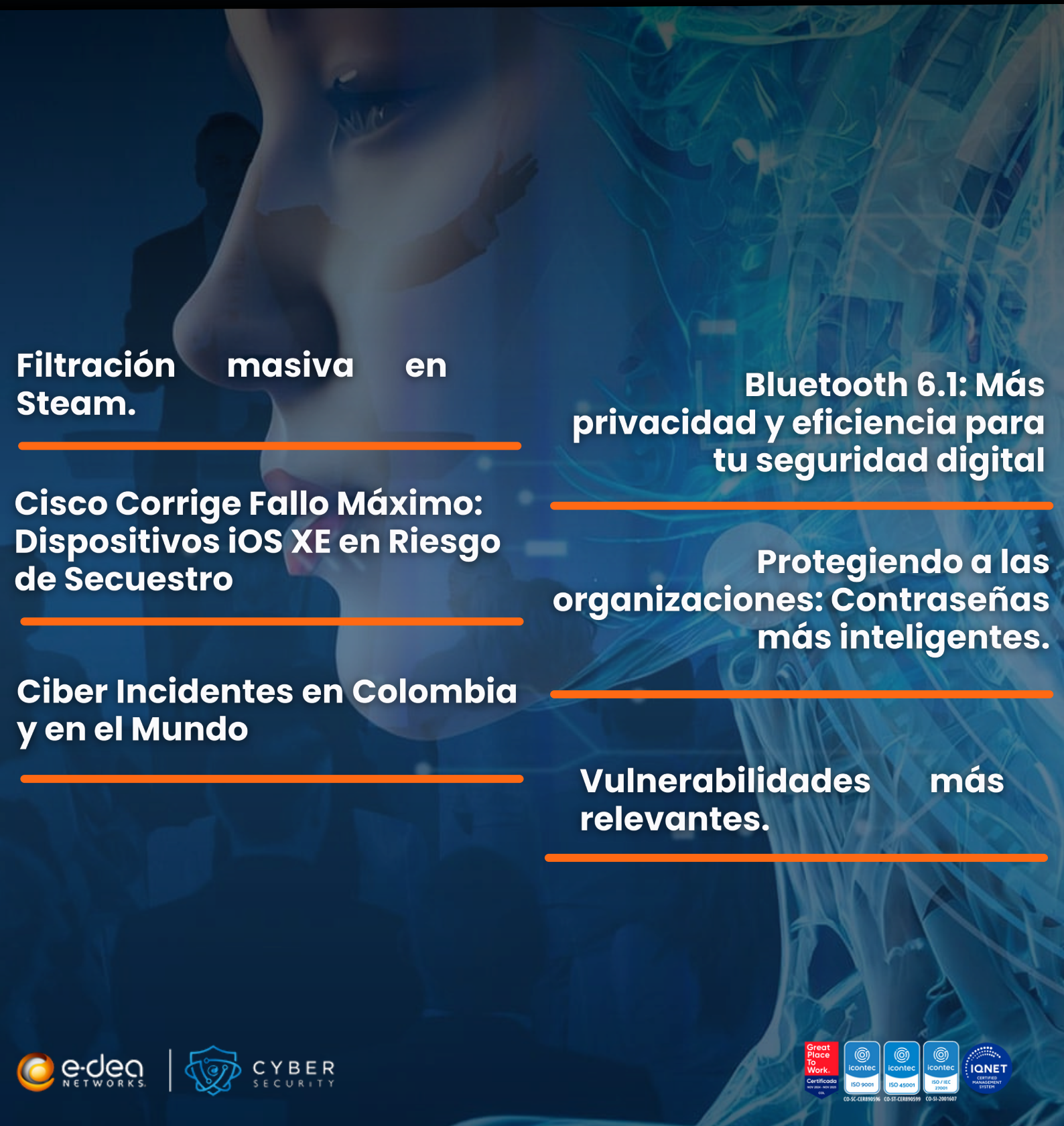
CIBER E-DEA

Boletín de Seguridad



Filtración masiva en Steam.

Cisco Corrige Fallo Máximo: Dispositivos iOS XE en Riesgo de Secuestro

Ciber Incidentes en Colombia y en el Mundo

Bluetooth 6.1: Más privacidad y eficiencia para tu seguridad digital

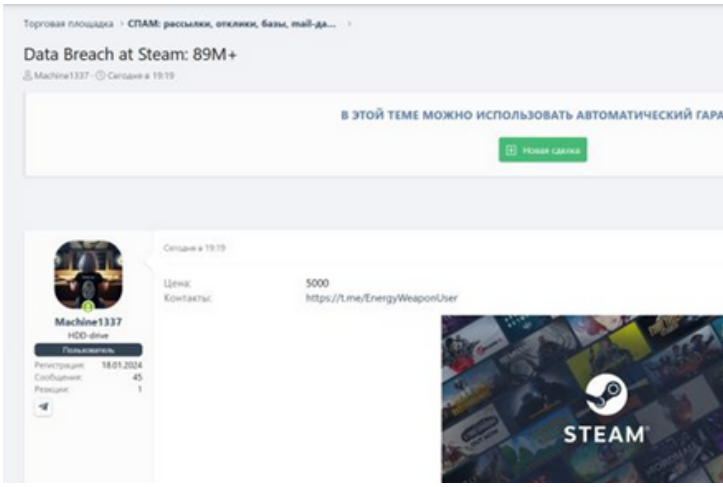
Protegiendo a las organizaciones: Contraseñas más inteligentes.

Vulnerabilidades más relevantes.

Filtración Masiva en Steam pone en riesgo 89 millones de cuentas.

En los últimos días, la comunidad de jugadores ha estado en alerta debido a la advertencia sobre una posible filtración masiva que afecta a más de 89 millones de cuentas de usuarios de Steam, una de las plataformas de videojuegos más importantes a nivel mundial.

La empresa de ciberseguridad israelí Underdark.ai fue la primera en revelar la magnitud de la brecha de seguridad el pasado 11 de mayo donde se indicaba que un hacker identificado como Machine1337 ofreció una base de datos por 5,000 dólares en un foro de la dark web.



Datos filtrados:

- Números de teléfono de usuarios de Steam.
- Mensajes SMS con códigos de autenticación de dos factores (2FA) enviados por Steam.
- Registros históricos de autenticación.

En que consistió la filtración?

La filtración consistió en mensajes de texto antiguos que incluían códigos de un solo uso, válidos durante un período de 15 minutos.

Recomendaciones:

- Cambiar la contraseña.
- Activar Steam Guard desde la app móvil.
- Revisar la actividad reciente en la cuenta y desconectar cualquier dispositivo no reconocido.
- Mantenerse alerta ante intentos de phishing disfrazados de promociones, regalos o mensajes de soporte técnico.
- Eliminar temporalmente los métodos de pago vinculados en la cuenta.

Más información

Cisco corrige fallo de Dispositivos iOS XE en riesgo de secuestro.

Una nueva alerta de seguridad de Cisco ha encendido las alarmas: una falla de máxima gravedad en iOS XE permite a los atacantes secuestrar dispositivos.Esta vulnerabilidad, identificada como CVE-2025-20188, ostenta una puntuación CVSS máxima de 10.0, lo que significa que un atacante puede comprometer completamente tus dispositivos.

Cisco menciona que "un atacante podría explotar esta vulnerabilidad enviando solicitudes HTTPS manipuladas a la interfaz de descarga de imágenes de AP. Una explotación exitosa podría permitir al atacante cargar archivos, atravesar rutas y ejecutar comandos arbitrarios con privilegios de root".
Aunque está deshabilitada por defecto, algunas implementaciones empresariales a gran escala o automatizadas pueden habilitarla para aprovisionar o recuperar los AP más rápidamente.

Esta vulnerabilidad es solo es explotable cuando la función «Descarga de imágenes de AP fuera de banda» está habilitada en el dispositivo, lo cual no está habilitado por defecto. Esta función permite a los puntos de acceso (AP) descargar imágenes del sistema operativo mediante HTTPS en lugar del protocolo CAPWAP.

Los siguientes dispositivos son vulnerables a ataques si se cumplen los requisitos de explotación:

- **Controlador inalámbrico Catalyst 9800-CL para la nube**
- **Controlador inalámbrico integrado Catalyst 9800 para switches de las series Catalyst 9300, 9400 y 9500**
- **Controladores inalámbricos de la serie Catalyst 9800**

Controlador inalámbrico integrado en puntos de acceso Catalyst
Por otro lado, los productos que se ha confirmado que no se ven afectados por el problema de JWT codificado son: Cisco IOS (no XE), Cisco IOS XR, productos Cisco Meraki, Cisco NX-OS y WLC basados en Cisco AireOS.

Más información

Bluetooth 6.1: Más privacidad, eficiencia y ciclos de innovación más rápidos

El lanzamiento de Bluetooth® Core 6.1 no solo representa un salto técnico, sino también un avance importante desde la perspectiva de la ciberseguridad y la protección de la privacidad del usuario.

Al introducir una aleatorización en las actualizaciones de RPA, se fortalece la defensa contra técnicas de rastreo y correlación de actividad que podrían comprometer la identidad o ubicación del usuario.

Esta medida es especialmente relevante en un entorno donde el uso masivo de dispositivos IoT y wearables puede exponer información personal sin que el usuario lo perciba.
Desde un enfoque de gestión de riesgos, es positivo ver cómo los estándares tecnológicos integran de forma nativa mejoras de privacidad y eficiencia, en lugar de dejarlas como añadidos opcionales.

En términos de privacidad y seguridad una de las principales actualizaciones es la aleatorización de las actualizaciones de direcciones privadas resolubles (RPA), que reemplazan a las direcciones MAC fijas de los dispositivos.

Esto hace que sea más difícil rastrear y seguir los dispositivos a lo largo del tiempo.

Sin embargo, como con cualquier tecnología, siempre existen riesgos potenciales. Aunque Bluetooth 6.1 ha mejorado la seguridad, es importante seguir buenas prácticas de ciberseguridad, cómo mantener los dispositivos actualizados y ser cauteloso con las conexiones desconocidas.

Más información

Protegiendo a las organizaciones: Contraseñas más inteligentes.

La necesidad de equilibrar seguridad y facilidad de uso en la gestión de contraseñas. Aunque las políticas tradicionales buscaban proteger, muchas se han vuelto obsoletas y contraproducentes, generando frustración y riesgos de seguridad.

Históricamente, las contraseñas evolucionaron de ser simples a complejas, pero esto llevó a patrones predecibles que los hackers explotan fácilmente. Además, prácticas como el cambio periódico de contraseñas resultaron ineficaces y molestos para los usuarios.

Casos recientes como las filtraciones de Powerschool y Obamacare demuestran las consecuencias de prácticas inseguras. Por ello, se promueve una modernización basada en los estándares del NIST, recomienda:

- **Eliminar los cambios periódicos innecesarios,**
- **Usar frases de contraseña memorables,**
- **Fomentar el uso de gestores de contraseñas.**

Además, se subraya la importancia de la autenticación multifactor (MFA) como una capa adicional de seguridad, combinando contraseñas con biometría o dispositivos físicos, lo que refuerza la protección ante accesos no autorizados.

La protección efectiva no depende de complicar las contraseñas, sino de adoptar soluciones más inteligentes, seguras y amigables para los usuarios.

¿Crees que tus credenciales están expuestas en la dark web?

Compruébalo gratis, aquí.

Vulnerabilidades destacadas

CVE-2025-22252

Esta vulnerabilidad permite que un atacante con conocimiento de credenciales admin acceda sin autenticación a sistemas FortiOS, FortiProxy y FortiSwitchManager.

La severidad es alta (9.0), y la solución recomendada es actualizar a las versiones parcheadas inmediatamente.

Fortinet

Versiones afectadas

FortiOS, FortiProxy y FortiSwitchManager

CVE-2025-32701

Microsoft

Versiones afectadas

Sistema de archivos de registro común de Windows.

Se trata de una vulnerabilidad de uso después de la liberación que, si se explota con éxito, podría permitir a un atacante elevar privilegios en el sistema afectado.

CVE-2025-41225

Una vulnerabilidad de ejecución de comandos autenticada donde un actor malintencionado con privilegios para crear o modificar alarmas y ejecutar acciones de script.

VmWare

Versiones afectadas

vCenter Server

Ciber incidentes en Colombia y en el mundo

Incidente cibernético en la Autoridad Nacional de Acuicultura y Pesca (AUNAP)

El 13 de mayo de 2025, la Autoridad Nacional de Acuicultura y Pesca (AUNAP) reportó un ciber incidente significativo en su página oficial de Facebook.

Aunque no se dieron detalles exhaustivos, se mencionó enfáticamente limitar el uso del sitio web: www.aunab.gov.co y tampoco hacer clic en los sitios provenientes del mismo.

Datos comprometidos: Información confidencial como licencias de pesca y registros de embarcaciones podrían haber sido accesibles de manera no autorizada.

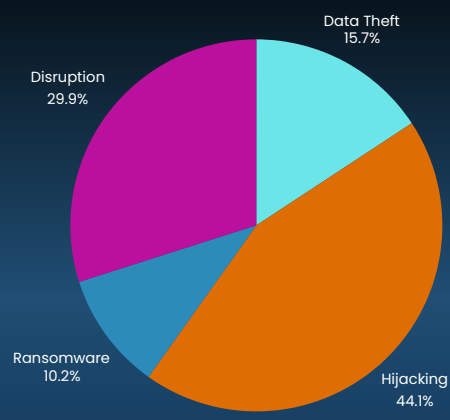
Servicios afectados: La capacidad de AUNAP para emitir permisos, supervisar actividades y registros podría verse comprometida, afectando a las comunidades pesqueras del país.

Más información

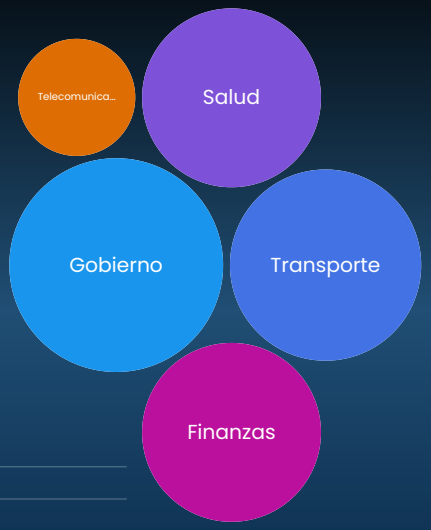
El mundo

60
Ciber incidentes

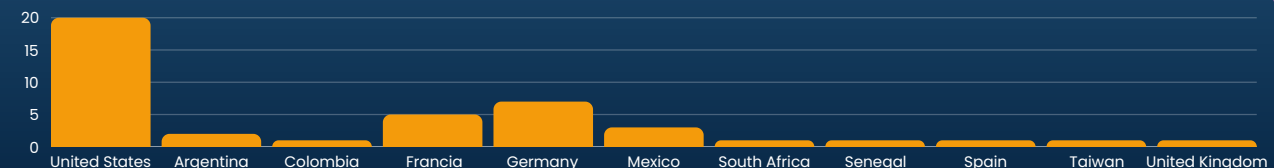
TIPO DE INCIDENTE



SECTORES AFECTADOS



PAISES ATACADOS



Más información

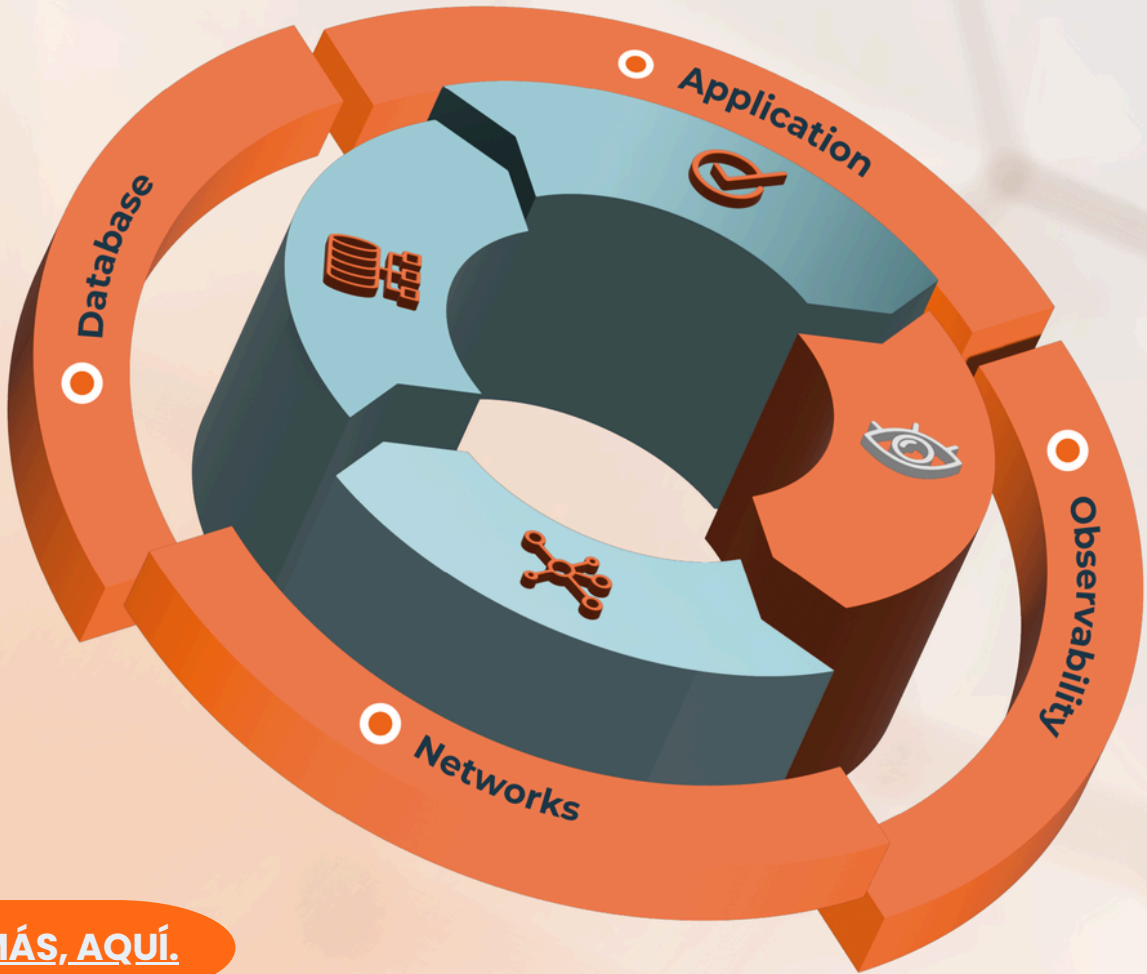
59ª Convención Bancaria
La voz de Colombia

e-dea NETWORKS. | SOLARWINDS Elite Partner | Aso Ban Caria

Database Observability

Junio 4, 5 y 6 | Stand 24

Centro de Convenciones, Cartagena de Indias



CONOCE MÁS, AQUÍ.

CYBER SECURITY

e-dea NETWORKS

CIBER E-DEA

Boletín de Seguridad

E-dea Networks

@e_deanetworks

E-dea Networks

Csirt E-dea

e-dea.co