

17.1 Check Point: PHP2Shell con explotación confirmada

Check Point confirmó explotación real de **CVE-2026-109618 / CVE-2026-109619** combinadas con **CVE-2026-123039**, que permite elevación local de privilegios en Gaia. Los ataques examinados ocurrieron entre el 30/10 y el 04/11, afectaron a sistemas sin corregir y, en pocos casos, incluyeron actividad destructiva. El anuncio es del 12/11, por lo tanto **no debe presentarse como un ataque ocurrido hoy** [A09].

- Instalar el **November Jumbo Hotfix** en Security Gateways y Management Servers según indicaciones de Check Point; priorizar Mobile Access expuesto a Internet.

- Revisar especialmente logs, persistencia, ficheros de sesión PHP y procesos anómalos. Preservar evidencia si se detectan indicadores de intrusión.

17.2 Citrix NetScaler Console: CVE-2026-120869

Citrix publicó el 12/11 una evasión de autenticación en **NetScaler Console 14.1 anterior a 14.1-74.34**, con **CVSS v4.0: 9,4**. Requiere acceso de red a la IP de la consola, por lo que la exposición debe evaluarse de forma específica. La corrección publicada es **14.1-74.34 o posterior**; no se constató explotación activa en el aviso [A10].

- Actualizar la consola conforme al fabricante, aislarla en la red de administración y auditar accesos administrativos y cambios de configuración.

18. Instrucciones de cierre para organismos y empresas

Plazo sugerido	Acción responsable	Evidencia de cierre
0-24 horas	Localizar NocoDB, Vvveb, Citrix Console y Check Point expuestos. Revisar los productos ya en KEV y aplicar corrección o aislamiento.	Inventario por IP y versión, ticket, responsable y decisión de contención.
24-72 horas	Actualizar NocoDB y Citrix; aislar funciones Vvveb sin parche; aplicar hotfix Check Point y revisar indicios.	Versiones antes/después, registros preservados, pruebas funcionales y validación del proveedor.
Durante 7 días	Validar procesos KMS/SLMGR, restauración de respaldos, vigilancia de sesiones y cuadro de riesgos residuales.	Resultados de pruebas, acta de revisión y excepciones firmadas.

Conclusión: sí surgieron nuevos registros de CVE formalizados el 13/11 y un seguimiento operativo de Microsoft, pero no se identificaron nuevas incorporaciones KEV al corte. La prioridad institucional sigue siendo **verificar el inventario y corregir equipos realmente afectados**, con controles compensatorios cuando no exista versión reparada.

18.1 Fuentes y trazabilidad de la ampliación

[A01] CISA KEV, catálogo y seguimiento (última adición del 10/11)
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[A02] CVE-2026-126269, registro del 13/11
https://app.opencve.io/cve/CVE-2026-126269

[A03] CVE-2026-126274, registro del 13/11
https://app.opencve.io/cve/CVE-2026-126274

[A04] CVE-2026-126286, registro del 13/11
https://app.opencve.io/cve/CVE-2026-126286

[A05] NocoDB GHSA, versiones corregidas
https://github.com/nocodb/nocodb/security/advisories/GHSA-3f7w-wqf7-786q

[A06] Vvveb, GHSA-2mq4-4q7r-q52q, sin parche publicado
https://github.com/givanz/Vvveb/security/advisories/GHSA-2mq4-4q7r-q52q

[A07] Microsoft: KB5131080, incidencia 0x80041008
https://support.microsoft.com/es-es/servicing/os/windows-server/2026/11/kb5131080-windows-server-2025-security-update

[A08] BleepingComputer: incidencia de activación, 13/11
https://www.bleepingcomputer.com/news/microsoft/microsoft-confirms-windows-activation-failures-after-november-updates/

[A09] Check Point: explotación PHP2Shell y Gaia, 12/11
https://blog.checkpoint.com/security/security-advisory-active-exploitation-of-php2shell-and-local-privilege-escalation/

[A10] Citrix: CVE-2026-120869, aviso oficial 12/11
https://support.citrix.com/external/article/CTX697320/citrix-netscaler-console-security-bullet.html

Nota metodológica: se priorizaron avisos originales de fabricantes y registros CVE con fecha identificable. El contenido puede evolucionar al publicarse nuevos parches o análisis forenses. Toda confirmación de exposición requiere contrastar el activo real, su configuración, versión y accesibilidad.