INSTEL & SEGURIDAD
ANÁLISIS FORENSE - AUDITORÍA - PENTESTING

PAPER TÉCNICO DE SEGURIDAD

ZERO-DAYS, VULNERABILIDADES EXPLOTADAS Y PARCHES DE SEGURIDAD

Informe consolidado del 27 al 29 de octubre de 2026
Impacto en infraestructuras empresariales y gubernamentales

CONTROL DOCUMENTAL	DEFINICIÓN
Edición / lugar	1.0 · Resistencia, Chaco · 29 de octubre de 2026
Ventana principal	27/10/2026 10:26 a 29/10/2026 10:26 (UTC-3) | 48 horas
Contexto complementario	Alertas y parches publicados entre 21 y 26 de octubre y CVE histórica de Microsoft Authenticator
Entidad / autoría institucional	Instel & Seguridad · Dirección técnica: Pedro M. Cacivio
Naturaleza	Inteligencia de vulnerabilidades y análisis documental; no constituye un pentest o un retest vigente
Destinatarios	Autoridades, responsables de TI, equipos de seguridad, redes, desarrollo y continuidad operativa
Clasificación	Confidencial · Difusión controlada · Sin datos de acceso ni evidencias sensibles

CONCLUSIÓN EJECUTIVA | Riesgo institucional provisional ALTO y necesidad de respuesta P0 para tecnologías realmente presentes con explotación confirmada. La prioridad se basa en exposición, funciones críticas, evidencia de explotación y disponibilidad real del parche. No se afirma que todos los productos estén instalados en los sitios históricos.

Autoría y validación: Instel & Seguridad | Revisión documental: 29/10/2026

Resumen ejecutivo / Abstract

Este paper consolida el barrido de inteligencia de vulnerabilidades efectuado al 29 de octubre de 2026, integra los avisos publicados y actualizados en las 48 horas precedentes y mantiene trazabilidad hacia boletines críticos anteriores. Se revisaron, entre otras fuentes, CISA KEV, Microsoft MSRC, Cisco PSIRT, Sophos, Juniper, Palo Alto, Broadcom, Google, Mozilla, ZDI, Tailscale, Dell, Apple y el seguimiento oficial Debian.

Resultados principales: cuatro incorporaciones a CISA KEV del 27–28/10; confirmación de explotación activa de una falla de disponibilidad en VPN Cisco ASA/FTD; una vulnerabilidad crítica en Sophos UTM al final de su soporte; múltiples correcciones en routers Juniper, navegadores, acceso remoto Tailscale y Valkey; siete divulgaciones ZDI de Ultralytics rotuladas 0Day; y una falla crítica UEFI/PXE cuyo parche de código aún no equivale a firmware desplegable. El informe incorpora de forma diferenciada CVE-2026-80097 de Microsoft Authenticator y las actualizaciones extraordinarias de .NET. [F01–F21]

Se mantiene como referencia la investigación gubernamental histórica consolidada el 03/09/2026 (32 URLs únicas), así como la planilla de 274 CVE del 24–26/10. Ninguno de esos recuentos demuestra exposición actual. La percepción operativa de escaso mantenimiento (“98%”) se consigna únicamente como testimonio de campo, no como métrica verificada.

REGLA DE LECTURA | “Explotada” significa evidencia pública razonablemente sustentada de abuso real; “0Day” puede referir a divulgación pública sin parche, aunque no consten intrusiones; “CVE nueva” exige fecha de publicación en NVD/CNA en la ventana; “revalidado” solo procede con comprobación autorizada y fechada.

Decisiones ejecutivas recomendadas

- Autorizar inventario cruzado de activos, versiones y superficies de administración; identificar responsables y dependencias de terceros.
- Aplicar contención y parches P0 donde coincidan producto vulnerable, exposición y explotación conocida; iniciar revisión de compromiso si la exposición existía antes de actualizar.
- Aprobar ventanas de cambio y rollback documentados para firewalls, kernel, hipervisores y sistemas de respaldo.
- Requerir evidencias verificables de cierre: versión efectiva, logs, pruebas funcionales, retest, respaldo y firma de aceptación del riesgo residual.

Contenido del informe

1. Alcance, método y control de evidencia

2. Cronología de alertas y clasificación temporal

3. Vulnerabilidades explotadas y prioridad P0

4. Vulnerabilidades nuevas y divulgaciones 0Day

5. Microsoft: AuthMask, .NET y activos corporativos

6. Software de usuario, datos, respaldo y dependencias

7. Matriz institucional de remediación

8. Plan 24/48/72 h y 30/90 días

9. Criterios de cierre, limitaciones y conclusiones

Anexo A. Matriz compacta de CVE y parches

Anexo B. Fuentes primarias y trazabilidad

1. Alcance, método y control de evidencia

1.1 Ámbito y universo documental

Ventana principal: 27/10/2026 10:26–29/10/2026 10:26, Argentina (UTC−3). Análisis extendido: alertas significativas del 21–26/10 y Microsoft Authenticator CVE-2026-80097, con aviso original de septiembre y divulgación técnica del 23/10. El informe es una fotografía documental; los portales oficiales y matrices de hotfixes pueden cambiar luego de la hora de cierre.

Fuentes: avisos primarios de fabricantes, CISA KEV, NVD/CNA, ZDI y fuentes institucionales de seguimiento de paquetes. Se contrastaron las versiones por rama y se separó publicación, corrección, explotación y afectación al entorno. Los avisos periodísticos o de terceros se utilizaron como señales y no sustituyen la posición oficial del proveedor.

1.2 Taxonomía y grados de certeza

Etiqueta	Criterio	Tratamiento
KEV / explotación	Incorporación a KEV o confirmación pública del proveedor de ataque activo	Prioridad elevada, con verificación de afectación por activo
Zero-day explotado	Evidencia de uso antes de corrección o divulgación	Separar fecha de explotación de fecha de publicación
0Day divulgado	Investigación pública que rotula 0Day sin corrección disponible	No implica ataques observados; evaluar compensaciones
Parche extraordinario	Release OOB o revisión material de una corrección previa	Reevaluar entornos ya parcheados y dependencias
Histórico / seguimiento	CVE anterior con situación vigente o actualización de aviso	No sumar al conteo de CVE nuevas en 48 h
Hipótesis institucional	Producto no inventariado o hallazgo antiguo sin retest	No atribuir exposición ni compromiso actual

1.3 Límites y custodia

No se realizaron nuevas conexiones a sistemas gubernamentales, explotación, recolección de credenciales ni pruebas de denegación de servicio. Las vulnerabilidades aquí detalladas no equivalen a hallazgos sobre un organismo concreto. No se reproducen IP, tokens, datos personales o PoC de explotación de producción. Los boletines de terceros deben mantenerse con URL, fecha de consulta y versión original en expediente de auditoría.

2. Cronología y evolución de la amenaza

Fecha	Hecho relevante	Lectura / estado
08/09	Microsoft corrige Authenticator CVE-2026-80097	Histórico, parche disponible
21–26/10	PHP2Shell, Microsoft .NET OOB, Apple y Valkey	Antecedente operativo y retest
23/10	Enclave publica análisis AuthMask	Divulgación técnica posterior al parche
27/10	CISA agrega Adobe Commerce y Brotli a KEV	Explotación conocida [F01]
27/10	Google Chrome y Mozilla publican actualizaciones	Correcciones de endpoint [F13–F15]
27–28/10	Palo Alto amplía matriz PAN-OS y eleva urgencia	Hotfixes escalonados [F06]
28/10	CISA KEV incorpora Linux y VMware ESX	Explotación conocida [F02]
28/10	Cisco, Sophos y Juniper divulgan avisos relevantes	Riesgo red/VPN [F03–F05]
28/10	ZDI publica siete 0Day Ultralytics	Sin explotación pública acreditada [F17–F18]
28/10	ZDI divulga Valkey; se revisan boletines Tailscale del 26/10	Corregir dependencias y canales remotos [F19–F21]
29/10	Cierre de investigación y correlación documental	No equivale a retest de producción

Las fechas son las de los avisos y eventos; la fecha original de un CVE puede diferir de la incorporación a KEV o de la publicación de su análisis.

3. Evidencia de explotación y controles P0

3.1 Cuatro nuevas incorporaciones CISA KEV (27–28/10)

CVE / fecha KEV	Producto y mecanismo	Impacto / primera medida
CVE-2026-111497 27/10	Brotli: error de manejo de retorno, posible corrupción de memoria	Inventariar bibliotecas incorporadas y actualizar productos dependientes. [F01,F09]

CVE / fecha KEV	Producto y mecanismo	Impacto / primera medida
CVE-2026-48356 27/10	Adobe Commerce/Magento: carga de archivo peligroso bajo interacción del usuario	Validar rama instalada, parche APSB26-73 y registros web. [F01,F23]
CVE-2026-46300 28/10	Kernel Linux: fallo en tratamiento de fragmentos en XFRM/ESP	Aplicar kernel del proveedor; reiniciar; revisar indicios de abuso previo. [F02,F07]
CVE-2026-41709 28/10	VMware ESX: registros de auditoría insuficientes ante un administrador malicioso	Aplicar build corregido; exportar logs fuera de hipervisor. [F02,F08]

La inclusión en KEV significa explotación observada en entornos reales, NO que todos los equipos vulnerables estén comprometidos. La CVE de VMware tiene CVSS 2.7, pero su pertenencia a KEV demuestra que CVSS no reemplaza inteligencia de explotación y criticidad del activo. Los vencimientos de la administración federal de EE. UU. no obligan a entidades argentinas. [F01,F02,F08]

3.2 Cisco ASA / Firepower Threat Defense: CVE-2026-76418

Cisco publicó el 28/10 una vulnerabilidad CVSS 8.6 en el servicio SSL VPN de acceso remoto. Un atacante sin autenticación puede provocar reinicio del equipo y denegación de servicio cuando existe autenticación secundaria configurada en el grupo de túnel vulnerable. Cisco reconoce evidencia de explotación activa; no se ha demostrado por esta CVE robo de datos ni ejecución remota. No hay workaround general equivalente al parche. [F03]

ASA: rama	Versión correctiva	FTD: rama	Versión correctiva
9.16 y anteriores	9.16.4.104	7.0 y anteriores	7.0.11
9.18	9.18.4.96	7.2 / 7.4	7.2.13 / 7.4.9
9.20	9.20.4.50	7.6 / 7.7	7.6.7 / 7.7.14
9.22	9.22.3.200	10.0 / 10.1	10.0.3 / 10.1.1
9.23 / 9.24	9.23.1.48 / 9.24.1.27 o 9.24.10.1	—	—

Acciones: identificar equipos con RA SSL VPN, confirmar configuración de autenticación secundaria, registrar versiones/alta disponibilidad, respaldar configuración y actualizar mediante procedimiento Cisco; observar reinicios, caídas de túneles y logs de VPN durante ventana definida. No deshabilitar MFA como mitigación improvisada. [F03]

3.3 Palo Alto PAN-OS y PHP2Shell: CVE-2026-109618 / 109619

Palo Alto registra explotación real y urgencia máxima de las dos fallas de PHP que afectan determinadas versiones de PAN-OS y Panorama, especialmente superficies de administración accesibles. Los hotfixes se distribuyen por rama y subversión; algunas entregas permanecían sujetas a fecha estimada al corte. El perfil de riesgo aumenta cuando la interfaz de gestión se expone públicamente. GlobalProtect App no figura afectada en la matriz consultada. [F06]

Rama	Ejemplos de corrección publicada	Cautela
12.2	12.2.4-h1	Verificar subrama exacta
12.1	12.1.7-h11	Otras subramas con ETA; validar matriz
11.2	11.2.16-h1 o 11.2.10-h16	11.2.10-h17 contempla además Brotli
11.1	11.1.16-h4	Confirmar patch level instalado
10.2	10.2.18-h13	No asumir compatibilidad con todas las subramas

Contención inmediata: interfaz MGT restringida a redes confiables, administración mediante bastión, registro y correlación de accesos, respaldo previo, actualización oficial y búsqueda de IoC. La firma IPS o una política temporal reducen la exposición, pero no sustituyen los hotfixes. [F06]

3.4 Kernel Linux: CVE-2026-46300, conocida como Fragnesia

CISA incorporó la falla a KEV el 28/10. El problema se relaciona con fragmentos compartidos del buffer de red durante procesamiento XFRM/ESP-in-TCP y puede provocar modificación no prevista de contenido respaldado por page cache. Se publicaron análisis de explotación con impacto elevado; su explotación requiere condiciones de kernel y configuración concretas. No debe afirmarse root automático ni compromisos gubernamentales locales sin evidencias. [F02,F07]

En Debian, el tracker registra como hitos de corrección del paquete fuente Bookworm 6.1.174-1 y Trixie 6.12.90-1; los paquetes de seguridad posteriores incorporan esas correcciones. La comparación válida se hace contra el paquete de la distribución, considerando backports, y se confirma con el kernel efectivamente cargado tras reiniciar. [F07]

3.5 VMware ESX: CVE-2026-41709

Broadcom documenta una falla de logging (CVSS 2.7) que puede ser usada por un administrador malicioso para ocultar ciertas operaciones. Su registro en KEV y los reportes de utilización histórica la vuelven prioritaria para plataformas de virtualización de alta criticidad. No debe presentarse como acceso inicial no autenticado. [F02,F08]

Entorno	Build / versión corregida de referencia
ESX 8.0	ESXi80U3j-25429389
ESX 9.0	ESXi-9.0.2.0100-25595025
ESX 9.1	ESXi-9.1.0.0-25370933
VMware Cloud Foundation 5.x	5.2.4

Acciones: aplicar parches oficiales, revisar cuentas y permisos administrativos, exportar logs a SIEM inmutable o remoto, correlacionar acciones sensibles del plano de gestión y documentar historial de vCenter/hosts. [F08]

4. Nuevas vulnerabilidades y divulgaciones tipo 0Day

4.1 Sophos UTM: CVE-2026-118633 (28/10)

Sophos calificó como crítica una falla de path traversal que, en escenarios con proxy de correo y análisis habilitado, puede permitir a un atacante remoto sin autenticar ejecutar comandos como root si logra una condición de carrera. El producto UTM está en fin de vida: la corrección requiere parche manual y Sophos recomienda migrar a Sophos Firewall. No informa workaround integral. Se exige identificar producto y función exacta antes de elevar alerta por exposición real. [F04]

4.2 Juniper Session Smart Router / Conductor (28/10)

Juniper publicó JSA112183 con múltiples CVE identificadas internamente: CVE-2026-103406 (RCE en gestión de claves, CVSS 9.8), 103407 (gestión PKI), 103408 (RCE al procesar opciones DHCP) y 103409 (privilegios administrativos bajo condiciones específicas, CVSS 9.8), junto con otras de disponibilidad y configuración. Corrige en ramas 7.0.5, 7.1.7 y 7.2.3 o posteriores. El fabricante no conoce explotación maliciosa de este grupo al momento del boletín. [F05]

4.3 Siete avisos ZDI 0Day contra Ultralytics (28/10)

ZDI divulgó siete fallas que califica 0Day en cargas de modelos, parsing y procesamiento de datasets. En los avisos consultados se documentan deserialización insegura, inyección de código/comandos y recorrido de rutas, normalmente con interacción del usuario (archivos o recursos maliciosos). La etiqueta de ZDI no prueba explotación en campañas ni implica necesariamente una CVE de uso remoto sin interacción. [F17,F18,F27]

CVE	Módulo / mecanismo	Tratamiento hasta corrección verificable
CVE-2026-118613	torch_load: deserialización insegura	No cargar modelos no confiables
CVE-2026-118614	check_det_dataset: inyección de código	Aislar datasets externos
CVE-2026-118615	torch_safe_load: ejecución de comandos	Ejecutar con usuario no privilegiado
CVE-2026-118616	parse_model: ejecución/inyección	Validación y sandbox
CVE-2026-118617	Caché de datasets: deserialización	Prohibir artefactos externos sin revisión
CVE-2026-118618	parse_model: segunda variante	Separar entornos de entrenamiento
CVE-2026-118619	Descargas Google Drive: recorrido de rutas	Limitar red y filesystem accesible

Estado: avisos ZDI públicos del 28/10; no se ha acreditado una versión universalmente corregida para las siete entradas ni ataques reales. Verificar cada boletín antes de afirmar cierre. [F17,F18,F27]

4.4 UEFI / TianoCore EDK II PXE: CVE-2026-97631

El aviso oficial del 22/10 asigna CVSS v4.0 9.5 a una escritura fuera de límites durante arranque PXE en EDK II. Un atacante capaz de enviar ciertos mensajes ICMP al equipo durante la ventana de arranque por red puede provocar corrupción en firmware previo al SO, con posible ejecución previa a controles de carga. La exposición está condicionada a implementación vulnerable y PXE operativo. Existe una corrección propuesta en el repositorio, pero el

advisory indica que no hay todavía una versión parcheada estable del proyecto; mucho menos puede suponerse que todos los BIOS/UEFI de fabricantes ya incorporan el arreglo. [F16]

Acciones temporales: desactivar arranque PXE cuando no sea indispensable, usar redes aisladas de aprovisionamiento, bloquear fuentes no autorizadas y solicitar al fabricante del servidor una imagen de firmware validada. Evitar reinicios de aprovisionamiento no controlados si existe exposición, sin interferir con la continuidad de sistemas críticos. [F16]

4.5 Valkey: ZDI-26-833, error de truncamiento y buffer

ZDI publicó el 28/10 un fallo en manejo de mensajes PUBLISH del clúster que permite a un cliente autenticado provocar corrupción de memoria y posible ejecución de código. El advisory ZDI-26-833 no exhibe CVE asignada; por rigor se conserva su identificador ZDI. Las correcciones fueron publicadas por Valkey el 26/10: 7.2.15, 8.0.12, 8.1.11, 9.0.7 y 9.1.3. [F19,F20]

4.6 Tailscale: boletines TS-2026-014 a 017

El proveedor documenta cuatro fallas que incluyen reenvío SSH a sockets privilegiados, agotamiento de memoria por sesiones Tailscale SSH, acceso a sockets desde Tailscale Serve y mezcla de capacidades entre montajes HTTP/2. La versión 1.104.4 o posterior corrige las condiciones identificadas. Algunas requieren que un peer tenga una sesión SSH permitida por la política o que existan configuraciones Serve específicas. [F21]

Mitigación específica: TS_SSH_DISABLE_FORWARDING=1 puede desactivar el forwarding de Tailscale SSH para la primera condición; debe evaluarse su impacto y reiniciar el servicio. Aplicar la actualización sigue siendo la medida preferente. [F21]

5. Microsoft: identidad y aplicaciones corporativas

5.1 AuthMask / Microsoft Authenticator: CVE-2026-80097

Aviso original: 08/09/2026. CWE-287, CVSS 3.1 8.6 (alto). La investigación de Enclave, publicada el 23/10, explica un defecto de validación de identidad en el broker de Microsoft Authenticator para Android, por el que una aplicación maliciosa instalada localmente puede hacerse pasar por una aplicación Microsoft legítima y obtener tokens de cuentas corporativas. El investigador mostró obtención de tokens con una app sin permisos Android declarados; esto no implica que cualquier ataque remoto web robe tokens sin instalación local. [F11,F12,F25]

Versiones afectadas documentadas: 6.0.0 hasta antes de 6.2606.4246; versión corregida 6.2606.4246 o posterior. Microsoft clasifica el vector con interacción del usuario (UI:R); los investigadores no requirieron interacción adicional en sus condiciones experimentales una vez instalada la aplicación. Debe evitarse presentar la disparidad como prueba de que Microsoft está equivocado. No se confirmó explotación masiva pública ni incorporación de esta CVE a KEV al corte. [F11,F12,F25]

VALOR INSTITUCIONAL | Un segundo factor robusto no impide por sí solo el abuso de tokens de sesión si fallan los controles entre aplicaciones. Priorizar administradores, responsables de sistemas y cuentas con acceso a correo, Microsoft Graph, expedientes y almacenamiento corporativo.

Plan: inventario MDM, actualización de Authenticator, control de instalaciones Android no confiables, revisión de inicios de sesión y consentimientos sospechosos en Entra ID; revocar sesiones y credenciales si aparecen indicadores. No revocar indiscriminadamente todas las sesiones sin plan operativo. [F11,F12]

5.2 .NET: actualizaciones extraordinarias del 25/10

Microsoft corrigió CVE-2026-111497 (Brotli) y CVE-2026-114148 (metadatos de propiedad en tarballs Linux) y relanzó correcciones de CVE-2026-70197 (SocketAsyncEventArgs) y CVE-2026-102870 (depurador Blazor WebAssembly), porque los parches originales del 13/10 no cubrían completamente los escenarios afectados. Es un antecedente crítico, no un aviso nuevo del 27–29. [F10]

Rama .NET	Release de corrección	Control específico
.NET 8	8.0.33	Runtime, ASP.NET Core tarball, contenedores
.NET 9	9.0.22	Runtime, ASP.NET Core tarball, contenedores
.NET 10	10.0.14	Runtime y paquetes Blazor relevantes
.NET 11 RC	RC3	Actualizar desde RC2

Aplicaciones framework-dependent requieren runtime corregido y reinicio. Las aplicaciones self-contained deben recompilarse; las imágenes Docker deben reconstruirse y desplegarse; en Blazor hay que verificar paquetes NuGet afectados. Un dotnet --list-runtimes correcto en el host no demuestra seguridad de imágenes autocontenidas. [F10]

5.3 Windows, Exchange y administración institucional

El seguimiento de actualizaciones extraordinarias de octubre para Windows/Windows Server y listas de certificados de confianza debe continuar en redes aisladas, repositorios WSUS y sistemas que no reciben actualizaciones directas. La validación debe hacerse por KB y compilación exacta de cada familia de Windows y tras pruebas de servicios, particularmente Exchange. No se atribuye una nueva CVE a cada actualización acumulativa, dado que pueden abordar confianza de certificados u otras correcciones operativas.

6. Endpoints, bibliotecas, datos y respaldos

6.1 Google Chrome, ChromeOS, Mozilla Firefox y Thunderbird

Chrome Stable del 27/10 corrige 52 fallas de seguridad, entre ellas cuatro críticas: CVE-2026-118306 (FileSystem), 118331 (FileAPI), 118348 (Skia) y 118344 (Layout). Versiones: Windows/macOS 156.0.8078.73/.74; Linux 156.0.8078.73. ChromeOS estable publicó aviso el 28/10 con navegador 156.0.8078.77 y entradas que incluyen CVE-2026-118331. [F13,F26]

Mozilla publicó Firefox 159 el 27/10, con CVE-2026-117860 (same-origin policy), 117861 (sandbox escape) y 117862 (elevación de privilegios), además de Firefox ESR 153.6 y 115.44 y Thunderbird 159 y 153.6. El uso de versiones ESR requiere confirmar rama elegida y políticas de actualización. No se presume explotación activa de las CVE críticas de Chrome por su sola calificación. [F14,F15]

6.2 Brotli: impacto transversal sobre software incorporado

Brotli CVE-2026-111497 ya aparece en KEV. El centro canadiense de ciberseguridad advierte que la biblioteca está incorporada en numerosas dependencias —incluidos Node.js, Microsoft .NET, PowerShell y otros—, de modo que corregir solo el paquete brotli del sistema puede dejar copias vulnerables en binarios y contenedores. Versiones correctivas dependen de la rama (por ejemplo 1.0.10, 1.1.1, 1.2.1), y debe preferirse la release corregida del producto que incorpora la biblioteca. [F09,F10]

6.3 Dell PowerProtect Data Domain: seguridad de los backups

El boletín Dell DSA-2026-416 es anterior al corte (publicación original 01/10, actualización 19/10), pero mantiene relevancia por problemas que abarcan credenciales, cuentas privilegiadas y ejecución de comandos según la versión. Debe verificarse cada CVE en la tabla oficial y aplicar DD OS corregido con respaldo/rollback. Se recomienda aislar interfaces de gestión, segmentar las redes de backup, exigir MFA donde esté soportado y conservar copias inmutables u offline. [F22]

Rama DD OS	Versión correctiva de referencia
Feature Release	8.9.0.0
LTS2024	7.13.1.90
LTS2025	8.3.1.50
LTS2026	8.6.1.30

6.4 Actualizaciones Apple del 26/10

Apple distribuyó iOS/iPadOS 27.2, macOS 27.2 y ramas anteriores con múltiples correcciones. Quedan fuera de la ventana 27–29 pero pueden afectar dispositivos de directivos, administradores o custodios de información. Deben incluirse en gestión de endpoints/MDM, sin afirmar una explotación activa no publicada por Apple. [F24]

6.5 Otros frentes bajo seguimiento documental

Se conservan como asuntos condicionados a inventario: complementos WordPress con carga de archivos, GitLab, EPICS Base, MLflow, Node.js, NGINX, Oracle Java/GraalVM, Python/eMudhra, Apache Traffic Server, Apache Airflow y Fortinet. Su presencia o severidad no se presume automáticamente sobre los 32 sitios históricos; una nueva sección de hallazgos por host requerirá versiones y pruebas autenticadas. Deben contrastarse sus versiones con avisos actuales antes de emitir una orden de parcheo.

7. Matriz institucional de prioridad y remediación

La prioridad propuesta combina: (a) presencia y exposición confirmadas; (b) evidencia de explotación/KEV; (c) valor y criticidad del servicio; (d) impacto en confidencialidad, integridad y disponibilidad; (e) disponibilidad y factibilidad del parche; (f) mitigaciones verificables. No equivale a clasificación automática por CVSS.

P	Tecnologías a comprobar	Primera acción / evidencia de cierre
P0	Cisco ASA/FTD SSL VPN con condición vulnerable	Patch+prueba HA/VPN y análisis de reinicios/logs [F03]
P0	Sophos UTM con correo proxy activo	Parche manual o migración; versión y correo funcional [F04]
P0	PHP2Shell / PAN-OS administración expuesta	Restricción MGT+hotfix de subrama+IoC [F06]
P0	Brotli, Linux, Adobe Commerce, VMware si hay KEV aplicable	Inventario+parche+análisis retrospectivo [F01,F02]
P1	Juniper Session Smart y Tailscale	Release segura, validación de políticas VPN/SSH [F05,F21]
P1	Microsoft Authenticator / .NET	Versión por dispositivo y build/pipeline [F10–F12]
P1	Chrome, Firefox/ESR, Thunderbird	Versiones de endpoint + telemetría [F13–F15]
P1	Valkey clúster y Dell Data Domain	Corrección, segmentación, pruebas de continuidad [F19,F20,F22]
P2	TianoCore PXE, Ultralytics, Apple y otros especializados	Mitigaciones específicas y parches fabricante [F16–F18,F24]

8. Hoja de ruta: 24/48/72 horas y 30/90 días

8.1 Primeras 24 horas: contención documentada

1. Designar responsable por activo, evaluar cambios en alta disponibilidad y registrar ticket/aprobación. Congelar información de versiones y configuración antes de modificar.
2. Identificar servicios de administración expuestos, VPN Cisco, PAN-OS, Sophos UTM, routers Juniper, hipervisores y dependencias Brotli con KEV.
3. Priorizar aislamiento de consolas desde Internet y copia segura de logs; no borrar evidencias al aplicar parches.
4. Aplicar parches P0 por subrama y confirmar restauración de servicios críticos: VPN, correo, identidad, telefonía, interfaces administrativas y backups.

8.2 De 24 a 48 horas: despliegue validado

5. Actualizar kernels/distribuciones desde repositorios compatibles y verificar reinicio con kernel efectivo.
6. Actualizar runtimes .NET y reconstruir contenedores/autocontenidas; revisar Authenticator Android y flujos Entra ID.
7. Distribuir navegadores, Thunderbird, Tailscale y Valkey según inventario; probar funcionalidad de integraciones.
8. Planificar parche de equipos UTM EOL y migración formal; mantener compensaciones en EDK II/PXE y estaciones de IA.

8.3 De 48 a 72 horas: evidencia y seguimiento

9. Realizar validaciones autenticadas de versiones y exposición en alcance expresamente autorizado.
10. Correlacionar logs de acceso, autenticación, reinicios, cuentas privilegiadas y cambios de configuración con el período previo al parche.
11. Probar restauración de backups, alta disponibilidad y recuperación operativa; documentar evidencia SHA-256 de artefactos de prueba.
12. Abrir excepciones por sistema sin parche, con compensaciones, responsable, fecha de vencimiento y autorización de riesgo.

8.4 Plan de 30 y 90 días

Hito	Resultado verificable
Día 7–15	Inventario de software y firmware por activo, propietarios, versiones y dependencias; revisión de privilegios e interfaces públicas

Hito	Resultado verificable
Día 30	SLAs de remediación establecidos; escaneos autenticados regulares; SIEM/logging centralizado; pruebas básicas de restauración
Día 60	Revisión de EOL/EOS, segmentación de backups y administración, gestión MDM, SBOM/artefactos CI/CD
Día 90	Retest integral autorizado; tablero de cumplimiento, excepciones residuales y plan de inversiones aprobado

9. Verificación técnica, aceptación y conclusiones

9.1 Evidencia mínima de cierre por CVE

Campo	Documento / prueba requerida
Activo	Código, responsable, entorno, criticidad y alcance autorizado
Producto	Versión real, distribución / build, hash de paquete si aplica
Exposición	Interfaz, servicio y prerrequisitos; sin publicar secretos
Corrección	KB/hotfix/commit/release oficial y fecha real de despliegue
Validación	Salida autenticada, servicio en ejecución, test funcional y evidencias antes/después
Amenaza previa	Logs/EDR/IoC, ventana retrospectiva y decisión de respuesta a incidentes
Cierre	Riesgo residual, responsable, aprobación, ticket y fecha de próximo retest

9.2 Comprobaciones no invasivas sugeridas

Linux: uname -r; lectura del gestor de paquetes para verificar la revisión de seguridad (Debian dpkg-query / apt-cache policy, Arch pacman -Q). Entornos web: php -v, apache2/nginx -v según corresponda y versiones reales de los procesos. .NET: dotnet --list-runtimes. Tailscale: tailscale version. Navegadores: consultar versión desde la propia aplicación o el gestor de paquetes. Windows: Get-HotFix y Get-ComputerInfo; corroborar compilación y parches para cada rama. Estas comprobaciones son de inventario, NO sustituyen retest funcional.

9.3 Limitaciones y conclusión de auditoría

La base documental del 24–26/10 contabilizaba 274 CVE, pero no se repite como total nuevo ni se extrapola al entorno del Gobierno del Chaco. La cifra de mantenimiento insuficiente del “98%” proviene de experiencia operativa reportada y no de una medición formal. El histórico de 32 URLs conserva valor como referencia de superficie, no como prueba de exposición actual. No se confirma intrusión o fuga de datos locales en este trabajo.

DICTAMEN DE INTELIGENCIA | Persisten amenazas de máxima urgencia en los casos de productos expuestos con explotación documentada; el riesgo general provisional se mantiene ALTO hasta completar inventario y retest. La recomendación es aprobar contención P0, remediar según el proveedor, comprobar compromiso retrospectivo y exigir evidencia de cierre por activo.

9.4 Firma y aprobación

Preparado por: Instel & Seguridad · Dirección Técnica / Auditoría y Análisis Forense

Validación del responsable del organismo: _____

Fecha de aceptación / orden de remediación: _____

Observaciones, excepciones autorizadas y vencimiento: _____

ANEXO A. Matriz compacta de identificación y parche

Los valores de esta matriz son una lista técnica de comprobación, no el resultado de un escaneo de producción. “Revisar” indica que hay que verificar subrama/fabricante o parche antes de cerrar.

ID	Producto	Estatus	Parches / medidas	Pri.
CVE-2026-76418	Cisco ASA/FTD	Activa	Ramas corregidas PSIRT, según modelo	P0
CVE-2026-118633	Sophos UTM	Nueva 28/10	Parche manual Sophos / migrar producto	P0
CVE-2026-103406	Juniper Conductor	Nueva 28/10	7.0.5 / 7.1.7 / 7.2.3	P1
CVE-2026-103407	Juniper SSR/Conductor	Nueva 28/10	7.0.5 / 7.1.7 / 7.2.3	P1
CVE-2026-103408	Juniper SSR	Nueva 28/10	7.0.5 / 7.1.7 / 7.2.3	P1
CVE-2026-103409	Juniper SSR	Nueva 28/10	7.0.5 / 7.1.7 / 7.2.3	P1
CVE-2026-111497	Brotli / dependencias	KEV 27/10	Actualizar producto y biblioteca	P0
CVE-2026-48356	Adobe Commerce	KEV 27/10	Parche APSB26-73 rama instalada	P0
CVE-2026-46300	Linux kernel	KEV 28/10	Kernel de distro / reinicio	P0
CVE-2026-41709	VMware ESX	KEV 28/10	Build matriz Broadcom VMSA	P0
CVE-2026-109618	PHP / PAN-OS	KEV anterior	PHP seguro / hotfix PAN-OS	P0
CVE-2026-109619	PHP / PAN-OS	KEV anterior	PHP seguro / hotfix PAN-OS	P0
CVE-2026-80097	Authenticator Android	Hist. 08/09	6.2606.4246 o posterior	P1
CVE-2026-70197	.NET SAEA	OOB 25/10	8.0.33 / 9.0.22 / 10.0.14	P1
CVE-2026-102870	.NET Blazor	OOB 25/10	10.0.14 / 11 RC3 y NuGet	P1
CVE-2026-114148	.NET tarballs Linux	OOB 25/10	8.0.33 / 9.0.22 / 10.0.14	P1
CVE-2026-118306	Chrome FileSystem	Nueva 27/10	Chrome 156 estable corregido	P1
CVE-2026-118331	Chrome FileAPI	Nueva 27/10	Chrome 156 estable corregido	P1
CVE-2026-118348	Chrome Skia	Nueva 27/10	Chrome 156 estable corregido	P1
CVE-2026-118344	Chrome Layout	Nueva 27/10	Chrome 156 estable corregido	P1
CVE-2026-117860	Firefox DOM	Nueva 27/10	Firefox 159	P1
CVE-2026-117861	Firefox sandbox	Nueva 27/10	Firefox 159	P1
CVE-2026-117862	Firefox red	Nueva 27/10	Firefox 159	P1
CVE-2026-97631	TianoCore PXE	0Day anterior	Mitigar; firmware del fabricante pendiente	P1
CVE-2026-118613	Ultralytics	0Day 28/10	Sin parche confirmado al corte	P2
CVE-2026-118614	Ultralytics	0Day 28/10	Sin parche confirmado al corte	P2
CVE-2026-118615	Ultralytics	0Day 28/10	Sin parche confirmado al corte	P2
CVE-2026-118616	Ultralytics	0Day 28/10	Sin parche confirmado al corte	P2
CVE-2026-118617	Ultralytics	0Day 28/10	Sin parche confirmado al corte	P2
CVE-2026-118618	Ultralytics	0Day 28/10	Sin parche confirmado al corte	P2
CVE-2026-118619	Ultralytics	0Day 28/10	Sin parche confirmado al corte	P2
ZDI-26-833	Valkey clúster	Aviso 28/10	7.2.15 / 8.0.12 / 8.1.11 / 9.0.7 / 9.1.3	P1
TS-2026-014	Tailscale SSH	Boletín oct.	1.104.4	P1
TS-2026-015	Tailscale SSH	Boletín oct.	1.104.4	P1
TS-2026-016	Tailscale Serve	Boletín oct.	1.104.4	P1
TS-2026-017	Tailscale HTTP/2	Boletín oct.	1.104.4	P1

ANEXO B. Fuentes primarias y referencias

Consultas efectuadas y contrastadas al 29/10/2026. URL exacta de la fuente para su consulta posterior. La referencia por código [F##] se usa a lo largo del informe.

F01 CISA: KEV, dos nuevas incorporaciones 27/10
https://content.govdelivery.com/accounts/USDHSCISA/bulletins/430af9d

F02 CISA: catálogo KEV vigente y fichas Linux/VMware
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

F03 Cisco PSIRT: ASA/FTD SSL VPN CVE-2026-76418
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-tunnel-dos-s6mgkb75

F04 Sophos: Sophos UTM CVE-2026-118633 (28/10)
https://www.sophos.com/en-us/security-advisories/sophos-sa-20261028-utm-rce

F05 Juniper SIRT JSA112183: Session Smart Router / Conductor
https://supportportal.juniper.net/s/article/2026-10-On-Demand-Security-Bulletin-Session-Smart-Router-and-Session-Smart-Conductor-Multiple-internally-discovered-vulnerabilities-resolved

F06 Palo Alto: CVE-2026-109618/619 y matriz PAN-OS
https://security.paloaltonetworks.com/CVE-2026-109618

F07 Debian Security Tracker: CVE-2026-46300
https://security-tracker.debian.org/tracker/CVE-2026-46300

F08 Broadcom: VMSA y matriz CVE-2026-41709 ESX
https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017

F09 Cyber Centre Canada: impacto de Brotli CVE-2026-111497
https://www.cyber.gc.ca/en/alerts-advisories/al26-027-critical-vulnerability-impacting-google-brotli-cve-2026-111497

F10 Microsoft .NET: out-of-band security updates 25/10
https://devblogs.microsoft.com/dotnet/dotnet-october-2026-oob-security-updates/

F11 Microsoft MSRC: CVE-2026-80097
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-80097

F12 Enclave: investigación AuthMask 23/10
https://enclave.ai/blog/authmask-we-made-microsoft-authenticator-hand-over-tokens

F13 Google Chrome: actualización estable 27/10
https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-desktop_0562499947.html

F14 Mozilla: MFSA 2026-118 Firefox 159
https://www.mozilla.org/en-US/security/advisories/mfsa2026-118/

F15 Mozilla: tabla de avisos 27/10 Firefox/ESR/Thunderbird
https://www.mozilla.org/en-US/security/advisories/

F16 TianoCore EDK II: GHSA-99cj-7hg9-mp4m
https://github.com/tianocore/edk2/security/advisories/GHSA-99cj-7hg9-mp4m

F17 ZDI: Ultralytics torch_load ZDI-26-812
https://www.zerodayinitiative.com/advisories/ZDI-26-812/

F18 ZDI: Ultralytics check_det_dataset ZDI-26-813
https://www.zerodayinitiative.com/advisories/ZDI-26-813/

F19 ZDI: Valkey ZDI-26-833
https://www.zerodayinitiative.com/advisories/ZDI-26-833/

F20 Valkey: versiones de seguridad del 26/10
https://github.com/valkey-io/valkey/releases

F21 Tailscale: boletines TS-2026-014 a 017
https://tailscale.com/security-bulletins

F22 Dell: DSA-2026-416 PowerProtect Data Domain
https://www.dell.com/support/kbdoc/en-in/000515178/dsa-2026-416-security-update-for-dell-powerprotect-data-domain-multiple-vulnerabilities

F23 Adobe Commerce / Magento APSB26-73
https://www.adobe.com/trust/security/products/commerce/apsb26-73.html

F24 Apple: actualizaciones de seguridad de octubre
https://support.apple.com/es-es/100100

F25 CVE/NVD: ficha CVE-2026-80097
https://nvd.nist.gov/vuln/detail/CVE-2026-80097

F26 Google ChromeOS estable: aviso 28/10
https://chromereleases.googleblog.com/2026/10/stable-channel-update-for-chromeos_01748991111.html

F27 ZDI: lista de avisos públicos
https://www.zerodayinitiative.com/advisories/published/

F28 CISA: validación técnica de la explotación y catálogo
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

FIN DEL DOCUMENTO — INSTEL & SEGURIDAD