INGENIERÍA
TELEMÁTICA S.A.S.

BOLETÍN DE CIBERSEGURIDAD · INTELIGENCIA DE AMENAZAS

TLP:CLEAR · EDICIÓN 2026-W43 · SEMANAL

Semana del 19 oct 2026 al 25 oct 2026 · publicado el 26 de octubre de 2026

Boletín de Ciberseguridad

Las vulnerabilidades con explotación activa, las campañas de malware y las noticias de la semana, en español y con acciones concretas para su empresa.

RESUMEN EJECUTIVO

Entre el 20 y el 23 de octubre de 2026, CISA, la agencia de ciberseguridad de Estados Unidos, añadió siete vulnerabilidades a su catálogo KEV, que reúne las fallas con explotación activa confirmada. De ellas, una es crítica, dos son altas y cuatro son medias, y se reparten en cuatro productos: Arista VeloCloud Orchestrator, Plex Media Server, SiteGuard Server Edition y Siemens Software Center. Lo más urgente es la inyección SQL en Arista VeloCloud Orchestrator (CVSS 9.9), explotada como día cero contra la consola que gobierna redes SD-WAN; su plazo de CISA venció el 26 de octubre de 2026, y los plazos de SiteGuard y de dos de las cuatro fallas de Plex vencieron el 23 de octubre de 2026, por lo que estas correcciones deben aplicarse de inmediato. Las fallas de Plex se encadenan para instalar criptomineros y puertas traseras, y la de Siemens se usa en campañas ClickFix para desplegar un troyano de acceso remoto; el siguiente plazo de CISA es el 3 de noviembre de 2026. Fuera del catálogo, los grupos de ransomware Qilin e INC explotan CVE-2026-0257 en Palo Alto Networks para evadir la autenticación multifactor, las fallas PHP2Shell de PHP reciben millones de intentos de explotación para instalar Mirai, se publicó un exploit para FortiSIEM y tres ataques a la cadena de suministro de software (LiteLLM, OVHcloud CLI y paquetes npm) obligan a revisar dependencias y rotar secretos en los equipos de desarrollo.

4	4	6
VULNERABILIDADES	CON EXPLOTACIÓN ACTIVA	CAMPAÑAS DE MALWARE

Ciberseguridad 360°
Protección avanzada con Fortinet.

Nube híbrida
AWS, Azure, Google Workspace, M365.

Continuidad (DRP)
Veeam y Acronis.

SOC gestionado
Monitoreo y respuesta.

Boletín informativo de distribución pública (TLP:CLEAR).
Fuentes: CISA KEV, NVD y avisos de fabricante. No sustituye un análisis de su entorno.

Ver detalle →

NIT 816007833-0 · Pereira, Colombia · +57 314 682 5259 · ingenieriatelematica.com.co · soporte@ingetele.com

VISTA RÁPIDA

severidad CVSS · explotación activa según CISA KEV

1	2	1	0
CRÍTICA	ALTA	MEDIA	BAJA
CVSS 9,0 – 10	CVSS 7,0 – 8,9	CVSS 4,0 – 6,9	CVSS 0,1 – 3,9

4 vulnerabilidades, 4 con explotación activa confirmada · 6 campaña(s) de malware · 6 noticia(s) · semana del 19 oct 2026 al 25 oct 2026

VULNERABILIDADES

de mayor a menor criticidad

Crítica · CVSS 9.9 | Explotación activa | CVE-2026-114625

Inyección SQL en Arista VeloCloud Orchestrator explotada como día cero

Arista VeloCloud Orchestrator (on-prem) · CWE-89 — Inyección SQL · Versiones afectadas: `5.2.0 – <5.2.3.18; 6.1.0 – <6.1.3.10; 6.4.0 – <6.4.2.12`

El orquestador VeloCloud (VCO) es la consola que administra de forma centralizada una red SD-WAN, es decir, una red de área amplia definida por software que interconecta sedes. El VCO instalado en infraestructura propia no valida correctamente ciertos datos antes de usarlos en consultas a su base de datos. Por eso, un atacante remoto puede inyectar instrucciones SQL (el lenguaje de consulta de bases de datos), llegar a funciones internas privilegiadas y afectar al servidor que aloja el orquestador. La falla se explotó como día cero, es decir, se atacó antes de que existiera una corrección pública.

Impacto: Quien controla el orquestador puede leer y alterar la configuración y los datos de todas las sedes conectadas a la SD-WAN. También puede desviar rutas de tráfico o dejar sin servicio la red corporativa, lo que compromete la confidencialidad, la integridad y la disponibilidad de la operación.

> **Acción a seguir:** Actualizar el VCO on-prem a 5.2.3.18, 6.1.3.10 o 6.4.2.12, según la rama instalada. El plazo de CISA venció el 26 de octubre de 2026, por lo que la actualización debe aplicarse de inmediato. Además, conviene restringir la consola de administración a redes de gestión y revisar las cuentas y los cambios de configuración recientes.

Ampliar información: NVD — CVE-2026-114625 CISA KEV

Alta · CVSS 8.6 | Explotación activa | CVE-2026-96656, CVE-2026-96654, CVE-2026-96655, CVE-2026-96652

Cadena Plex2Shell: cuatro fallas encadenadas en Plex Media Server para instalar criptomineros y puertas traseras

Plex Media Server · CWE-73 — Control externo de nombre o ruta de archivo; CWE-84 — Neutralización incorrecta de esquemas URI codificados en una página web; CWE-918 — Falsificación de solicitudes del lado del servidor (SSRF) · Versiones afectadas: `Anteriores a 1.43.3.10861`

CISA incorporó cuatro fallas del servidor multimedia Plex que los atacantes combinan en la cadena conocida como Plex2Shell. Dos de ellas son de tipo SSRF, una falla que obliga al servidor a enviar peticiones a direcciones elegidas por el atacante: CVE-2026-96652 (CVSS 4.3) acepta cualquier valor de X-Plex-Token y permite indicar una URL completa en el parámetro 'protocol', y CVE-2026-96655 (CVSS 4.3) permite a un usuario autenticado consultar direcciones internas o externas mediante la ruta '/video/:/transcode/universal'. CVE-2026-96654 (CVSS 6.9) permite invocar funciones de otros complementos con parámetros propios. CVE-2026-96656 (CVSS 8.6) permite que un usuario administrador escriba archivos arbitrarios que se ejecutan al cargarse. Encadenadas, estas fallas terminan en ejecución de código en el servidor y ya se usan para instalar programas de minería de criptomonedas y puertas traseras.

Impacto: Un servidor Plex instalado en un equipo de oficina o en un servidor compartido se convierte en un punto de entrada a la red interna. El atacante consume recursos con minería y deja un acceso persistente. Además, puede usar las fallas SSRF para alcanzar servicios internos que no están publicados en internet.

> **Acción a seguir:** Actualizar Plex Media Server a la versión 1.43.3.10861 de inmediato. El plazo de CISA venció el 23 de octubre de 2026 para CVE-2026-96656 y CVE-2026-96654, y vence el 3 de noviembre de 2026 para CVE-2026-96655 y CVE-2026-96652. Hay que revisar el servidor en busca de procesos de minería, archivos nuevos en los directorios de complementos y conexiones salientes inusuales, y retirar el servicio de los equipos corporativos que no lo necesiten para el negocio.

Ampliar información: NVD — CVE-2026-96656 CISA KEV

Alta · CVSS 7.8 **Explotación activa** CVE-2026-106931

Inyección de comandos del sistema operativo en SiteGuard Server Edition

EG Secure Solutions SiteGuard Server Edition · CWE-78 — Inyección de comandos del sistema operativo · Versiones afectadas: `Ver2.20 – <Ver8.00 Update 5; Ver2.20 – <Ver7.00 Update 6`

SiteGuard Server Edition es un cortafuegos de aplicaciones web (WAF, filtro que inspecciona el tráfico dirigido a un sitio) que se instala en el propio servidor web. El producto no depura ciertos datos de entrada, de modo que un atacante puede introducir comandos del sistema operativo a través de ellos. Esos comandos se ejecutan con privilegios de root en Linux o de SYSTEM en Windows.

Impacto: El atacante obtiene el control total del servidor que el producto debía proteger. Con ese control puede robar los datos del sitio, modificar sus contenidos, instalar programas maliciosos y usar el equipo como punto de salto hacia otros sistemas de la red.

> **Acción a seguir:** Actualizar a Ver8.00 Update 5 o a Ver7.00 Update 6, según la rama instalada. El plazo de CISA venció el 23 de octubre de 2026, por lo que la corrección debe aplicarse de inmediato. En los servidores afectados conviene revisar los procesos, usuarios y tareas programadas creados recientemente.

Ampliar información: NVD — CVE-2026-106931 CISA KEV

Media · CVSS 6.7 **Explotación activa** CVE-2026-110936

Carga de DLL por ruta de búsqueda no controlada en Siemens Software Center, usada en campañas ClickFix

Siemens Software Center · CWE-427 — Elemento de ruta de búsqueda no controlado · Versiones afectadas: `Anteriores a V4.0.9.8`

La aplicación busca bibliotecas DLL (bibliotecas de enlace dinámico de Windows) en directorios donde un usuario autenticado puede escribir. Si un atacante con acceso local coloca allí una DLL preparada, la aplicación la carga y ejecuta su código con los privilegios del programa. La falla se ha visto en ataques ClickFix, una técnica de ingeniería social que convence a la víctima de copiar y ejecutar un comando. En esos ataques, el comando instala una DLL maliciosa que el programa legítimo carga (técnica conocida como DLL sideloading) y que despliega un troyano de acceso remoto (RAT).

Impacto: El atacante obtiene control remoto persistente del equipo, camuflado detrás de un programa legítimo de Siemens, lo que dificulta su detección. Desde las estaciones de ingeniería o los equipos de usuario afectados puede avanzar hacia otros sistemas de la red, incluidos los de operación cuando esas estaciones se conectan a ellos.

> **Acción a seguir:** Actualizar Siemens Software Center a V4.0.9.8 antes del 3 de noviembre de 2026, plazo fijado por CISA. Mientras tanto, conviene restringir los permisos de escritura en los directorios de instalación de la aplicación y alertar sobre comandos pegados en el cuadro Ejecutar o en PowerShell que descarguen archivos desde internet.

Ampliar información: NVD — CVE-2026-110936 CISA KEV

MALWARE Y CAMPAÑAS técnicas MITRE ATT&CK

Ransomware Qilin e INC: explotación de CVE-2026-0257 en PAN-OS y Prisma Access para evadir la MFA

Los grupos de ransomware Qilin e INC aprovechan la vulnerabilidad CVE-2026-0257 en PAN-OS y Prisma Access de Palo Alto Networks para eludir la autenticación multifactor. Esta autenticación, conocida como MFA, exige un segundo factor de verificación además de la contraseña. Al saltarse esa barrera, los atacantes entran a redes corporativas por el acceso remoto y preparan el cifrado de sistemas para extorsionar a la víctima. Una empresa colombiana que publique su VPN o su portal de acceso remoto en equipos Palo Alto debe confirmar que tiene aplicada la corrección y no depender de la MFA como única barrera de acceso.

MITRE ATT&CK `T1190 — Explotación de aplicación expuesta al público` `T1133 — Servicios remotos externos` `T1486 — Cifrado de datos para impacto`

> **Acción a seguir:** Vigilar los inicios de sesión en el acceso remoto de PAN-OS o de Prisma Access que no registren el segundo factor, los accesos desde ubicaciones u horarios atípicos y la creación de cuentas nuevas en el dominio. La corrección del fabricante para CVE-2026-0257 debe aplicarse de inmediato.

Ampliar información: Ransomware Qilin e INC Explotan Falla Crítica en Palo Alto Networks para Bypassear MFA

PHP2Shell: explotación masiva de fallas de ejecución remota en PHP para desplegar la botnet Mirai

PHP publicó parches de emergencia para dos fallas de ejecución remota de código (RCE), conocidas como PHP2Shell: CVE-2026-109618 y CVE-2026-109619, con CVSS 9.2. Tras la publicación se registran millones de intentos de explotación cuyo objetivo es instalar Mirai. Mirai es un malware que convierte servidores y dispositivos en parte de una red de equipos controlados a distancia (botnet), usada para lanzar ataques de denegación de servicio. Las pymes y entidades con sitios web, tiendas en línea o portales de trámites en PHP, ya sea en servidores propios o en hosting contratado, deben confirmar con su proveedor que los parches están aplicados y que hay un WAF delante de esas aplicaciones.

MITRE ATT&CK `T1190 — Explotación de aplicación expuesta al público` `T1105 — Transferencia de herramientas de entrada` `T1498 — Denegación de servicio de red`

> **Acción a seguir:** Bloquear en el WAF las peticiones que intenten explotar CVE-2026-109618 y CVE-2026-109619 y aplicar de inmediato los parches de emergencia de PHP. En los servidores web hay que vigilar la descarga de binarios desde direcciones externas, los procesos desconocidos y los picos de tráfico saliente.

Ampliar información: Millones de Intentos de Explotación PHP2Shell Apuntan a Desplegar el Malware Mirai PHP2Shell: Parches Urgentes para Fallas Críticas RCE en PHP (CVSS 9.2) Vulnerabilidades PHP2Shell RCE: Parches de emergencia críticos y mitigaciones

Backdoor Vasilek: puerta trasera oculta en VMware Tools durante una intrusión de dos años

El grupo hacktivista Partisan Zmiy mantuvo durante dos años una intrusión en una organización de salud de Rusia. Para lograrlo ocultó la puerta trasera Vasilek dentro de VMware Tools, el conjunto de utilidades que se instala en las máquinas virtuales de VMware. Al camuflarse en un componente legítimo y presente en casi todos los servidores virtualizados, la puerta trasera pasó inadvertida durante un periodo prolongado. Para las entidades de salud y las entidades públicas en Colombia con infraestructura virtualizada, el caso indica que deben verificar la integridad de los componentes de virtualización y no excluirlos de la supervisión de su EDR, la herramienta de detección y respuesta en los equipos.

MITRE ATT&CK `T1036.005 — Enmascaramiento: coincidir con nombre o ubicación legítimos` `T1554 — Comprometer binario de software del equipo`

> **Acción a seguir:** Vigilar los cambios en los archivos y servicios de VMware Tools dentro de las máquinas virtuales, comparar sus firmas y hashes con los oficiales del fabricante y alertar sobre conexiones salientes de esos procesos hacia destinos externos.

Ampliar información: Backdoor Vasilek: Hacktivistas Usan VMware Tools en Intrusión Larga en Salud Rusa

LiteLLM 1.107.0: paquete Python comprometido con robo de credenciales y puerta trasera

LiteLLM es una biblioteca de Python muy usada para conectar aplicaciones con distintos modelos de inteligencia artificial, y su versión 1.107.0 se publicó comprometida en un ataque a la cadena de suministro. El paquete incluía código que roba credenciales e instala una puerta trasera en los equipos y servidores donde se instala. Los equipos de desarrollo y los proveedores de software en Colombia que integren inteligencia artificial deben revisar si esa versión llegó a sus entornos o a sus canalizaciones de integración y despliegue continuos (CI/CD) y, de ser así, rotar todas las claves accesibles desde ellos.

MITRE ATT&CK `T1195.002 — Compromiso de la cadena de suministro de software` `T1552.001 — Credenciales no protegidas: credenciales en archivos` `T1059.006 — Intérprete de comandos y scripts: Python`

> **Acción a seguir:** Bloquear LiteLLM 1.107.0 en los repositorios internos y en los archivos de dependencias, y buscar esa versión en servidores, contenedores y canalizaciones de CI/CD. También hay que vigilar las conexiones salientes inusuales desde esos entornos.

Ampliar información: Ataque a la cadena de suministro LiteLLM: robo de credenciales y backdoor

OVHcloud CLI: versiones distribuidas en GitHub con malware para robar secretos

Unos atacantes comprometieron versiones de la herramienta de línea de comandos (CLI) de OVHcloud distribuidas a través de GitHub. En ellas insertaron malware diseñado para robar secretos, como claves de acceso y tokens de la nube. Quien descargó esas versiones puede haber entregado las credenciales con las que administra su infraestructura. Las empresas colombianas que alojan servicios en OVHcloud, o los proveedores que lo hacen por ellas, deben identificar qué equipos descargaron la herramienta desde GitHub y rotar las credenciales de la cuenta.

MITRE ATT&CK `T1195.002 — Compromiso de la cadena de suministro de software` `T1552 — Credenciales no protegidas`

> **Acción a seguir:** Vigilar el uso de las claves de API de OVHcloud desde direcciones desconocidas. Además, hay que reinstalar la CLI desde una fuente verificada y rotar los secretos almacenados en las estaciones donde se ejecutó.

Ampliar información: Hackers inyectan malware en OVHcloud CLI a través de GitHub para robar secretos

Paquetes npm maliciosos contra desarrolladores Web3 y tráfico de agentes de IA

Una campaña se hace pasar por un programa de aceleración de empresas Web3, es decir, de aplicaciones basadas en cadenas de bloques, para llevar a desarrolladores a instalar paquetes npm maliciosos. Estos paquetes despliegan ladrones de información y puertas traseras en Windows y macOS. Además, secuestran el tráfico de los agentes de inteligencia artificial que usan los equipos afectados. Las startups y los equipos de desarrollo en Colombia que reciben ofertas de aceleración o pruebas técnicas deben ejecutar el código de terceros en entornos aislados y no en equipos con acceso a repositorios y credenciales corporativas.

MITRE ATT&CK `T1195.002 — Compromiso de la cadena de suministro de software` `T1204 — Ejecución por el usuario` `T1555 — Credenciales de almacenes de contraseñas` `T1557 — Adversario en el medio`

> **Acción a seguir:** Vigilar la instalación de paquetes npm no aprobados en los equipos de desarrollo y los scripts de instalación que lanzan procesos persistentes en Windows y macOS. También hay que vigilar los cambios en la configuración de proxy o en los destinos de conexión que usan los agentes de inteligencia artificial.

Ampliar información: Malware en Paquetes npm Dirigido a Desarrolladores Web3 y Tráfico de Agentes de IA

NOTICIAS DE CIBERSEGURIDAD lo que cambia esta semana

Exploit público para la falla crítica CVE-2026-106173 en FortiSIEM

Se liberó un exploit de prueba de concepto (PoC, código que demuestra cómo aprovechar una falla) para CVE-2026-106173. Se trata de una vulnerabilidad crítica de FortiSIEM, la plataforma de Fortinet para correlacionar eventos de seguridad, que permite ejecutar código de forma remota sin autenticación. La disponibilidad pública de este código reduce el tiempo que necesitan los atacantes para usar la falla. Las organizaciones colombianas que operan FortiSIEM deben verificar cuanto antes que tienen aplicada la corrección de Fortinet y que la interfaz de administración no está expuesta a internet, porque quien compromete esta plataforma obtiene visibilidad sobre toda la red monitoreada.

Ampliar información: Alerta Crítica: FortiSIEM Expuesto a RCE por Vulnerabilidad con Exploit Público

GitLab: ejecución remota de código sin autenticación (CVE-2026-110264, CVSS 10.0) y correcciones en Ruby

GitLab publicó parches para CVE-2026-110264, una falla con CVSS 10.0 que permite ejecutar código sin autenticación y que afecta a todas las versiones autogestionadas desde 2014. En paralelo, el proyecto Ruby corrigió fallas críticas de ejecución remota de código relacionadas con el procesamiento de expresiones regulares, que también afectaron a GitLab. Las empresas y los proveedores de software en Colombia que alojan su propio GitLab deben aplicar los parches cuanto antes, actualizar Ruby en las demás aplicaciones que lo usen y revisar quién puede alcanzar el servidor desde internet, porque allí residen el código fuente y los secretos de despliegue.

Ampliar información: Vulnerabilidad Crítica de GitLab (CVSS 10.0): RCE sin Autenticación Afecta 12 Años de Versiones Ruby corrige fallas críticas de RCE que afectaron a GitLab: Parche urgente para expresiones regulares

Incidente en ConnectWise compromete identidades de aplicación y expone inquilinos de Microsoft 365

Un incidente en ConnectWise, proveedor de herramientas de gestión remota usadas por empresas de servicios de TI, permitió el acceso no autorizado a identidades de aplicación. Como consecuencia quedaron expuestos inquilinos de Microsoft 365, es decir, los entornos de nube de sus clientes. Las identidades de aplicación tienen permisos propios que no dependen de la contraseña ni de la MFA de un usuario, lo que las hace atractivas para los atacantes. Las empresas colombianas que trabajan con un proveedor de servicios gestionados deben preguntarle si usa ConnectWise y revisar en Microsoft Entra ID qué aplicaciones empresariales tienen consentimiento otorgado y con qué permisos.

Ampliar información: Ataque a ConnectWise Compromete Identidades y Expone Inquilinos de Microsoft 365

Dos fallas de ejecución remota con CVSS 9.0 en KSMBD del kernel de Linux, sin parche disponible

Se descubrieron dos vulnerabilidades de ejecución remota de código con CVSS 9.0 en KSMBD, el servidor SMB integrado en el kernel de Linux; SMB es el protocolo que se usa para compartir archivos en red. Por ahora no hay parche disponible. Solo están expuestos los servidores que tienen KSMBD activo. Las empresas deben inventariar qué servidores Linux o equipos de almacenamiento en red tienen KSMBD habilitado, desactivarlo donde no sea necesario y limitar el acceso SMB a redes internas de confianza mientras se publica la corrección.

Ampliar información: Vulnerabilidades RCE CVSS 9.0 en KSMBD de Linux exponen servidores sin parche

Brecha en OpenCode Console pudo exponer claves API de OpenAI, Anthropic y Google

Una brecha en OpenCode Console pudo exponer las claves de API que sus usuarios registraron para acceder a los servicios de inteligencia artificial de OpenAI, Anthropic y Google; una API es la interfaz que permite a un programa usar un servicio de otro. Con esas claves, un tercero puede consumir los servicios a nombre de la víctima o acceder a los datos que se procesan con ellas. Las empresas que usen esta herramienta deben rotar las claves de API registradas, revisar el consumo reciente en cada proveedor y definir qué plataformas de terceros están autorizadas para guardar credenciales corporativas.

Ampliar información: Brecha en OpenCode Console Expone Claves API de OpenAI, Anthropic y Google

Node2Shell: ejecución remota de código en Node.js mediante datos Brotli manipulados (CVE-2026-111497)

La vulnerabilidad CVE-2026-111497, bautizada Node2Shell, permite ejecutar código de forma remota en Node.js 22.x, 24.x y 26.x. El ataque funciona cuando la aplicación procesa datos comprimidos con el formato Brotli que han sido manipulados por un atacante. El proyecto ya publicó versiones corregidas. Los equipos de desarrollo y los proveedores que mantienen aplicaciones o API en Node.js deben identificar qué servicios usan esas ramas, actualizarlos cuanto antes a las versiones corregidas y revisar también las imágenes de contenedor que incluyen Node.js.

Ampliar información: Node2Shell: Vulnerabilidad de RCE en Node.js por datos Brotli maliciosos (CVE-2026-111497)

ACCIÓN A SEGUIR

Cómo te acompaña nuestro SOC

1. Actualizar Arista VeloCloud Orchestrator on-prem a 5.2.3.18, 6.1.3.10 o 6.4.2.12 de inmediato (el plazo de CISA venció el 26 de octubre de 2026) y revisar las cuentas y los cambios de configuración recientes en el orquestador.
2. Actualizar Plex Media Server a 1.43.3.10861 de inmediato (el plazo de CISA venció el 23 de octubre de 2026 para CVE-2026-96656 y CVE-2026-96654, y vence el 3 de noviembre de 2026 para CVE-2026-96655 y CVE-2026-96652) o retirarlo de los equipos corporativos.
3. Actualizar EG Secure Solutions SiteGuard Server Edition a Ver8.00 Update 5 o Ver7.00 Update 6 de inmediato (el plazo de CISA venció el 23 de octubre de 2026).
4. Aplicar de inmediato la corrección de Palo Alto Networks para CVE-2026-0257 en PAN-OS y Prisma Access, explotada por los grupos de ransomware Qilin e INC.
5. Aplicar de inmediato los parches de emergencia de PHP para CVE-2026-109618 y CVE-2026-109619 y activar reglas de WAF frente a los servidores web expuestos.
6. Actualizar Siemens Software Center a V4.0.9.8 antes del 3 de noviembre de 2026 y aplicar cuanto antes la corrección de Fortinet para CVE-2026-106173 en FortiSIEM, con su interfaz de administración restringida a la red de gestión.
7. Vigilar estas señales: procesos de minería y conexiones salientes inusuales en servidores Plex y web (Plex2Shell y Mirai), accesos remotos por VPN sin segundo factor registrado (Qilin e INC), cambios en los archivos de VMware Tools (Vasilek) y presencia de LiteLLM 1.107.0, de la CLI de OVHcloud descargada desde GitHub o de paquetes npm no aprobados en equipos de desarrollo; si aparece alguna, rotar los secretos expuestos.
8. El SOC acompaña con monitoreo y respuesta gestionada (FortiGuard SOCaaS) centrado en estas señales y en la verificación de los parches aplicados.

AVISO: Boletín informativo TLP:CLEAR de Ingeniería Telemática S.A.S. Datos provenientes de CISA KEV, NVD y avisos de fabricante. De carácter informativo; no sustituye un análisis de su entorno.