INGENIERÍA
TELEMÁTICA S.A.S.

BOLETÍN DE CIBERSEGURIDAD · INTELIGENCIA DE AMENAZAS

TLP:CLEAR · EDICIÓN 2026-W44 · SEMANAL

Semana del 26 oct 2026 al 1 nov 2026 · publicado el 2 de noviembre 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 26 de octubre y el 1 de noviembre de 2026, la agencia de ciberseguridad de EE. UU. (CISA) añadió 8 vulnerabilidades a su catálogo KEV, la lista de fallas con explotación activa confirmada. Tres son de severidad crítica y cuatro tienen el plazo de corrección de CISA vencido al 2 de noviembre de 2026. La prioridad es GitLab Community y Enterprise Edition (CVE-2026-97229, CVSS 10.0, en una escala de gravedad de 0 a 10): permite a un atacante sin credenciales ejecutar código en el servidor, su plazo venció el 1 de noviembre de 2026 y ya hubo un intento de explotación contra el servidor de Alpine Linux. En el perímetro también hay plazos vencidos: los firewalls Cisco ASA y FTD pueden reiniciarse a distancia a través de la VPN SSL (plazo vencido el 1 de noviembre de 2026) y la VPN Ivanti Connect Secure tiene una cadena de fallas cuyo primer plazo venció el 2 de noviembre de 2026. Los siguientes plazos son el 10 de noviembre de 2026 para Adobe Commerce y Magento (PolyShell) y para la biblioteca de compresión Brotli. Además, cuatro campañas apuntan al robo de accesos a Microsoft 365 y Teams y a las claves de cifrado de Cisco Catalyst SD-WAN, lo que obliga a revisar la autenticación en la nube además de parchear.

7	7	4
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

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

7 vulnerabilidades, 7 con explotación activa confirmada · 4 campaña(s) de malware · 5 noticia(s) · semana del 26 oct 2026 al 1 nov 2026

VULNERABILIDADES

de mayor a menor criticidad

Crítica · CVSS 10.0 | Explotación activa | CVE-2026-97229

GitLab permite ejecutar código sin autenticación mediante expresiones regulares en la configuración de CI/CD

GitLab Community Edition and Enterprise Edition · CWE-190 — Desbordamiento o ajuste de enteros · Versiones afectadas: `19.2 a anteriores a 19.2.8; 19.3 a anteriores a 19.3.5; 19.4 a anteriores a 19.4.2`

GitLab no valida bien las expresiones regulares que recibe en la configuración de CI/CD (integración y despliegue continuos, los flujos que compilan y publican software). Esa validación insuficiente provoca un desbordamiento de enteros. Con una expresión regular manipulada, un usuario sin autenticar puede ejecutar código arbitrario en el servidor. Ya se registró un intento de explotación contra el servidor GitLab de Alpine Linux, y el caso mostró que en las instalaciones que usan un Ruby propio actualizar GitLab no basta.

Impacto: El atacante obtiene control del servidor de desarrollo. Desde ahí puede robar código fuente, secretos y credenciales de despliegue guardados en los flujos de CI/CD, y alterar el software que la empresa entrega a sus clientes. Si el servidor está publicado en internet, cualquier persona puede intentar el ataque sin cuenta.

> **Acción a seguir:** Actualizar a la versión 19.2.8, 19.3.5 o 19.4.2, según la rama instalada. El plazo de CISA venció el 1 de noviembre de 2026, por lo que la corrección debe aplicarse de inmediato. En instalaciones que usan un Ruby propio, verificar y actualizar también ese componente. Después, revisar los registros de CI/CD en busca de configuraciones con expresiones regulares anómalas y rotar los secretos de los flujos de despliegue.

Ampliar información: NVD — CVE-2026-97229 CISA KEV

Crítica · CVSS 9.3 | Explotación activa | CVE-2026-48356

PolyShell: carga de archivos peligrosos en Adobe Commerce y Magento permite ejecutar código

Adobe Commerce and Magento · CWE-434 — Carga sin restricciones de archivos de tipo peligroso · Versiones afectadas: `≤2.4.9, 2.4.8-p5, 2.4.7-p10, 2.4.6-p15; ≤1.20.0 (según el registro de CISA)`

La falla, conocida como PolyShell, permite subir a la tienda archivos de tipo peligroso, como scripts ejecutables, porque la plataforma no restringe qué se carga. Una vez en el servidor, el archivo ejecuta código con los permisos del usuario actual. Esto puede dar al atacante acceso elevado o el control de la cuenta o la sesión de la víctima.

Impacto: Una tienda en línea comprometida puede usarse para robar datos de clientes y de pago, insertar código que capture tarjetas en la página de compra o servir de puerta de entrada a la red interna. Las tiendas son, por naturaleza, accesibles desde internet.

> **Acción a seguir:** Instalar la actualización de seguridad de Adobe que corrige CVE-2026-48356 en las ramas 2.4.9, 2.4.8-p5, 2.4.7-p10 y 2.4.6-p15 antes del 10 de noviembre de 2026, plazo fijado por CISA. Mientras se aplica, impedir la ejecución de scripts en los directorios de carga de archivos. También conviene revisar si hay archivos recientes inesperados en esas rutas.

Ampliar información: NVD — CVE-2026-48356 CISA KEV

Crítica · CVSS 9.2 Explotación activa CVE-2026-111497

Falla en la biblioteca de compresión Google Brotli permite corromper memoria con un flujo manipulado

Google Brotli · CWE-252 — Valor de retorno no verificado · Versiones afectadas: `1.0.3 a anteriores a 1.0.10; 1.1.0 a anteriores a 1.1.1; 1.2.0 a anteriores a 1.2.1`

Brotli es una biblioteca de compresión que se integra en entornos como Node.js y PHP. Su decodificador no verifica el valor de retorno de una operación interna. Con un flujo comprimido manipulado, un atacante remoto sin autenticar puede corromper la memoria contigua del decodificador. Según el caso, eso le permite leer información sensible, provocar una denegación de servicio o incluso ejecutar código.

Impacto: Cualquier aplicación web o servicio que descomprima contenido Brotli de origen externo puede caerse, filtrar datos de memoria o quedar bajo control del atacante. El riesgo es mayor porque la biblioteca suele estar embebida en dependencias que el equipo de TI no tiene inventariadas.

> **Acción a seguir:** Actualizar Brotli a la versión 1.0.10, 1.1.1 o 1.2.1, según la rama, antes del 10 de noviembre de 2026, plazo de CISA. También hay que aplicar las versiones corregidas de Node.js y PHP que incorporan la biblioteca. Para no dejar copias vulnerables, revisar la lista de dependencias de cada aplicación e identificar los componentes que incluyen Brotli internamente.

Ampliar información: NVD — CVE-2026-111497 CISA KEV

Alta · CVSS 8.6 Explotación activa CVE-2026-76418

Cisco ASA y FTD pueden reiniciarse a distancia a través de la VPN SSL

Cisco Secure Firewall ASA Software and Cisco Secure FTD Software · CWE-476 — Desreferencia de puntero nulo (originada en un valor de retorno no verificado, CWE-252) · Versiones afectadas: `9.16.1; 9.16.1.28; 9.16.2; 9.16.2.3; 9.16.2.7 (listado de CISA)`

El servicio de VPN SSL (red privada virtual sobre cifrado SSL/TLS) de los firewalls ASA y FTD no verifica un valor de retorno. Eso termina en un acceso a un puntero nulo. Un atacante remoto sin credenciales puede aprovecharlo para forzar el reinicio inesperado del equipo y provocar una denegación de servicio (DoS).

Impacto: Cada reinicio corta la conectividad de la sede y desconecta a los usuarios de teletrabajo que dependen de la VPN. Los reinicios repetidos pueden dejar la operación sin acceso a internet ni a sistemas remotos. El servicio VPN SSL está expuesto a internet, así que el ataque no requiere estar dentro de la red.

> **Acción a seguir:** Aplicar la versión corregida que indica el aviso de Cisco para CVE-2026-76418 en los equipos ASA y FTD de la rama 9.16. El plazo de CISA venció el 1 de noviembre de 2026, por lo que debe hacerse de inmediato. Mientras tanto, vigilar los reinicios no programados del firewall y limitar el acceso a la VPN SSL a los orígenes necesarios cuando sea viable.

Ampliar información: NVD — CVE-2026-76418 CISA KEV

Alta · CVSS 7.8 **Explotación activa** CVE-2026-46300

Variable sin inicializar en el kernel de Linux permite alterar datos en caché durante el procesamiento IPsec

Linux Kernel · CWE-456 — Falta de inicialización de una variable · Versiones afectadas: `Rango de commits desde cef401de7be8c4e155c6746bfccf721a4fa5fab9 hasta anteriores a 3599e6b3cc1ada96883d496a50a210d3afbb6987 (según CISA)`

El kernel de Linux combina búferes de red al procesar paquetes. En esa operación no conserva la marca que indica que un fragmento de memoria es compartido. Como resultado, el procesamiento de entrada de ESP (el protocolo que cifra el tráfico en las VPN IPsec) descifra esos fragmentos en su sitio. Eso puede modificar sin intención datos respaldados por la caché de páginas, es decir, el contenido de archivos que el sistema mantiene en memoria.

Impacto: Un atacante puede alterar el contenido de archivos en memoria en servidores y equipos Linux. Esto compromete la integridad del sistema y abre la puerta a manipular programas o configuraciones sin dejar rastro en el disco. Afecta tanto a servidores propios como a dispositivos de red basados en Linux.

> **Acción a seguir:** Instalar la actualización del kernel de la distribución que incluya el commit 3599e6b3cc1ada96883d496a50a210d3afbb6987 y reiniciar los equipos para que el cambio surta efecto. El plazo de CISA venció el 31 de octubre de 2026, por lo que la corrección debe aplicarse de inmediato. Hay que dar prioridad a los servidores que terminan túneles IPsec.

Ampliar información: NVD — CVE-2026-46300 CISA KEV

Alta · CVSS 7.0 **Explotación activa** CVE-2026-111357, CVE-2026-118527

Ivanti Connect Secure: dos fallas encadenables permiten escribir archivos en disco y elevar privilegios

Ivanti Connect Secure · CWE-306 — Falta de autenticación para función crítica; CWE-340 — Generación de números o identificadores predecibles · Versiones afectadas: `22.8R2.4 (CVE-2026-111357); CISA no detalla versiones para CVE-2026-118527`

Son dos fallas que se encadenan entre sí y con CVE-2026-104935. La primera, CVE-2026-111357 (CVSS 7.0), deja sin autenticación una función crítica y permite a un atacante local autenticado elevar sus privilegios. La segunda, CVE-2026-118527, usa identificadores predecibles: un atacante remoto autenticado puede subir archivos con el contenido que elija a una ubicación conocida del disco. CISA no publicó puntuación CVSS ni severidad para CVE-2026-118527. La agrupamos con la primera porque afectan el mismo producto y se explotan en cadena.

Impacto: Combinadas, permiten que alguien con una cuenta en el concentrador VPN coloque archivos en el equipo y obtenga privilegios elevados. Esa es la base para tomar el control del punto de entrada remoto de la empresa, que por diseño está expuesto a internet.

> **Acción a seguir:** Aplicar la actualización de Ivanti que corrige CVE-2026-111357 en la versión 22.8R2.4 y, en el mismo mantenimiento, CVE-2026-118527 y CVE-2026-104935. El plazo de CISA para CVE-2026-111357 venció el 2 de noviembre de 2026, así que debe aplicarse de inmediato. El plazo para CVE-2026-118527 es el 13 de noviembre de 2026. Después, ejecutar la herramienta de verificación de integridad de Ivanti, revisar las cuentas locales y buscar archivos inesperados en disco.

Ampliar información: NVD — CVE-2026-111357 CISA KEV

Baja · CVSS 2.7 **Explotación activa** CVE-2026-41709

VMware ESX permite a un administrador realizar operaciones sin dejar registro, explotada por el grupo Warp Panda

Broadcom VMware ESX · CWE-778 — Registro insuficiente · Versiones afectadas: `9.1.x.x anteriores a ESXi-9.1.0.0-25370933; 9.0.x.x anteriores a ESXi-9.0.2.0100-25595025; 5.x anteriores a 5.2.4`

VMware ESX no registra ciertas operaciones que realiza un usuario con acceso de administrador. Su puntuación es baja porque exige privilegios previos. Aun así, el grupo chino Warp Panda la explotó como vulnerabilidad de día cero (sin parche disponible en ese momento) para evadir los registros de auditoría de los hipervisores.

Impacto: Un atacante que ya obtuvo credenciales de administrador puede operar sobre los hipervisores, y por lo tanto sobre todas las máquinas virtuales que alojan, sin dejar rastro. Eso dificulta detectar la intrusión y reconstruir lo ocurrido durante una investigación forense.

> **Acción a seguir:** Actualizar a ESXi-9.1.0.0-25370933 o ESXi-9.0.2.0100-25595025, según la rama, y a 5.2.4 en la rama 5.x, antes del 11 de noviembre de 2026, plazo de CISA. También conviene revisar las cuentas con privilegios de administrador en vCenter y ESXi y enviar los registros a un servidor externo que el atacante no pueda alterar.

Ampliar información: NVD — CVE-2026-41709 CISA KEV

MALWARE Y CAMPAÑAS técnicas MITRE ATT&CK

KeyDrift (Cisco Catalyst SD-WAN)

Cisco Talos documentó KeyDrift, un malware que explotó la vulnerabilidad CVE-2026-20127 en Cisco Catalyst SD-WAN (red de área amplia definida por software, que interconecta sedes). Con ella copió las claves de cifrado AES que protegen el tráfico entre sedes. Con esas claves, el atacante puede descifrar o suplantar las comunicaciones entre oficinas sin necesidad de romper el cifrado. Para una empresa colombiana con varias sedes o sucursales conectadas por Cisco SD-WAN, esto implica verificar la versión instalada y planear la rotación de claves después de parchear.

MITRE ATT&CK `T1190 — Explotación de aplicación expuesta a internet` `T1552.004 — Credenciales no protegidas: claves privadas`

> **Acción a seguir:** Aplicar las versiones corregidas que publicó Cisco para CVE-2026-20127 en Catalyst SD-WAN y restringir el acceso a las interfaces de gestión de la solución a redes administrativas. Después del parche, rotar las claves de cifrado entre sedes y vigilar conexiones de gestión desde orígenes no habituales.

Ampliar información: KeyDrift: malware explota falla de Cisco Catalyst SD-WAN para robar claves de cifrado

Reutilización de tokens en Microsoft 365

Investigadores revelaron una campaña de reutilización (replay) de tokens en Microsoft 365. Un token es la credencial temporal que se emite después de iniciar sesión; los atacantes los roban y los vuelven a presentar para entrar a las cuentas sin conocer la contraseña. La campaña comprometió 97 cuentas en 79 organizaciones. Como el token se emite cuando el usuario ya superó la autenticación, el ataque puede saltarse la autenticación multifactor (MFA). Para cualquier organización colombiana en Microsoft 365, esto significa que tener MFA activo no basta: hay que revisar cuánto duran las sesiones y desde dónde se usan.

MITRE ATT&CK `T1528 — Robo de token de acceso de aplicación` `T1550.001 — Uso de material de autenticación alternativo: token de acceso de aplicación` `T1078.004 — Cuentas válidas: cuentas en la nube`

> **Acción a seguir:** Vigilar en los registros de inicio de sesión de Microsoft Entra ID las sesiones que reutilizan un mismo token desde direcciones IP o países distintos. Revocar las sesiones de las cuentas sospechosas y aplicar políticas de acceso condicional que exijan un dispositivo administrado.

Ampliar información: Microsoft 365: Ataques de Replay de Tokens Comprometen 97 Cuentas en 79 Organizaciones

Skyw4lker: phishing por código de dispositivo

La campaña Skyw4lker envía documentos protegidos que llevan a páginas alojadas en Google Sites. Allí se induce a la víctima a introducir un código en el flujo legítimo de autenticación por código de dispositivo de Microsoft. Al hacerlo, la víctima autoriza sin saberlo al atacante, que obtiene tokens de acceso a Microsoft 365 sin necesidad de robar contraseñas. Para una pyme o entidad pública colombiana, la decisión práctica es bloquear ese flujo de autenticación para los usuarios que no lo usan, porque la mayoría nunca lo necesita.

MITRE ATT&CK `T1566.002 — Phishing: enlace malicioso` `T1528 — Robo de token de acceso de aplicación` `T1078.004 — Cuentas válidas: cuentas en la nube`

> **Acción a seguir:** Bloquear con acceso condicional el flujo de código de dispositivo para los usuarios que no lo requieren. Vigilar los inicios de sesión por ese método y los correos con documentos protegidos que remiten a Google Sites.

Ampliar información: Skyw4lker: phishing por código de dispositivo roba accesos a Microsoft 365 sin robar contraseñas

Falso soporte de TI en Microsoft Teams

Arctic Wolf documentó cientos de casos en los que atacantes contactan a empleados por chats externos de Microsoft Teams haciéndose pasar por soporte de TI. Con ese pretexto los convencen de conceder acceso remoto al equipo, que luego se usa para instalar malware y desplegar ransomware (secuestro de datos mediante cifrado). Para una empresa colombiana, esto implica revisar si Teams acepta mensajes de cualquier organización externa y avisar a los usuarios que el soporte interno nunca inicia contacto por ese canal.

MITRE ATT&CK `T1566.003 — Phishing: a través de servicio` `T1219 — Software de acceso remoto` `T1486 — Cifrado de datos para impacto`

> **Acción a seguir:** Restringir el acceso externo de Teams a dominios de confianza. Vigilar la instalación o ejecución de herramientas de acceso remoto no autorizadas poco después de un chat externo y bloquear las que la organización no usa oficialmente.

Ampliar información: Falsos soportes de TI en Microsoft Teams abren la puerta a malware y ransomware

NOTICIAS DE CIBERSEGURIDAD

lo que cambia esta semana

Atacantes explotan una falla crítica de omisión de autorización en Drupal Commerce Core

Drupal confirmó la explotación activa de CVE-2026-118539 en Commerce Core, el módulo de comercio electrónico de la plataforma. La falla permite omitir los controles de autorización en tiendas en línea, y Drupal ya publicó versiones corregidas y mitigaciones. Las empresas y entidades colombianas que venden o reciben pagos en sitios Drupal deben confirmar si usan Commerce Core y actualizarlo de inmediato.

Ampliar información: Drupal Commerce Core: atacantes explotan una falla crítica de omisión de autorización

El día cero de Oracle PeopleSoft explotado por ShinyHunters eran tres fallas encadenadas

La vulnerabilidad CVE-2026-35273 en Oracle PeopleSoft PeopleTools 8.61 y 8.62 combina una falsificación de solicitudes del lado del servidor (SSRF, que obliga al servidor a hacer peticiones en nombre del atacante) con ejecución remota de código sin autenticación. El grupo de extorsión ShinyHunters la explotó, y Oracle ya publicó el parche. Universidades, entidades públicas y empresas colombianas que gestionan nómina o recursos humanos en PeopleSoft deben aplicarlo y revisar si hubo extracción de datos.

Ampliar información: Oracle PeopleSoft: el zero-day explotado por ShinyHunters eran tres fallas encadenadas

Falla de ejecución remota en WordPress Core 4.7 a 7.1.3 recibe casi 63.000 intentos de ataque en 24 horas

WordPress 7.1.4 corrige una falla de ejecución remota de código (RCE) causada por una condición de carrera, es decir, por dos operaciones que compiten en el tiempo. La falla afecta a Core desde la versión 4.7 hasta la 7.1.3. Wordfence bloqueó 62.969 intentos de ataque en 24 horas, lo que muestra un escaneo masivo. Cualquier pyme colombiana con su sitio en WordPress debe confirmar que está en la versión 7.1.4 y, si su proveedor de alojamiento gestiona las actualizaciones, pedirle constancia.

Ampliar información: Falla RCE en WordPress Core 4.7 a 7.1.3 recibe casi 63.000 intentos de ataque en 24 horas

Atacantes sondean la falla crítica CVE-2026-101767 en Oracle E-Business Suite días después del parche

Se detectaron intentos de explotación de CVE-2026-101767 (CVSS 9.8) en Oracle E-Business Suite pocos días después de publicado el parche. Se trata de una inyección SQL sin autenticación: el atacante manipula las consultas a la base de datos y puede llegar a ejecutar código en el servidor. Las empresas colombianas que manejan finanzas, compras o logística en E-Business Suite deben aplicar el parche y verificar que el sistema no esté publicado directamente en internet.

Ampliar información: Atacantes sondean falla crítica CVE-2026-101767 en Oracle E-Business Suite días después del parche

Atacantes explotan PHP2Shell en interfaces de gestión de Palo Alto Networks expuestas a internet

Palo Alto Networks confirmó la explotación activa de PHP2Shell, nombre que agrupa las vulnerabilidades CVE-2026-109618 y CVE-2026-109619 en PAN-OS, el sistema operativo de sus firewalls. Los ataques se dirigen a interfaces de gestión expuestas a internet, y el fabricante ya publicó parches y mitigaciones. Las organizaciones colombianas con firewalls Palo Alto deben retirar de internet la interfaz de gestión y aplicar los parches. Es también una buena ocasión para revisar que la gestión de cualquier firewall, de cualquier marca, sea accesible solo desde redes administrativas.

Ampliar información: Atacantes explotan PHP2Shell en interfaces de gestión de Palo Alto Networks expuestas a internet

ACCIÓN A SEGUIR

Cómo te acompaña nuestro SOC

1. Actualizar GitLab Community y Enterprise Edition a 19.2.8, 19.3.5 o 19.4.2 de inmediato, porque el plazo de CISA venció el 1 de noviembre de 2026; actualizar también el Ruby propio si se usa uno y rotar los secretos de CI/CD.
2. Aplicar de inmediato la corrección de Cisco para CVE-2026-76418 en ASA y FTD 9.16.x (plazo de CISA vencido el 1 de noviembre de 2026) y la de Ivanti Connect Secure 22.8R2.4 para CVE-2026-111357 (plazo vencido el 2 de noviembre de 2026); completar CVE-2026-118527 antes del 13 de noviembre de 2026.
3. Instalar de inmediato el kernel de Linux con el commit 3599e6b3cc1ada96883d496a50a210d3afbb6987 en servidores que terminan túneles IPsec, porque el plazo de CISA venció el 31 de octubre de 2026.
4. Actualizar de inmediato WordPress a 7.1.4 y aplicar los parches de PAN-OS para PHP2Shell, retirando de internet las interfaces de gestión, porque ambos casos tienen explotación activa.
5. Corregir Adobe Commerce y Magento (CVE-2026-48356, PolyShell) y actualizar Brotli a 1.0.10, 1.1.1 o 1.2.1 junto con las versiones corregidas de Node.js y PHP antes del 10 de noviembre de 2026.
6. Actualizar VMware ESXi a ESXi-9.1.0.0-25370933 o ESXi-9.0.2.0100-25595025 (y a 5.2.4 en la rama 5.x) antes del 11 de noviembre de 2026, y enviar los registros de vCenter y ESXi a un servidor externo.
7. Vigilar en Microsoft 365 los inicios de sesión por código de dispositivo, la reutilización de tokens desde IP o países distintos, los chats externos de Teams de supuesto soporte de TI seguidos de herramientas de acceso remoto y las conexiones de gestión inusuales en Cisco Catalyst SD-WAN.
8. El SOC acompaña la verificación de parches y la vigilancia de estas señales con monitoreo y respuesta gestionada (FortiGuard SOCaaS).

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.