CSIRTAmericas:

Comunidad que transita del intercambio de amenazas al conocimiento compartido

OEA | CICTE

Comité Interamericano contra el Terrorismo
Secretaría de Seguridad Multidimensional
www.oas.org/ext/es/seguridad/prog-ciber

OEA | CICTE

Escenario actual

Hospitales

Filtración de más de 100 mil registros de pacientes en hospital

Empresas

Robo de 11 millones de credenciales de tarjeta de crédito

Sector militar

Logran robar 6 Terabytes de información confidencial

Escenario actual

Las **fugas de información** en su mayoría provienen de

Exploits

- Gitconfig
- Moodle
- Exchange
- Sharepoint

Credenciales expuestas

- 12345678
- Urosario1
- 1111
- 12345

Fuente: Mandiant 2024 & CSIRTAmericas

OEA | CICTE

Escenario actual

Una fuga de información promedio toma

48 minutos

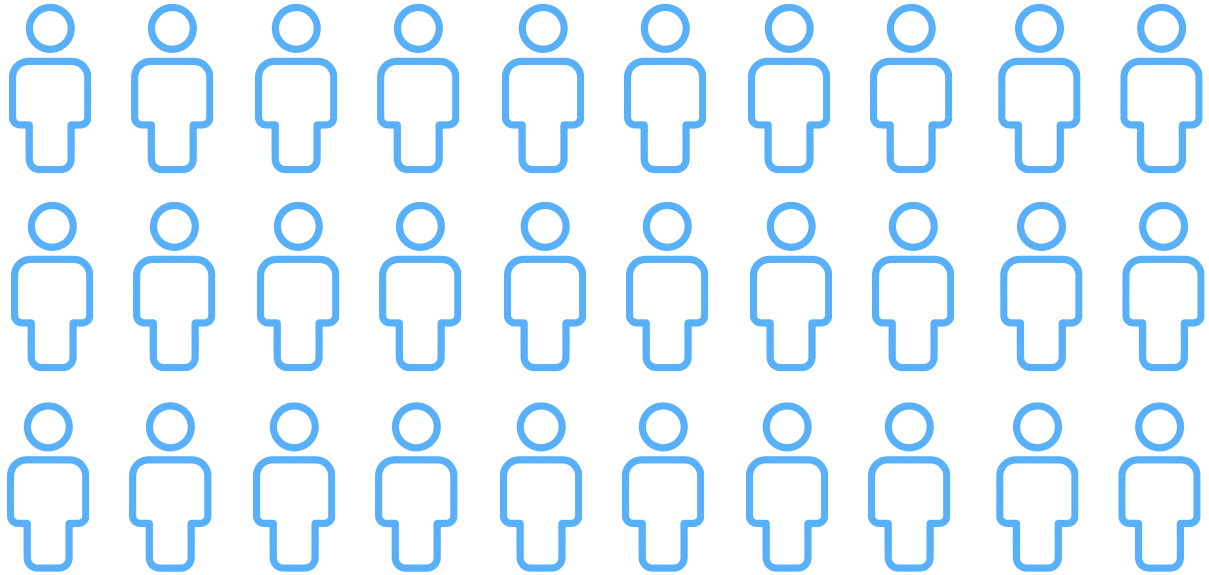
Explotación inicial

Fuga de información

Source: https://www.crowdstrike.com/

OEA | CICTE

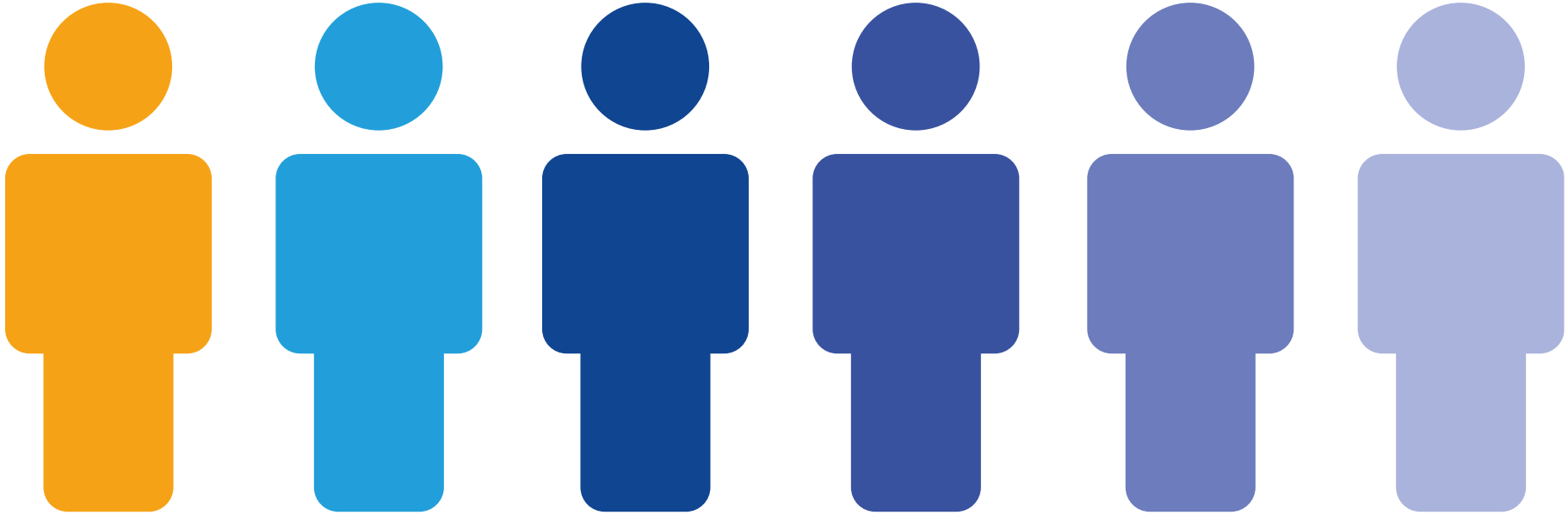
Escenario actual



50 Personas conforman grupos criminales de **Ransomware**
(Promedio)

Source: conti leaks https://cyberint.com/blog/research/contileaks/

Nuestra realidad



6 Miembros por CSIRT
mediana regional

Source: CSIRTAmericas.org (Incluye solo CSIRTs nacionales)

¿Qué hacemos ante este escenario?

Compartir

¿Qué estamos haciendo en la OEA para fomentar el intercambio de información?

CSIRTAmericas

Comunidad regional impulsada por la OEA que conecta y fortalece a los (**CSIRTs) gubernamentales** mediante preparación, intercambio de información y colaboración, para una región más segura para las personas, los servicios y las instituciones de los **Estados Miembros.**

¿Qué es un CSIRT?

(Equipo de Respuesta ante Incidentes de ciberseguridad)

Grupo técnico que ayuda a identificar y enfrentar amenazas cibernéticas que pueden afectar la operación de instituciones de un sector.

Miembros de la red CSIRTAmericas

- Argentina (7)
- Barbados (1)
- Bolivia (1)
- Brasil (1)
- Canadá (1)
- Chile (3)
- Colombia (8)
- Costa Rica (1)
- República Dominicana (3)
- Ecuador (4)
- Guatemala (2)
- Guyana (1)
- Jamaica (1)
- Bahamas (1)
- México (3)
- Panamá (1)
- Perú (7)
- Paraguay (1)
- Suriname (1)
- Trinidad & Tobago (1)
- Estados Unidos(1)
- Uruguay (2)

508 Especialistas

52 CSIRTs

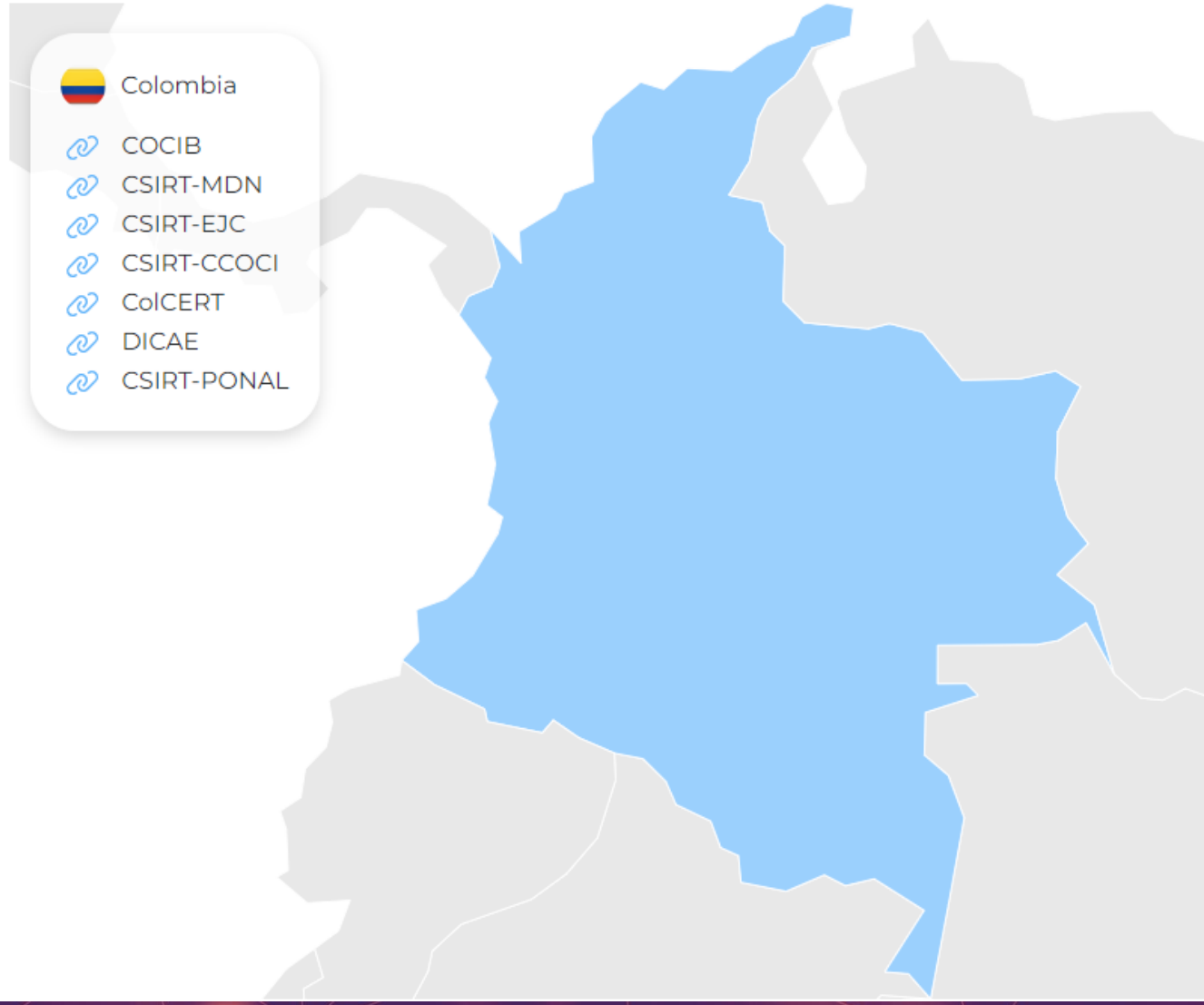
22 Países

8

CSIRTs

de Colombia forman parte de la red

csirtamericas.org



OEA | CICTE

CSIRTAmericas Network

¿Cómo apoyamos a los CSIRTs?

www.csirtamericas.org

Compartimos

Información sobre amenazas cibernéticas

Para anticipar y apoyar a la protección de servicios esenciales

OEA | CICTE

CSIRTAmericas Network

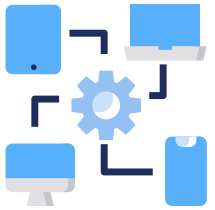
OEA | CICTE CSIRTAmericas Network

Información sobre amenazas cibernéticas

Brindamos a cada **Estado Miembro** información **estructurada** sobre amenazas cibernéticas (Feeds)

Sitios comprometidos

Correos electrónicos comprometidos



Sistemas vulnerables críticos

Distribución de malware

Fugas de credenciales

Divulgación de ransomware

Lo que compartimos con los CSIRTs de Colombia

Sitios comprometidos	Correos comprometidos	Fuga de credenciales	Vulnerabilidades críticas	Alertas de Ransomware
612	54k	265k	3.312	33

📌 Source: CSIRTAmericas data.
Date: 04/Aug/2025 17:41:28 UTC.

¿Cómo distribuye CSIRTAmericas información 24/7?

OEA | CICTE

CSIRTAmericas Network

OEA | CICTE CSIRTAmericas Network

¿Cómo lo hace CSIRTAmericas?

Información accionable

(Compartimos lo que sirve)

Taxonomía de incidentes

(Clasificamos)

Traffic light protocol (TLP)

(Decidimos a quién compartir)

Proveedores

(De quién recibimos)

Infraestructura de intercambio

(Distribución automatizada)

OEA CICTE CSIRTAmericas Network

Información accionable

(Compartimos lo que sirve)

Taxonomía de incidentes

(Clasificamos)

Traffic light protocol (TLP)

(Decidimos a quién compartir)

Proveedores

(De quién recibimos)

Infraestructura de intercambio

(Distribución automatizada)

Compartimos lo que sirve
Información accionable

Relevante	Importante para quien lo recibe
Oportuna	¿Me sirve información de hace 2 meses?
Precisa	Información que es verdadera
Completa	¿Me pasas una cuenta de correo, y no las cabeceras?
Procesable	Fácil de procesar en nuestros sistemas

Source: ENISA - https://www.enisa.europa.eu/publications/actionable-information-for-security

No Accionable

“Alerta, Alerta Me llegó esto por **WhatsApp:** ‘Cuidado, están robando cuentas bancarias con un **virus** nuevo que se **activa** si abres un correo con asunto "Confirmación de transferencia". ¡No lo abras!’

Accionable

Campaña de phishing activa detectada: dominio **hxxps://bancomx-cliente[.]com**, suplantando al **Banco X**. El correo simula una confirmación de transferencia. **IOC disponible (adjunto),** ya está en **listas negras(link).** Recomendamos bloqueo y alerta a usuarios del sector financiero." [**TLP:AMBER** | Fuente: **CSIRT XXX** | **Fecha: 04/08/2025**]

OEA | CICTE | CSIRTAmericas Network

Información accionable

(Compartimos lo que sirve)

Taxonomía de incidentes

(Clasificamos)

Traffic light protocol (TLP)

(Decidimos a quién compartir)

Proveedores

(De quién recibimos)

Infraestructura de intercambio

(Distribución automatizada)

OEA | CICTE | CSIRTAmericas Network

Clasificamos lo que compartimos

Taxonomía regional de incidentes CSIRTAmericas

- Defacement
- Malware
- DDOS
- Phishing
- SPAM
- Botnet
- Fastflux
- Cryptojacking
- XSS
- SQLi
- Vulnerability
- infoleak
- Compromise
- Other

De uso público

Github.com/MISP

OEA | CICTE | CSIRTAmericas Network

Información accionable

(Compartimos lo que sirve)

Taxonomía de incidentes

(Clasificamos)

Traffic light protocol (TLP)

(Decidimos a quién compartir)

Proveedores

(De quién recibimos)

Infraestructura de intercambio

(Distribución automatizada)

OEA | CICTE

Decidimos con quién se puede compartir una información sensible

Traffic light protocol (TLP)

TLP:RED	Unicamente oidos y ojos del destinatario individual
TLP:AMBER+STRICT	Divulgación limitada, solo para participantes de una organización
TLP:AMBER	Divulgación limitada, para participantes de una organización y sus clientes
TLP: GREEN	Divulgación limitada, puede difundir a su comunidad
TLP: CLEAR	Divulgación a todo el mundo

Source: https://www.first.org/tlp/

OEA | CICTE | CSIRTAmericas Network

Información accionable

(Compartimos lo que sirve)

Taxonomía de incidentes

(Clasificamos)

Traffic light protocol (TLP)

(Decidimos a quién compartir)

Proveedores

(De quién recibimos)

Infraestructura de intercambio

(Distribución automatizada)

¿De dónde viene lo que compartimos?

Principales proveedores

Publicwww	*Código web expuesto*
Shodan	*Dispositivos expuestos*
Abusix	*IPs maliciosas*
Zone-h	*webs comprometidos*
Phishtank	*Urls phishing*
Microsoft	*C&C*
Intelx	*Buscador de leaks*
LeakIX	*Sistemas expuestos*
Falconfeeds	*Actividades en la darkweb*
CISCO	*Campañas maliciosas*

OEA | CICTE | CSIRTAmericas Network

Información accionable

(Compartimos lo que sirve)

Taxonomía de incidentes

(Clasificamos)

Traffic light protocol (TLP)

(Decidimos a quién compartir)

Proveedores

(De quién recibimos)

Infraestructura de intercambio

(Distribución automatizada)

CSIRTAmericas Network | OEA CICTE

Infra que hace que la información llegue a todos

OEA | CICTE CSIRTAmericas Network

Así reciben la información los CSIRTs

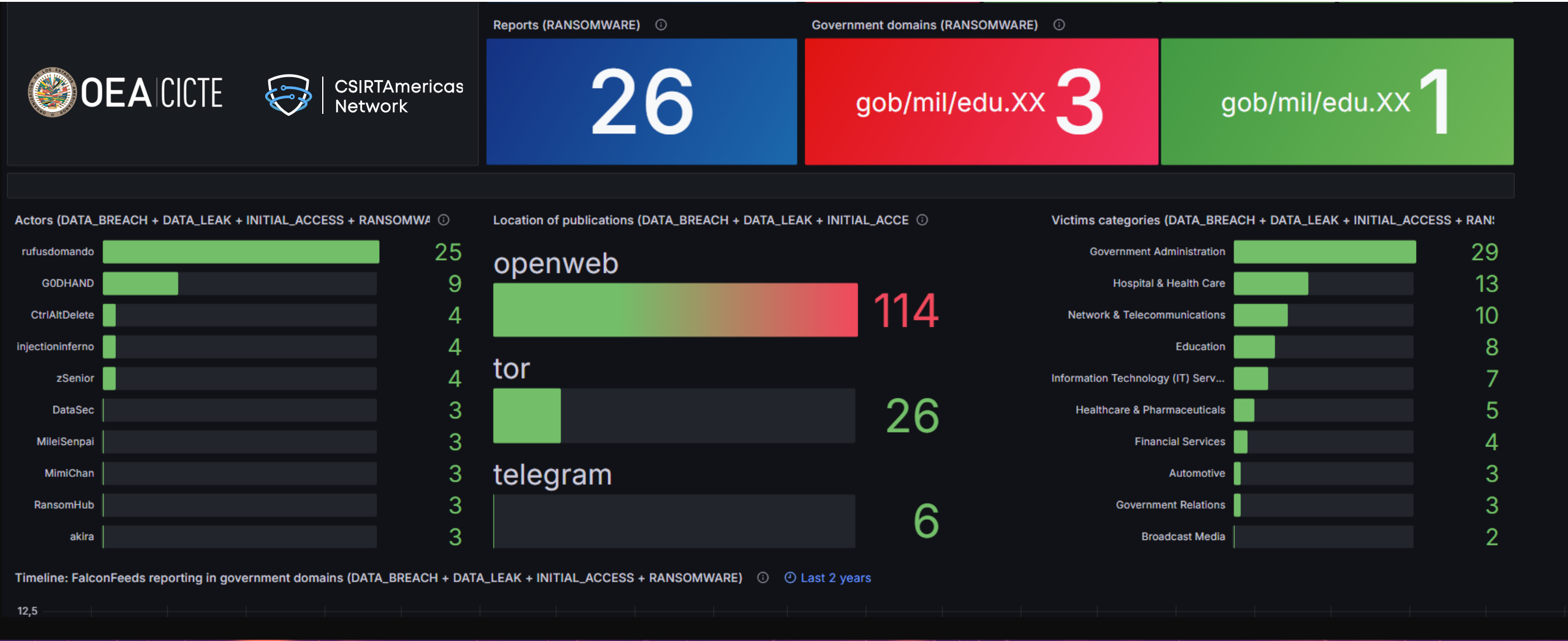
Entregamos la misma información, adaptada a cada perfil

Acceso automatizado a datos de amenazas

Tableros para la toma de decisiones

Reporte para altas autoridades

Información a la medida



Información a la medida

Informe automático para Altas Autoridades

Más de 265,000 de contraseñas filtradas, y **30.074** son de **organismos del Estado**

54,000 correos expuestos, con más de **2400** vinculados a **instituciones públicas** y **educativas**

3.312 sistemas con vulnerabilidades críticas, con riesgos para **agua**, **luz** y **aeropuertos**

📌 Source: CSIRTAmericas data - Colombia.
📅 Date: 04/aug/2025 18:55:44 UTC.

Comunicación ágil

OEA | CICTE | CSIRTAmericas Network

Lo que aún tenemos por construir

OEA | CICTE

CSIRTAmericas Network

Lo que aún tenemos por construir

- Documentar aprendizajes: lecciones útiles tras cada incidente
- Memoria técnica regional: tener una biblioteca viva (herramientas, alianzas, campañas)
- **Fomentar una cultura activa de compartir:** no es solo tener la opción de compartir, sino hacerlo parte de nuestro día a día

Fomentar una cultura activa de compartir

Guía de MISP para facilitar colaboración y el intercambio de información sobre amenazas cibernéticas .

(*MISP es una Plataforma de Código Abierto utilizadas por equipos de Ciberseguridad para compartod datos de amenazas y responder más rapido ane ataques)*

SPANISH

ENGLISH

csirtamericas.org/es/resources


OAS CICTE
“El conocimiento solo crece cuando se comparte”

Thank you!
Merci
Gracias
Obrigado

Suscríbete a nuestra lista de correo

X (Twitter)

@OEA_Cyber

Comité Interamericano contra el Terrorismo
Secretaría de Seguridad Multidimensional
www.oas.org/ext/es/seguridad/prog-ciber