ALERTA TÉCNICA DE CIBERSEGURIDAD

INSTEL & SEGURIDAD

ANÁLISIS FORENSE - AUDITORÍA - PENTESTING

NUEVAS VULNERABILIDADES, ATAQUES Y RIESGO DE RANSOMWARE

Java4Shell · Bancos y gobiernos · CISA KEV · Infraestructura crítica

DESTINATARIOS	Empresas, gobiernos, sector financiero, salud y TI
ELABORADO POR	Pedro Matías Cacivio · Instel & Seguridad
PERÍODO	13 al 20 de noviembre de 2026 (Argentina, UTC-3)
PRIORIDAD	Corrección urgente y prevención de ransomware

DOCUMENTO PREVENTIVO DE INTELIGENCIA Y RESPUESTA · FUENTES CITADAS

Una CVE o un incidente público no acreditan compromiso de un sistema concreto.
La intervención requiere inventario, autorización, pruebas de recuperación y evidencia.

1. Resumen ejecutivo y alcance

Entre el **13 y el 18 de noviembre de 2026** aparecieron alertas de explotación confirmada sobre equipos de seguridad perimetral, servicios de administración centralizada y aplicaciones web, junto con una vulnerabilidad de alto impacto en Java y un aviso extraordinario del FBI sobre ataques automatizados contra entidades financieras, gobiernos y proveedores. El riesgo de ransomware exige medidas urgentes, pero técnicamente verificadas.

La principal novedad técnica es **Java4Shell (CVE-2026-114938)**, divulgada y corregida el 17 de noviembre. Paralelamente, Oracle publicó **655 nuevos parches** para distintas familias de productos, de los cuales 11 corresponden a Java SE. Esta cifra describe correcciones publicadas, no 655 ataques ni 655 sistemas comprometidos. [F01-F04]

Entre las vulnerabilidades incorporadas por CISA a KEV desde el 13 de noviembre destacan **Check Point CVE-2026-123039**, **UnrealIRCd CVE-2026-114713** y **Perforce Puppet CVE-2026-115731**. Estar en KEV implica evidencia de explotación real; no implica que todas hayan sido utilizadas en campañas de ransomware. [F06-F09]

El FBI difundió el 13 de noviembre la alerta FLASH-20261113-001 sobre el uso malicioso de la plataforma ARTEX en operaciones automatizadas contra sectores financiero, público, sanitario y tecnológico. El reporte describe intrusiones que, en determinados casos, alcanzaron privilegios elevados en menos de tres horas. [F10]

> **Decisión institucional recomendada:** activar una evaluación extraordinaria de exposición; corregir primero sistemas explotados o accesibles desde Internet, localizar Java integrado en aplicaciones, inspeccionar accesos de terceros, comprobar copias offline/inmutables y preparar comunicaciones y continuidad de negocio. Registrar evidencias y responsables para cada intervención.

Criterios de lectura y alcance

Se incluyen: avisos y actualizaciones hechos públicos durante la ventana; confirmaciones de explotación o publicaciones oficiales que cambian la urgencia; incidentes comunicados en este intervalo aunque el acceso inicial haya ocurrido antes; y antecedentes del 12 de noviembre solo cuando su seguimiento sigue siendo relevante. No se pretende enumerar individualmente todas las CVE del mundo: se priorizan aquellas con impacto operativo real sobre entornos empresariales y gubernamentales.

Estados diferenciados: (A) parche o vulnerabilidad anunciados; (B) prueba de concepto pública; (C) explotación activa confirmada; (D) incidente de disponibilidad sin atribución maliciosa; (E) afirmación de actores criminales aún no verificada. El nivel de severidad CVSS no prueba explotación. Los plazos P0/P1 del informe son metas sugeridas de gestión, salvo vencimientos regulatorios expresos.

2. Matriz de alertas prioritarias: 13 a 18 de noviembre

Fecha	CVE / Aviso	Riesgo	Evidencia	Prioriz.
17-18/11	CVE-2026-114938	Java/OpenJDK: memoria, potencial RCE; hardware específico	Parche publicado; PoC público; sin explotación real confirmada en fuentes oficiales	P0 si expuesto
13/11	CVE-2026-123039	Check Point Gaia DynamicCLI: escalada local a root	KEV / explotación confirmada; investigar compromiso	P0
13/11	CVE-2026-114713	UnrealIRCd: inyección de comandos / respuesta etiquetada	KEV / explotación confirmada	P0
17/11	CVE-2026-115731	Puppet: deserialización y ejecución en servidor	KEV / explotación confirmada	P0
Nov.	CVE-2026-115732	Puppet: evasión de validación de identidad de certificados	Parche del proveedor; revisar CA y agentes	P0/P1
17/11	CVE-2026-129448	Apache Roller: XML-RPC sin autenticación; RCE	Apache informa explotación activa; mismo problema CVE-2026-82384	P0
12/11*	CVE-2026-120869	Citrix NetScaler Console: evasión de autenticación	Alerta anterior; seguimiento correctivo	P0/P1
17/11	Oracle CSPU Nov.	655 parches en familias Oracle; 11 de Java SE	Parches publicados; verificar matrices y exposición	P0/P1

* Citrix se incluye como **seguimiento**: la publicación original es del 12/11, fuera del intervalo principal. La columna de evidencia no atribuye ransomware sin prueba. [F01-F09,F13]

3. Java4Shell: vulnerabilidad que requiere actuación urgente

3.1 Identificación, alcance y gravedad

CVE-2026-114938 | publicación de correcciones: 17/11/2026. Se trata de una corrupción de memoria en el decodificador Base64 acelerado por hardware de HotSpot/OpenJDK. Datos Base64 especialmente manipulados podrían provocar caída de la JVM y, en determinadas circunstancias, ejecución remota de código sin autenticación. Oracle consigna CVSS v3.1 **8,1**; otros sistemas de puntuación, como CVSS v4, informan **9,2**. No se deben mezclar escalas. [F01-F04]

La explotación **no es universal**. Deben concurrir tres condiciones: procesador x86-64 con instrucciones **AVX512F, AVX512BW, AVX512VBMI y BMI2**; intrínseco de Base64 habilitado; y una aplicación que entregue al decodificador Base64 datos controlados por un atacante. Pueden intervenir autenticación HTTP, JWT, SAML, cookies u otros flujos. Los sistemas ARM64 no forman parte del escenario descrito. [F02]

Es prioritario verificar servidores con aplicaciones Java de gobierno, portales de usuarios, integraciones de identidad, middleware, autenticadores y aplicaciones financieras. Ejemplos de tecnologías que deben inventariarse: Keycloak, Jenkins, Jira, Confluence, Artifactory y otros productos que empaqueten un JDK propio. Su mera presencia **no confirma** una condición explotable. [F02,F04]

3.2 Versiones corregidas publicadas

Distribución / rama	Versión de referencia corregida	Observación
Oracle Java SE / OpenJDK 17	17.0.21.1	Revisar mantenimiento y distribución exactos
Oracle Java SE / OpenJDK 21	21.0.13.1	Actualizar runtime y reiniciar JVM
Oracle Java SE / OpenJDK 25	25.0.5.1	Seguir aviso de distribución instalada
Oracle Java SE / OpenJDK 27	27.0.1.1	Seguir aviso de distribución instalada
Oracle Java SE 8 performance	8u513	Caso especial: compilaciones performance afectadas
Eclipse Temurin	17.0.21.1+2 / 21.0.13.1+2 / 25.0.5.1+2 / 27.0.1.1+4	JDK 8 y 11 Temurin no afectados por esta falla específica

Las versiones mostradas corresponden a las matrices oficiales de CERT-EU y Adoptium. GraalVM y distribuciones OpenJDK (Corretto, Zulu, Liberica, SapMachine, Red Hat, Microsoft Build of OpenJDK) requieren consultar sus propios boletines. No asumir que actualizar el paquete del sistema corrige el JRE incluido dentro de un producto o contenedor. [F02,F04]

3.3 Mitigación temporal si no es posible corregir inmediatamente

La medida preferente es **actualizar a una versión corregida y reiniciar las JVM**. Si el proveedor aún no ofrece un paquete, CERT-EU documenta deshabilitar el intrínseco vulnerable usando **-XX:+UnlockDiagnosticVMOptions -XX:-UseBASE64Intrinsics**; alternativamente, limitar AVX en hosts x86-64 con **-XX:UseAVX=2**. El cambio debe validarse sobre la versión concreta y puede afectar rendimiento. **No utilizar UseAVX=2 en ARM**. [F02-F05]

```
# Verificaciones de solo lectura sobre servidor Linux autorizado
java -version
lscpu | grep -E "Architecture|Model name|Flags"
ps -ef | grep "[j]ava"
# Inspección de propiedad (comprobar flags avx512f, avx512bw, avx512vbmi y bmi2)
```

Registrar fabricante y ruta del runtime, línea de comando efectiva, host, procesador, contenedor o appliance y versión anterior/posterior. La aplicación puede contener varias JVM. Ningún comando de inspección anterior prueba si existe una vía de explotación alcanzable desde Internet.

4. Oracle: 655 correcciones y riesgos colaterales de actualización

Oracle publicó el **17 de noviembre** un Critical Security Patch Update con **655 parches** distribuidos entre numerosas familias de productos (bases de datos, aplicaciones empresariales, middleware y otros componentes). El apéndice de Java SE contiene **11 nuevas correcciones**, entre ellas CVE-2026-114938, CVE-2026-86144, CVE-2026-114939, CVE-2026-114940, CVE-2026-114941 y CVE-2026-114942. Su aplicabilidad depende de componentes y versiones concretos. [F03]

CVE	Componente Java	CVSS v3.1	Tratamiento operativo
CVE-2026-114938	Compiler / Base64	8,1	Identificar CPU, runtime y entrada controlable; priorizar RCE
CVE-2026-86144	JavaFX / libxml2	7,5	Verificar despliegues JavaFX y procesamiento de contenido
CVE-2026-114939	JGSS	7,4	Actualizar bibliotecas de autenticación y runtimes
CVE-2026-114940	JSSE / TLS	7,4	Revisar proveedores TLS y runtimes embebidos

CVE	Componente Java	CVSS v3.1	Tratamiento operativo
CVE-2026-114941	Compiler	7,0	Actualizar compilaciones afectadas de Java 21/25/27
CVE-2026-114942	Libraries	7,0	Actualizar bibliotecas de runtimes de ramas afectadas

Oracle también recuerda alertas de **octubre** por certificados eMudhra (**CVE-2026-91403**, **CVE-2026-114820**) y PHP2Shell (**CVE-2026-109618/109619**). No deben contarse como CVE nuevas del 13 al 18; sí se debe comprobar su remediación si continúa pendiente. [F03]

Precauciones antes de actualizar infraestructura crítica

- Preparar copia de seguridad y recuperación, especialmente de bases de datos, máquinas virtuales, truststores y configuraciones SAML/TLS.
- Ensayar el parche en un entorno que reproduzca integraciones bancarias, sistemas de expedientes, portales, historia clínica y aplicaciones de terceros.
- Programar actualización escalonada con verificación de servicios, rutas de rollback, responsables y comunicación de contingencia.
- Conservar telemetría previa y posterior: registros de JVM, errores, tiempos de respuesta y autenticaciones; reiniciar procesos para activar cambios.
- No posponer indefinidamente las correcciones en sistemas expuestos bajo pretexto de pruebas: aislar temporalmente mientras se ejecutan.

5. Explotación confirmada: nuevos ingresos al catálogo CISA KEV

5.1 Check Point Gaia OS — CVE-2026-123039

CISA incorporó la falla el **13/11**. Un socket local de DynamicCLI con permisos demasiado amplios puede permitir que un usuario local autenticado ejecute operaciones como **root**. La explotación pública afecta plataformas Check Point y puede formar parte de una cadena de intrusión: una vulnerabilidad remota separada aporta acceso inicial y luego se utiliza esta escalada. Check Point reporta explotación real; existen informes de encadenamiento con PHP2Shell y daños posteriores en infraestructura de virtualización. [F06,F07]

- Actualizar appliances, Gaia, gateways, consolas y servidores de gestión según matriz de Check Point; respetar ramas y compatibilidad.
- Restringir accesos de gestión y administración, revisar usuarios locales, acceso VPN, cambios de reglas, tareas y sockets.
- Si hubo exposición durante el período vulnerable, preservar logs, realizar búsqueda de persistencia y comprobar hosts de virtualización y sistemas asociados.
- No interpretar que el parche de escalada local, por sí solo, corrige cualquier vía remota de entrada o repara un compromiso previo.

5.2 UnrealIRCd — CVE-2026-114713

Ingresó en KEV el **13/11** por explotación confirmada. Es relevante principalmente si la institución utiliza servicios IRC o bots conectados a una red UnrealIRCd; no representa una falla genérica de todos los servidores Linux. El fabricante indica corrección en **UnrealIRCd 6.2.7.1** y un paquete hot-patch; aplicar conforme a la instalación y comprobar que todos los nodos estén corregidos. [F08]

5.3 Perforce Puppet — CVE-2026-115731 y CVE-2026-115732

CVE-2026-115731 fue incorporada a KEV el **17/11**. Una deserialización de datos no confiables en reportes permite ejecución de código en el Puppet Server cuando un cliente posee certificado firmado por la CA; una configuración de autofirma insegura puede agravar el acceso inicial. La CVE-2026-115732 afecta la validación de nombres de certificados. [F09]

El riesgo institucional es excepcional: Puppet controla numerosos equipos desde un punto central, por lo que una intrusión podría facilitar la propagación de cambios, instalación de herramientas maliciosas o alteraciones coordinadas. El proveedor ofrece correcciones **Puppet Enterprise 2026.0.1, 2025.12.1, 2023.8.13** y en Puppet Core **9.1.3 y 8.22.1** según sus notas de noviembre. Validar versión y paquete concretos. [F09]

- Actualizar Puppet Server antes de permitir nuevas operaciones de administración remota no indispensables.
- Deshabilitar o restringir firmas automáticas de certificados; revisar CA, certificados emitidos, nodos desconocidos y reportes inusuales.
- Limitar puertos de Puppet a la red de gestión; preservar logs antes de rotar certificados o reinstalar servicios.
- Revisar reglas de orquestación y cambios recientes a todos los hosts gestionados; considerar la cadena de confianza comprometida si hay indicios.

6. Apache Roller: nueva alerta de ejecución remota

El **17/11**, Apache divulgó **CVE-2026-129448 (CVSS 9,8)**, deserialización de datos no confiables a través del endpoint XML-RPC en Roller **4.0.0 a 6.1.4**. La fundación aclara que se trata de la misma vulnerabilidad ya registrada para Roller 6.1.5 como **CVE-2026-82384**; la corrección alcanza **6.1.6 o posterior**. Apache indica que el problema está siendo explotado. [F11]

Para organizaciones que no puedan actualizar de inmediato, el aviso de Apache sugiere establecer **enabledForExtensions=false** en WEB-INF/web.xml o eliminar el mapeo del servlet **/roller-services/xmlrpc** y reiniciar el servicio. **Desactivar XML-RPC desde el panel de administración no es suficiente** en versiones anteriores: la deserialización puede ocurrir antes de comprobar esa opción. [F11]

- Localizar instancias Apache Roller en portales, aplicaciones Java y servidores heredados.
- Aislar XML-RPC si no es indispensable y actualizar a versión corregida.
- Revisar logs HTTP, procesos Java, modificaciones de archivos y conexiones salientes anómalas.
- Validar que los plugins y la base de datos sean compatibles antes del cambio y preservar evidencias si existen síntomas de intrusión.

Seguimiento: Citrix NetScaler Console (aviso del 12/11)

Citrix publicó **CVE-2026-120869** con CVSS v4 **9,4**: un atacante sin autenticación con acceso a la IP de NetScaler Console puede eludir controles y alcanzar recursos restringidos. Afecta la rama 14.1 anterior a **14.1-74.34**. Aunque el aviso original es anterior al período, su exposición y función administrativa justifican reiterar la revisión. No existe aquí confirmación de explotación de esa CVE. [F13]

7. Ataques a bancos, gobiernos y proveedores: hechos comprobados

7.1 Alerta FBI del 13/11 sobre ARTEX

El FBI publicó el boletín **FLASH-20261113-001** el 13 de noviembre. Describe el uso malicioso de ARTEX —una plataforma de automatización de pruebas mediante agentes de IA— por distintos actores desde agosto, con campañas contra **servicios financieros, gobiernos, salud, defensa, industria y tecnología**. Documenta campañas en entidades financieras surcoreanas con extracción de datos de aproximadamente **67.000 personas** y un incidente de cadena de suministro de ConnectWise Cloud Backup con más de **2.250 entornos de clientes** potencialmente alcanzables. Son incidentes anteriores citados en una alerta nueva, no ataques todos ocurridos esta semana. [F10]

El boletín registra que algunas intrusiones pasaron de la selección del objetivo a privilegios elevados en **menos de tres horas**. Destaca entradas por vulnerabilidades de aplicaciones web, API, credenciales expuestas, proveedores, federaciones B2B y permisos de nube. La automatización reduce tiempos de respuesta, pero los vectores principales siguen siendo conocidos. [F10]

Recomendación para autoridades: tratar las relaciones con terceros como parte de la superficie crítica: auditar permisos de aplicaciones conectadas, cuentas de servicio, integraciones SSO/OAuth/SAML y accesos de proveedores. Una intrusión del contratista no debe proporcionar acceso administrativo irrestricto a la red institucional.

7.2 Sector financiero: incidentes y afirmaciones no verificadas

El **17/11**, Visa divulgó un informe propio sobre amenazas observadas entre enero y junio de 2026: los incidentes en terceros aumentaron **62 %** respecto del semestre anterior y los casos de ransomware observados por su equipo PERC subieron **19 %**. Son métricas del conjunto analizado por Visa, **no una tasa universal** de todos los bancos. [F12]

En paralelo, un grupo de extorsión denominado **n0n** afirmó haber comprometido empresas financieras. Visa reconoció la investigación de un incidente de un proveedor externo y declaró que sus propios sistemas no estaban involucrados y que no había indicios de exposición de números de tarjeta. La afirmación del grupo sobre JPMorgan Chase **no constituye confirmación** de acceso a ese banco. [F14]

La interrupción de transacciones de JPMorgan Chase del **16/11** se atribuyó públicamente a un defecto de software en equipos internos; no fue presentada por el banco como ciberataque. Esta distinción es necesaria para no confundir una falla de disponibilidad con ransomware. [F14,F15]

7.3 Otros casos que evidencian riesgo en servicios públicos

La Universidad de Texas en Arlington informó el **13/11** que una investigación confirmó robo de información personal en un incidente ocurrido en octubre. Qilin reivindicó el ataque, pero la adjudicación criminal y el alcance efectivo deben tratarse por separado. La institución mantuvo fuera de servicio un portal de formularios. [F16]

Monadnock Community Hospital confirmó el **16/11** que una interrupción prolongada de sus sistemas estaba relacionada con un incidente de ciberseguridad. Esa confirmación no identifica por sí sola ransomware ni autor. Es relevante para hospitales por la necesidad de mantener atención y comunicación aun cuando fallen servidores. [F17]

7.4 Las interrupciones de servicios no son, por sí mismas, ataques

Microsoft 365 (12-14/11), FAA (13/11), JPMorgan Chase y United (16/11), Apple y una red interna de la NSA (17/11) registraron interrupciones. Los responsables informaron fallas técnicas, actualizaciones o mantenimiento; no existe sustento para afirmar que formaron una operación criminal única ni que Java4Shell fue la causa. Algunos incidentes pueden estar todavía bajo investigación. [F15]

8. Ransomware: consecuencias y controles imprescindibles

El ransomware actual puede combinar **cifrado, robo de datos y extorsión**. Un atacante no necesita comenzar cifrando archivos: primero puede comprometer cuentas, extraer información, desactivar respaldos y usar herramientas legítimas de administración para desplazarse. Las nuevas alertas sobre accesos privilegiados y herramientas de gestión deben evaluarse teniendo presente esa cadena de ataque.

8.1 Medidas preventivas obligatorias

- **Respaldos 3-2-1-1-0:** mantener tres copias, dos soportes, una externa, una offline o inmutable y cero errores detectados en pruebas de restauración. Separar identidades, claves y plano de gestión de las copias.
- **Protección de identidades:** MFA resistente al phishing para administradores y accesos remotos; credenciales individuales, cuentas privilegiadas separadas, PAM/JIT donde exista y rotación controlada de secretos expuestos.
- **RDP y SMB:** no exponer RDP o SMB a Internet; desactivar SMBv1; utilizar SMB3 con firma/cifrado cuando corresponda; segmentar redes y limitar SMB2/3 por origen/destino. No deshabilitar SMB2 indiscriminadamente, pues Windows puede afectar SMB3.
- **Segmentación estricta:** separar usuarios, servidores, virtualización, bases de datos, telefonía, infraestructura hospitalaria, redes de administración, backups y proveedores; restringir tráfico este-oeste.

- **Protección EDR/SIEM:** alertar sobre cifrado masivo, extracción de secretos, creación anómala de servicios/tareas, acceso administrativo inesperado, manipulación de logs y desactivación de protección.
- **Correo y navegación:** actualizar Outlook, navegadores y clientes; restringir NTLM y SMB saliente, filtrar adjuntos, revisar extensiones e impedir macros o software no autorizado.
- **Aplicaciones e infraestructura perimetral:** corregir Java, VPN, WAF, firewalls, gestores de configuración, WordPress, servidores de transferencia y servicios remotos antes de que la exposición se prolongue.
- **Proveedor y cadena de suministro:** exigir MFA, cuentas nominativas, registros, segmentación, revisión de permisos OAuth/SSO, notificación temprana de incidentes y evidencias de actualizaciones.
- **Monitoreo y retención:** centralizar logs fuera del dominio de compromiso, sincronizar NTP, verificar integridad y preservar evidencias conforme a procedimientos forenses.
- **Comunicación de crisis:** designar un portavoz técnico y uno institucional; disponer de canal externo al correo o nube afectada para empleados, ciudadanos y pacientes.

8.2 Cuándo considerar contención inmediata

Ante accesos remotos desconocidos, alertas EDR correlacionadas, tareas de cifrado, eliminación de copias, actividad inesperada de cuentas administrativas o uso anómalo de una herramienta de configuración centralizada: **elevar el incidente, aislar segmentos afectados de forma controlada y preservar evidencias**. No realizar reinicios masivos ni borrar registros sin evaluar el riesgo asistencial u operativo. La decisión debe quedar documentada.

9. Plan de intervención para empresas y gobierno

Tiempo sugerido	Instrucciones a responsables	Evidencia exigible
0-24 horas	Inventario Java y CPU; ubicar Puppet, Check Point, Apache Roller, UnrealIRCd y Citrix; aislar expuestos sin parche. Comprobar canales de contingencia y copias inmutables.	Listado de activos, versiones y dueños; tickets P0; responsables; respaldos y estado de restauración.
24-72 horas	Aplicar correcciones prioritarias, validar JVM tras reinicio y pruebas de identidad; auditar accesos privilegiados, proveedores, redes de gestión y logs.	Registro de cambios con versión antes/después, pruebas funcionales, alertas investigadas y excepciones.
Días 4-7	Completar auditoría de servidores Windows/Linux, WordPress, controladores de dominio, VPN/EDR, correo, servicios de nube y virtualización.	Matriz de vulnerabilidades residuales, registros EDR/SIEM, informe de exposición externa.
Días 8-15	Ejecutar simulacro de respuesta ransomware y restauración de servicios críticos; revisar contratos con terceros y flujos de comunicación pública.	Acta de ensayo, RPO/RTO medidos, problemas detectados, plan de mejora aprobado.
Continuo	Revisión diaria de avisos KEV, incidentes de proveedores y novedades de Java; mesa de gestión de parches y tendencias.	Tablero de riesgos, fecha de cierre, responsable, validación por seguridad y reporte a autoridades.

Los períodos anteriores son una **propuesta operativa de Instel & Seguridad**. Una entidad con servicios esenciales debe adaptar ventanas de mantenimiento a continuidad asistencial, seguridad operacional y obligaciones propias. Si un sistema explotado está accesible y no puede corregirse, debe contenerse sin esperar la ventana ordinaria.

10. Procedimiento resumido ante ataque o indicios de ransomware

- **Activación:** registrar hora local y UTC, indicadores iniciales, sistemas afectados, responsables técnicos y autoridades de la crisis.
- **Contención:** segmentar red y revocar accesos comprometidos; conservar canales de comunicación de contingencia; priorizar sistemas de atención crítica.
- **Preservación:** proteger originales, logs, memoria y volúmenes cuando sea viable; calcular SHA-256, documentar cadena de custodia y toda acción.

- **Determinación de alcance:** investigar cuentas, IAM, correo, conexiones con proveedores, backups, hipervisores, dominios, RDP/SMB y exfiltración.
- **Erradicación:** eliminar persistencia y credenciales expuestas; reparar fallas; reconstruir desde medios confiables cuando sea necesario.
- **Recuperación:** restaurar copias verificadas en entorno controlado, reintroducir servicios por prioridad y monitorear recurrencia.
- **Comunicación:** informar de manera verificada al sector administrativo, directivos, ciudadanía y organismos regulatorios según proceda.
- **Cierre:** emitir informe técnico y ejecutivo, lecciones aprendidas, cambios en políticas y seguimiento de vulnerabilidades pendientes.

> **Advertencia:** un parche no elimina por sí solo un acceso previamente obtenido. Si la institución estuvo expuesta a una vulnerabilidad explotada, la tarea incluye **búsqueda de indicios de compromiso**, revisión de secretos y verificación de integridad. La ausencia de alerta antivirus no acredita ausencia de intrusión.

11. Indicadores a presentar a autoridades y responsables de área

- Cantidad y porcentaje de sistemas con Java vulnerable, clasificados por exposición, uso y condición real de CPU/intrínsecos.
- Porcentaje de equipos perimetrales y de gestión centralizada con correcciones confirmadas y búsqueda de compromiso documentada.
- Porcentaje de respaldos inmutables y restauraciones exitosas, con tiempos reales RTO/RPO por servicio.
- Número de cuentas privilegiadas sin MFA o sin dueño identificable, aplicaciones OAuth de terceros y accesos VPN sin justificación.
- Cantidad de servidores con RDP/SMB expuestos, servicios heredados e incumplimientos de segmentación.
- Tiempo promedio desde aviso oficial hasta evaluación, corrección, verificación y comunicación de riesgo residual.

Mensaje institucional propuesto

La ola reciente combina ataques genuinos y fallas de servicios de gran alcance. La prioridad pública no consiste en suponer un mismo atacante detrás de todas las interrupciones, sino en reducir la exposición verificable y preservar la capacidad de prestar servicios. Los organismos deben contar con personas responsables, procedimientos escritos, parches comprobados, respaldo recuperable y comunicación preparada antes del incidente.

12. Conclusión técnica y recomendación institucional

Instel & Seguridad recomienda declarar una **revisión de seguridad extraordinaria** de infraestructura crítica, iniciando por Java y sus distribuciones embebidas, los componentes de gestión centralizada, los equipos perimetrales y las rutas de acceso de proveedores. Los avisos de CISA y FBI demuestran que los atacantes explotan vulnerabilidades conocidas, identidades y cadenas de confianza con mayor automatización; estas condiciones elevan la necesidad de vigilancia y de plazos efectivos de remediación.

La amenaza de ransomware debe tratarse como un **riesgo operacional continuo**, no como un hecho inevitable o la causa presunta de toda caída. La protección más eficaz combina prevención, detección, contención, recuperación y comunicación institucional. Debe verificarse la aplicación real de cada medida mediante evidencias técnicas y pruebas periódicas.

Este informe es preventivo y no reemplaza una auditoría de vulnerabilidades, un análisis de compromiso o un dictamen pericial. Las cifras y atribuciones se refieren a las fuentes públicas disponibles al **18/11/2026** y pueden actualizarse. Todo cambio sobre sistemas productivos debe contar con autorización, plan de reversión y control de continuidad.

13. Anexo ejecutivo: instrucciones para ministerios y empresas

OBJETIVO: prevenir una intrusión que pueda culminar en robo de información, paralización de servicios o ransomware; y garantizar respuesta organizada ante la caída de plataformas esenciales.

INSTRUCCIÓN 1 — INFORMAR Y PRIORIZAR

Cada ministerio o dirección designará un responsable de infraestructura, enviará inventario de servidores, Java, firewall, VPN, servicios web, proveedores y administradores y declarará activos críticos.

INSTRUCCIÓN 2 — CORREGIR LO EXPLOTADO

La infraestructura afectada por CVE presentes en CISA KEV o por Java4Shell, cuando las condiciones de exposición se cumplan, se corregirá o aislará con urgencia. Se documentará el resultado.

INSTRUCCIÓN 3 — PROTEGER LOS RESPALDOS

Se dispondrán copias independientes, aisladas o inmutables de la red principal y se verificará la restauración de al menos un servicio crítico.

INSTRUCCIÓN 4 — EVITAR PROPAGACIÓN

Se controlarán privilegios, accesos de proveedores, redes compartidas y servicios SMB/RDP. Ningún proveedor debe disponer de credenciales administrativas genéricas permanentes.

INSTRUCCIÓN 5 — COMUNICAR UNA CRISIS

Cada organismo identificará un vocero técnico y un responsable de comunicación institucional, con instrucciones para empleados y ciudadanos ante suspensión preventiva de servicios.

INSTRUCCIÓN 6 — ENTREGAR EVIDENCIAS

Los responsables remitirán reportes de parches, incidentes, excepciones, pruebas de recuperación y vulnerabilidades pendientes para seguimiento por seguridad informática.

14. Fuentes oficiales y técnicas utilizadas

[F01] CISA: Critical Java Vulnerability Requires Immediate Patching (17/11)
content.govdelivery.com · abrir fuente

[F02] CERT-EU 2026-021: Java SE y OpenJDK (18/11)
cert.europa.eu · abrir fuente

[F03] Oracle: Critical Security Patch Update - November 2026
www.oracle.com · abrir fuente

[F04] Eclipse Adoptium: Temurin - Java4Shell y versiones (18/11)
adoptium.net · abrir fuente

[F05] NHS England: CVE-2026-114938 y mitigaciones (18/11)
digital.nhs.uk · abrir fuente

[F06] Centro Canadiense de Ciberseguridad: Check Point AV26-1154 (13/11)
www.cyber.gc.ca · abrir fuente

[F07] Check Point Research: boletín semanal 9-15/11
research.checkpoint.com · abrir fuente

[F08] ThaiCERT: CVE-2026-123039 y CVE-2026-114713 en KEV
www.thaicert.or.th · abrir fuente

[F09] Puppet: actualizaciones de seguridad Enterprise y Core
www.puppet.com · abrir fuente

[F10] FBI FLASH-20261113-001: abuso de ARTEX (13/11)
www.ic3.gov · abrir fuente

[F11] Apache / oss-security: CVE-2026-129448 (17/11)
www.openwall.com · abrir fuente

[F12] Visa PERC: Threats Report - Fall 2026 (17/11)
visa.gcs-web.com · abrir fuente

[F13] Citrix: CVE-2026-120869 NetScaler Console (12/11)
support.citrix.com · abrir fuente

[F14] TechRadar: Visa, proveedor externo y alegaciones de n0n (18/11)
www.techradar.com · abrir fuente

[F15] Reuters: interrupciones no coordinadas y causas informadas (18/11)
www.reuters.com · abrir fuente

[F16] The Record: U. Texas Arlington, incidente y robo de datos (13/11)
therecord.media · abrir fuente

[F17] Monadnock Community Hospital: confirmación de incidente (16/11)
www.classaction.org · abrir fuente

[F18] CISA: Known Exploited Vulnerabilities - catálogo
www.cisa.gov · abrir fuente

Fuentes consultadas hasta el 18/11/2026, hora argentina. En caso de discrepancia posterior, prevalecen el boletín vigente del fabricante y las versiones oficialmente soportadas. No atribuir ransomware a una falla o incidente sin evidencia independiente y verificable.

11. Actualización extraordinaria: 19 y 20 de noviembre de 2026

Cierre: viernes 20/11/2026, 22:58 (Argentina, UTC−3). Este documento conserva el análisis elaborado para el intervalo 13-18/11 y agrega novedades y confirmaciones verificadas hasta el nuevo corte. Las fechas de las CVE no necesariamente coinciden con las fechas de publicación del parche o con su incorporación a CISA KEV.

Desde el cierre anterior sobresalen **ocho incorporaciones adicionales a CISA KEV** (cuatro del 18/11 y cuatro del 20/11), una vulnerabilidad de autenticación crítica en **VMware vCenter** cuyo abuso se documentó antes del parche, explotación de la falla de instalación de **Drupal**, nuevas correcciones en **NGINX y PHP** y exposición de datos por **proveedores de entidades financieras**. [U01-U10]

> **Mensaje al directorio:** ordenar una revisión extraordinaria de hipervisores, servidores virtuales, web institucional, accesos remotos, servidores Java y respaldos. Los dispositivos con explotación confirmada requieren, además del parche, búsqueda de persistencia y verificación de integridad. El ransomware sigue siendo una hipótesis de impacto y un escenario de preparación: no se debe atribuir a ninguna CVE concreta sin evidencias.

Hito	Publicación	Lectura operativa
18/11	CISA KEV: 4 CVE	REDCap; Apache Axis; LiteLLM; Synology DSM. Explotación activa confirmada en sus contextos.
18/11	NGINX 1.30.7 y 1.31.9	Actualización por múltiples problemas de memoria, TLS y validación.
18/11	Drupal SA-CORE-2026-017	Parche de RCE en instalador; posteriormente reportó explotación real.
19/11	Broadcom VMSA-2026-0009 y -0010	vCenter: evasión de autenticación; Aria/VCF: RCE en Apache mod_http2.
19/11	PHP: parches de seguridad	8.2.36, 8.3.37, 8.4.28 y 8.5.13; PHP 8.6.0 es una versión mayor.
20/11	CISA KEV: 4 CVE	Cisco Expressway; Apache Roller; VMware vCenter; SAP NetWeaver.
20/11	Cisco: actualización Java4Shell	Ampliación del inventario de productos potencialmente afectados; no atribuye explotación maliciosa.

Criterio: KEV significa explotación demostrada en algún entorno, pero **no** que todo sistema afectado haya sido vulnerado ni que la explotación se empleara en ransomware. Las fechas límite estadounidenses de KEV no constituyen plazos legales argentinos; en este informe se emplean como referencia operativa de urgencia. [U01]

12. Ocho novedades con explotación activa incorporadas a CISA KEV

La versión del catálogo KEV consultada, fechada el 20/11/2026, identifica los siguientes ocho ingresos desde el cierre inicial. Las fechas consignadas son las de incorporación al catálogo, no necesariamente descubrimiento o publicación del CVE. [U01]

Ingreso	CVE / producto	Exposición y decisión
18/11	CVE-2026-90817 **REDCap**	Inyección de código mediante rutas de encuestas/importación. Actualizar a rama corregida; revisar endpoints públicos, registros e integridad.
18/11	CVE-2026-90436 **Apache Axis 1 / Confluence**	RCE; Axis 1 sin mantenimiento. Desactivar API remota donde corresponda, actualizar Confluence o migrar componente.
18/11	CVE-2026-40217 **LiteLLM**	Escape de límites en pruebas de código personalizado para guardrails. Restringir endpoint y cuentas; aplicar mitigación del proveedor.
18/11	CVE-2024-10441 **Synology DSM**	Lectura no autorizada de archivos limitados en webapi. Aplicar DSM/BSM corregido, revisar exposición de NAS.

Ingreso	CVE / producto	Exposición y decisión
20/11	CVE-2026-76466 **Cisco Expressway**	Uso de credenciales estáticas en servicio de base de datos de equipos en clúster. Actualizar a versión corregida.
20/11	CVE-2026-129448 **Apache Roller**	Deserialización XML-RPC; el aviso del 17/11 ya señalaba explotación. Estado nuevo: CISA lo incorpora a KEV.
20/11	CVE-2026-123890 **VMware vCenter**	Evasión de autenticación en Directory Service. CVSS 9,8; sin workaround del fabricante.
20/11	CVE-2025-42884 **SAP NetWeaver EP**	Inyección JNDI; posible divulgación o alteración de información. Revisar SAP Note 3660969.

El boletín original del 13-18 conserva el análisis de Check Point, UnrealIRCd y Puppet, incorporados a KEV el 13 y el 17/11. No se contabilizan nuevamente como nuevas del 19-20. [U01]

13. Hipervisores, equipos de comunicaciones y ERP

13.1 VMware vCenter: CVE-2026-123890 — explotación confirmada

Broadcom publicó **VMSA-2026-0009 el 19/11**. Una vulnerabilidad de VMware Directory Service permite a un atacante con conectividad a vCenter evadir autenticación. CVSS v3.1: **9,8**; el fabricante declara **sin solución alternativa**. La inclusión en KEV el 20/11 confirma explotación previa. El conjunto de avisos incluye además CVE-2026-123891, -123892, -123893 y -123894 en componentes del ecosistema. [U02-U03]

Instalación	Compilación de referencia corregida
vCenter 8.0	8.0 Update 3m
vCenter 9.0.x	9.0.2.0200
vCenter 9.1.x	9.1.1.0200
VMware Cloud Foundation 5.x	5.2.5
vCenter 7.0	Consultar contrato de soporte extendido y asistencia Broadcom

- **Acción 1:** inventariar servidores vCenter, direcciones de gestión, versión exacta, instancias conectadas, certificados y cuentas con privilegios.
- **Acción 2:** aplicar la actualización de la rama correspondiente; antes, preservar configuración y respaldos consistentes de gestión. Validar clústeres, SSO, vMotion y estado de máquinas virtuales.
- **Acción 3:** investigar sesiones, cambios de roles y permisos, usuarios y certificados inesperados, operaciones recientes de hipervisores, creación de snapshots y alteraciones de respaldos.
- **Acción 4:** aislar la red de gestión de redes de usuarios e Internet. Si hay indicios de compromiso, no considerar saneado el entorno solo porque se instaló la corrección.

13.2 VMware Aria / VCF Operations: CVE-2026-119618

El aviso **VMSA-2026-0010**, publicado el 19/11, identifica RCE de severidad crítica (CVSS 9,8) en mod_http2 de Apache HTTP Server integrado en VMware Aria Operations, VCF Operations y VCF Operations HCX. **Al corte, Broadcom consigna parche pendiente para los productos listados y remite a KB463005 o KB463022 para mitigaciones.** Priorizar aislamiento del plano de administración y aplicar únicamente las medidas compatibles con la instalación. [U04]

13.3 Cisco Expressway: CVE-2026-76466

No es una CVE publicada el 20/11: su aviso inicial es de **21/10**, pero CISA confirmó explotación al incorporarla a KEV el **20/11**. Afecta Expressway-C y -E en clúster con versiones vulnerables; un atacante con acceso al servicio y cookies persistentes puede lograr ejecución de comandos como root. Cisco indica **X15.5.20** como corrección para X15.5.3 y anteriores; X14 y anteriores deben migrar a una versión corregida. Sin workaround oficial. [U05]

13.4 SAP NetWeaver Enterprise Portal: CVE-2025-42884

La falla de inyección JNDI era conocida desde 2025 y tiene CVSS v3.1 6,5; sin embargo, CISA la incorporó a KEV el 20/11. Puede facilitar consulta o modificación de información en SAP NetWeaver Enterprise Portal por entradas especialmente construidas. Verificar los componentes **EP-BASIS / EP-RUNTIME 7.50**, aplicar la **SAP Security Note 3660969** y preservar logs de aplicaciones y accesos administrativos. La explotación reportada no prueba que se haya usado ransomware. [U01,U06]

14. Web institucional: nuevas correcciones Drupal, NGINX y PHP

14.1 Drupal Core: CVE-2026-132165 — ejecución de código y explotación reportada

Drupal publicó **SA-CORE-2026-017 el 18/11**. Bajo condiciones específicas, la ruta del instalador puede habilitar reinstalación no autorizada, toma de control del sitio o ejecución de código. El equipo de seguridad del proyecto comunicó reportes de abuso en sitios reales desde el **19/11 a las 19:00 UTC**. [U07]

Rama vulnerable	Versión corregida	Acción
Drupal 10.6.x anterior a 10.6.22	10.6.22	Actualizar núcleo, revisar settings.php e instalador.
Drupal 11.3.x anterior a 11.3.22	11.3.22	Verificar permisos, plugins y registros web.
Drupal 11.4.x anterior a 11.4.13	11.4.13	Revisar persistencia si el sitio estuvo expuesto.
Ramas 8/9, 10.5 o 11.2 y anteriores	Sin mantenimiento de seguridad	Plan de migración y contención temporal.

- **Contención:** impedir que el servidor web modifique settings.php, proteger el instalador y restringir toda administración. Una regla WAF reduce exposición, pero no reemplaza la actualización.

14.2 NGINX: parches del 18/11 para múltiples CVE

NGINX publicó **1.30.7 estable y 1.31.9 mainline**. Corrigen varias condiciones de corrupción de memoria, use-after-free y otras fallas en HTTP/2, HTTP/3, resolver, proxy de correo y flujos TLS. Entre las CVE: 2026-123007, -123634, -121810, -123633, -118899, -113425, -120993, -125283, -120967 y -123640. CERT-EU señala demostración técnica de CVE-2026-123007, pero no explotación real confirmada en su aviso del 18/11. [U08]

- Identificar versión y módulos habilitados; actualizar a la rama corregida o al paquete del distribuidor con backport verificado. Validar servicios de proxy inverso, TLS, HTTP/2, balanceo y correo tras reiniciar.
- No ejecutar pruebas de explotación sobre el frontal productivo. Conservar configuración antes y después; monitorizar accesos, reinicios inesperados, procesos de worker y tráfico saliente.

14.3 PHP: parches de seguridad del 19/11

PHP publicó versiones de seguridad **8.2.36, 8.3.37, 8.4.28 y 8.5.13** entre el 18 y 19/11. La 8.6.0, también del 19/11, es una **versión mayor** que requiere pruebas de migración; no debe asumirse compatible automáticamente con WordPress y aplicaciones legadas. Las CVE PHP2Shell de octubre continúan siendo un antecedente relevante, no se redistribuyen como descubrimientos de noviembre. [U09]

- Inventariar FPM, mod_php, contenedores, PHP de CLI y runtimes propios de hosting; comprobar el parche del proveedor y reiniciar el servicio efectivo. Probar aplicaciones y plugins antes de modificar rama principal.

15. Salud, NAS, APIs e inteligencia artificial

15.1 Apache Axis 1.x / Atlassian Confluence: CVE-2026-90436

CISA incorporó el fallo a KEV el 18/11. Apache Axis 1 está fuera de soporte. En **Confluence Data Center** la explotación depende de tener habilitada la opción **Remote API (XML-RPC & SOAP)**. Atlassian ofrece **Confluence 9.2.28** como referencia corregida y aclara que Confluence 10.x no es vulnerable; como mitigación temporal, deshabilitar la API y verificar respuesta HTTP 403 de la ruta SOAP afectada. La falla no afecta Atlassian Cloud según el aviso. [U10]

- Buscar dependencias Axis embebidas en productos de terceros y sistemas Java antiguos. Si no hay parche viable, desactivar el servicio o migrar a un componente soportado. Revisar logs por ejecución de comandos, tareas inesperadas y accesos a interfaces SOAP.

15.2 REDCap: CVE-2026-90817

Inyección de código en el flujo de encuestas/importación, con impacto sobre sistemas de investigación y salud. KEV 18/11. Las referencias del registro CVE enumeran **16.0.49 LTS, 17.3.10 LTS y 17.4.4** como compilaciones corregidas. La disponibilidad de una rama no implica cobertura para cualquier instalación: confirmar con el proveedor de REDCap y sus administradores. [U01,U11]

- Priorizar instancias de encuestas públicas, separar servidor web de las bases de datos de pacientes e investigación y revisar integridad y cuentas privilegiadas. Evitar cargar datos reales en ambientes de ensayo.

15.3 Synology DSM: CVE-2024-10441

CVE previamente conocida, incorporada a KEV el 18/11. En determinados DSM/BSM vulnerables permite lectura limitada de archivos mediante webapi. El fabricante indica correcciones en **DSM 7.2.2-72806-1, 7.2.1-69057-6, 7.2-64570-4, 7.1.1-42962-7** y **BSM 1.1-65374**, según rama. [U12]

- Prioridad especial si el NAS hospeda respaldos o expedientes: restringir DSM por VPN, no publicarlo directamente, usar MFA y redes de administración aisladas; mantener una copia inmutable o desconectada con credenciales independientes.

15.4 LiteLLM: CVE-2026-40217

La incorporación a KEV del 18/11 destaca una vía de ejecución de código por pruebas de guardrails personalizados mediante un canal insuficientemente protegido. En despliegues con LiteLLM, identificar la versión y si está activa la función de código personalizado. Revisar el aviso GHSA-wxxx-gvqv-xp7p del proveedor antes de aplicar una versión o mitigación: no se indica aquí un número de parche no confirmado. [U01,U13]

- Aislar la API de administración, aplicar autorización, no ofrecer pruebas de código personalizado a usuarios externos y auditar secretos de proveedores cloud/LLM. Rotar credenciales solo en el alcance justificado por evidencias.

16. Java4Shell, navegadores y seguimiento de parches

16.1 CVE-2026-114938: ampliación del análisis original

La CVE de Java4Shell está desarrollada en la sección 3 del informe original. **Novedad:** Cisco actualizó su matriz de productos el **20/11 a las 20:37 GMT**. Entre los productos marcados afectados o pendientes de corrección figuran componentes de comunicaciones, plataformas de gestión y servicios virtualizados, con diferencias por versión. Cisco indicó que **Catalyst Center no está afectado** en la revisión 1.3 y que, al corte, conocía código PoC pero no uso malicioso confirmado de la falla. [U14]

No se debe afirmar que cualquier sistema Java está automáticamente expuesto: el escenario descrito involucra determinadas combinaciones **x86-64, AVX-512 y procesamiento Base64**. Si el fabricante del appliance aún no entregó una versión corregida, aislar superficies expuestas y solicitar una ruta de actualización; la mitigación documentada para una JVM independiente no equivale a un workaround validado para Cisco. [U14]

- Inventariar JRE/JDK de sistema, instaladores Java, agentes empaquetados, servidores de identidad, middleware y contenedores; registrar java -version y opciones efectivas del proceso sin modificar la JVM mientras se inspecciona.

- Aplicar el parche de la distribución o proveedor, reiniciar procesos de Java y verificar flujos de autenticación, SAML, TLS, conexiones de base de datos, procesamiento de archivos y rendimiento.

16.2 Google Chrome: nuevo ciclo estable

Google promovió Chrome 158 estable y publicó correcciones de seguridad el **17/11**. Para los paquetes de escritorio de ese aviso se indican **158.0.8127.36/.37** para Windows/macOS y **158.0.8127.36** para Linux. Los fabricantes de navegadores Chromium derivados requieren verificar sus propias compilaciones. [U15]

- Implantar actualización centralizada, inventariar navegadores secundarios, bloquear extensiones no aprobadas y forzar relanzamiento para que el parche se active.

16.3 Microsoft, VPN y activos con alertas anteriores

Mantener controles del ciclo de Microsoft del 10/11 y la falla explotada de Outlook **CVE-2026-124194** descrita en los informes previos; la ausencia de nuevas CVE de Microsoft en este apartado no implica que las estaciones Windows estén al día. Revisar también parches pendientes de Ivanti, Fortinet, Check Point, Puppet y servidores de escritorio remoto. No se confirma una nueva causa maliciosa para las caídas de Microsoft 365 de días anteriores.

17. Bancos, gobiernos y proveedores: confirmaciones del 19/11

El 19/11, **JPMorgan Chase, Visa y Mastercard** comunicaron incidentes relacionados con terceros que brindan servicios a esas entidades. Las comunicaciones públicas y reportes periodísticos describen principalmente exposición limitada de datos de contacto o de marketing; **no demuestran compromisos de procesamiento de pagos ni una intrusión en los sistemas centrales de esas empresas**. El grupo de extorsión n0n difundió afirmaciones cuya amplitud no está independientemente corroborada. [U16,U17]

La interrupción de operaciones bancarias del 16/11 fue reportada por separado como un incidente técnico. No debe confundirse con la exposición de datos divulgada posteriormente, ni afirmarse que fue provocada por el mismo atacante. Esta distinción es esencial para comunicaciones de crisis y reportes periciales. [U16]

Medidas exigibles a bancos, empresas y administraciones públicas

- **Terceros:** inventariar proveedores con acceso a datos, correo, IAM, API, VPN y sistemas de marketing; exigir MFA, segmentación, contratos con notificación temprana y evidencias de control.
- **Datos personales:** determinar exactamente qué registros y campos pudieron exponerse. Si hubo direcciones de correo o teléfonos, activar medidas contra phishing dirigido y suplantación bancaria; informar según obligaciones aplicables.
- **Integraciones:** revisar OAuth, federación SSO, tokens de API, cuentas de servicio, secretos almacenados en proveedores y accesos privilegiados temporales.
- **Servicios esenciales:** mantener comunicaciones offline de emergencia para empleados, autoridades, pacientes y ciudadanos; respaldos de información crítica accesibles aun sin el proveedor principal.
- **Comunicación:** no atribuir ataques sin evidencia, no publicar datos no confirmados de víctimas y separar caída de servicio, filtración, cifrado y extorsión en los comunicados.

> **Alerta sobre ransomware:** la existencia de un grupo que reivindica datos no significa que una entidad haya sufrido cifrado. La extorsión basada en filtración y los ataques de ransomware pueden coincidir, pero requieren evidencia específica. La investigación debe preservar archivos originales, trazas, registros de proveedor y hashes.

18. Protocolo técnico anti-ransomware: aplicación inmediata

Las nuevas fallas afectan rutas que un atacante podría aprovechar para obtener acceso inicial, elevar privilegios, comprometer gestores centralizados o destruir disponibilidad. El siguiente conjunto de controles reduce el riesgo combinado, independientemente de cuál sea el exploit de entrada.

Control	Medida verificable	Evidencia / responsable
Identidad	MFA resistente a phishing, privilegios mínimos, cuentas separadas y acceso JIT para administradores.	Reportes IAM, auditoría de sesiones, dueño de cuenta.
Red y SMB	Desactivar SMBv1; restringir SMB2/SMB3 y RDP por VLAN y ACL; no exponer SMB/RDP a Internet.	Firewall, análisis de flujo este-oeste, reglas documentadas.
Virtualización	Separar vCenter, hipervisores, almacenamiento y consolas de backup de puestos de trabajo.	Inventario, ACL de gestión, MFA, cambios de roles.
Respaldos	Estrategia 3-2-1-1-0; copia inmutable/offline; credenciales independientes y pruebas reales de restauración.	Acta de restauración, RPO/RTO medidos, reportes de integridad.
EDR y registros	Alertar por cifrado masivo, desactivación de EDR, abuso de VSS, cambios de GPO, tickets Kerberos y uso anómalo de herramientas administrativas.	SIEM/EDR, NTP sincronizado, retención externa.
Servicios web	Actualizar Drupal, NGINX, PHP, Java y plugins; revisar cuentas administradoras y directorios de carga.	Versión antes/después, logs HTTP, hashes y WAF.
Terceros	Acceso nominativo vía VPN/ZTNA, MFA, sesiones registradas, horarios y notificación de incidentes.	Contratos, tickets, export de accesos, revocación de tokens.

Señales que obligan a activar el plan de respuesta

- Conexiones a hipervisores desde segmentos no autorizados; creación imprevista de usuarios o certificados; modificación de políticas de respaldo.
- Velocidad anómala de modificación y renombrado de archivos, borrado de snapshots, interrupción de agentes EDR, ejecución de scripts o servicios desconocidos.
- Autenticaciones simultáneas imposibles, exportaciones de datos, token OAuth nuevo sin aprobación, operaciones de administración efectuadas por proveedores fuera de horario.

Si hay sospecha: documentar fecha y hora local/UTC, operador, host y evidencias. Contener por segmentos con autorización, preservar registros y memoria cuando sea viable, generar SHA-256 y mantener cadena de custodia. No reiniciar indiscriminadamente infraestructura sanitaria o de emergencia. El parche no sustituye el análisis de compromiso.

19. Plan de intervención actualizado — responsables y plazos

Cuándo	Acción de cumplimiento	Documento a presentar
0 a 24 h	Identificar/aislar instalaciones expuestas de vCenter, Cisco Expressway, Apache Axis/Confluence, REDCap, Synology, Drupal, LiteLLM, Apache Roller, SAP. Confirmar copias offline.	Matriz de activos, dueños, versiones, exposición, ticket y contención.
24 a 72 h	Aplicar parches de rama, actualizar PHP/NGINX/Drupal, revisar Java/Cisco, auditar accesos y credenciales. Iniciar hunting en KEV potencialmente explotados.	Evidencias pre/post, logs preservados, prueba de servicio y rollback.
Días 4 a 7	Examinar servidores Windows/Linux, redes de administración, herramientas de despliegue, VPN, terceros y portales. Validar restauración aislada.	Informe de exposición residual, test de recuperación, acta.
Días 8 a 30	Ejercicio de respuesta a ransomware, simulacro de caída de nube, comunicaciones a personal y ciudadanía; aprobación de mejoras.	RPO/RTO, indicadores de parcheo, excepciones, responsables.

Los plazos anteriores son **objetivos propuestos por Instel & Seguridad**, adaptables a riesgo real, complejidad y continuidad operativa. No reemplazan las obligaciones de reguladores específicos; una vulnerabilidad KEV expuesta y explotable requiere tratamiento antes de la ventana regular de mantenimiento.

Instrucción ejecutiva para funcionarios

- Ordenar en cada organismo, por escrito, el inventario de servidores, páginas web, VPN, NAS y sistemas críticos con versión, responsable y última actualización.
- Exigir que ningún equipo de administración de servidores o respaldos esté accesible desde las redes generales de usuarios.
- Asignar presupuesto, personal y ventana de mantenimiento para corregir los productos efectivamente afectados; exigir informe de resultado y evidencias.
- Garantizar planes de atención y comunicación para operar durante un incidente o apagado preventivo, particularmente en fines de semana largos.
- Solicitar una prueba de restauración de un sistema crítico y una copia desconectada o inmutable, no solo una captura del software de backup.
- Informar semanalmente al directorio: vulnerabilidades pendientes, sistemas expuestos, fechas de corrección, hallazgos de compromiso y pruebas de continuidad.

20. Referencias de actualización y criterio de cierre

Las referencias identificadas como U01-U18 corresponden exclusivamente a la actualización del 19-20/11. Las referencias F01-Fxx del cuerpo original se conservan para permitir comprobar el análisis publicado hasta el 18/11. Todas las versiones deben contrastarse otra vez al momento de intervenir un sistema.

[U01] CISA KEV, catálogo actualizado 20/11/2026 (lista de incorporaciones)
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[U02] Broadcom VMSA-2026-0009, 19/11: vCenter/Tools/SDDC Manager
https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/39495

[U03] Consulta KEV, incorporaciones 18 y 20/11 (reflejo de catálogo)
https://playciso.com/tools/kev-checker/latest

[U04] Broadcom VMSA-2026-0010, 19/11: Apache mod_http2 en Aria/VCF
https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/39625

[U05] Cisco PSIRT, Expressway CVE-2026-76466
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vcs-static-cred-hr7EWZ8t

[U06] CSIRT Panamá, 20/11: SAP NetWeaver CVE-2025-42884
https://cert.pa/?p=6332

[U07] Drupal, SA-CORE-2026-017, actualizado con explotación reportada
https://www.drupal.org/sa-core-2026-017

[U08] NGINX, cambios y CVE corregidas el 18/11
https://nginx.org/news.html

[U09] PHP, archivo oficial de comunicados y parches de noviembre
https://www.php.net/archive/2026.php

[U10] Atlassian, Confluence / Apache Axis CVE-2026-90436
https://confluence.atlassian.com/security/cve-2026-90436-remote-code-execution-in-confluence-data-center-1874560038.html

[U11] NVD, registro REDCap CVE-2026-90817
https://nvd.nist.gov/vuln/detail/CVE-2026-90817

[U12] Synology, SA-24:20 para CVE-2024-10441
https://www.synology.com/en-us/security/advisory/Synology_SA_24_20

[U13] LiteLLM GHSA-wxxx-gvqv-xp7p
https://github.com/BerriAI/litellm/security/advisories/GHSA-wxxx-gvqv-xp7p

[U14] Cisco, Java4Shell: revisión PSIRT al 20/11
https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-nov2026-java-rce-eCa6ss9z.html

[U15] Chrome Releases, canal estable 17/11
https://chromereleases.googleblog.com/2026/11/

[U16] Associated Press, 19/11: datos de clientes y proveedores financieros
https://apnews.com/article/8470d475450721b66858bdace47091c0

[U17] Cybersecurity Dive, 20/11: incidente de proveedor y alcance confirmado
https://www.cybersecuritydive.com/news/jpmorgan-visa-customer-data-leaked-third-party-hacks/875333/

[U18] CERT-EU, alerta NGINX 18/11/2026
https://cert.europa.eu/publications/security-advisories/2026

Nota final: explotación confirmada en KEV, PoC pública, afirmación criminal, interrupción de disponibilidad y ransomware son conceptos distintos; preservar evidencia antes de emitir atribuciones.