Alerta

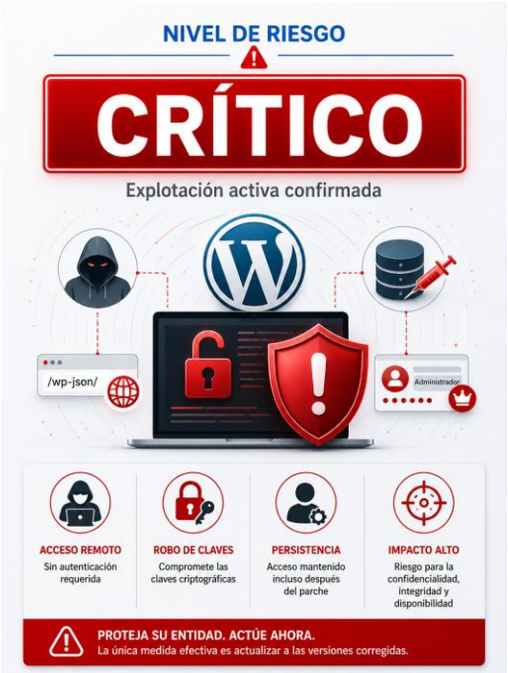
Vulnerabilidad crítica en WordPress — cadena wp2shell

COLCERT AL - 20260805 - 109

TLP:CLEAR

Resumen Ejecutivo

Una cadena de dos vulnerabilidades críticas permite que un visitante anónimo obtenga el control total de un sitio WordPress mediante una única petición al servicio web. La cadena, identificada como CVE-2026-63030 y CVE-2026-60137 y conocida conjuntamente como «wp2shell», combina una falla de confusión de rutas con una vulnerabilidad de inyección SQL, permitiendo la ejecución remota de código sin requerir credenciales, interacción del usuario ni componentes adicionales.



No se requiere usuario, contraseña, complemento, plantilla ni configuración particular. Basta una instalación estándar de WordPress publicada en internet y una única petición al servicio web. El desenlace observado en ataques reales es la creación de una cuenta de administrador controlada por el atacante y la instalación de un archivo malicioso persistente.

WordPress sostiene los portales de un número muy alto de alcaldías, gobernaciones, empresas de servicios públicos, instituciones educativas y pequeñas y medianas empresas del país. Por su naturaleza, esos sitios están siempre expuestos a internet. Toda organización que administre un sitio en WordPress debe verificar hoy su versión y actualizar.

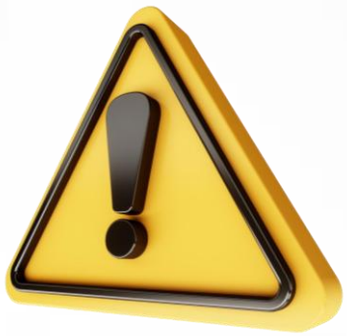
Vulnerabilidad identificada

CVE0	Tipo de falla	CVSS 3.1	SSVC	Descripción	CISA KEV
CVE-2026-63030	**Conflicto de interpretación (CWE-436)**	**9.8 (Crítica)**	**Track** en origen; ColCERT eleva a Act	Confusión de rutas en el procesador de peticiones agrupadas de la REST API. Cuando una subpetición malformada falla, el error se registra en el arreglo de validación pero no en el de coincidencias de ruta. Esa desincronización hace que las subpeticiones siguientes se ejecuten bajo el manejador equivocado, eludiendo las comprobaciones de autorización, método, ruta y esquema de validación.	**TRUE**
CVE-2026-60137	**Inyección SQL (CWE-89)**	**Ver nota**	**Track**	Saneamiento insuficiente del parámetro author__not_in de la clase WP_Query. El valor solo se sanea cuando se entrega como arreglo de enteros; al llegar como cadena de texto se interpola directamente en la consulta SQL. La validación de parámetros lo impediría en condiciones normales, pero la falla anterior permite eludirla.	**TRUE**

Origen y trazabilidad de esta alerta

La vulnerabilidad fue puesta en conocimiento de ColCERT mediante el Vulnerability Exchange de la red CSIRT Américas (OEA), en un aporte del Canadian Centre for Cyber Security (CCCS) marcado TLP:CLEAR.

Ese aporte comunicó ambos identificadores, una clasificación SSVC «Track» y una puntuación de 7.5 para CVE-2026-60137.



SSVC es el marco de priorización de CISA: Track significa vigilar y corregir en el ciclo normal; Act, remediar de inmediato. La categoría depende del estado de explotación, y este cambió después de emitido el aporte de origen.

Divergencias documentadas. ColCERT eleva la prioridad de CVE-2026-63030 de «Track» a «Act» por tres razones verificadas con fuentes primarias: explotación activa confirmada, incorporación al catálogo KEV de CISA y disponibilidad pública de código de explotación funcional. Respecto de CVE-2026-60137, las puntuaciones publicadas difieren entre fuentes; ColCERT se abstiene de fijar un valor único y remite al registro oficial de la vulnerabilidad. La discrepancia no altera la acción recomendada, que es idéntica en ambos casos: actualizar.

¿Cómo podría aprovechar esta vulnerabilidad un ciberdelincuente?

1. **Localización del sitio:** el atacante rastrea internet buscando sitios construidos con WordPress. No necesita conocer la organización ni tener relación previa con ella. La detección es trivial y automatizable a gran escala, la organización ni tener relación previa con ella; basta con que el servicio responda desde la red.

2. **Envío de una petición agrupada:** remite al sitio una única petición POST al endpoint que permite agrupar varias llamadas en una sola. Ese endpoint es accesible de forma anónima por diseño.

3. **Ruptura deliberada del índice interno:** dentro de esa agrupación incluye una subpetición malformada a propósito. Al fallar, WordPress registra el error en un arreglo pero no en el otro, y ambos quedan desalineados.

4. **Ejecución bajo el manejador equivocado:** por efecto de ese desfase, la subpetición siguiente, de alto privilegio, se procesa con el manejador y el contexto de permisos de otra. Se omiten las comprobaciones de autorización y también las de método, ruta y esquema.

5. **Inyección SQL en la base de datos:** aprovechando la omisión de validaciones, el atacante envía un parámetro de tipo texto donde el sistema espera una lista de números. Ese valor llega sin sanear a la consulta SQL.

6. **Creación de una cuenta de administrador:** con control sobre la consulta, el atacante inserta un usuario administrador propio. A partir de ese momento entra al panel por la puerta principal, sin volver a explotar nada.

7. **Instalación de un archivo malicioso persistente:** desde el panel de administración despliega un archivo que le permite ejecutar comandos en el servidor. En los ataques observados, ese archivo es el objetivo final y el que garantiza la permanencia.

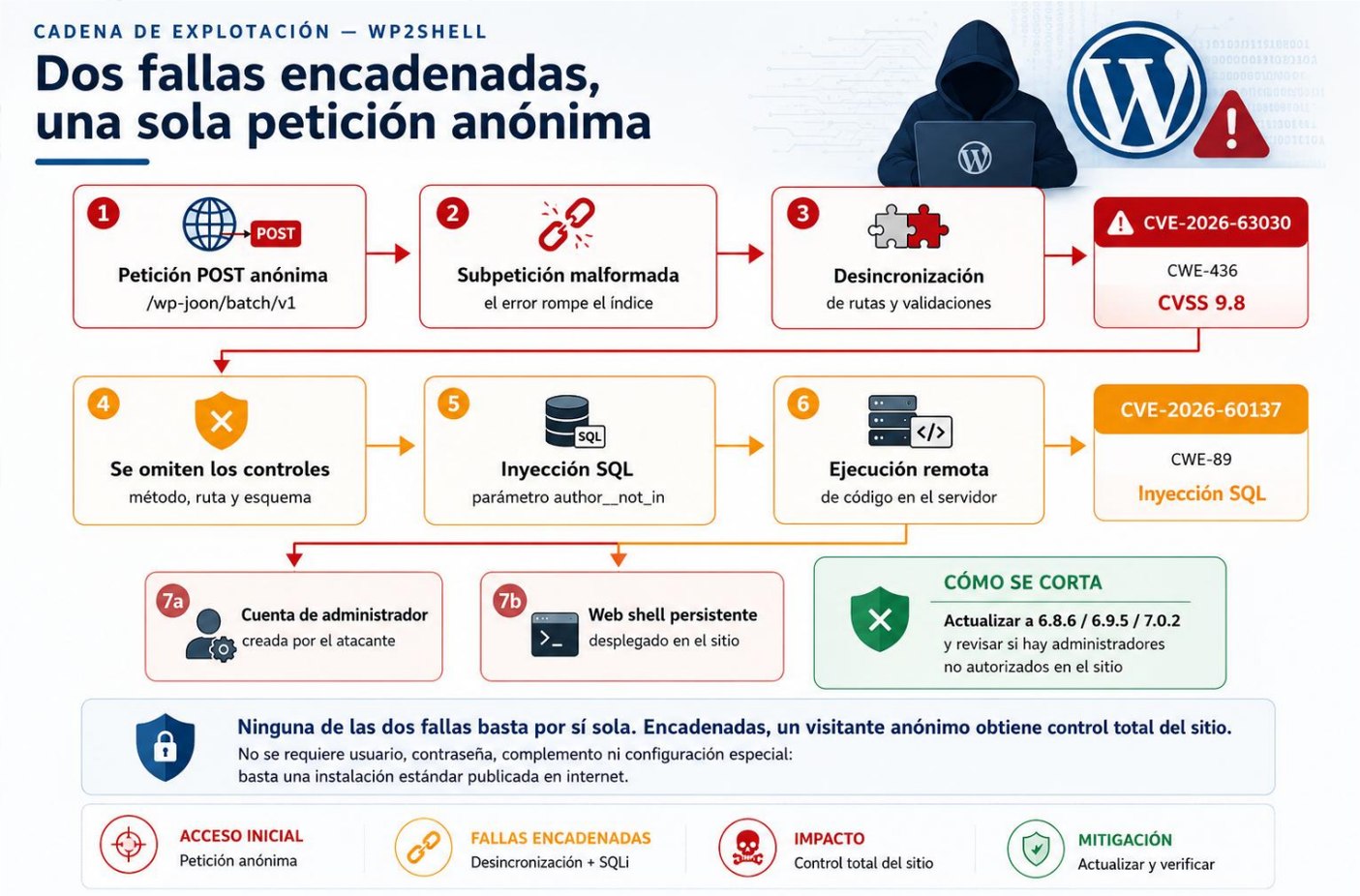


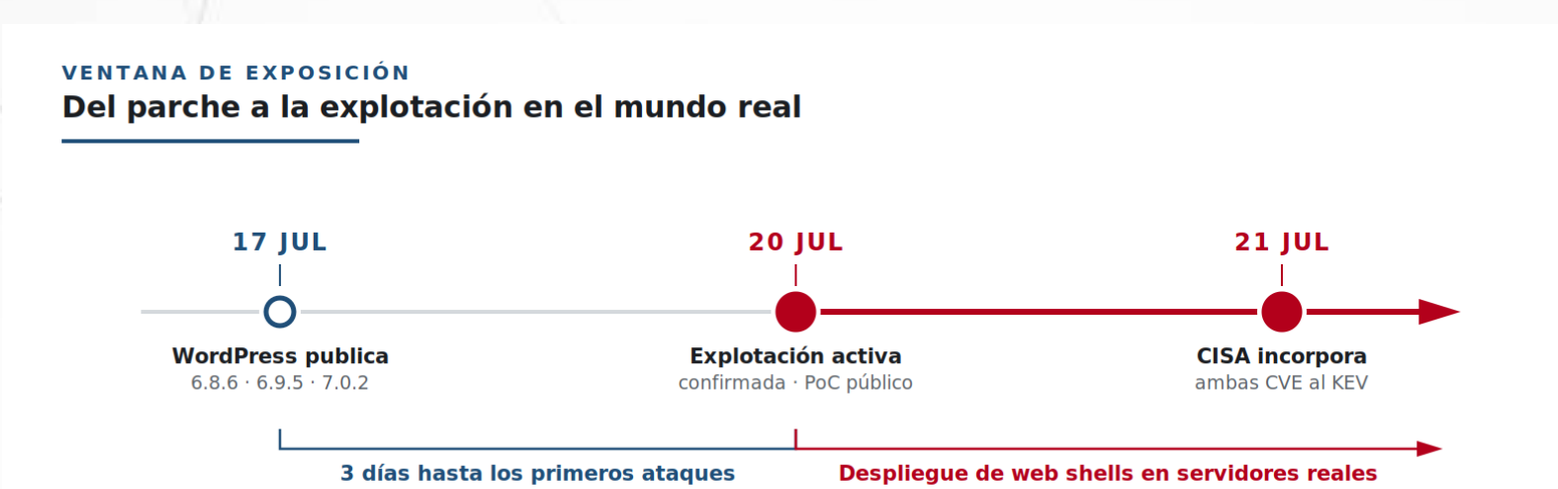
Figura 1: Encadenamiento de las dos vulnerabilidades, desde la petición anónima hasta el control del sitio.

Explotación actual

WordPress publicó tres versiones correctivas de emergencia el 17 de julio de 2026 y activó actualizaciones automáticas forzadas a escala mundial. La divulgación de los detalles técnicos completos y la aparición de código de explotación público ocurrieron en los días inmediatamente siguientes.

El 20 de julio se confirmó explotación en el mundo real. Investigadores de seguridad reportaron el despliegue de archivos maliciosos persistentes en servidores vulnerables. El 21 de julio, CISA incorporó ambas vulnerabilidades a su catálogo de vulnerabilidades explotadas conocidas (KEV).

Existen herramientas públicas que verifican en segundos si un sitio es vulnerable y que, en su modo de explotación, crean la cuenta de administrador y despliegan el archivo malicioso de forma automática. Esto sitúa el ataque al alcance de personas sin conocimiento técnico avanzado.



Magnitud de la exposición

Mediciones publicadas por firmas de seguridad indican que, al momento de divulgarse estas vulnerabilidades, alrededor del 60 % de las organizaciones que utilizan WordPress tenía al menos una instancia vulnerable y cerca del 25 % exponía a internet un servidor vulnerable. No se trata de un escenario de nicho.

¿Mi sitio está afectado?

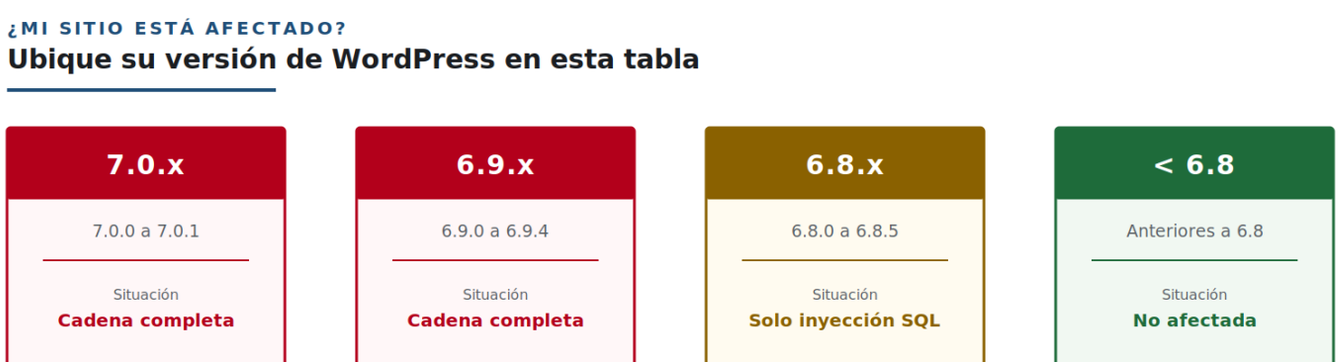


Figura 3: Situación según la versión de WordPress instalada.

Versión instalada	Situación	Versión corregida
7.0.0 a 7.0.1	**Afectada por la cadena completa.** Ejecución remota de código sin autenticación.	**7.0.2**
6.9.0 a 6.9.4	**Afectada por la cadena completa.** La falla de confusión de rutas se introdujo en la versión 6.9.	**6.9.5**
6.8.0 a 6.8.5	**Afectada solo por la inyección SQL.** No alcanza la ejecución remota de código, pero requiere actualización igualmente.	**6.8.6**
Anteriores a 6.8	**No afectadas** por estas dos vulnerabilidades. Advertencia: una versión antigua no es una versión segura; probablemente acumula otras fallas sin corregir.	Migrar a una versión con soporte
Rama 7.1 (beta)	**Afectada** en versiones anteriores a la segunda beta.	7.1 beta 2

Sobre las actualizaciones automáticas forzadas

WordPress activó actualizaciones automáticas forzadas para las instalaciones afectadas que tuvieran esa función habilitada. Es probable que una parte de los sitios ya esté corregida sin intervención del administrador.

Esto no exime de verificar. Las instalaciones con actualizaciones automáticas deshabilitadas, alojadas en entornos gestionados con control de versiones, o con el núcleo modificado, pueden no haber recibido la corrección. Y si el sitio fue comprometido antes de actualizarse, la actualización no elimina la cuenta de administrador ni el archivo malicioso que el atacante haya dejado.

¿Cómo verificar la versión y descartar un compromiso?

La versión instalada aparece en el panel de administración, en Escritorio → Actualizaciones, y también al pie del panel. Desde la línea de comandos, si dispone de WP-CLI: wp core version · wp core check-update · wp user list --role=administrator.

Actualizar no es suficiente si el sitio ya fue comprometido. Si su sitio estuvo publicado en internet con una versión afectada entre el 17 y el 27 de julio de 2026, revise como mínimo lo siguiente:g

- ❑ Cuentas de administrador no reconocidas. Es el resultado característico de este ataque. Revise la lista completa de usuarios con rol de administrador y verifique la fecha de registro de cada uno. Una cuenta creada en ese periodo y que nadie reconozca es un indicador de compromiso.
- ❑ Archivos PHP nuevos o modificados en los directorios del sitio, especialmente en las carpetas de contenido, complementos y plantillas. Compare contra una copia de seguridad anterior al 17 de julio.
- ❑ Complementos o plantillas que usted no instaló. Un archivo malicioso puede desplegarse disfrazado de complemento legítimo.

- Peticiones POST al endpoint de agrupación en los registros del servidor web: /wp-json/batch/v1 y también /?rest_route=/batch/v1. El endpoint es alcanzable por esas dos rutas, y desactivar los enlaces permanentes no elimina la exposición.
- Tareas programadas y usuarios de base de datos que no correspondan a la operación normal del sitio.

Conserve la evidencia antes de limpiar

Si encuentra indicadores de compromiso, preserve los registros del servidor web, una copia de la base de datos y una imagen de los archivos del sitio antes de eliminar nada o restaurar una copia de seguridad.

Borrar el rastro impide determinar el alcance real y complica cualquier actuación judicial posterior,restaurar una copia de seguridad posterior al compromiso reinstala la puerta trasera.

Si no puedes actualizar de inmediato

La actualización es la única corrección real. Cuando exista una restricción operativa que impida aplicarla en el momento, puede bloquear temporalmente el acceso al endpoint de agrupación de la REST API mediante un cortafuegos de aplicaciones web o reglas del servidor, teniendo en cuenta dos advertencias:

- **El endpoint es alcanzable por dos rutas distintas:** /wp-json/batch/v1 y /?rest_route=/batch/v1. Una regla que solo cubra una de ellas deja el sitio expuesto; desactivar los enlaces permanentes no cierra la segunda vía.
- **Riesgo crítico:** la explotación no requiere credenciales, ni engaño al usuario, ni complementos vulnerables. Un sitio publicado en internet con una versión afectada es alcanzable por cualquiera, y la explotación es automatizable a gran escala.
- **Consecuencias posibles:** alteración del contenido del portal institucional; publicación de información falsa a nombre de la entidad; acceso a la base de datos y a los datos personales de ciudadanos registrados; uso del servidor como punto de apoyo para atacar otros sistemas; y despliegue de contenido malicioso contra los propios visitantes del sitio.
- **Confianza institucional:** la alteración del portal de una entidad pública tiene un efecto que excede lo técnico. Afecta la credibilidad de la información oficial y puede aprovecharse para campañas de desinformación o para suplantar trámites.
- **Datos personales y marco normativo:** los portales que gestionan registros, formularios de contacto, PQRSD o trámites almacenan datos personales. Su exposición activa las obligaciones de la Ley 1581 de 2012 y la notificación a la Superintendencia de Industria y Comercio.

Técnica MITRE ATT&CK asociadas

TÉCNICA	CÓDIGO	DESCRIPCIÓN
Exploit Public-Facing Application	**T1190**	Explotación del servicio web publicado en internet para obtener acceso inicial, sin credenciales ni interacción del usuario.
Create Account: Local Account	**T1136.001**	Creación de una cuenta de administrador propia dentro de la aplicación, que permite el acceso posterior por vías legítimas.
Server Software Component: Web Shell	**T1505.003**	Despliegue de un archivo malicioso en el servidor que permite ejecutar comandos y garantiza la permanencia del atacante.
Valid Accounts	**T1078**	Uso de la cuenta administrativa creada para operar sobre el sitio sin volver a explotar la vulnerabilidad.
Data from Information Repositories	**T1213**	Extracción de contenido y datos personales almacenados en la base de datos del portal.

Mitigaciones MITRE

MITIGACIÓN	CÓDIGO	RELEVANCIA
Update Software	**M1051**	Actualizar el núcleo de WordPress a 6.8.6, 6.9.5 o 7.0.2 según la rama instalada. Es la única corrección real.
Application Isolation and Sandboxing	**M1048**	Interponer un cortafuegos de aplicaciones web y restringir el acceso al endpoint de agrupación como medida temporal.
Audit	**M1047**	Revisar cuentas de administrador no reconocidas, archivos PHP nuevos o modificados y complementos no instalados por la organización.
User Account Management	**M1018**	Mantener el inventario de cuentas administrativas y eliminar las que no correspondan a personas identificadas y vigentes.
Filter Network Traffic	**M1037**	Restringir el acceso al panel de administración por dirección de origen cuando la operación lo permita.

Recomendaciones

- **Actualice hoy el núcleo de WordPress a 6.8.6, 6.9.5 o 7.0.2 según su rama.** Actualice también complementos y plantillas en el mismo ejercicio.
- **Verifique la lista de administradores.** Es el punto de control más importante: una cuenta administrativa creada entre el 17 y el 27 de julio que nadie reconozca indica un compromiso probable.
- **Confirme que la actualización se aplicó.** No dé por hecho que las actualizaciones automáticas cubrieron todos sus sitios; verifique cada uno.
- **Busque archivos maliciosos persistentes:** archivos PHP nuevos o modificados y complementos que la organización no instaló.

- **Conserve la evidencia antes de limpiar.** Preserve registros, base de datos y archivos antes de restaurar. Una copia de seguridad posterior al compromiso reinstala la puerta trasera.
- **Inventaríe sus sitios en WordPress.** Muchas entidades desconocen cuántos portales secundarios, micrositios o sitios de campaña mantienen publicados. Los sitios olvidados son los que no se actualizan.

¿Cómo validar la postura de seguridad de su portal?

El ColCERT, a través de su línea de gestión de vulnerabilidades y gestión de superficie de ataque (ASM), puede evaluar el grado de exposición de los portales de su entidad, identificar las desviaciones priorizadas por criticidad y entregar un informe técnico con recomendaciones de remediación.

Las entidades del Estado pueden solicitar este acompañamiento a través de

Los canales oficiales del ColCERT.

Fuentes

WordPress.org, 17 de julio de 2026 — versiones de seguridad 6.8.6, 6.9.5 y 7.0.2. Anuncio oficial del proyecto. wordpress.org/news

GitHub Security Advisory, 2026 — GHSA-ff9f-jf42-662q, rangos de versión afectados y corregidos para CVE-2026-63030

CISA, 21 de julio de 2026 — Known Exploited Vulnerabilities Catalog. Incorporación de ambas CVE. cisa.gov/known-exploited-vulnerabilities-catalog

National Vulnerability Database (NIST), 2026 — registros oficiales de ambas CVE. nvd.nist.gov/vuln/detail/CVE-2026-63030

Searchlight Cyber / Assetnote, julio de 2026 — divulgación e informe técnico de la cadena wp2shell. Investigación original, comunicada de forma coordinada al proyecto WordPress.

Canadian Centre for Cyber Security (CCCS), julio de 2026 — WordPress security advisory (AV26-723). Fuente secundaria.

Red CSIRT Américas (OEA) — Vulnerability Exchange, 27 de julio de 2026 — aporte del CCCS, TLP:CLEAR. Origen de la notificación a ColCERT.