INSTEL & SEGURIDAD
ANÁLISIS FORENSE - AUDITORÍA - PENTESTING

PAPER TÉCNICO DE SEGURIDAD

Vulnerabilidades y parches críticos en las últimas 48 horas

Impacto y plan de remediación para servicios digitales gubernamentales

CONTROL EDITORIAL	ALCANCE
Ventana del análisis	24/10/2026 13:02 UTC - 26/10/2026 13:02 UTC | 48 horas
Corte local (Argentina)	24/10/2026 10:02 - 26/10/2026 10:02, UTC-3
Base cuantitativa	274 CVE de la planilla adjunta; 8 críticas y 61 altas
Base institucional	Informe integral gubernamental de 03/09/2026; 32 URLs únicas en inventario histórico
Autoría institucional	Pedro M. Cacivio | Instel & Seguridad
Clasificación	Análisis documental / inteligencia de vulnerabilidades. No constituye retest.

CONCLUSIÓN CENTRAL | Riesgo institucional provisional ALTO; respuesta P0 prioritaria ante PHP2Shell, gestión de confianza TLS e infraestructura desactualizada. La exposición efectiva de cada CVE exige cruce con inventario y verificación autorizada.

Versión 1.0 · Resistencia, Chaco · 26 de octubre de 2026

CONFIDENCIAL · DIFUSIÓN CONTROLADA

Resumen / Abstract

Se presenta una síntesis crítica, trazable y orientada a decisión de 274 registros CVE cuyo campo de publicación en NVD cae dentro de una ventana fija de 48 horas (24 al 26 de octubre de 2026), complementada con comunicados de fabricantes, investigadores y CSIRT. La investigación distingue fecha de publicación del registro CVE, fecha del aviso original, liberación de parches y evidencias de explotación. Su aplicación al ámbito gubernamental parte del informe de septiembre de 2026 sobre sitios y servicios vinculados al Gobierno del Chaco, sin convertir automáticamente sus hallazgos históricos en exposiciones vigentes.

Hallazgo principal: 69 registros (25,2%) están clasificados como críticos o altos. Sin embargo, las prioridades operativas inmediatas surgen también fuera de ese subconjunto temporal: PHP2Shell (parches del 21/10, confirmación de explotación a partir de análisis de honeypots), actualizaciones fuera de banda .NET (25/10), medidas de desconfianza de certificados eMudhra en Python/Java/RHEL, avisos de PAN-OS, reconstrucción de paquetes PHP Windows (26/10) y un riesgo PHP adicional con mitigación aún necesaria.

Palabras clave: gestión de vulnerabilidades; CVE; NVD; sistemas gubernamentales; PHP2Shell; eMudhra; respuesta a incidentes; hardening; remediación; evidencia digital.

Contribución y límites de inferencia

Este documento NO afirma que los 32 sitios históricos ejecuten los productos afectados, ni que hayan sido comprometidos. El porcentaje operativo de “98% sin actualizaciones” es una estimación facilitada por personal familiarizado con esos entornos; no es una medición de la planilla ni del retest.

Decisiones recomendadas en las primeras 24 horas

- Aprobar acciones P0 sin explotación: reducir superficies administrativas públicas; aislar paneles de gestión, bases de datos y rutas de depuración; preservar registro de cambios.
- Determinar qué hosts, aplicaciones, imágenes y productos incorporan PHP, .NET, Python, Java/GraalVM, PAN-OS y plugins de autenticación afectados; no deducir vulnerabilidad por banner.
- Aplicar parches oficiales por rama con pruebas de regresión y rollback; verificar la versión real en ejecución y el paquete proveedor, no solamente el archivo de instalación.
- Iniciar revisión de indicadores de compromiso cuando exista exposición plausible, priorizando web/PHP y eventos de autenticación o administradores inesperados.

1. Fuentes, alcance y metodología

1.1 Universo documental

Fuente primaria cuantitativa: archivo “seguridad_ultimas_48h_2026-10-26.xlsx” provisto para este trabajo, con hojas Resumen, CVE completas (274 filas de datos), Eventos operativos y Metodología. Los conteos se recalcularon directamente a partir de sus filas. El universo NVD depende del campo “published” de cada entrada y del instante de corte; incorporaciones tardías pueden cambiarlo. La consulta reproducible declarada en la planilla se referencia en [S01].

Referencia institucional recuperada: “Informe_Integral_Ciberseguridad_Sitios_Gobierno_Chaco_2026.docx”, fechado 03/09/2026. Resume 33 entradas fuente y 32 URLs únicas, de las cuales 31 corresponden a organismos/proveedores provinciales y una a una entidad nacional que exige autorización específica. Conserva evidencia histórica de 2025/2026; no fue reescaneada para esta publicación.

1.2 Reglas de clasificación

Categoría	Criterio técnico
NVD / CVE nueva	Publicación NVD en ventana. No implica que vulnerabilidad, advisory o parche hayan nacido en ese momento.
Advisory nuevo/actualizado	Nota publicada o cambiada materialmente durante la ventana, incluso si usa CVE anteriores.
Parche verificable	Fabricante o mantenedor indica versión, build, paquete, commit o solución documentada.

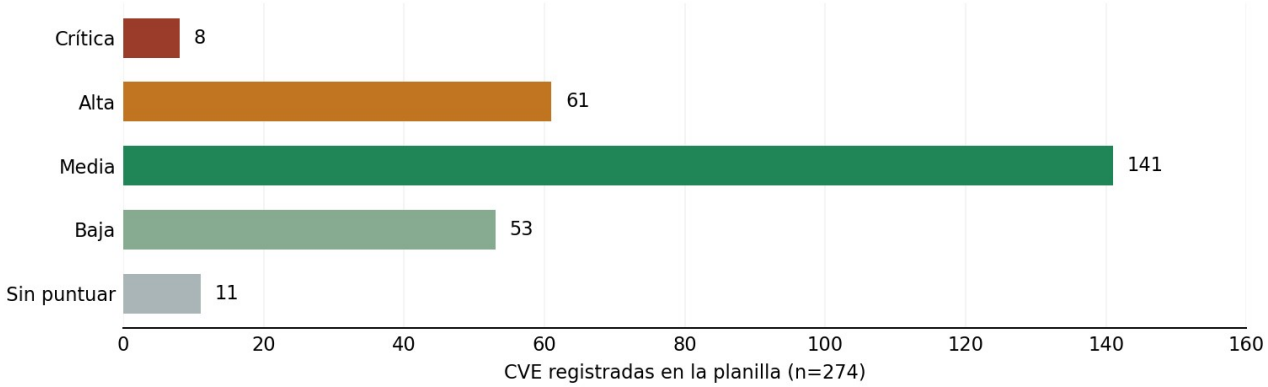
Explotación reportada	Investigación documentada en sensores/honeypots; separar de ataques verificados sobre activos propios.
Aplicabilidad institucional	Solo confirmada tras inventario, versión instalada, configuración, ruta de exposición y evidencia de revisión.
Hallazgo histórico	Evidencia del estudio anterior. Sigue pendiente revalidación autorizada y fechada.

1.3 Priorización ajustada al entorno

Se utiliza la clasificación CVSS como indicador de severidad técnica, no como orden automático de ejecución. La prioridad operativa resulta de la combinación de criticidad del servicio público, exposición a Internet, viabilidad real de explotación, explotación conocida, tipo de datos, privilegios, dependencia de terceros y disponibilidad de mitigación o parche. Los CVSS 3.1 y 4.0 son escalas distintas y aquí no se promedian ni comparan como si fueran equivalentes.

El estudio excluye cualquier explotación nueva, análisis autenticado de producción, enumeración agresiva de puertos, acceso a consolas, datos personales o ejecución de PoC. Las recomendaciones operativas se limitan a verificación defensiva, mantenimiento y controles autorizados.

2. Resultados cuantitativos (NVD, n = 274)



Severidad	Cantidad	Proporción	Lectura operativa
CRITICAL	8	2,9%	Verificar en inventario con preferencia P0 cuando exista exposición.
HIGH	61	22,3%	Priorizar según servicio, ruta, disponibilidad del parche y explotación.
MEDIUM	141	51,5%	Corregir en ciclo de sprint y cuando multipliquen otro riesgo.
LOW	53	19,3%	Gestionar por baseline y dependencias.
UNSCORED	11	4,0%	No asumir riesgo bajo: pendiente puntuación o análisis.

2.1 Disponibilidad de remediación documentada

Estado registrado	Cantidad	Interpretación
Parche/versión identificada	36	La planilla registra una recomendación de corrección suficientemente específica.
Versión corregida indicada	89	Existe una versión objetivo en el registro; verificar alcance y distribuidor.
Referencia de corrección disponible	48	Hay referencia a corrección; requiere revisión manual del enlace.
Sin parche identificado en el registro	101	No se identificó parche en esa fuente; NO equivale a que no exista.

Total con algún indicio de corrección en la planilla: 173 de 274 (63,1%). El conteo representa el estado del registro y NO una validación completa de cada proveedor.

2.2 Sesgos y precauciones

La abundancia de registros de severidad media no indica que la infraestructura del gobierno contenga esas tecnologías. Algunos CVE publicados ahora se difundieron días antes como avisos de proveedores. Además, la existencia de un CVE no prueba por sí misma que un host esté afectado: se requiere paquete instalado, configuración vulnerable y exposición relevante. La ausencia de una entrada nueva en KEV dentro del período tampoco descarta explotación activa.

3. Ocho CVE clasificados como críticos en el corte

CVE / CVSS	Producto / condición	Riesgo esencial	Corrección referenciada
2026-115933 **9,9 v3.1**	Postiz / firma de tokens compartida	Falsificación de sesión, invitación o recuperación.	v2.25.3; revisar rotación e invalidez de tokens.
2026-115214 **9,8 v3.1**	WordPress Datawiza Proxy Auth < 1.1.1	Suplantación de identidad/rol mediante cabeceras confiadas.	Plugin 1.1.1; garantizar cabeceras exclusivamente del proxy.
2026-115932 **9,6 v3.1**	Postiz / rutas de medios sin confinamiento	Lectura y envío de archivos internos mediante publicación.	v2.25.3; restringir auto-registro e integraciones hasta actualizar.
2026-115557 **9,4 v4.0**	Python / módulo ssl y CA comprometida	Aceptación de certificados ligados a claves comprometidas.	3.15.2, 3.14.10, 3.13.18, 3.12.16, 3.11.18.
2026-115995 **9,4 v4.0**	Unitree Go2 / chat_go	Inyección de comandos remota condicionada al componente.	Firmware 1.1.11.5 según registro; confirmar canal oficial.
2026-116199 **9,2 v4.0**	Snipe-IT con Google SSO y usuario desactivado	Reingreso de cuentas desactivadas bajo condiciones específicas.	v8.6.3; revocar sesiones y completar baja en IdP.
2026-114820 **9,1 v3.1**	Oracle Java / GraalVM, componente JSSE	Confianza en raíces eMudhra; riesgo MITM para TLS.	Alerta Oracle 24/10; truststore corregido o mitigación.
2026-116163 **9,1 v4.0**	Parse Server / AuthAdapter personalizados	Omisión de validación que permite bypass de autenticación.	8.6.102 o 9.10.5-alpha.2; revisar compatibilidad.

Las puntuaciones reproducen la clasificación del registro NVD/CNA de la planilla; algunos avisos de proyectos usan severidades distintas. Fuente por CVE: planilla anexa; corroboración por fabricante o mantenedor en [S08]–[S12].

3.1 Acciones técnicas y evidencia de cierre

Postiz — CVE-2026-115933 y CVE-2026-115932

En despliegues existentes, actualizar a v2.25.3; invalidar credenciales/sesiones susceptibles; limitar auto-registro e integraciones durante el mantenimiento; revisar acceso a ficheros y acciones de publicación. Verificar versión desplegada, logs de autenticación y ausencia de rutas arbitrarias. [S08]

Datawiza WordPress — CVE-2026-115214

Confirmar la existencia del plugin reverse-proxy-auth-widget. Actualizar a 1.1.1. Asegurar que el reverse proxy elimine cabeceras suministradas por el cliente y reinyecte la identidad desde un canal autenticado; comprobar cuentas administrativas creadas o modificadas recientemente. [S09]

Python — CVE-2026-115557

Actualizar la rama a su release de seguridad (3.13/3.12/3.11 están disponibles como source-only). Comprobar intérpretes reales, entornos virtuales, imágenes y truststores, y reiniciar servicios afectados. La release trae otros fixes por rama (tarfile y Expat). [S03]

Unitree Go2 — CVE-2026-115995

Solo prioridad institucional si existe ese equipo en inventario; aislar chat_go y aplicar el firmware indicado después de confirmar integridad, soporte y compatibilidad con el fabricante. No extender este CVE a equipos robóticos genéricos.

Snipe-IT — CVE-2026-116199

Afecta el recorrido Google SSO en escenarios con usernames en formato correo, cuentas desactivadas localmente e identidad Google activa. Actualizar a v8.6.3, revocar sesiones y sincronizar procesos de baja. El advisory del mantenedor es del 08/10: la “novedad” del corte corresponde al registro CVE, no a la primera divulgación. [S10]

Oracle Java/GraalVM — CVE-2026-114820

Aplicar el paquete oficial publicado por Oracle el 24/10; revisar sistemas que solo recibieron la primera acción del 21/10. Validar truststore, procesos JVM y conexiones críticas. Un riesgo de CA comprometida requiere posibilidad de intercepción de tráfico: no equivale a una RCE directa de Java. [S04]

Parse Server — CVE-2026-116163

Solo instalaciones que utilizan adaptadores propios construidos como subclases AuthAdapter. Actualizar rama estable 8.x a 8.6.102 o seguir el ciclo aprobado en 9.x; la rama 9.10.5-alpha.2 es prerelease, por lo que producción exige valorar soporte y estabilidad. Aviso original 10/10. [S11]

4. Boletines de alto impacto publicados o actualizados

4.1 Microsoft .NET — parche fuera de banda del 25/10

Microsoft lanzó .NET 8.0.33, 9.0.22, 10.0.14 y 11 RC3. Corrige CVE-2026-111497 (Brotli) y CVE-2026-114148 (metadatos de propiedad en tarballs Linux), e incorpora correcciones rehechas para CVE-2026-70197 y CVE-2026-102870, inicialmente tratadas el 13/10 de forma incompleta. La exposición a Brotli depende de rutas y características de descompresión: no debe asumirse habilitada por defecto. [S02]

Modalidad de despliegue	Acción y comprobación
Framework-dependent	Instalar runtime del fabricante; reiniciar aplicación; verificar dotnet --list-runtimes y versión de proceso.
Self-contained	Reconstruir/publicar aplicación con runtime actualizado; una actualización del servidor por sí sola no alcanza.
Contenedores	Recompilar imágenes base, reimplementar, revisar digest y SBOM.
ASP.NET Core por tarball	Revisar específicamente distribuciones tarball en .NET 8/9 y source-build según aviso.

4.2 PHP2Shell — alta prioridad aunque el parche sea del 21/10

CVE-2026-109618 y CVE-2026-109619 permiten ejecución remota no autenticada bajo condiciones vulnerables del runtime PHP. Las primeras versiones corregidas son 8.5.12, 8.4.27, 8.3.36 y 8.2.35. El 26/10 se difundió evidencia atribuida a honeypots Apache mod_php 8.4.26 de ejecución real; esto exige triaje acelerado, sin convertir esa evidencia externa en compromiso de los activos propios. Unit 42 retiró otra atribución anterior a una agencia europea por falta de confirmación de vector inicial. [S05] [S13] [S14]

Nueva precisión del 26/10: el proyecto PHP publicó builds Windows 8.5.12-1, 8.4.27-1, 8.3.36-1 y 8.2.35-1, recompilados con Brotli 1.2.1 para CVE-2026-111497. La numeración del runtime PHP no cambia, pero el paquete Windows sí debe sustituirse cuando corresponda. [S06]

ATENCIÓN: CVE-2026-115560 (aviso PHP del 23/10). Es una ruta adicional y poco común de RCE vinculada a session upload progress y cambio dinámico del serializador. Las versiones del 21/10 NO la corrigen. Hasta la próxima actualización, usar session.upload_progress.enabled=0 en las aplicaciones alcanzadas y comprobar configuración efectiva. [S06] [S15]

4.3 eMudhra y confianza criptográfica transversal

El incidente no es un fallo único de aplicación sino compromiso de claves de certificación con impacto potencial sobre conexiones TLS interceptables. Python liberó cinco versiones de seguridad el 26/10; Oracle publicó una alerta Java/GraalVM el 24/10 que amplía el tratamiento de raíces; Red Hat actualizó el boletín el 24/10 con erratas para RHEL 8, 9 y 10. Es indispensable revisar almacenes de certificados del sistema, de Java, contenedores, appliances y librerías con truststores propios. [S03] [S04] [S07]

Control de cierre: guardar versión instalada y paquete actualizado, reconstruir imágenes base, reiniciar procesos que cargan el almacén al inicio y realizar pruebas funcionales TLS. El equipo PKI determinará cualquier eliminación manual de CA tras validar cadenas y dependencias, evitando revocaciones indiscriminadas.

4.4 Oracle Communications / Solaris y Palo Alto PAN-OS

Oracle emitió una alerta el 25/10 para CVE-2026-109618 y -109619 que cubre productos Communications y Solaris 11. El paquete necesario depende del producto y soporte contratados, no basta con modificar un PHP visible en el host. [S16]

Palo Alto publicó su matriz de impacto PHP2Shell: afecta a configuraciones de PAN-OS/Panorama mediante la interfaz web/XML de administración, no a la aplicación GlobalProtect. Algunos hotfixes ya estaban disponibles y otros tenían fechas previstas posteriores al corte. Restringir inmediatamente la administración a redes de confianza o jump hosts; instalar solo build que el proveedor declare corregido para la rama real. El fabricante indicó que no conocía explotación maliciosa de su producto. [S17]

5. Correlación con la auditoría histórica gubernamental

El informe institucional del 03/09/2026 preserva una imagen heterogénea de 32 URLs y 12 familias de fallas. No se usaron los datos originales para atribuir ninguno de los CVE de octubre a un organismo concreto. El cruce siguiente constituye una matriz de verificación priorizada, no un dictamen de exposición vigente.

Familia histórica / control	Relación con el corte 48h	Prueba de aplicabilidad y respuesta
F-01 Debug/profiler; F-07 backups expuestos	Posible fuga de secretos y ampliación del impacto de otras fallas.	Desactivar depuración pública; retirar copias del webroot; rotar secretos si se exponen.
F-02 phpMyAdmin; F-03 SQL/FTP expuestos	PHP2Shell y mantenimiento de software aumentan la urgencia perimetral.	Cerrar administración/3306/21 desde Internet; VPN/bastión; actualización de PHP y base de datos.
F-04 Drupal 7; F-08 CMS/plugins viejos	Falta de soporte y dependencias PHP; Datawiza solo si está instalado.	SBOM CMS/plugins; migración de versiones fuera de soporte; parches y retest.
F-05 Roundcube antiguo	Correo como pivote a identidad y recuperación de cuentas.	Actualizar webmail por canal oficial; MFA, registro de accesos y endurecimiento PHP.
F-06 SNMP/SSH gestión	La visibilidad de gestión amplifica riesgo de intrusión y movimiento lateral.	Red de administración separada; SNMPv3; SSH seguro; bastión, MFA y logs.
F-09 TLS heredado	Compromiso eMudhra exige inventario de truststores y cadenas.	TLS 1.2/1.3; actualizar CA en Java/Python/OS/containers; pruebas.
F-10 Cabeceras/cookies; F-11 identidad	Abuso de privilegios y sesión en plugins/autenticación.	MFA; revisión de proxies/cabeceras; controles de sesiones y cuentas.
F-12 Runtimes/servidores antiguos	Aparecen correcciones urgentes PHP, Python, .NET y Java.	Versiones locales, gestor de paquetes, OVAL/errata, backports y evidencia de cierre.

5.1 Cadenas de ataque plausibles sin presunción de intrusión

- Componente PHP vulnerable + aplicación expuesta + procesos con permisos excesivos → potencial ejecución de código → acceso a datos, defacement o indisponibilidad.
- Consola de gestión visible + credenciales comprometidas o bypass de autenticación → control administrativo del servicio → movimiento lateral si no existe segmentación.
- Truststore desactualizado + adversario en posición de intermediario → posible suplantación TLS → robo o modificación de información transmitida.
- CMS/plugin no mantenido + falta de rotación de credenciales → persistencia de cuentas privilegiadas y propagación a sistemas dependientes.

5.2 Evaluación de riesgo institucional

Calificación provisional: ALTO, con tratamiento inmediato P0 para servicios potencialmente afectados por PHP2Shell, interfaces de gestión públicas y componentes de confianza criptográfica en uso. La calificación NO se extrapola a cada URL ni a cada CVE sin verificación. El supuesto de mantenimiento insuficiente se deberá corroborar con historial de parches, CMDB, tickets, agentes de actualización y evidencia firmada de responsables.

6. Programa de remediación de 90 días

Ventana	Acciones y entregables	Criterio de aceptación
0–24 h	Congelar inventario crítico y rutas públicas; restringir consola	Lista firmada de activos críticos; reglas de firewall/WAF

P0 / contención	de administración; priorizar PHP expuesto y PAN-OS; comunicar riesgos; asignar dueño.	exportadas; control de cambios; incident triage iniciado.
24–72 h P0 / parche	Actualizar PHP y builds Windows; .NET OOB; Python/Java/CA; appliances; reconstruir contenedores; evidenciar servicios reiniciados.	Versión real en ejecución; changelog/errata; pruebas funcionales; comprobación desde red no autorizada.
Días 4–14 P1 / cierre	Revalidación autenticada no destructiva; CMS, plugins, Roundcube/Drupal; deshabilitar puertos legados; MFA y segmentación.	Tickets asociados a CVE/host y controles; retest reproducible; evidencias fechadas y hashing.
Días 15–45 P1/P2	Migrar EOL y dependencias; endurecer TLS, cookies, CSP; detección de webshells y backups; ejercitar restauración.	Inventario SBOM actualizado; sin críticos/altos expuestos injustificados; respaldo restaurado en prueba.
Días 46–90 Sostenibilidad	Patch management centralizado; ciclo CAB; baseline por rol; métricas; simulacro de incidente y revisión trimestral.	SLA medidos; revisión ejecutiva; excepciones con riesgo aceptado y vencimiento definido.

6.1 SLA propuestos (política sugerida, no normativa vigente)

Prioridad	Objetivo	Condición
P0	Contención inmediata y parche verificable ≤72 h.	RCE explotada, gestión pública comprometible, autent. bypass en activo crítico.
P1	Corrección ≤7 días.	CVE alto con exposición real y parche disponible.
P2	Corrección ≤30 días.	Impacto acotado, servicio sin exposición directa o mitigación acreditada.
P3	Ciclo trimestral documentado.	Hallazgo bajo con impacto y dependencias controlados.

Los SLA requieren aprobación del organismo. Si una dependencia crítica impide cumplir, documentar excepción con mitigación, dueño, validación compensatoria y fecha de caducidad.

7. Guía de revalidación segura y evidencia técnica

7.1 Cadena mínima de evidencias por activo

- ID unívoco y organismo responsable; FQDN/IP interna mantenidos en anexo restringido; criticidad del servicio y ventana de cambio.
- Sistema operativo, paquetes, ramas y fecha de último parche; inventario de runtimes, módulos, plugins, contenedores y appliances.
- Control de red: interfaces públicas y de administración; segmentación y reglas aplicadas; captura fechada de verificación.
- Artefactos de despliegue: ticket, hash SHA-256 de respaldo/configuración, versión antes/después, logs y rollback.
- Evidencia de cierre: escaneo autenticado aprobado, prueba funcional, comprobación no autenticada de ausencia de exposición y firma del responsable.

7.2 Comprobaciones de solo lectura sugeridas

Tecnología	Verificación inicial (según plataforma)
PHP / entorno web	php -v; php --ini; php -i (local y con resguardo); revisar versión del pool FPM/mod_php efectiva.
Python	python3 --version; inventario de venv, servicios systemd e imágenes que embeben intérprete.
.NET	dotnet --list-runtimes; dotnet --list-sdks; inspección de manifests y DLL self-contained.
Java	java -version; identificar java.home y truststore por aplicación; paquete del JDK.
Debian/Ubuntu	dpkg-query -W; apt-cache policy <paquete>; changelog de seguridad del proveedor.
RHEL	rpm -q ca-certificates; dnf updateinfo list security (o comando soportado en la rama).
WordPress / CMS	WP-CLI/administración autorizada, inventario de core y plugins; sin enumeración pública de usuarios.
Contenedores	Lista de imágenes y digests; SBOM; validación del runtime interno, no solo versión del host.

Los comandos son ilustrativos, locales y de lectura; deben adecuarse al sistema, privilegios y alcances autorizados. Nunca incorporar secretos, hashes de contraseñas ni datos clínicos/personales al informe de distribución ejecutiva.

7.3 Estado normalizado por CVE/activo

Estado	Prueba exigida
No aplica	Producto/componente ausente, o versión/configuración fuera del rango, con evidencia de inventario.
Pendiente	No hay evidencia suficiente para determinar exposición o parche.
Vulnerable confirmado	Versión y condición afectada verificadas en host; sin necesidad de PoC de explotación.
Mitigado	Control compensatorio probado, sin afirmar que el software quedó corregido.
Corregido	Paquete/build o código seguro instalado + servicio reiniciado + retest aprobado.
Riesgo aceptado	Aprobación formal, caducidad, justificación, controles y responsable institucional.

8. Indicadores, responsabilidades y gobierno del proceso

Indicador	Fórmula / meta de referencia
Cobertura de inventario	Activos con dueño, OS, runtimes y criticidad / activos identificados. Meta: 100%.
P0 en plazo	Tickets P0 contenidos/corregidos dentro del SLA / P0 vencidos en el período.
Exposición administrativa	Consolas accesibles desde Internet sin justificación formal. Meta: cero.
MTTR crítico	Mediana del tiempo desde conocimiento de vulnerabilidad aplicable hasta cierre verificado.
Obsolescencia	Componentes EOL sin soporte/plan aprobado, separados por criticidad y servicio.
Verificación de backups	Última restauración probada y fecha; RPO/RTO aprobados para cada servicio.
Cumplimiento del ciclo	Parches instalados y verificados / parches aprobados, por sistema y proveedor.

Modelo de responsables

Responsable institucional: autoriza alcance y acepta riesgo residual. Seguridad: clasifica CVE, valida aplicabilidad, supervisa evidencia y retest. Sistemas/Infraestructura: despliega actualizaciones y revisa dependencias. Desarrollo/DevOps: recompila aplicaciones y contenedores, realiza regresión. Redes: restringe gestión y confirma segmentación. Mesa de cambios: verifica ventana, reversión y continuidad. Auditoría/Pericia: conserva trazabilidad, redacta resultados y evita divulgar información sensible.

9. Discusión y conclusiones

El corte de 48 horas evidencia que la gestión de vulnerabilidades ya no puede depender de alertas CVE aisladas ni de la periodicidad de un único escaneo. El problema operativo es la asincronía: un aviso previo puede transformarse en nueva evidencia de explotación; un parche del martes puede corregirse nuevamente fuera de banda; una CA comprometida obliga a revisar la confianza TLS en varias plataformas; y la versión que aparece en un banner puede ser idéntica pese a un backport de seguridad.

Para los servicios gubernamentales, el escenario adverso emerge de la coincidencia entre deuda técnica, accesos administrativos mal segmentados, falta de inventario y ciclos de actualización no verificables. Esto respalda una calificación de riesgo provisional ALTO para planificar, pero no una afirmación de explotación o de vulnerabilidad efectiva sobre los 32 activos históricos.

La recomendación central es formalizar un programa operativo de 90 días, comenzando con contención P0, corrección de PHP y dependencias, verificación del truststore, patching extraordinario .NET y revisión de controles de autenticación. Cada cierre debe sustentarse en evidencia del host o appliance, boletín del fabricante, retest autorizado, impacto funcional y responsable. Mantener el registro de 274 CVE como anexo vivo, incorporando nuevas modificaciones y notas de parche a medida que las CNAs y proveedores actualicen sus registros.

Decisión institucional solicitada

Aprobar el plan 0–72 horas, designar un responsable por activo, autorizar el retest 2026 no destructivo y establecer un tablero de seguimiento semanal hasta completar la remediación y aceptación documentada de riesgos residuales.

Referencias principales y trazabilidad

[S01] NVD API 2.0 (consulta de la planilla; campo published). https://services.nvd.nist.gov/rest/json/cves/2.0/?pubStartDate=2026-10-24T13:02:00.000&pubEndDate=2026-10-26T13:02:00.000&resultsPerPage=2000

[S02] Microsoft .NET OOB, 25/10/2026. https://devblogs.microsoft.com/dotnet/dotnet-october-2026-oob-security-updates/

[S03] Python Insider: releases 3.11–3.15, 26/10/2026. https://blog.python.org/2026/10/python-3152-31410-31318-31216-31118/

[S04] Oracle Alert CVE-2026-114820, 24/10/2026. https://www.oracle.com/security-alerts/alert-cve-2026-114820.html

[S05] PHP Security Advisory, 21/10/2026. https://www.php.net/archive/2026.php

[S06] PHP: novedades 26/10 builds Windows y aviso 23/10 CVE-2026-115560. https://www.php.net/

[S07] Red Hat RHSB-2026-012, eMudhra, modificado 24/10. https://access.redhat.com/security/vulnerabilities/RHSB-2026-012

[S08] Postiz v2.25.3, notas de seguridad 24/10. https://github.com/gitroomhq/postiz-app/releases/tag/v2.25.3

[S09] WPScan Datawiza Proxy Auth, CVE-2026-115214. https://wpscan.com/vulnerability/2c6c7d10-2281-4a98-a0d6-769da5cce416/

[S10] Snipe-IT GHSA-xf36-wx48-5rqp (publicación 08/10). https://github.com/grokability/snipe-it/security/advisories/GHSA-xf36-wx48-5rqp

[S11] Parse Server GHSA-rq3w-5c6f-p7wr (publicación 10/10). https://github.com/parse-community/parse-server/security/advisories/GHSA-rq3w-5c6f-p7wr

[S12] CISA KEV: catálogo de explotación conocida. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[S13] BleepingComputer: atribución de evidencias de honeypots 26/10. https://www.bleepingcomputer.com/news/security/php2shell-security-flaws-now-sucessfully-exploited-in-the-wild/

[S14] Unit 42: actualización y rectificación PHP2Shell 25/10. https://unit42.paloaltonetworks.com/cve-2026-109618-cve-2026-109619/

[S15] Centro Canadiense de Ciberseguridad, actualización CVE-2026-115560. https://www.cyber.gc.ca/en/alerts-advisories/al26-026-critical-vulnerabilities-impacting-php-cve-2026-109618-and-cve-2026-109619

[S16] Oracle Security Alert PHP2Shell, 25/10. https://www.oracle.com/security-alerts/alert-cve-2026-109618.html

[S17] Palo Alto: impacto PHP2Shell sobre PAN-OS y hotfixes. https://security.paloaltonetworks.com/CVE-2026-109618

Fuentes consultadas al 26/10/2026. No se afirma exhaustividad universal: los avisos CNA, NVD y proveedores pueden corregirse retroactivamente; conservar capturas/snapshots de referencia para auditoría.

Anexos y custodia documental

A. Inventario tabular íntegro de CVE

La hoja “CVE completas” del archivo original anexo conserva los 274 registros con CVE, severidad, CVSS, fecha de publicación, fuente CNA, CWE, vector, texto descriptivo, estado de remediación y referencias. No se repite aquí el texto íntegro de todas las entradas para preservar legibilidad editorial del paper y evitar divergencia con futuras revisiones. La hoja “Eventos operativos” preserva los avisos cuyo interés deriva de un cambio material de la ventana, no necesariamente de una nueva fecha de CVE.

B. Integridad de documentos utilizados

Archivo	SHA-256
seguridad_ultimas_48h_2026-10-26.xlsx	e6d8f51c5875f49812c0286e0618e7c3b6faa6fc820440f804f2bf8bd827be5f
Informe_Integral_Ciberseguridad_Sitios_Gobierno_Chaco_2026.docx	19d694acda31e43482e4ace62360c942fb2fcb1c7d2b354d838c1937fd5754b6

Estos hashes identifican los archivos exactos analizados. No implican certificación de la adquisición original ni custodia judicial retroactiva.

C. Firmas y aprobación

Elaborado por: Pedro M. Cacivio — Instel & Seguridad — Auditoría, análisis forense y pentesting.

Revisado / aprobado por autoridad del organismo: _____

Fecha de aprobación y número de expediente/ticket: _____

D. Planilla de aprobación de remediaciones críticas

Registro sugerido para incorporar al sistema de tickets del organismo. Completar exclusivamente con evidencia de los sistemas incluidos en el alcance autorizado.

Control P0	Dueño y fecha	Evidencia / ticket	Estado
Inventario de superficies web y consolas	_____	_____	_____
PHP2Shell y PHP Windows reempaquetado	_____	_____	_____
.NET OOB: runtime, self-contained y contenedores	_____	_____	_____
Truststores eMudhra: Python/Java/SO/containers	_____	_____	_____
Gestión remota y segmentación de administración	_____	_____	_____
Análisis de logs y posible compromiso	_____	_____	_____
Retest no destructivo y pruebas funcionales	_____	_____	_____

E. Dictamen de cierre

Estado de cierre (marcar): ☐ Corregido y verificado ☐ Mitigado temporalmente ☐ Pendiente / excepción documentada

Riesgo residual y justificación: _____

_____

Responsable técnico: _____ Fecha: _____

Autoridad que acepta el riesgo: _____ Fecha: _____

La validación se realizará con control de cambios, registros de instalación y evidencias técnicas preservadas. Esta publicación no incorpora firma manuscrita ni digital.