

**BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC**



El impostor digital: XMRig se oculta tras la apariencia de Microsoft Edge

TLP:CLEAR
19.10.2026

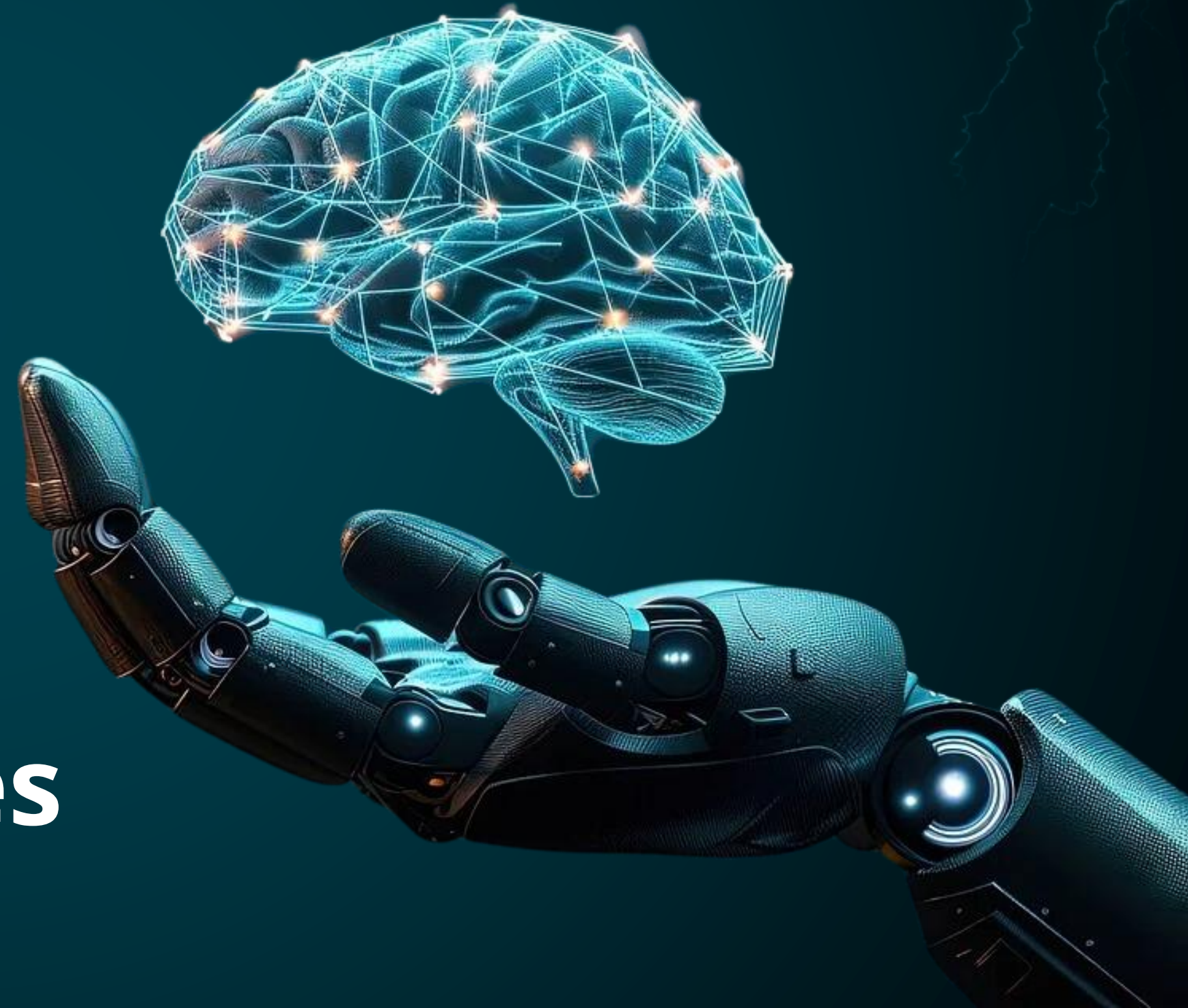
CLICK PARA
EMPEZAR



CONTENIDO



-  **Nuestra Esencia**
-  **Vulnerabilidades**
-  **Noticias**
-  **Recomendaciones**



NUESTRA ESENCIA



BOLETÍN CIBERSEGURIDAD

Este boletín está diseñado para mantener al lector informado y brindarle pautas de seguridad en un entorno digital en constante evolución. Incluye contenido sobre las últimas amenazas, vulnerabilidades y las mejores prácticas de protección.



EMPRESA

DataSec es una empresa colombiana líder en servicios tecnológicos, enfocada en la implementación, administración, soporte, monitoreo y gestión de plataformas de Seguridad Informática y Networking, con años de experiencia en proyectos de ciberseguridad y conectividad para diversos sectores.



SOC

DataSec cuenta con un Centro de Operaciones de Seguridad Cibernética (CSOC) especializado en la detección, análisis y respuesta a amenazas. Este centro opera de manera continua 24/7, contribuyendo a la prevención y mitigación de incidentes en tiempo real.



Cisco Nexus 3000 and 9000 Series Switches NGOAM Remote Code Execution Vulnerabilities

CVE-2026-76485 – CVE-2026-76486



Critical
(9.8)

Impacto: Ejecución remota de código y denegación de servicio (DoS).

Resumen: Se identificaron múltiples vulnerabilidades en la función NGOAM de Cisco NX-OS Software que permiten a un atacante remoto no autenticado ejecutar código arbitrario con privilegios root o provocar fallos en procesos y la recarga del dispositivo mediante el envío de paquetes IP especialmente diseñados a switches Cisco Nexus 3000 y 9000 Series vulnerables.

Producto Afectado

- Switches Cisco Nexus 3000 Series con Cisco.
- Switches Cisco Nexus 9000 Series con

[Ver +INFO.](#)

Solución:

Actualizar Cisco NX-OS Software a una versión corregida

[Ver + INFO.](#)

Fecha de Publicación: 07/OCT/2026 [+ INFO](#)



Microsoft Exchange Server Elevation of Privilege Vulnerability

CVE-2026-96940



High
(8.8)

Impacto: Elevación de privilegios e inyección de scripts.

Resumen: Se identificó una vulnerabilidad en Microsoft Exchange OWA que permite realizar ataques de inyección de contenido y engañar a los usuarios para obtener información sensible mediante enlaces maliciosos enviados por correo electrónico o aplicaciones de chat.

Producto Afectado

- Microsoft Exchange Server con Outlook Web Access (OWA) vulnerable.

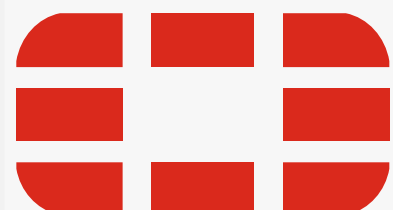
[Ver +INFO.](#)

Solución:

Instalar las actualizaciones de seguridad de Microsoft

[Ver +INFO.](#)

Fecha de Publicación: 08/OCT/2026 [+ INFO](#)



Fortinet FortiMail Arbitrary File Write Vulnerability

CVE-2026-104286



Critical
(9.8)

Impacto: Escritura arbitraria de archivos.

Resumen: Se identificó una vulnerabilidad en Fortinet FortiMail que permite a un atacante remoto no autenticado escribir archivos arbitrarios en el sistema subyacente mediante solicitudes HTTP o HTTPS especialmente diseñadas.

Producto Afectado

- Fortinet FortiMail 8.0.0 a 8.0.1.
- Fortinet FortiMail 7.6.0 a 7.6.6.
- Fortinet FortiMail 7.4.0 a 7.4.8.
- Fortinet FortiMail 7.2.0 a 7.2.9.

Ver +[INFO](#).

Solución:

Actualizar Fortinet FortiMail a una versión corregida que solucione la vulnerabilidad.

Ver +[INFO](#).

Fecha de Publicación: 07/OCT/2026



Tenable Identity Exposure Command Injection Vulnerability

CVE-2026-106126



Critical
(9.9)

Impacto: Ejecución arbitraria de comandos.

Resumen: Se identificó una vulnerabilidad en Tenable Identity Exposure (SaaS) que permite a un atacante autenticado con privilegios bajos ejecutar comandos arbitrarios como SYSTEM en el controlador de dominio principal (PDCe).

Producto Afectado

- Tenable Identity Exposure (SaaS), versiones anteriores a la 3.126.0.

Ver +[INFO](#).

Solución:

Actualizar Tenable Identity Exposure (SaaS) a la versión 3.126.0

Ver + [INFO](#).

Fecha de Publicación: 09/OCT/2026

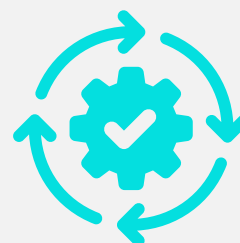




android

Android October 2026 Security Update

CVE-2026-28625 – CVE-2026-28640
CVE-2026-28641 – CVE-2026-28647



Google lanzó las actualizaciones de seguridad de Android de octubre de 2026, que corrigen 25 vulnerabilidades, incluidas siete críticas que podrían permitir la elevación de privilegios, ejecución remota de código y denegación de servicio. Google recomienda actualizar los dispositivos lo antes posible.

Recomendación:

- Aplicar oportunamente las actualizaciones de seguridad de Android correspondientes a octubre de 2026 para corregir las vulnerabilidades identificadas.

Productos Afectados

Algunos de los productos afectados son:

- Android Framework
- Android System
- Android Automotive

[Ver +INFO](#)

Fecha de Publicación: 05/OCT/2026



Google chrome releases

CVE-2026-106382 – CVE-2026-106197
CVE-2026-106358 – CVE-2026-106347



Google lanzó Chrome 155, una actualización de seguridad que corrige 247 vulnerabilidades, incluidas cuatro críticas y 53 de gravedad alta. Los fallos afectan a componentes como Chromecast, Navegador, Navegación y Seguimiento. Google recomienda actualizar el navegador lo antes posible.

Recomendación:

- Actualizar Google Chrome a la versión más reciente disponible.

Productos Afectados:

Los productos afectados son:

- Google Chrome para Windows
- Google Chrome para MacOS
- Google Chrome para Linux

[Ver +INFO](#)

Fecha de Publicación: 06/OCT/2026



LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
08/10/2026	CVE-2026-76471	Cisco	9.8	Cisco corrigió una vulnerabilidad en NX-API de Cisco NX-OS que permite a atacantes remotos no autenticados ejecutar código con privilegios root o provocar una denegación de servicio (DoS).
01/10/2026	CVE-2026-86950	Apple	8.8	Apple corrigió una vulnerabilidad de escritura fuera de límites que podría permitir la ejecución de código arbitrario al procesar archivos maliciosos. La compañía informó que el fallo pudo haber sido explotado en ataques dirigidos contra personas específicas.
07/10/2026	CVE-2026-106382	Google	9.6	Google corrigió una vulnerabilidad crítica de uso después de liberar memoria en Chromecast de Chrome, que permitía a un atacante remoto ejecutar código arbitrario fuera del sandbox mediante una página HTML maliciosa. La vulnerabilidad afecta a versiones anteriores a Chrome 155.0.8059.39.
06/10/2026	CVE-2026-63718	Apache	7.5	Apache corrigió una vulnerabilidad de contrabando de respuestas HTTP en el módulo `mod_proxy_uwsgi`, causada por una interpretación inconsistente de solicitudes HTTP. El fallo afecta a Apache HTTP Server desde la versión 2.4.30 hasta la 2.4.68.
07/10/2026	CVE-2026-20328	Cisco	9.1	Cisco identificó múltiples vulnerabilidades en Cisco License On-Prem que podrían permitir el acceso no autorizado, la exposición de información sensible, la elevación de privilegios y ataques de denegación de servicio (DoS). La compañía publicó actualizaciones de software para corregir los fallos.

El impostor digital: XMRig se oculta tras la apariencia de Microsoft Edge

Actores maliciosos están explotando dos vulnerabilidades en la utilidad de respaldo AhsayCBS para evadir la autenticación, ejecutar comandos remotamente y comprometer los sistemas afectados. Según Huntress, los ataques permiten desplegar web shells e instalar mineros de criptomonedas XMRig, disfrazados como Microsoft Edge, además de utilizar scripts de PowerShell para dificultar la detección.

La actividad maliciosa comenzó el 7 de octubre de 2026 y, al día siguiente, se habían identificado cinco organizaciones afectadas. Las vulnerabilidades CVE-2026-105133 y CVE-2026-105134 corresponden a fallos de autenticación e inyección de comandos, respectivamente, y también se reportó que la versión 10.3.4 de AhsayCBS podría seguir siendo vulnerable.

A continuación, compartimos IoC para ser agregados a las herramientas de seguridad perimetral. Ver [+INFO](#).

EL ATAQUE

El ataque contra AhsayCBS comienza mediante la explotación encadenada de dos vulnerabilidades que permiten eludir la autenticación y ejecutar comandos arbitrarios de forma remota en los sistemas afectados.

Una vez obtenido el acceso, los atacantes realizan tareas de reconocimiento, despliegan web shells para mantener el control del sistema e instalan mineros de criptomonedas XMRig, camuflados como el proceso legítimo `edge.exe` de Microsoft Edge.

Además, utilizan un script de PowerShell que supervisa el Administrador de tareas de Windows y lo cierra para dificultar la detección de la actividad minera. En algunos incidentes, también se identificó la descarga de un controlador vulnerable mediante `certutil.exe`, posiblemente para obtener acceso a nivel de núcleo y optimizar la minería.

CONTEXT	INDICATOR	(MD5)
SHA256	481728a7c9c4c02be07051d9c1958d902ea6397ebb8952ab83944818e3d25d21	a06d4672f6f95852dda532701d17d669
SHA256	4dcb0202fe8b2d4d7b183764e38184cd6ed50132786cc7e7d1f7f4bce1dd6f3d	c78d9355b8b1a4bd64ca09b56e24998c
IPv4	104[.]234[.]26[.]10	N/A
IPv4	123[.]202[.]208[.]37	N/A
IPv4	177[.]4[.]12[.]11	N/A
IPv4	185[.]220[.]236[.]49	N/A
IPv4	38[.]60[.]252[.]110	N/A



IOC

+ INFO



ÚLTIMAS NOTICIAS

Warlock explota SharePoint para desplegar ransomware

Warlock explota vulnerabilidades en Microsoft SharePoint para infiltrarse en organizaciones de infraestructuras críticas, gobiernos y universidades de países de habla hispana y portuguesa. El ataque permite ejecutar código malicioso, desactivar herramientas de seguridad, acceder a redes corporativas y desplegar ransomware a gran escala mediante técnicas avanzadas de evasión. Se recomienda actualizar SharePoint, aplicar los parches de seguridad y reforzar la monitorización de la red para prevenir intrusiones y proteger los sistemas comprometidos.

[+ INFO](#)

FortiBleed compromete 86.000 cortafuegos

FortiBleed compromete más de 86.644 dispositivos FortiGate en 194 países mediante el uso de credenciales robadas y contraseñas débiles. Los atacantes crean cuentas de administrador para mantener el acceso, bloquean a las organizaciones de sus propios dispositivos y venden accesos a grupos de ransomware, facilitando futuras intrusiones y el cifrado de redes corporativas. Se recomienda restringir la administración remota, cambiar contraseñas, activar la autenticación multifactor (MFA) y reforzar el almacenamiento seguro de credenciales.

[+ INFO](#)

La contraseña 123456 expone 8,8 millones de registros

Una contraseña de administrador débil, 123456, habría permitido a un atacante aprovechar el acceso autorizado de la empresa danesa Pays al Registro Central de Personas (CPR) y extraer cerca de 8,8 millones de registros personales. La información expuesta incluye números de identificación y direcciones de personas vivas y fallecidas. El incidente evidencia los riesgos de las credenciales inseguras y la falta de controles sobre accesos a datos sensibles. Se recomienda utilizar contraseñas robustas, activar la autenticación multifactor y supervisar las consultas masivas para prevenir filtraciones similares.

[+ INFO](#)

El factor humano: el objetivo favorito de los atacantes

En ciberseguridad, contar con certificaciones y conocimientos técnicos es fundamental para identificar vulnerabilidades y proteger sistemas. Sin embargo, incluso los profesionales más preparados pueden convertirse en víctimas de la ingeniería social, una técnica que explota la confianza, las emociones y los errores humanos para obtener información confidencial o conseguir accesos no autorizados.

🎭 Verifica antes de confiar: los atacantes pueden hacerse pasar por compañeros, directivos o personal de soporte técnico.

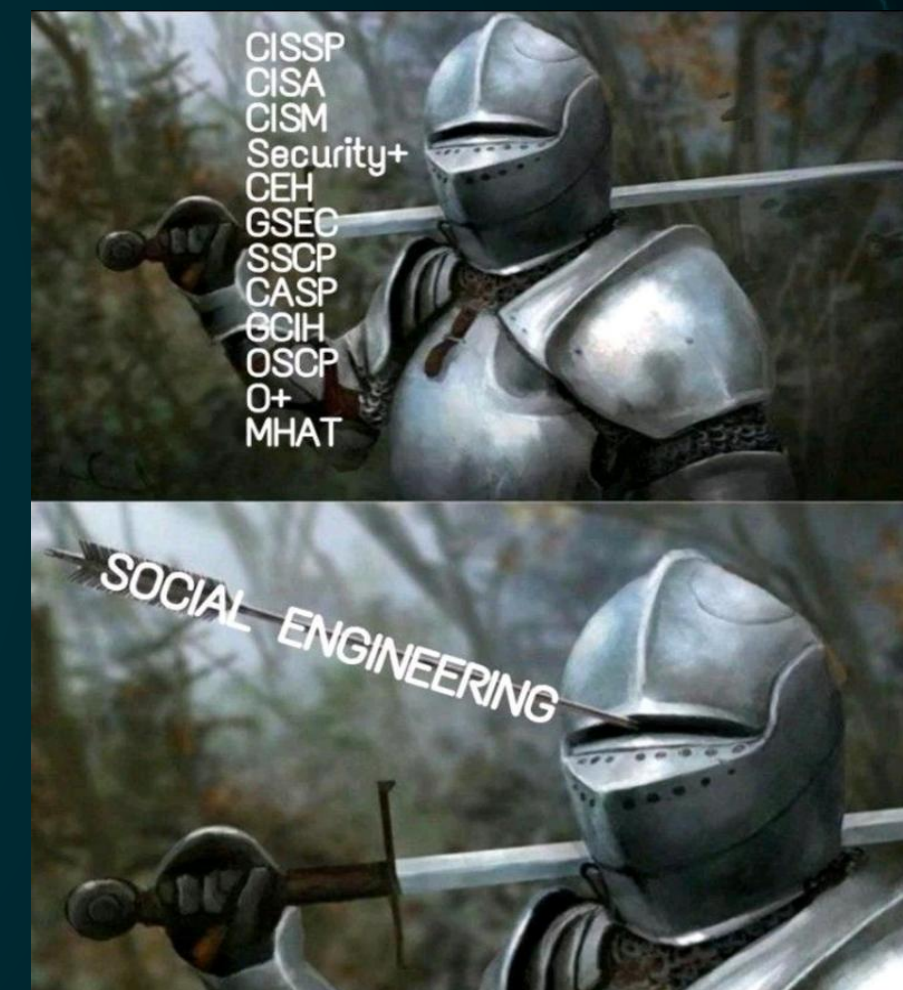
📁 Verifica las solicitudes inusuales: especialmente aquellas que exigen contraseñas, códigos de autenticación o información sensible.

🧠 Reconoce las señales de alerta: la urgencia, el miedo, la presión y las ofertas demasiado buenas para ser verdad son tácticas frecuentes.

🔒 Aplica los protocolos de seguridad: nunca omitas los procedimientos de verificación, aunque la solicitud parezca provenir de una persona de confianza.

🚨 Reporta cualquier intento sospechoso: informar a tiempo puede evitar que un engaño afecte a toda la organización.

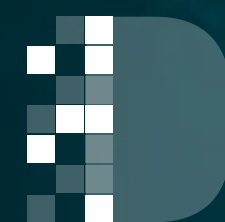
El eslabón más atacado no siempre es una máquina: muchas veces es la confianza humana.





ISO/IEC 27001 • ISO/IEC 20000-1

LL-C (Certification)



DataSec



CYBERSOCDTS



csirt_datasec@datasec.com.co



+57 310 315 9346 Ext. 4



© 2025 DataSec SAS. Todos los Derechos Reservados
CYBERSOCDTS by DataSec