ALERTA TÉCNICA DE CIBERSEGURIDAD



INSTEL & SEGURIDAD

ANÁLISIS FORENSE - AUDITORÍA - PENTESTING

VULNERABILIDADES CRÍTICAS, NUEVOS EXPLOITS Y PARCHES DE SEGURIDAD

WordPress · Navegadores · VPN · NAS · Administración de servidores · IA

IDENTIFICACIÓN	ALCANCE Y FECHA
DESTINATARIOS	Responsables de TI, empresas, organismos gubernamentales, centros de salud y proveedores.
ELABORADO POR	Pedro Matías Cacivio · Instel & Seguridad
PERÍODO	30/10/2026 22:00 al 02/11/2026 17:10 (hora argentina)
CRITERIO OPERATIVO	Prioridad crítica · Corrección y contención inmediata según exposición

DOCUMENTO TÉCNICO DE DIFUSIÓN CONTROLADA · FUENTES OFICIALES Y TÉCNICAS CITADAS

El presente informe constituye una alerta preventiva: la afectación de un activo requiere verificar producto, versión y exposición. No acredita por sí mismo una intrusión ni autoriza pruebas de explotación sobre producción.

1. Resumen ejecutivo

La revisión identificó vulnerabilidades recientes que permiten ejecución remota de código (RCE), subida de archivos peligrosos, evasión de autenticación y acciones administrativas no autorizadas. Los principales vectores son componentes expuestos a Internet, plugins de WordPress, plataformas de acceso remoto, herramientas de administración, NAS con servicios PHP y componentes de IA. La corrección debe priorizar activos realmente afectados, exposición, importancia de los datos y evidencia de explotación, no únicamente la puntuación CVSS.

La novedad operativa más urgente del 2 de noviembre es la publicación de correcciones adicionales para Ivanti Connect Secure. La cadena de fallas había sido utilizada en ataques reales; los parches iniciales de octubre cerraban la vía principal de entrada, pero no corregían todas las fallas asociadas. Las ramas corregidas para las dos vulnerabilidades adicionales incluyen 25.1.1.3 y 22.8R2.6. [F01–F02]

El segundo foco es WordPress: varios CVE formalizados el 31 de octubre afectan plugins específicos, algunos con CVSS 9.8 y explotación posible sin autenticación. Su severidad no implica que todos los WordPress sean vulnerables: deben coexistir el complemento y la versión afectados. [F03–F08]

Por último, los navegadores requieren una política institucional propia. Aunque las publicaciones relevantes de Chrome, Firefox y Edge anteceden al corte inicial, la instalación efectiva puede retrasarse y dejar estaciones de trabajo expuestas durante días o semanas. [F14–F16]

Conclusiones que requieren decisión directiva

- Aprobar actualización urgente de cualquier VPN Ivanti afectada y una revisión de compromiso incluso después de parchear.
- Disponer un inventario exhaustivo de sitios WordPress, plugins, temas y servidores PHP; retirar componentes sin mantenimiento o sin corrección disponible.
- Hacer obligatoria la actualización gestionada de navegadores y el reinicio controlado del proceso para completar la instalación.
- Verificar que NAS y respaldos no compartan el mismo dominio de compromiso; mantener copias aisladas e inmutables cuando sea posible.
- Exigir evidencia de versión antes/después, pruebas funcionales, control de integridad y cierre documentado de cada hallazgo.

2. Alcance y criterio de clasificación

La ventana principal es el 30/10/2026 desde las 22:00 hasta el 02/11/2026 a las 17:10 (UTC−3). Algunos avisos originales son anteriores, pero se incluyen cuando su registro CVE, corrección o ampliación oficial ocurrió dentro de la ventana. Para navegadores y amenazas explotadas previamente se incorpora una sección de seguimiento por su valor preventivo, identificada expresamente como antecedente.

Estados diferenciados: (a) vulnerabilidad publicada; (b) solución disponible; (c) prueba de concepto/exploit público; (d) explotación en ataques reales confirmada. La existencia de un exploit público NO prueba explotación activa, y un CVSS alto NO prueba afectación a un cliente específico.

3. Matriz de prioridad técnica

Activo / CVE	Condición y efecto	Corrección / contingencia	Prioridad
Ivanti ICS: CVE-2026-104935, -111357, -118527	Explotación real confirmada; cadena de acceso y escalamiento.	25.1.1.3 / 22.8R2.6 o rama soportada correcta; investigar compromiso. [F01–F02]	P0
WP Project Manager CVE-2026-116512	RCE sin autenticación; plugin <=4.1.1.	>=4.1.2; desactivar si no puede corregirse. [F03]	P0
WP SimpleForm CVE-2026-118235	Subida de archivo peligroso; <=3.10.2; RCE posible.	>=3.11.0; revisar uploads y permisos. [F04]	P0

Activo / CVE	Condición y efecto	Corrección / contingencia	Prioridad
WP PDF Invoice CVE-2026-109220	Inyección de objetos PHP/RCE; <=7.1.1.	>=7.2.0; revisar pedidos y logs. [F05]	P0
Prefab UI CVE-2026-120338	Escape de sandbox de código generado por IA; 0.14.0–0.20.2 bajo condiciones específicas.	>=0.21.0; desactivar función vulnerable hasta actualizar. [F09]	P0/P1
Jpom CVE-2026-120201	Evasión de autenticación y administración remota; 2.10.0–2.11.12.	Aislamiento / ACL / VPN / revisión de fabricante; parche no confirmado. [F10]	P0/P1
WAVLINK CVE-2026-120345	Inyección remota de comandos; firmware señalado; exploit público.	Sin parche verificado; restringir exposición / sustituir si corresponde. [F11]	P0/P1
Synology PHP2Shell -109618, -109619	RCE potencial en determinados paquetes PHP; aviso ampliado el 31/10.	Actualizar PHP y paquetes DSM según matriz oficial; PHP 7.3 sin parche. [F12]	P0/P1
WP LearnDash CVE-2026-119096	Evasión de aprobación/suspensión CON credenciales válidas; <=3.8.2.	>=3.8.3; invalidar sesiones y revisar cuentas. [F06]	P1
WP Popup Builder CVE-2026-89270	Despublicación masiva de popups; <=4.4.5; NO es RCE.	>=4.4.6; comprobar integridad de contenidos. [F07]	P1
GitLab CVE-2026-97229	RCE crítica previamente publicada y catalogada como explotada.	19.2.8 / 19.3.5 / 19.4.2 según rama. [F17]	P0/P1
Chrome / Firefox / Edge	Fallas de memoria, sandbox y origen; parches previos al intervalo.	Actualizar al último estable soportado por fabricante/OS y verificar reinicio. [F14–F16]	P1

P0: acción inmediata si el activo está instalado y expuesto o existe sospecha de explotación. P1: corrección prioritaria planificada, habitualmente dentro de 24–72 horas según riesgo. Los plazos son objetivos internos sugeridos, no instrucciones universales del fabricante.

4. WordPress: importancia crítica de los complementos

WordPress aloja portales de comunicación, trámites, turnos, inscripciones, sitios de instituciones y tiendas. El riesgo reside principalmente en la combinación entre núcleo, plugins, temas, bibliotecas, PHP, servidor web, cuentas y permisos. Un plugin vulnerable puede habilitar una intrusión sin que el atacante conozca contraseñas administrativas y aunque el sitio utilice HTTPS, antivirus o un firewall convencional.

4.1 Vulnerabilidades principales

CVE-2026-116512 — Project Manager (weDevs)

CVSS V3.1: 9.8 · CRÍTICA | Versiones <=4.1.1. Una validación insegura en la API REST permite ejecución de código sin autenticación antes de aplicar el control de permisos.

Medidas indicadas: Actualizar inmediatamente a 4.1.2 o posterior; si no es viable, desactivar el plugin y restringir acceso al sitio mientras se evalúa; revisar integridad de archivos PHP, usuarios administradores y registros REST.

Sustento: [F03].

CVE-2026-118235 — SimpleForm

CVSS V3.1: 9.8 · CRÍTICA | Versiones <=3.10.2. Un defecto de validación permite subir archivos peligrosos a través de formularios públicos y podría habilitar RCE en determinados servidores.

Medidas indicadas: Actualizar a 3.11.0 o posterior; verificar directorios de subida, evitar ejecución de PHP en uploads y comprobar cuentas nuevas o cambios no autorizados.

Sustento: [F04].

CVE-2026-109220 — PDF Invoice for WooCommerce

CVSS V3.1: 9.8 · CRÍTICA | Versiones <=7.1.1. Deserialización de datos derivados de notas del proceso de compra, con posibilidad de RCE sin autenticación en el flujo vulnerable.

Medidas indicadas: Actualizar a 7.2.0 o posterior; revisar eventos de checkout, modificaciones de archivos e integridad del servidor; conservar registros ante indicios.

Sustento: [F05].

CVE-2026-119096 — Uncanny Toolkit for LearnDash

CVSS V3.1: 9.8 · CRÍTICA | Versiones <=3.8.2. Elude comprobaciones de aprobación o suspensión de cuentas, pero requiere conocer las credenciales de una cuenta afectada. No es acceso universal sin contraseña.

Medidas indicadas: Actualizar a 3.8.3; revisar cuentas suspendidas, cerrar sesiones sospechosas, exigir MFA y rotar credenciales comprometidas.

Sustento: [F06].

CVE-2026-89270 — Popup Builder

CVSS V3.1: 9.1 · CRÍTICA | Versiones <=4.4.5. Permite enviar a la papelera popups publicados sin autenticación. El impacto principal es integridad/disponibilidad del contenido; no es ejecución de código.

Medidas indicadas: Actualizar a 4.4.6; comprobar que avisos de privacidad, seguridad o comunicaciones críticas no hayan sido ocultados.

Sustento: [F07].

CVE-2026-103882 — Acadlix LMS

CVSS V3.1: 9.1 · CRÍTICA | Versiones <=1.1.9. Eliminación de archivos arbitrarios, potencialmente con impacto grave según ubicación y privilegios. El comportamiento de la validación del endpoint puede reducir controles de acceso previstos.

Medidas indicadas: Retirar temporalmente de exposición si se usa; confirmar una versión reparada con el fabricante y restaurar únicamente archivos verificados si hubo alteraciones.

Sustento: [F08].

4.2 Medidas obligatorias para sitios WordPress

- Inventario: identificar cada dominio, subdominio, proveedor de hosting, versión del núcleo, PHP, plugins (incluso inactivos), temas y usuarios con privilegios.
- Actualización: aplicar primero los parches críticos en una ventana controlada tras copia verificable. Mantener política de actualizaciones automáticas para componentes compatibles y un circuito de pruebas para sitios complejos.
- Retirada: eliminar (no solo desactivar) plugins abandonados, duplicados, sin mantenimiento, sin necesidad operativa o sin corrección conocida.
- Autenticación: MFA para administradores, mínimo privilegio, cuentas individuales, restricción de inicio de sesión y revisión de sesiones y claves de aplicación.
- Servidor: impedir ejecución de scripts en directorios de archivos subidos, limitar permisos de escritura del usuario web, proteger secretos y no permitir edición de archivos PHP desde el panel.
- Aislamiento: separar cada instalación del resto de los portales y de servidores internos, bases de datos y respaldos. Aislar el sitio comprometido para evitar desplazamiento lateral.
- Controles compensatorios: WAF, reglas de API REST y limitación de solicitudes cuando estén justificadas; jamás considerarlos equivalentes a aplicar el parche.
- Monitoreo: registros HTTP/PHP/WAF, integridad de archivos, usuarios, tareas programadas, endpoints REST, alertas ante cambios y revisiones posteriores a las actualizaciones.

- Respaldo: copia de base de datos y archivos, retención de versiones, almacenamiento externo, recuperación ensayada y verificación de que el backup no contiene el compromiso.
- Revisión contractual: exigir al proveedor responsabilidades, tiempos de parcheo, notificación de incidentes, evidencias de actualizaciones y acceso a logs.

4.3 Cómo comprobar el estado sin hacer pruebas intrusivas

Con acceso administrativo autorizado se recomienda exportar el inventario de WordPress y plugins; comparar versiones exactas contra los avisos originales y registrar la hora de verificación. WP-CLI permite listar el estado, la versión y las actualizaciones pendientes con salida CSV. [F18]

Ejemplo de inventario local: `wp plugin list --fields=name,status,version,update,update_version,auto_update --format=csv`

No se recomienda validar estos CVE mediante cargas maliciosas contra sitios de producción. La confirmación de exposición se realiza preferentemente por inventario y comparación de versiones; las PoC, exclusivamente en laboratorios autorizados.

5. VPN, acceso remoto y explotación real: Ivanti Connect Secure

Las vulnerabilidades CVE-2026-104935, CVE-2026-111357 y CVE-2026-118527 pueden encadenarse para comprometer dispositivos Ivanti Connect Secure. Hay informes de explotación real confirmada. El 02/11/2026 se comunicaron correcciones adicionales: 25.1.1.3 y 22.8R2.6 para las fallas CVE-2026-111357 y -118527. Las correcciones de octubre para -104935 no eran suficientes para todo el conjunto. [F01–F02]

Medidas de contención y respuesta

- Verificar modelo, versión, rama y boletín de Ivanti; instalar la versión adecuada sin esperar el mantenimiento mensual.
- Antes de un reinicio, restauración o reconstrucción, preservar logs y evidencia volátil cuando el contexto lo permita y exista personal forense responsable.
- Revisar sesiones VPN, cuentas, certificados, cambios de configuración, rutas, reglas y eventos anómalos; no confiar en un único verificador de integridad negativo.
- Rotar contraseñas, tokens y secretos potencialmente expuestos según alcance del incidente; reforzar MFA y revocar sesiones no confiables.
- Si aparecen indicadores de intrusión, aislar de forma controlada y considerar reconstrucción desde imagen confiable con apoyo del fabricante.
- Correlacionar logs perimetrales, identidad, DNS, EDR y controladores de dominio para detectar movimiento lateral.

La incorporación de dos de estas vulnerabilidades a CISA KEV ocurrió el 30/10, antes del inicio de la ventana de 22:00; lo novedoso del 02/11 son las correcciones adicionales y la confirmación operativa del alcance de los parches. [F02]

6. PHP2Shell, Synology y seguridad de los respaldos

PHP2Shell comprende CVE-2026-109618 y CVE-2026-109619: vulnerabilidades críticas de corrupción de memoria con posible ejecución remota de código en determinados contextos PHP. Se publicaron parches upstream el 21/10. El aviso oficial Synology-SA-26:14 fue actualizado el 31/10 y especifica versiones corregidas para Calendar, Mail Station y PHP según DSM; también aclara que Hyper Backup NO está afectado en ese aviso y que PHP 7.3 carece de corrección. [F12–F13]

Es incorrecto concluir que cualquier NAS Synology está automáticamente explotable por el mero hecho de ejecutar DSM: la exposición depende del paquete, la versión, la configuración y su accesibilidad. Aun así, los NAS merecen máxima protección porque almacenan información y copias de seguridad esenciales.

Medidas de protección

- Actualizar DSM y paquetes PHP relacionados conforme a la matriz oficial de Synology; en PHP 7.3, migrar o desactivar la funcionalidad afectada.
- Eliminar exposición pública directa de paneles DSM, Web Station o servicios innecesarios; usar VPN, ACL, MFA y segmentación de gestión.

- Verificar privilegios, accesos SMB/NFS, cuentas de servicio y vínculos entre NAS y dominio corporativo.
- Mantener al menos una copia desconectada o inmutable que no pueda borrarse con las mismas credenciales utilizadas por el servidor operativo.
- Ensayar recuperaciones completas y parciales; registrar RPO/RTO factibles, resultado, responsable y fecha.
- Ante posible compromiso, preservar evidencias, cortar accesos de escritura sospechosos y evitar restaurar sobre sistemas aún comprometidos.

7. Herramientas de administración, IA e infraestructura de red

7.1 Jpom — CVE-2026-120201

Afecta Jpom 2.10.0–2.11.12 y se publicó el 31/10. La falla permite evadir autenticación y potencialmente obtener privilegios de superadministrador, desde los cuales podrían ejecutarse operaciones remotas. No se confirmó en la revisión una versión corregida publicada; no debe inventarse número de parche. [F10]

Medidas: comprobar uso de Jpom, restringir inmediatamente su interfaz a red de administración/VPN, aplicar listas de IP permitidas y autenticación aguas arriba; revisar comandos ejecutados, tokens y cambios; consultar al fabricante y retirar de exposición hasta que exista corrección validada.

7.2 Prefab UI / FastMCP — CVE-2026-120338

Publicada el 01/11, con severidad crítica (CVSS v3.1: 10.0 según el registro consultado). En Prefab UI 0.14.0–0.20.2 el sandbox de Generative UI puede permitir acceso indebido a archivos del servidor. El escenario depende de la función opcional de generación de UI, presencia de Deno y posibilidad de aportar código al servicio; no afecta automáticamente a todo servidor con IA. Corregida en Prefab UI 0.21.0. [F09]

Medidas: verificar presencia de Prefab UI y la función Generative UI; actualizar a >=0.21.0, desactivar temporalmente la integración vulnerable, exigir autenticación y autorización de herramientas MCP, eliminar permisos excesivos del proceso y monitorear modificaciones de archivos y dependencias.

7.3 WAVLINK WN551X3-A — CVE-2026-120345

Publicada el 02/11; se describió inyección de comandos en el manejador DNS del firmware M51X3_V251020-WO-182e965. Existe referencia a exploit público, pero ello no prueba explotación activa. No se identificó versión corregida del fabricante en el corte. [F11]

Medidas: localizar el modelo, identificar firmware, impedir administración desde WAN, restringir funciones expuestas y actualizar cuando exista firmware validado; si el producto no obtiene reparación dentro de una ventana aceptable, evaluar su retiro o sustitución. Evitar pruebas ofensivas sobre dispositivos en producción.

7.4 Otros antecedentes de riesgo relevante

WSO2 API Manager y componentes asociados — CVE-2025-11969: control de acceso incorrecto en API de sistema, aviso original de enero de 2026; una nueva ficha CVE no convierte el fallo en descubrimiento de noviembre. Requiere revisar versiones y correcciones del fabricante. [F19]

GitLab — CVE-2026-97229: RCE crítica que afecta ramas 19.2, 19.3 y 19.4 previas a 19.2.8, 19.3.5 y 19.4.2. Se incluye como antecedente de explotación y obligación de verificación, no como fallo descubierto durante el fin de semana. [F17]

8. Navegadores: una amenaza cotidiana que suele subestimarse

Chrome, Firefox y Microsoft Edge procesan contenido no confiable de manera permanente: páginas, documentos, scripts, publicidad, PDFs y extensiones. Las fallas de memoria, navegación, control de origen, uso de recursos liberados y sandbox pueden ser aprovechadas mediante contenido especialmente manipulado. No es necesario que el usuario instale conscientemente software malicioso para que exista riesgo.

Las actualizaciones de seguridad de navegadores son relevantes tanto en Windows como en GNU/Linux y macOS. Un navegador actualizado puede seguir siendo vulnerable si el sistema operativo, una extensión, WebView, un runtime o una biblioteca subyacente permanece sin corregir.

Publicaciones de referencia (anteriores al corte principal)

Navegador	Publicación verificada	Importancia operativa
Google Chrome	29/10/2026: rama estable 156.0.8078.79/.80 en Windows/macOS y 156.0.8078.79 en Linux. 21 correcciones de seguridad, incluida CVE-2026-76024 crítica. [F14]	Verificar build instalada y actualización concluida; si se publica otra versión, prevalece la más reciente soportada.
Mozilla Firefox	27/10/2026: Firefox 159; correcciones de SOP, escape de sandbox, elevación de privilegios y otros defectos. [F15]	Actualizar Firefox o ESR vigente por canal soportado; Firefox ESR 153.6.0 se identifica en documentación empresarial.
Microsoft Edge	30/10/2026: versión estable 156.0.4314.58. Publicada antes de las 22:00 (Argentina). [F16]	Administrar actualizaciones con políticas de empresa; comprobar reinicio y estado real, no solo descarga.

Política sugerida de actualización de navegadores

- Inventariar navegadores instalados, incluyendo secundarios, portables y motores embebidos cuando sea posible.
- Aplicar actualizaciones de seguridad críticas mediante canal estable soportado, gestión centralizada y reinicio o relanzamiento obligatorio en plazo definido.
- Definir SLA sugerido: explotación activa confirmada o vulnerabilidad crítica expuesta, lo antes posible y normalmente <=24 h; alta severidad, <=72 h tras validación.
- Bloquear extensiones no autorizadas, revisar permisos y restringir instalación de software en puestos de trabajo.
- Controlar navegación de administradores desde estaciones separadas de los entornos de usuario final y servicios públicos.
- Actualizar sistema operativo, runtime, bibliotecas, WebView y herramientas relacionadas; no asumir que la actualización del navegador corrige el resto del equipo.
- Exigir evidencia por equipo: nombre, usuario responsable, versión previa/nueva, canal, última comprobación y reinicio necesario o ejecutado.
- Revisar alertas EDR, descargas, redirecciones, autenticaciones anómalas y extensiones inesperadas ante sospecha de explotación.

Por qué esto importa a directivos y usuarios

El navegador es la puerta de acceso a correos, banca, gestión de expedientes, sistemas administrativos, historias clínicas y plataformas de colaboración. Un compromiso del navegador puede poner en riesgo sesiones, información visible, descargas y el acceso a otras aplicaciones. Las actualizaciones no son una mejora estética ni una elección individual: son una medida técnica de reducción de exposición institucional.

9. Guía de respuesta ante indicios de compromiso

- 1. Registrar alerta, hora local y UTC, equipo/activo afectado, versión, servicio, responsable y origen del indicador.
- 2. Identificar si hay explotación activa confirmada, exploit público o solo publicación de CVE; preservar esta distinción en el reporte.
- 3. Si existe amenaza activa, contener accesos expuestos; preservar evidencias antes de reinstalar, borrar logs o reiniciar siempre que la urgencia y el contexto lo permitan.
- 4. Preservar logs HTTP, WAF, VPN, autenticación, EDR, cambios de archivos, configuraciones, tareas programadas y eventos de red.
- 5. Calcular hashes de evidencias e identificar operador, origen, fecha, zona horaria y cadena de custodia.
- 6. Determinar alcance: datos accesibles, servidores vinculados, credenciales, sesiones y posible movimiento lateral.
- 7. Corregir la vulnerabilidad, rotar secretos que pudieran haberse filtrado, validar integridad y restaurar desde copia conocida si corresponde.
- 8. Verificar servicio, respaldos y telemetría después de la restauración; emitir acta de cierre con aprobación responsable.

Se desaconseja ejecutar exploits públicos contra sistemas productivos sin alcance de auditoría expresamente autorizado, evaluación de riesgos y procedimientos de reversión.

10. Plan institucional de acción

Plazo	Actividades	Evidencia de cumplimiento
0–24 horas	Identificar VPN Ivanti, WordPress con plugins críticos, Jpom, Prefab UI y WAVLINK; actualizar o aislar los activos realmente expuestos; preservar pruebas ante sospecha.	Inventario firmado, tickets, versiones anteriores/posteriores y acta de contención.
24–72 horas	Completar actualización de navegadores, PHP/Synology, GitLab y plugins; revisar cuentas/sesiones/logs; validar backups.	Reporte de despliegue, porcentaje de endpoints parcheados, revisión de alertas y prueba de restauración.
Días 4–15	Endurecimiento WordPress, servidores, NAS, VPN; MFA, segmentación, mínimos privilegios, WAF, control de extensiones.	Configuraciones comparadas, excepciones autorizadas, pruebas funcionales y documentación.
Días 16–30	Escaneos no intrusivos de versiones, verificación de correcciones y ejercicios de restauración; revisión de proveedores.	Matriz de vulnerabilidades residual, evidencias y retest.
Días 31–90	Consolidar gestión de cambios, inventario automático, monitoreo y revisiones periódicas.	KPIs mensuales, SLA, actas de comité, estado de riesgos y plan de mejoras.

Indicadores a informar a la mesa directiva

- % de sistemas con parches críticos dentro del SLA; por sistema operativo, navegador, WordPress, VPN y NAS.
- Cantidad de activos expuestos sin dueño identificado o sin soporte del fabricante.
- Número y antigüedad de vulnerabilidades críticas sin corregir, con compensaciones documentadas.
- % de sitios WordPress con inventario de plugins y MFA activo en roles privilegiados.
- % de endpoints con navegador en build estable vigente y reinicio completado.
- Tiempo medio entre publicación de aviso, evaluación de exposición, aplicación y verificación.
- % de respaldos con pruebas de restauración satisfactorias y separación efectiva de credenciales.

11. Implicancias en continuidad operativa y gestión de calidad

Las vulnerabilidades no solo amenazan información: pueden impedir turnos, trámites, acceso a resultados, registros, facturación y tareas administrativas. En organizaciones sanitarias la interrupción o alteración de sistemas puede generar demoras operativas significativas, por lo que las medidas deben integrarse en continuidad de negocio y recuperación ante desastres.

En instituciones con sistemas de gestión bajo ISO 9001:2015, una gestión documentada de infraestructura, cambios, incidentes, acciones correctivas y continuidad ayuda a sostener la operación y la evidencia de control. La presencia de un CVE por sí sola no constituye automáticamente una no conformidad: ello depende del requisito aplicable, los procesos afectados y la evidencia de gestión o incumplimiento.

Los proveedores deberán acreditar la ejecución de actualizaciones y el control de terceros; los contratos y los planes de contingencia deben contemplar ventanas de mantenimiento, RTO/RPO, notificación temprana, responsabilidades de respaldo y trazabilidad documental.

12. Recomendación institucional final

Instel & Seguridad recomienda clasificar como urgentes los sistemas con explotación real confirmada, los plugins que permitan ejecución remota sin autenticación y cualquier componente de administración o respaldo expuesto con una falla crítica. La prioridad no depende de que el sistema “funcione normalmente”: una plataforma comprometida puede conservar su funcionamiento visible durante un tiempo prolongado.

Se recomienda formalizar una política de actualización y corrección con responsables concretos, plazos verificables, presupuesto de mantenimiento y evidencias de cumplimiento; habilitar controles compensatorios cuando un parche no

esté disponible; y revisar periódicamente portales WordPress, equipos perimetrales, dispositivos de respaldo y navegadores de los puestos de trabajo.

La seguridad requiere mantenimiento continuo. No actualizar un sistema expuesto implica aceptar progresivamente riesgos conocidos, documentados y, en varios casos, fácilmente reproducibles por terceros.

Pedro Matías Cacivio

Auditor de Seguridad Informática · Perito Informático

Instel & Seguridad — Resistencia, Chaco

13. Referencias y documentos de respaldo

[F01] Rapid7: correcciones adicionales de Ivanti ICS (02/11/2026). https://www.rapid7.com/blog/post/etr-additional-ivanti-connect-secure-zero-days-exploited-in-the-wild-cve-2026-111357-cve-2026-118527/

[F02] Centro Canadiense de Ciberseguridad: Ivanti; actualización del 30/10/2026. https://www.cyber.gc.ca/en/alerts-advisories/ivanti-security-advisory-av26-1035

[F03] Wordfence: CVE-2026-116512 — Project Manager. https://www.wordfence.com/threat-intel/vulnerabilities/id/d3e300b3-39cc-4681-a8e8-02d9743f97ff

[F04] Wordfence: CVE-2026-118235 — SimpleForm. https://www.wordfence.com/threat-intel/vulnerabilities/id/6aac2178-f6ce-4444-9afc-7e014547cd48

[F05] Wordfence: CVE-2026-109220 — PDF Invoice for WooCommerce. https://www.wordfence.com/threat-intel/vulnerabilities/id/1bc3529c-6161-4b89-8a35-c3a9b7b8c308

[F06] Wordfence: CVE-2026-119096 — Uncanny Toolkit. https://www.wordfence.com/threat-intel/vulnerabilities/id/592b61a1-9ac9-4817-b154-1e39e50d8010

[F07] Wordfence: CVE-2026-89270 — Popup Builder. https://www.wordfence.com/threat-intel/vulnerabilities/id/13af3a6e-d3ef-41f0-9424-fe2c9b17c8bb

[F08] CVE-2026-103882 — Acadlix LMS (registro técnico). https://www.tenable.com/cve/CVE-2026-103882

[F09] GitHub advisory: CVE-2026-120338 — Prefab UI. https://github.com/advisories/GHSA-3g72-rrqc-f76c

[F10] GitHub advisory: CVE-2026-120201 — Jpom. https://github.com/advisories/GHSA-mr28-xw2h-9rw4

[F11] CVE-2026-120345 — WAVLINK, registro. https://app.opencve.io/cve/CVE-2026-120345

[F12] Synology-SA-26:14 — PHP2Shell (actualización 31/10). https://www.synology.com/en-us/security/advisory/Synology_SA_26_14

[F13] NCSC-NL: seguimiento de productos afectados por PHP2Shell (02/11). https://github.com/NCSC-NL/php2shell

[F14] Google: Chrome Stable 156, 29/10. https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_02107719452.html

[F15] Mozilla: MFSA 2026-118 — Firefox 159. https://www.mozilla.org/en-US/security/advisories/mfsa2026-118/

[F16] Microsoft Learn: Edge Stable, notas de versión. https://learn.microsoft.com/en-us/deployedge/microsoft-edge-relnote-stable-channel

[F17] CVE.org: GitLab CVE-2026-97229. https://www.cve.org/CVERecord?id=CVE-2026-97229

[F18] WordPress.org: WP-CLI, inventario de plugins. https://developer.wordpress.org/cli/commands/plugin/list/

[F19] WSO2: CVE-2025-11969, advisory original 26/01/2026. https://security.docs.wso2.com/en/latest/security-announcements/security-advisories/2026/WSO2-2025-4733/

Nota de interpretación: las referencias documentan la información disponible al corte. Los listados de versiones de cada fabricante y los reportes de explotación pueden cambiar; debe consultarse el aviso original antes de implementar cualquier actualización posterior.