



BIENVENIDA

Fernanda Ruíz
Channel Marketing



SECURITY
DAYS 2024

MEDIA SPONSORS 2024

REGIONALES



Prensario
TI Latin America



MEDIA SPONSORS 2024



AGENDA

| | |
|-----------------|--|
| 09:20 HS | Protección de datos, el nuevo oro del siglo 21 |
| 10:07 HS | Protección de datos: Resguardando el oro corporativo |
| 10:50 HS | Break |
| 11:05 HS | Leyes de protección de datos: un aliado más que un enemigo |
| 11:50 HS | La cultura de ciberseguridad la construimos entre todos |
| 12:20 HS | Preguntas |
| 12:40 HS | Sorteo Cierre de evento Networking |



iSorteo!



**ESCANEAR CÓDIGO QR
COMPARTIDO**



**INFORMAR CÓDIGO
EN LA MESA DE
ACREDITACIÓN**



CÓDIGO QR VIRTUAL



Gracias.



**SECURITY
DAYS2024**





Luis Vázquez

Country Manager de ESET México





CÓDIGO QR VIRTUAL





David González

*Security Researcher | Informática forense | M. En I.
Seguridad informática | Vulnerability Management*

ESET México



Protección de datos

El nuevo oro del siglo 21

David González C.

*Security Researcher | Informática forense | M. En I.
Seguridad informática | Vulnerability Management*



SECURITY
DAYS 2024

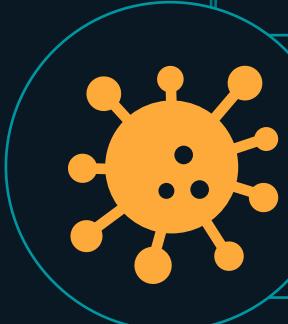
PRIVACIDAD

Panorama y tendencias legislativas sobre la Protección de Datos en Países de LATAM

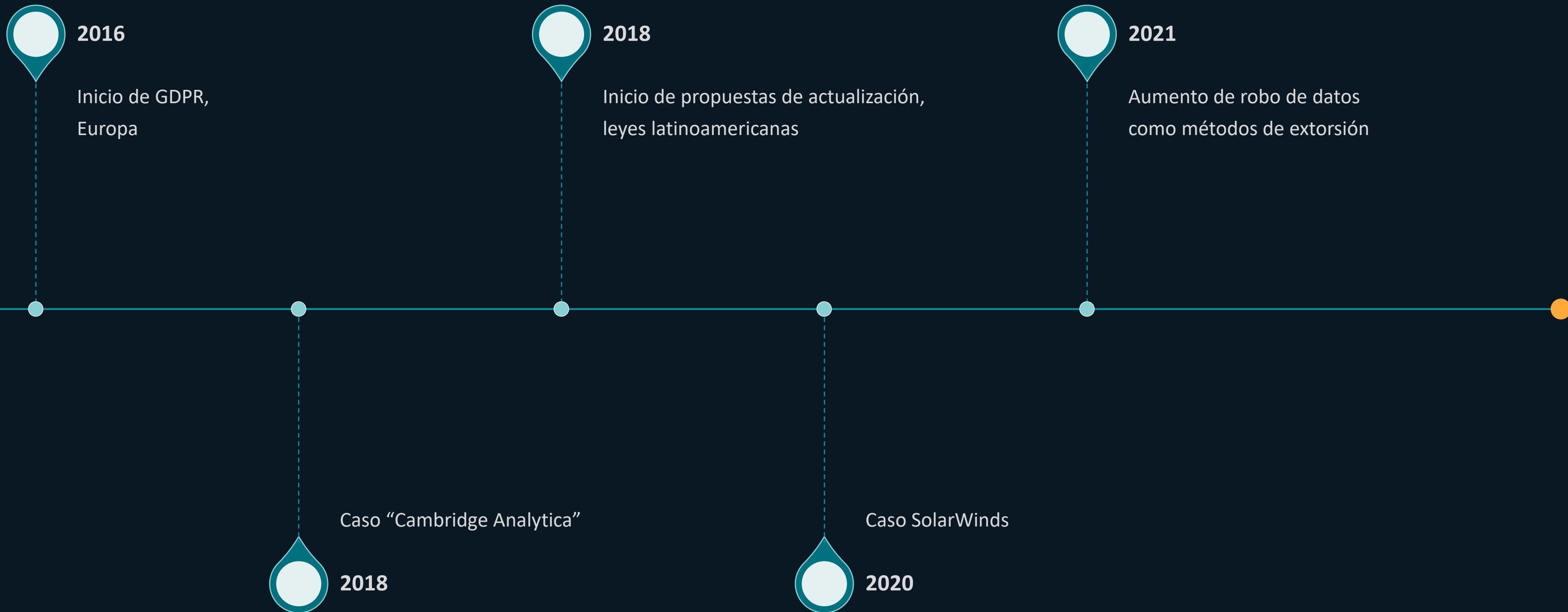
En muchos de los estados de Latinoamérica, las normativas relativas a la protección de datos personales son antiguas y varios países buscan actualizarse. Repasamos cuál es la situación en Argentina, Chile, Colombia, Ecuador y México.



Fabiana Ramírez Cuenca

-  Gobiernos con mayores motivaciones producen actualizaciones escalonadas
-  Avance tecnológico provoca rápidamente que el alcance de las leyes no sea suficiente
-  Organizaciones sufren ciberataques que mutan constantemente: Ransomware, robo de información, espionaje
-  Cibercrimen pone el foco en la monetización de información como fuente de dinero





Orígenes



Ransomware y
extorsión



Colaborador
descontento



Configuraciones
inseguras



Espionaje y
Campañas

Python, ZeroLogon y Telegram

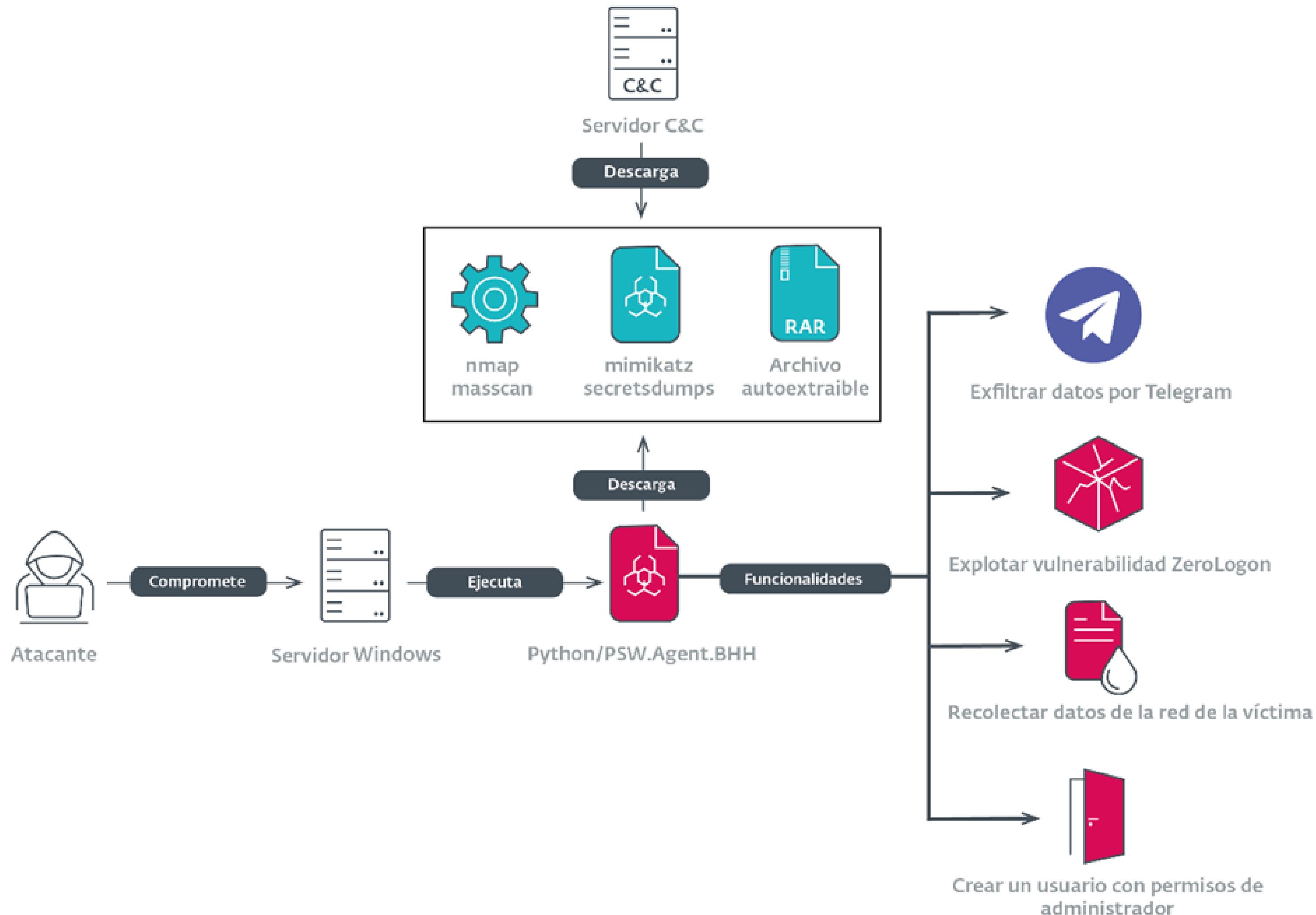
Cómo vulneran servidores Windows legacy para minado de criptomonedas

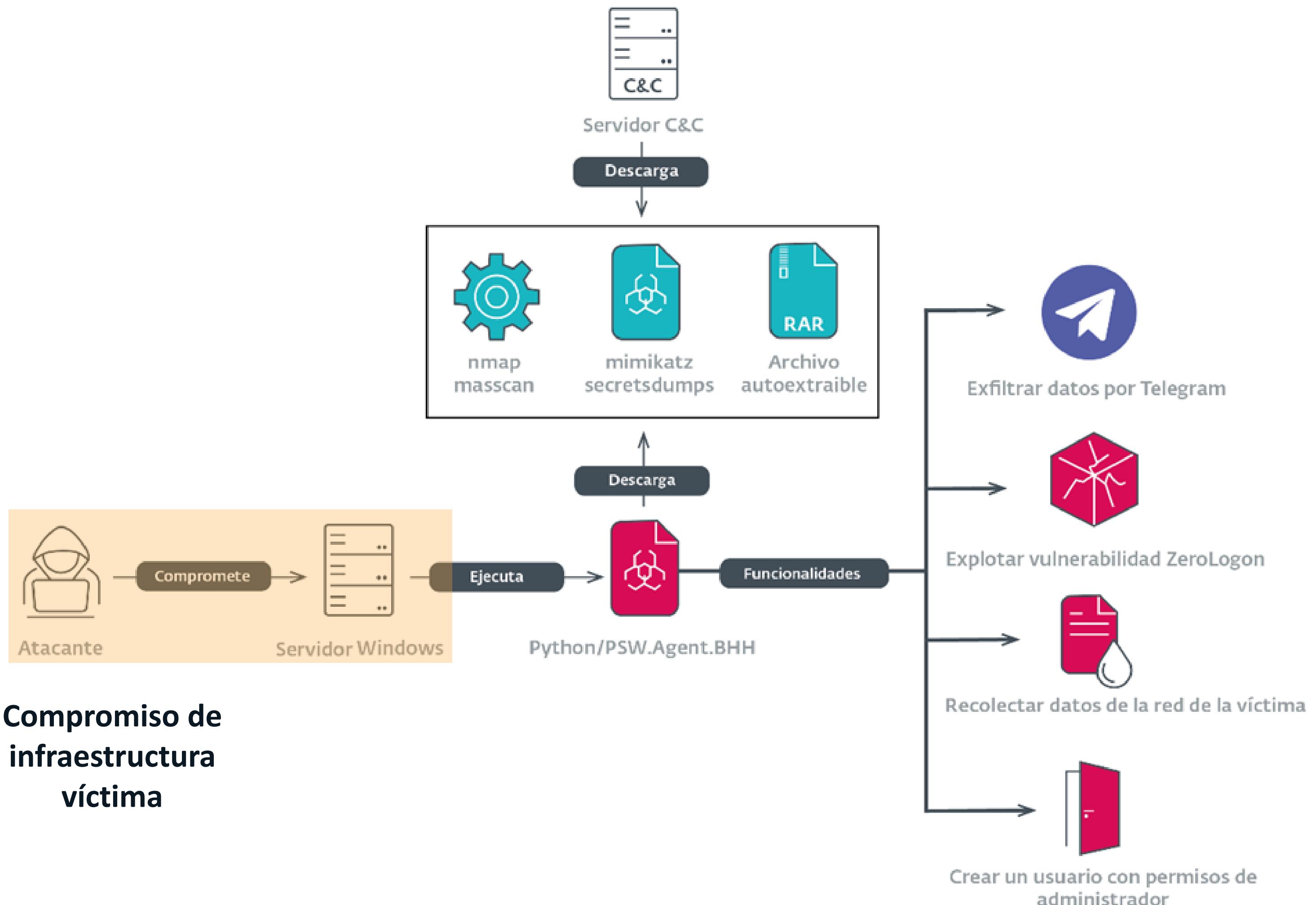
PUBLIC

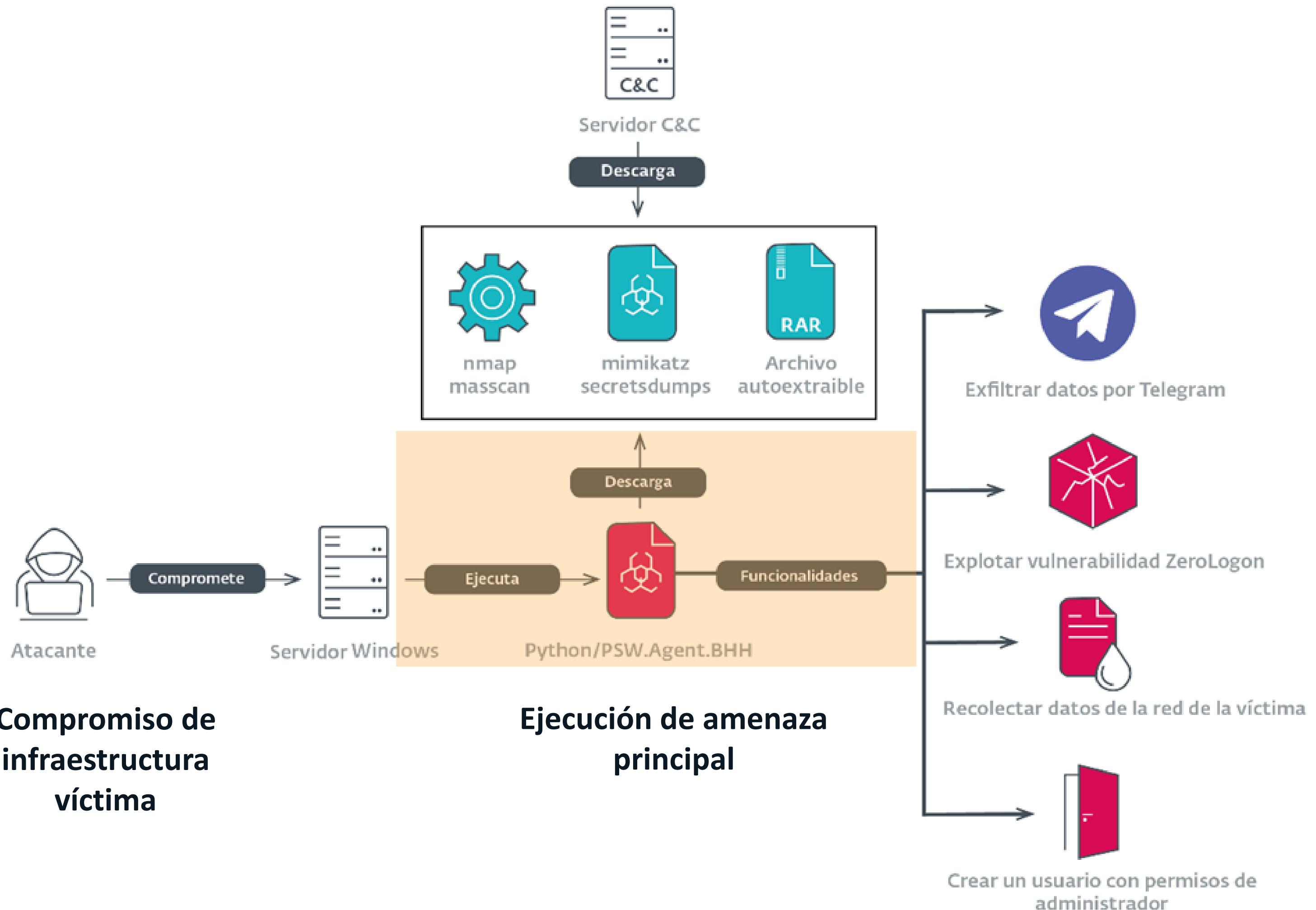
Comprendiendo estas amenazas en Latinoamérica

con una investigación del Laboratorio

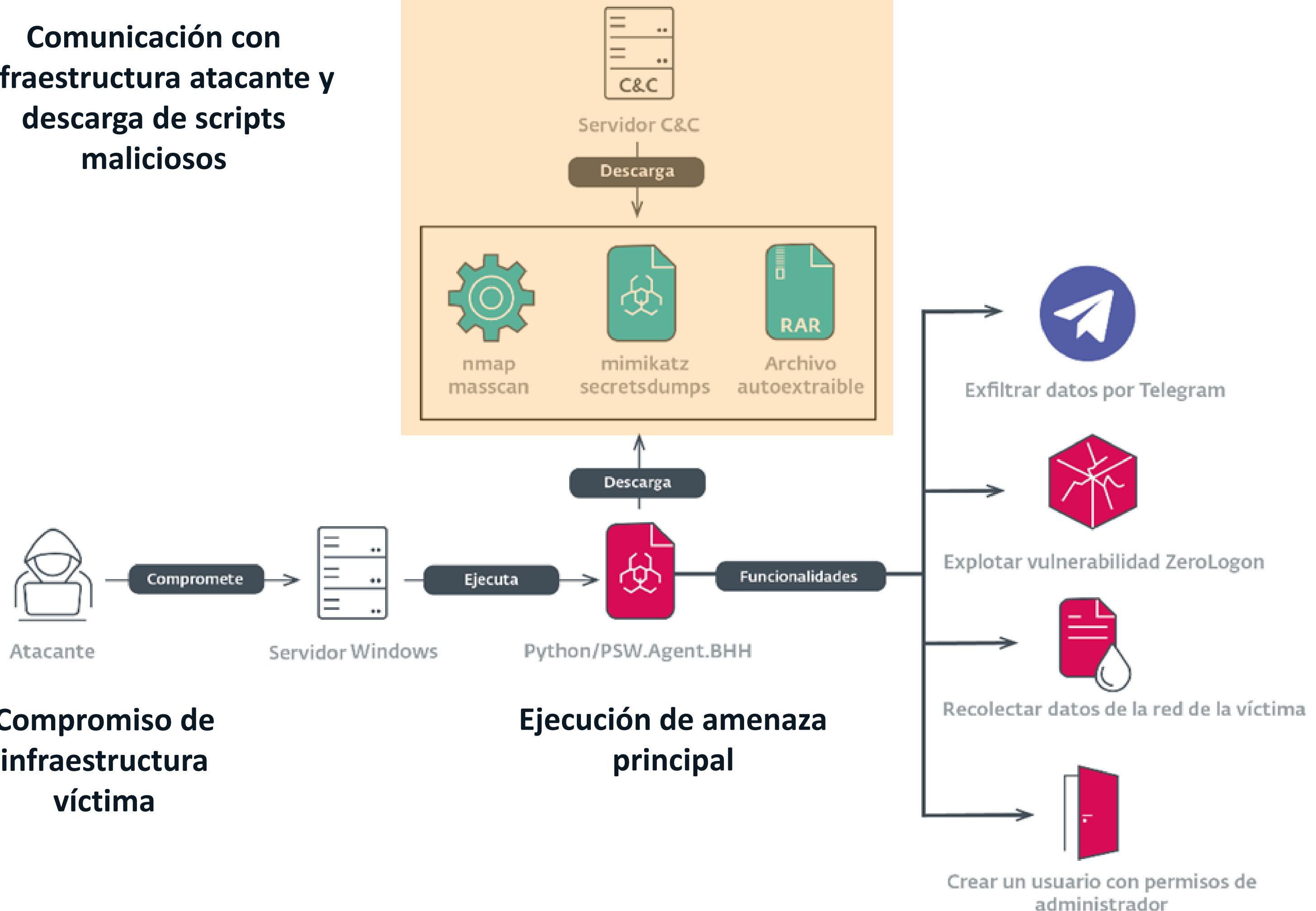




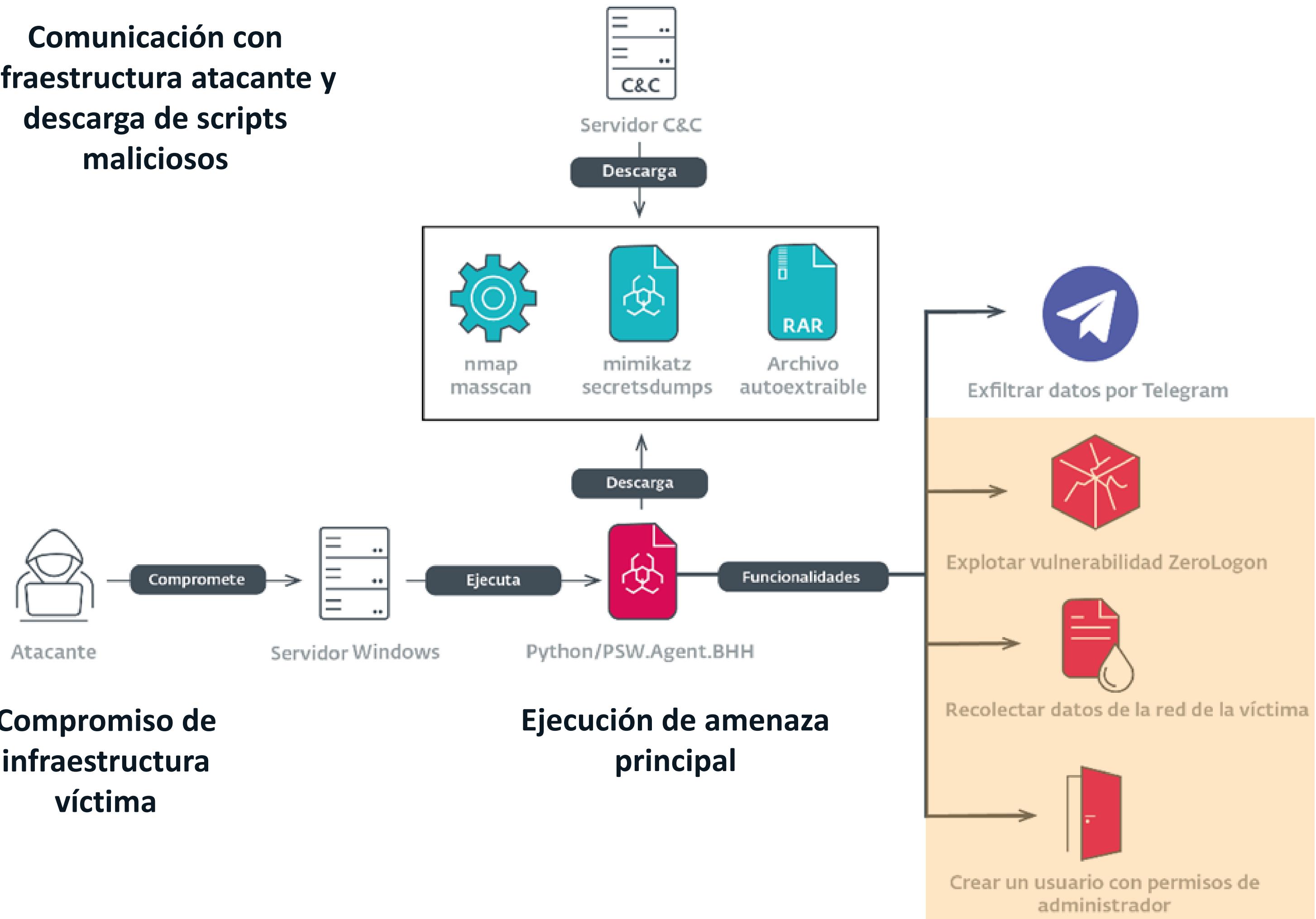




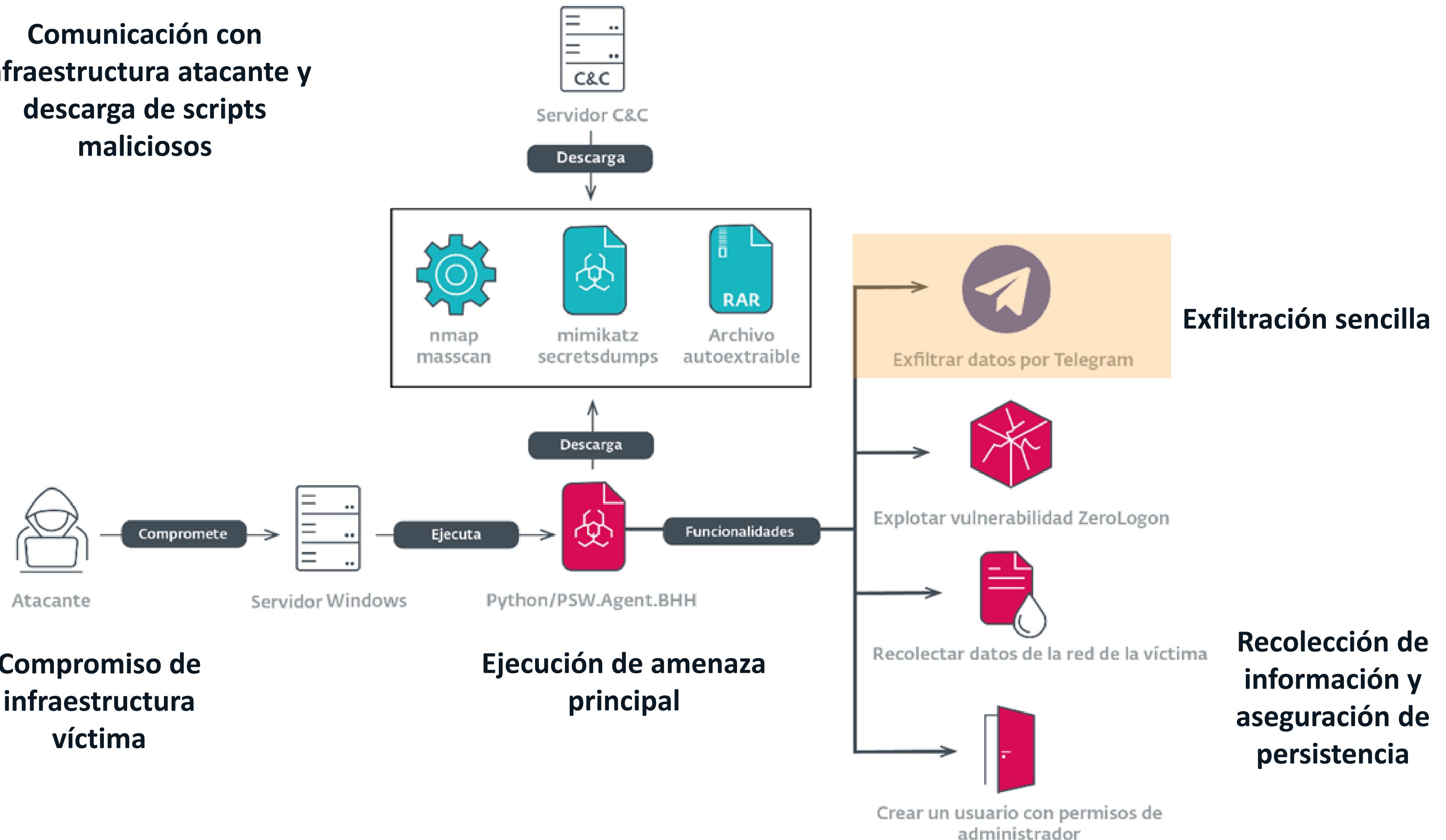
Comunicación con infraestructura atacante y descarga de scripts maliciosos



Comunicación con infraestructura atacante y descarga de scripts maliciosos



Comunicación con infraestructura atacante y descarga de scripts maliciosos



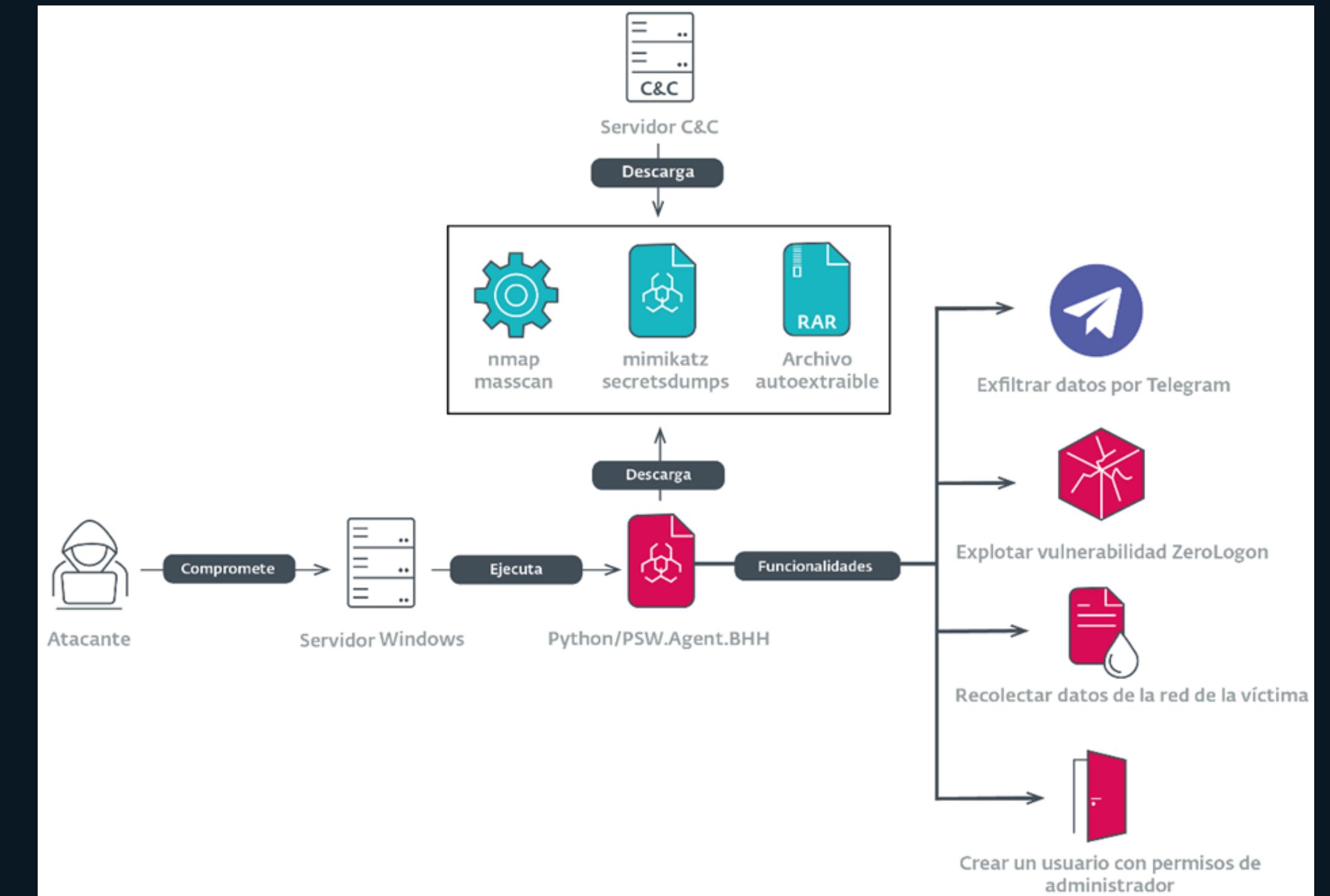
Compromiso de infraestructura víctima

Ejecución de **amenaza principal**

Comunicación con infraestructura atacante y descarga de scripts maliciosos

Recolección de información y aseguración de persistencia

Exfiltración sencilla



Presencia en Latinoamérica

103.398 muestras únicas, concentradas en 5 familias conocidas
Esto es...

≈ 8.600 muestras por mes

≈ 280 muestras por día

≈ 4 muestras por minuto



Hacked Aircanada.com Login

The diagram illustrates a network connection between two computers. On the left, a pink laptop icon is labeled "Atacante". An arrow points from it to a teal monitor and tower icon labeled "Víctima". Below the icons, the text "vía RDP" indicates the communication protocol used.

Sold by: Captain8 ⚠️
Product Type: Digital
Payment: Escrow
Coins: BTC XMR

Postage: Autofilled
Quantity
1
Add to Cart

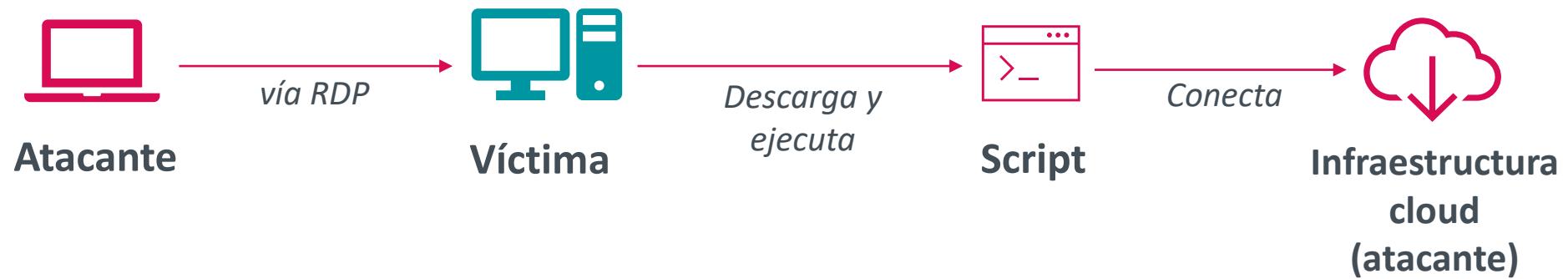
\$8
0.00029456 BTC
0.05281359 XMR

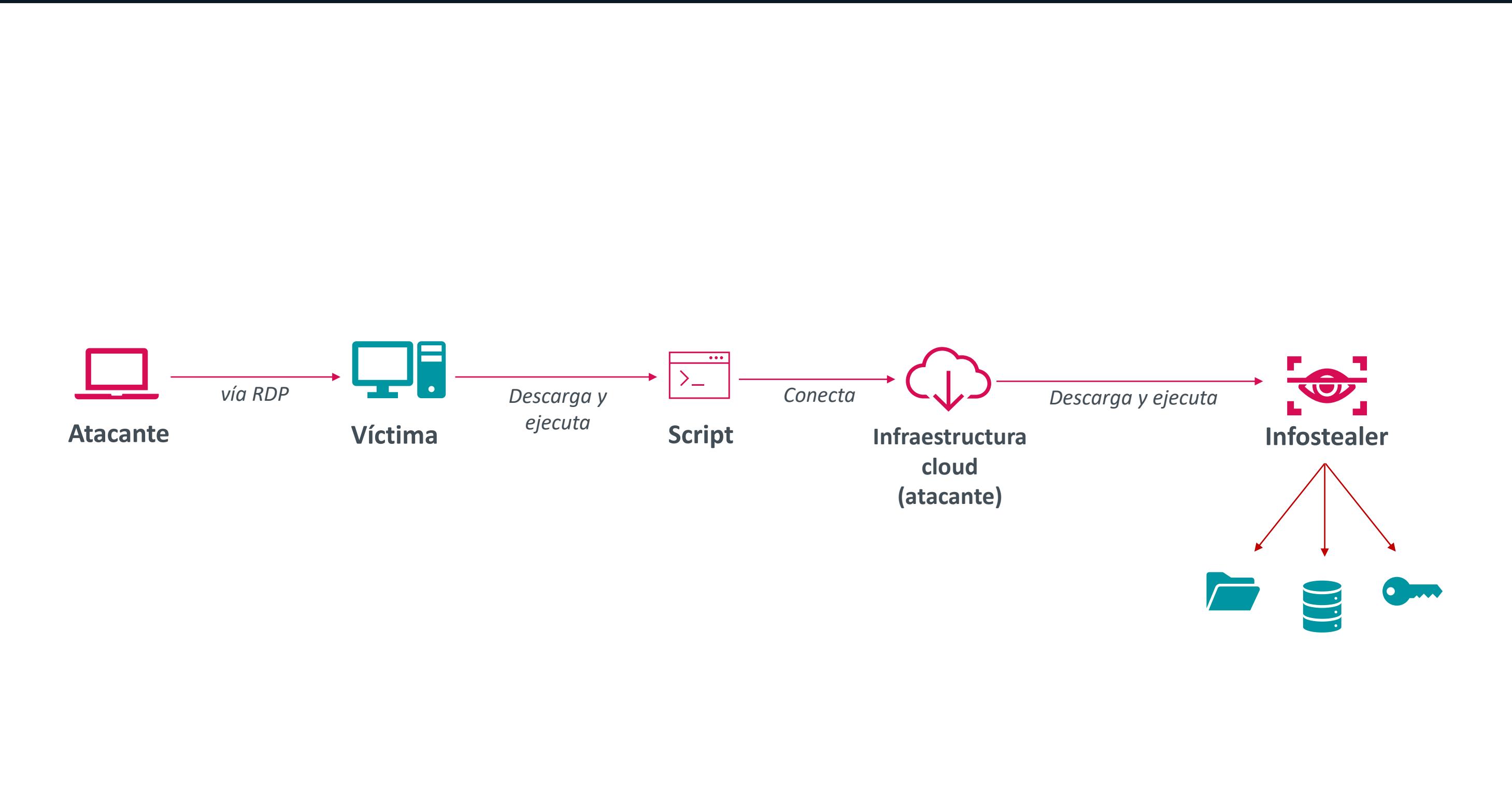
Product Description **Refund Policy** **Product Feedback** **Tags**

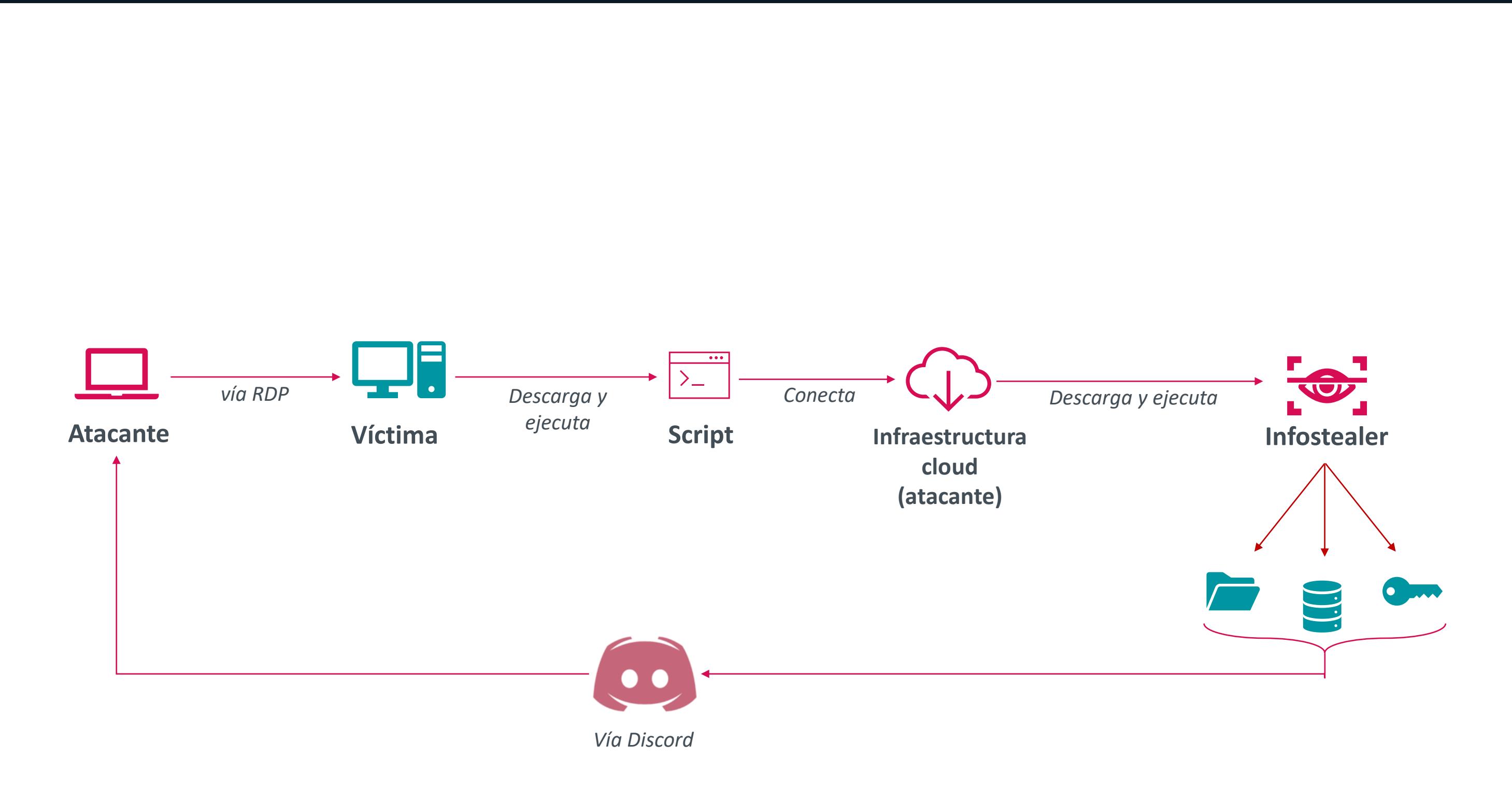
Hacked Aircanada.com Login

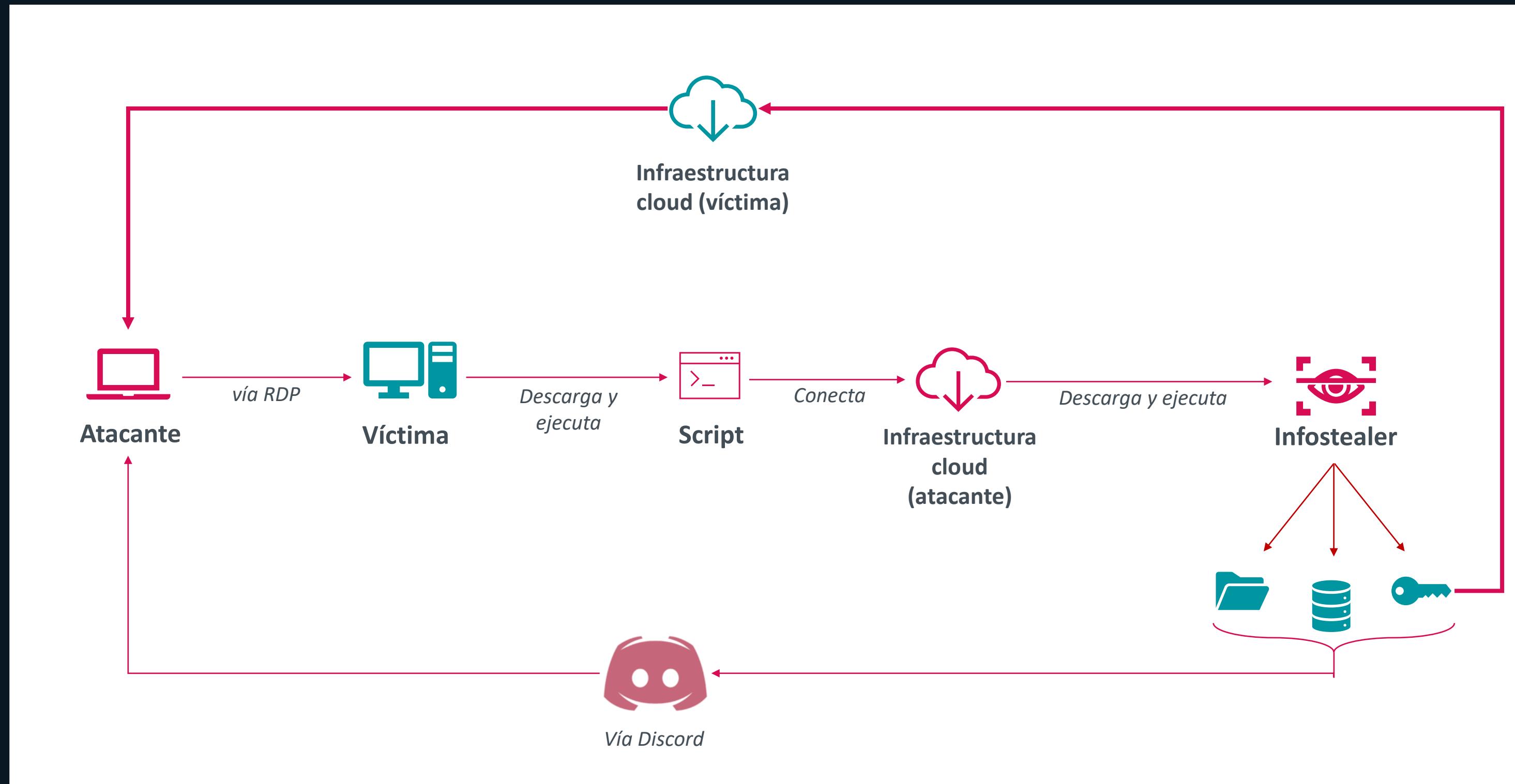
When you place an order, you will receive the login information. Account is fresh and are never resold. Only you will have exclusive access to the account.

These accounts are valid and 100% working. Sold only to you and no other person. Can use it to place orders and get free items / services / access.







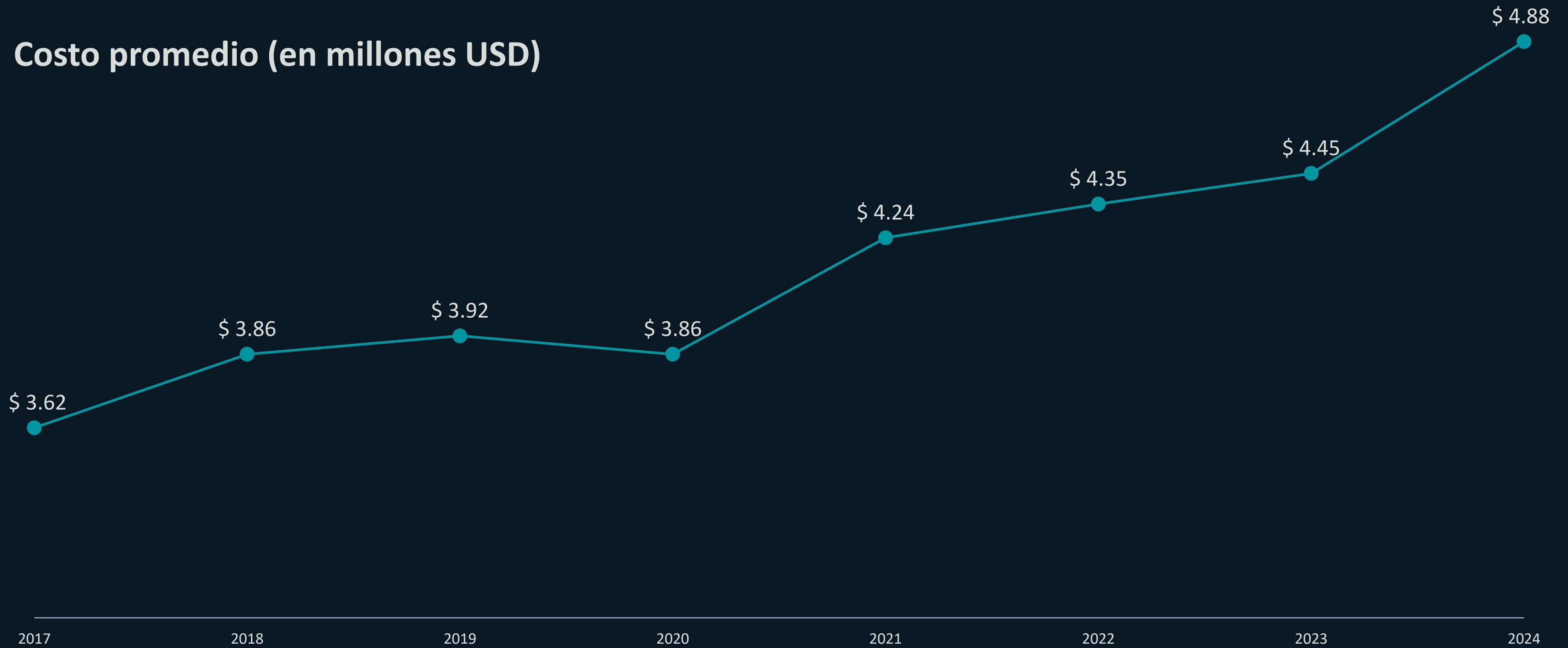


Cuantificando las consecuencias de una brecha de datos



Cuantificando las consecuencias

Costo promedio (en millones USD)



4.88M
USD

El costo aumentó en 10% con
respecto a 2023

1 de cada 3
empresas

Han sufrido de alguna fuga de
datos

2.22M
USD

Ahorro de costos promedio
para aquellas que
implementaron tecnologías de
ciberseguridad con IA

Presente y futuro



Big Data

Inteligencia
Artificial

IoT
(Internet de las cosas)

Articulando soluciones

Gobiernos

Estableciendo marcos legales sólidos, regulaciones efectivas y controles reales

Organizaciones

Implementando controles tecnológicos y de gestión, y cumpliendo las normativas

Usuarios

Tomando conciencia de los riesgos y aplicando medidas de protección

Regulaciones como aliados clave

- Bases sólidas para un problema complejo
- Las más completas sugieren elementos concretos, como ejercicios de seguridad o periodicidad (pentest)
- Identificar situaciones complejas, como el post-ataque
- Se deben fortalecer todas las fases de tratamiento de datos de manera integral, y no cumplir con una lista de requerimientos.



Gracias.



**SECURITY
DAYS2024**





CÓDIGO QR VIRTUAL





Samuel Guardia

Security Intelligence Analyst



Carlos Eng

Key Account Manager

Acceso inicial a Infraestructura Cloud



Acceso inicial

**Proceso de
infección**

**Ataque a
infraestructura
cloud**

Acceso inicial

- ✓ Exposición a ataques a través de Internet
- ✓ Utilización de Servicios y herramientas vulnerables
- ✓ Mecanismos deficientes o casi nulos de seguridad en las herramientas utilizadas



¿Cómo se podría evitar?



Exposición a Internet

- ✓ Conocer los riesgos de los servicios expuestos a Internet
- ✓ Utilizar mecanismos robustos para validar la identidad de los usuarios
- ✓ Implementar un segundo factor de autenticación



Control de vulnerabilidades

- ✓ Descubrir herramientas utilizadas en la organización
- ✓ Conocer vulnerabilidades presentes en el software instalado
- ✓ Priorizar riesgos y criticidad de vulnerabilidades
- ✓ Aplicar actualizaciones correspondientes



Protección de los endpoints

- ✓ Implementar herramientas de protección antimalware
- ✓ Contar con tecnologías específicas de protección: Brute Force Attack Protection
- ✓ Contar con soluciones de protección avanzada contra amenazas 0-day



- ✓ **Conocer los riesgos de los servicios expuestos a Internet**
- ✓ **Utilizar mecanismos robustos para validar la identidad de los usuarios**
- ✓ **Implementar un segundo factor de autenticación**



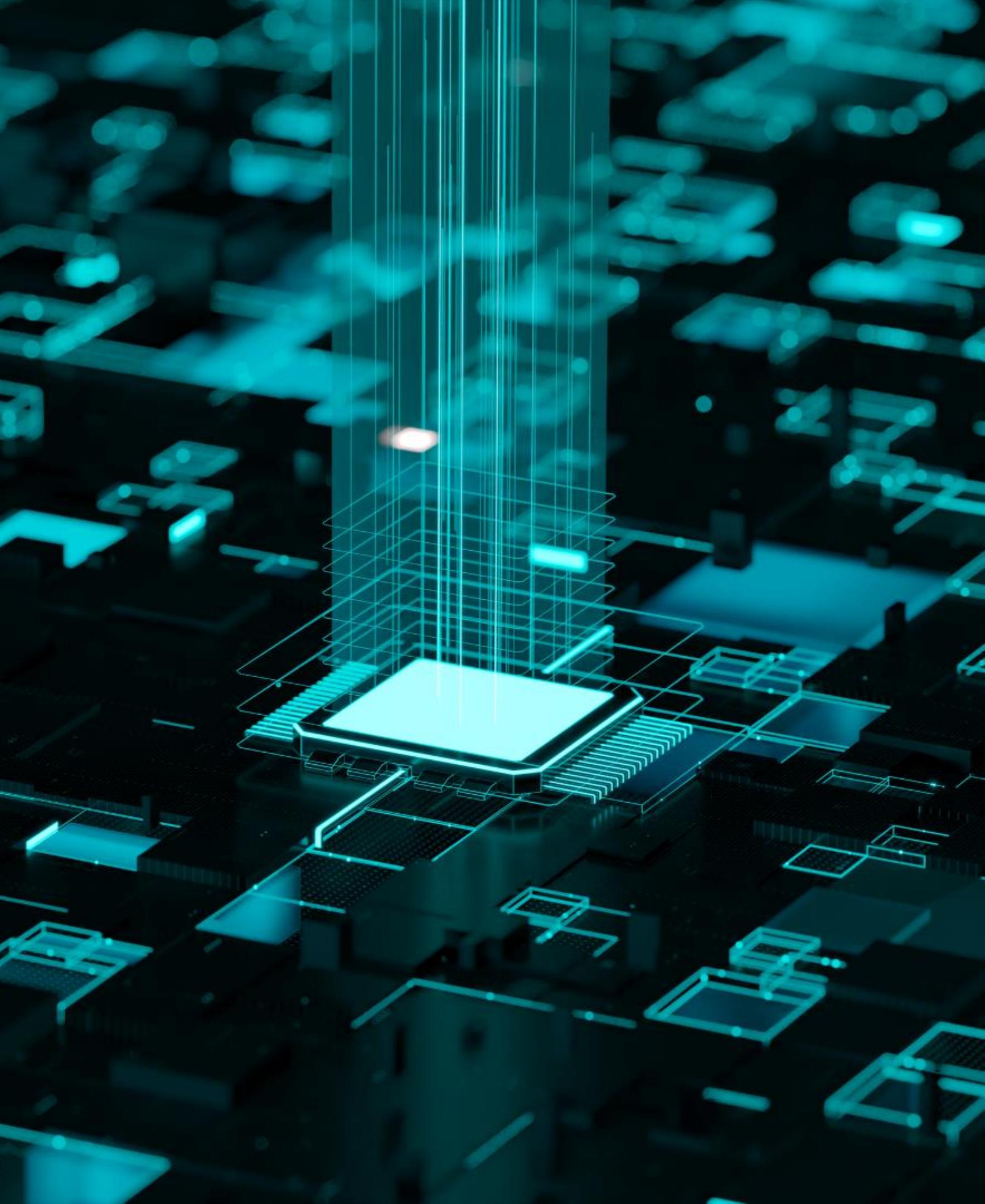
- ✓ Descubrir herramientas utilizadas en la organización
- ✓ Conocer vulnerabilidades presentes en el software instalado
- ✓ Priorizar riesgos y criticidad de vulnerabilidades
- ✓ Aplicar actualizaciones correspondientes

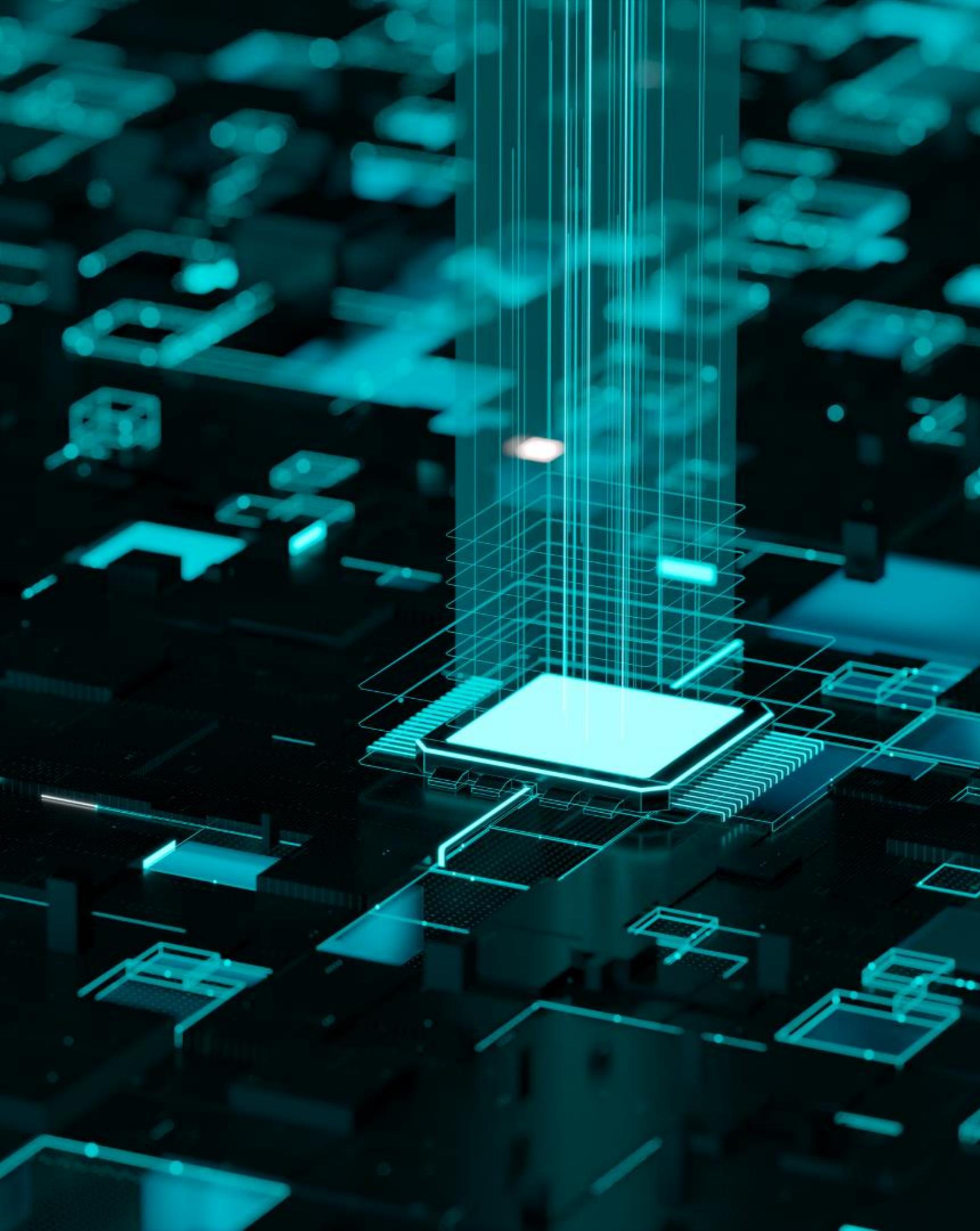


- ✓ **Implementar herramientas de protección antimalware**
- ✓ **Contar con tecnologías específicas de protección: Brute Force Attack Protection**
- ✓ **Contar con soluciones de protección avanzada contra amenazas 0-day**

Proceso de infección

- ✓ Ejecución de tareas con fines malicioso
- ✓ Modificaciones en el sistema operativo
- ✓ Descarga de amenazas de la web o infraestructura cloud
- ✓ Ejecución del código malicioso





Mecanismos de protección

- ✓ Soluciones de detección de malware
- ✓ Herramientas y tecnologías adicionales para la detección de amenazas avanzadas o 0-day
- ✓ Utilización de herramientas de detección y respuesta extendida – Mayor visibilidad



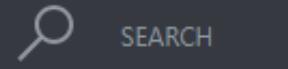
DASHBOARD



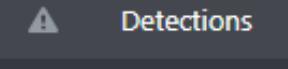
COMPUTERS



INCIDENTS



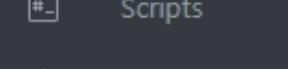
SEARCH



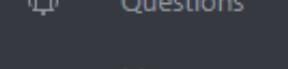
Detections



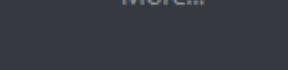
Executables



Scripts



Questions



More...

Detections

UNGROUPED



TAGS...

RESOLVED



| | DETECTIONS (18) | SEVERITY | PRIORITY | OCCURRENCES | RESOLVED | TIME OCCURRED | COMPUTER | EXECUTABLE |
|--------------------------|--|----------|----------|-------------|-----------------------------|-----------------|----------|------------|
| <input type="checkbox"/> | ⚠️ Antivirus Malware: MSIL/PSW.Agent.RXP | ! | 2 | 0/2 | 8 de mar. de 2024, 10:43:05 | desktop-b0s8iqu | Unknown | |

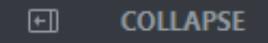
DETECTIONS

INCIDENT

MARK AS RESOLVED

MARK AS NOT RESOLVED

CREATE EXCLUSION



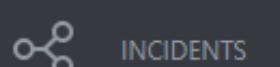
COLLAPSE



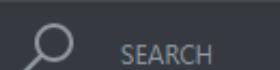
DASHBOARD



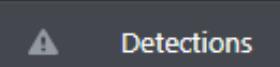
COMPUTERS



INCIDENTS



SEARCH



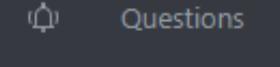
Detections



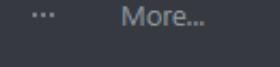
Executables



Scripts



Questions



More...

Detections

UNGROUPED



TAGS...



RESOLVED X

| | DETECTIONS (18) | SEVERITY | PRIORITY | OCCURRENCES | RESOLVED | TIME OCCURRED | COMPUTER | EXECUTABLE |
|--|---|----------|----------|-------------|----------|------------------------------|-----------------|----------------|
| | ⚠️ Antivirus Malware: MSIL/PSW.Agent.RXP | ! | | 2 | 0/2 | 8 de mar. de 2024, 10:43:05 | desktop-b0s8iqu | Unknown |
| | ⚠️ Rule Suspicious explorer parent process [F0427] | i | | 1 | 0/1 | 8 de mar. de 2024, 12:13:09 | desktop-b0s8iqu | explorer.exe |
| | ⚠️ Rule File and directory discovery via PowerShell [C1109c] | i | | 1 | 0/1 | 9 de mar. de 2024, 6:19:51 | desktop-b0s8iqu | powershell.exe |
| | ⚠️ Rule File and directory discovery via PowerShell [C1109c] | i | | 1 | 0/1 | 10 de mar. de 2024, 6:13:12 | desktop-b0s8iqu | powershell.exe |
| | ⚠️ Rule File and directory discovery via PowerShell [C1109c] | i | | 1 | 0/1 | 11 de mar. de 2024, 6:48:11 | desktop-b0s8iqu | powershell.exe |
| | ⚠️ Rule Disabling RDP authentication [C1010] | i | | 1 | 0/1 | 11 de mar. de 2024, 15:07:53 | desktop-b0s8iqu | rdpcheck.exe |
| | ⚠️ Rule Process communicating over potentially Suspicious Protocol ... | i | | 1 | 0/1 | 11 de mar. de 2024, 15:08:02 | desktop-b0s8iqu | svchost.exe |
| | ⚠️ Rule Process communicating over potentially Suspicious Protocol ... | i | | 1 | 0/1 | 11 de mar. de 2024, 15:08:02 | desktop-b0s8iqu | rdpcheck.exe |
| | ⚠️ Rule User login [F1004] | i | | 2 | 0/2 | 11 de mar. de 2024, 15:26:08 | desktop-b0s8iqu | lsass.exe |
| | ⚠️ Rule Remote user login [F0900] | i | | 1 | 0/1 | 11 de mar. de 2024, 15:26:08 | desktop-b0s8iqu | lsass.exe |

DETECTIONS ▾

INCIDENT ▾

MARK AS RESOLVED

MARK AS NOT RESOLVED

CREATE EXCLUSION

COLLAPSE



- DASHBOARD
- COMPUTERS
- INCIDENTS
- SEARCH
- Detections
- Executables
- Scripts
- Questions
- ... More...

COLLAPSE

Detections

| | UNGROUPED | | ● ● ● ● | TAGS... | RESOLVED X |
|-----------------|-----------|--|--------------|----------|------------------------------|
| DETECTIONS (18) | | | | | |
| | SEVERITY | PRIORITY | OCCURRENC... | RESOLVED | TIME OCCURRED |
| | Antivirus | Malware: MSIL/PSW.Agent.RXP | | 2 | 0/2 |
| | | | | | 8 de mar. de 2024, 10:43:05 |
| | Rule | Suspicious explorer parent process [F0427] | | 1 | 0/1 |
| | | | | | 8 de mar. de 2024, 12:13:09 |
| | Rule | File and directory discovery via PowerShell [C1109c] | | 1 | 0/1 |
| | | | | | 9 de mar. de 2024, 6:19:51 |
| | Rule | File and directory discovery via PowerShell [C1109c] | | 1 | 0/1 |
| | | | | | 10 de mar. de 2024, 6:13:12 |
| | Rule | File and directory discovery via PowerShell [C1109c] | | 1 | 0/1 |
| | | | | | 11 de mar. de 2024, 6:48:11 |
| | Rule | Disabling RDP authentication [C1010] | | 1 | 0/1 |
| | | | | | 11 de mar. de 2024, 15:07:53 |
| | Rule | Process communicating over potentially Suspicious Protocol ... | | 1 | 0/1 |
| | | | | | 11 de mar. de 2024, 15:08:02 |
| | Rule | Process communicating over potentially Suspicious Protocol ... | | 1 | 0/1 |
| | | | | | 11 de mar. de 2024, 15:08:02 |
| | Rule | User login [F1004] | | 2 | 0/2 |
| | | | | | 11 de mar. de 2024, 15:26:08 |
| | Rule | Remote user login [F0900] | | 1 | 0/1 |
| | | | | | 11 de mar. de 2024, 15:26:08 |
| | Rule | Suspicious PowerShell Script - Network [D0524] | | 1 | 0/1 |
| | | | | | 11 de mar. de 2024, 15:26:08 |
| | Rule | Powershell.exe creates an external network connection [A050... | | 1 | 0/1 |
| | | | | | 11 de mar. de 2024, 15:32:20 |

DETECTIONS

INCIDENT

MARK AS RESOLVED

MARK AS NOT RESOLVED

CREATE EXCLUSION



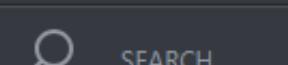
DASHBOARD



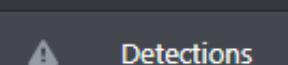
COMPUTERS



INCIDENTS



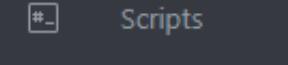
SEARCH



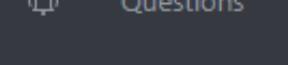
Detections



Executables



Scripts



Questions



More...

Detections

UNGROUPED



PRIORITY

OCCURRENC...

RESOLVED

TIME OCCURRED

COMPUTER

EXECUTABLE

| | DETECTIONS (18) | SEVERITY | PRIORITY | OCCURRENC... | RESOLVED | TIME OCCURRED | COMPUTER | EXECUTABLE |
|--|---|----------|----------|--------------|----------|------------------------------|-----------------|----------------|
| | ⚠️ Antivirus Malware: MSIL/PSW.Agent.RXP | ! | | 2 | 0/2 | 8 de mar. de 2024, 10:43:05 | desktop-b0s8iqu | Unknown |
| | ⚠️ Rule Suspicious explorer parent process [F0427] | i | | 1 | 0/1 | 8 de mar. de 2024, 12:13:09 | desktop-b0s8iqu | explorer.exe |
| | ⚠️ Rule File and directory discovery via PowerShell [C1109c] | i | | 1 | 0/1 | 9 de mar. de 2024, 6:19:51 | desktop-b0s8iqu | powershell.exe |
| | ⚠️ Rule File and directory discovery via PowerShell [C1109c] | i | | 1 | 0/1 | 10 de mar. de 2024, 6:13:12 | desktop-b0s8iqu | powershell.exe |
| | ⚠️ Rule File and directory discovery via PowerShell [C1109c] | i | | 1 | 0/1 | 11 de mar. de 2024, 6:48:11 | desktop-b0s8iqu | powershell.exe |
| | ⚠️ Rule Disabling RDP authentication [C1010] | i | | 1 | 0/1 | 11 de mar. de 2024, 15:07:53 | desktop-b0s8iqu | rdpcheck.exe |
| | ⚠️ Rule Process communicating over potentially Suspicious Protocol ... | i | | 1 | 0/1 | 11 de mar. de 2024, 15:08:02 | desktop-b0s8iqu | svchost.exe |
| | ⚠️ Rule Process communicating over potentially Suspicious Protocol ... | i | | 1 | 0/1 | 11 de mar. de 2024, 15:08:02 | desktop-b0s8iqu | rdpcheck.exe |
| | ⚠️ Rule User login [F1004] | i | | 2 | 0/2 | 11 de mar. de 2024, 15:26:08 | desktop-b0s8iqu | lsass.exe |
| | ⚠️ Rule Remote user login [F0900] | i | | 1 | 0/1 | 11 de mar. de 2024, 15:26:08 | desktop-b0s8iqu | lsass.exe |
| | ⚠️ Rule Suspicious PowerShell Script - Network [D0524] | ! | | 1 | 0/1 | 11 de mar. de 2024, 15:26:08 | desktop-b0s8iqu | powershell.exe |
| | ⚠️ Rule Powershell.exe creates an external network connection [A050... | ! | | 1 | 0/1 | 11 de mar. de 2024, 15:32:20 | desktop-b0s8iqu | powershell.exe |
| | ⚠️ Rule Suspicious process queried system information via WMI [A11... | i | | 14 | 0/14 | 11 de mar. de 2024, 15:40:35 | desktop-b0s8iqu | svchost.exe |
| | ⚠️ Rule Suspicious process queried processes information via WMI [... | i | | 14 | 0/14 | 11 de mar. de 2024, 15:40:35 | desktop-b0s8iqu | svchost.exe |
| | ⚠️ Rule Saving script file [Z0301] | i | | 6 | 0/6 | 11 de mar. de 2024, 15:40:35 | desktop-b0s8iqu | stub.exe |
| | ⚠️ Rule Process from SysWOW64 started by unpopular process [A04... | i | | 6 | 0/6 | 11 de mar. de 2024, 15:40:35 | desktop-b0s8iqu | cmd.exe |
| | ⚠️ Rule Command prompt with unpopular parent process [A0400] | i | | 6 | 0/6 | 11 de mar. de 2024, 15:40:35 | desktop-b0s8iqu | cmd.exe |
| | ⚠️ Rule Processes killing from command line [B0401] | i | | 6 | 0/6 | 11 de mar. de 2024, 15:40:35 | desktop-b0s8iqu | taskkill.exe |



COLLAPSE

DETECTIONS

INCIDENT

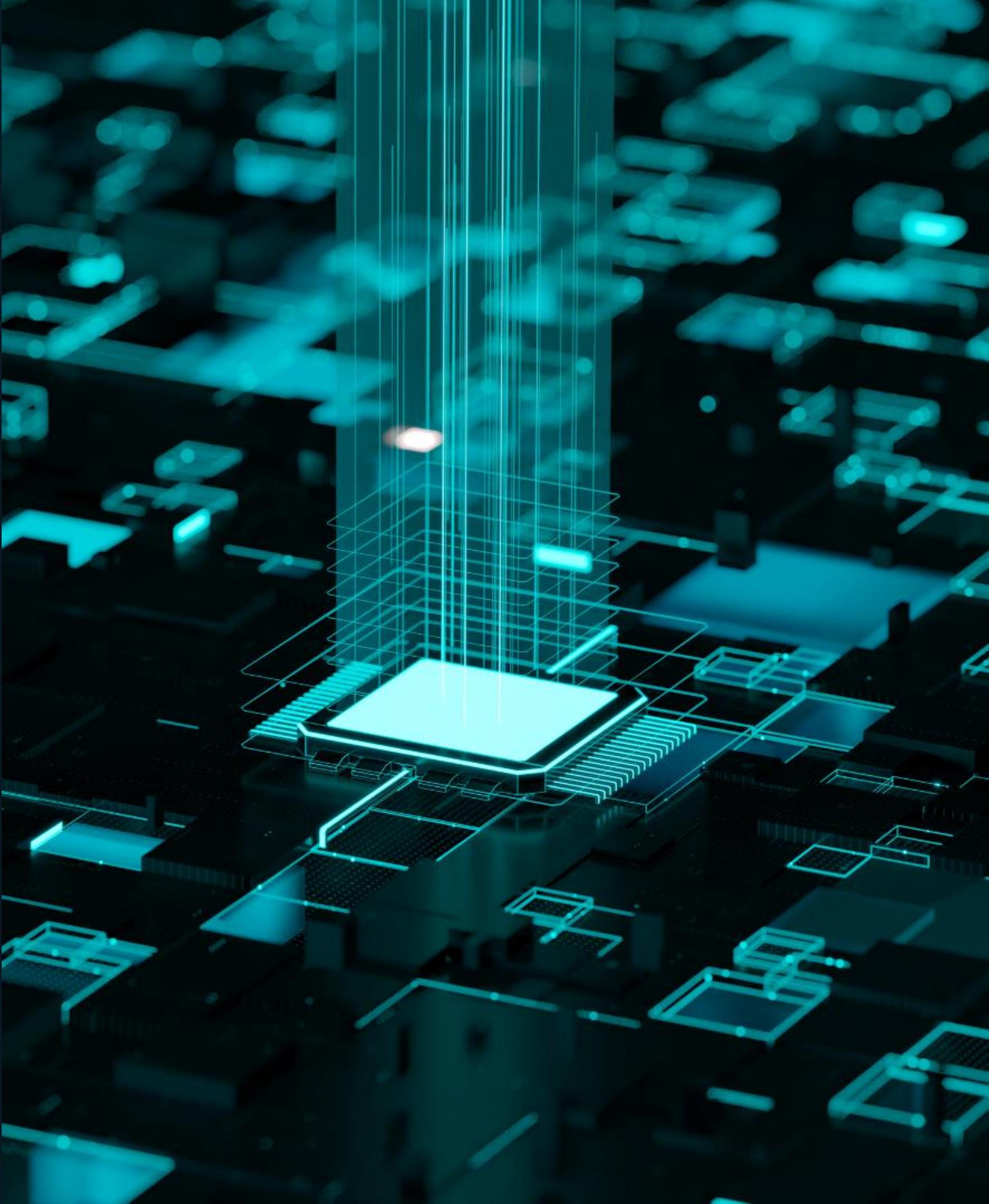
MARK AS RESOLVED

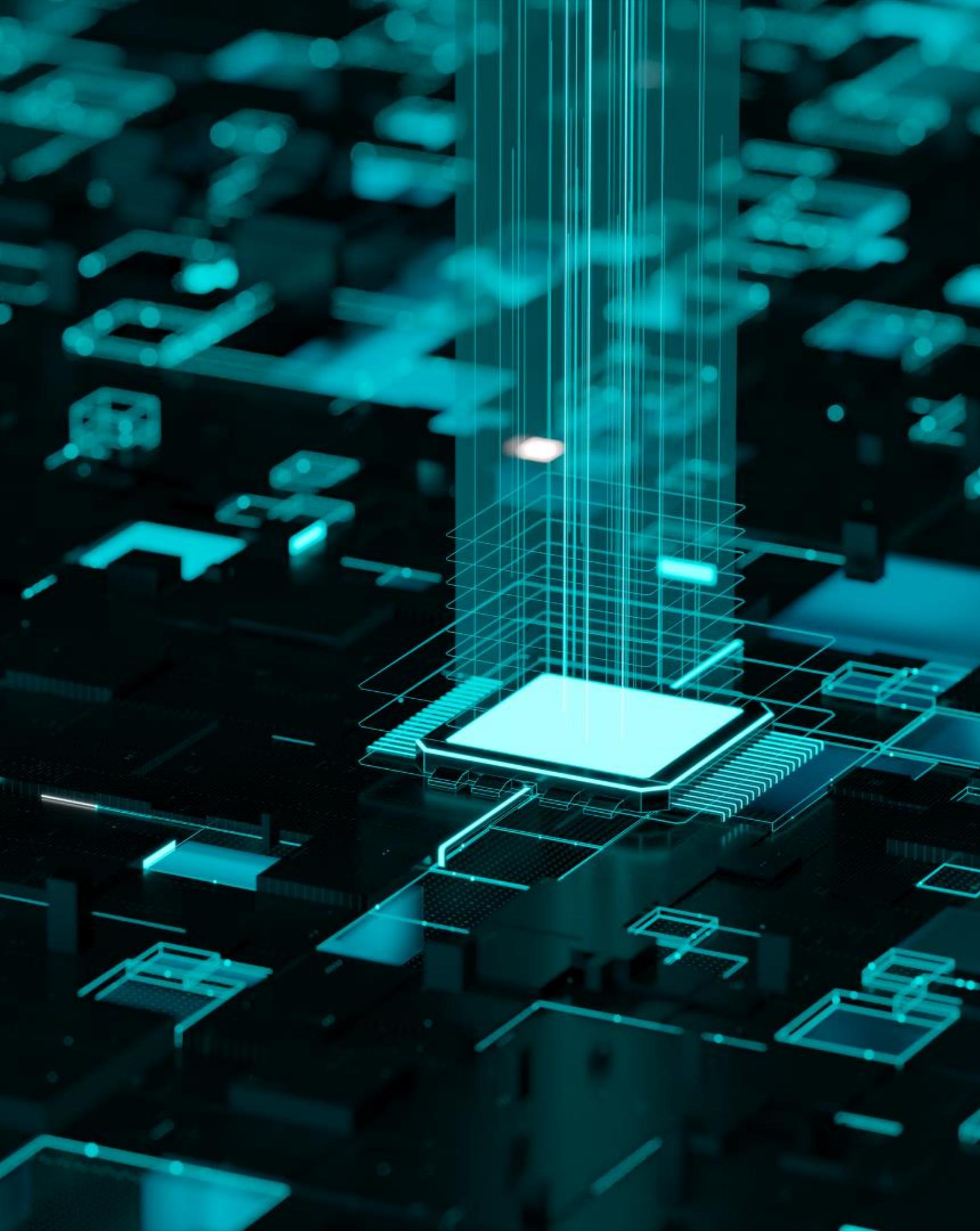
MARK AS NOT RESOLVED

CREATE EXCLUSION

Ataque a infraestructura cloud

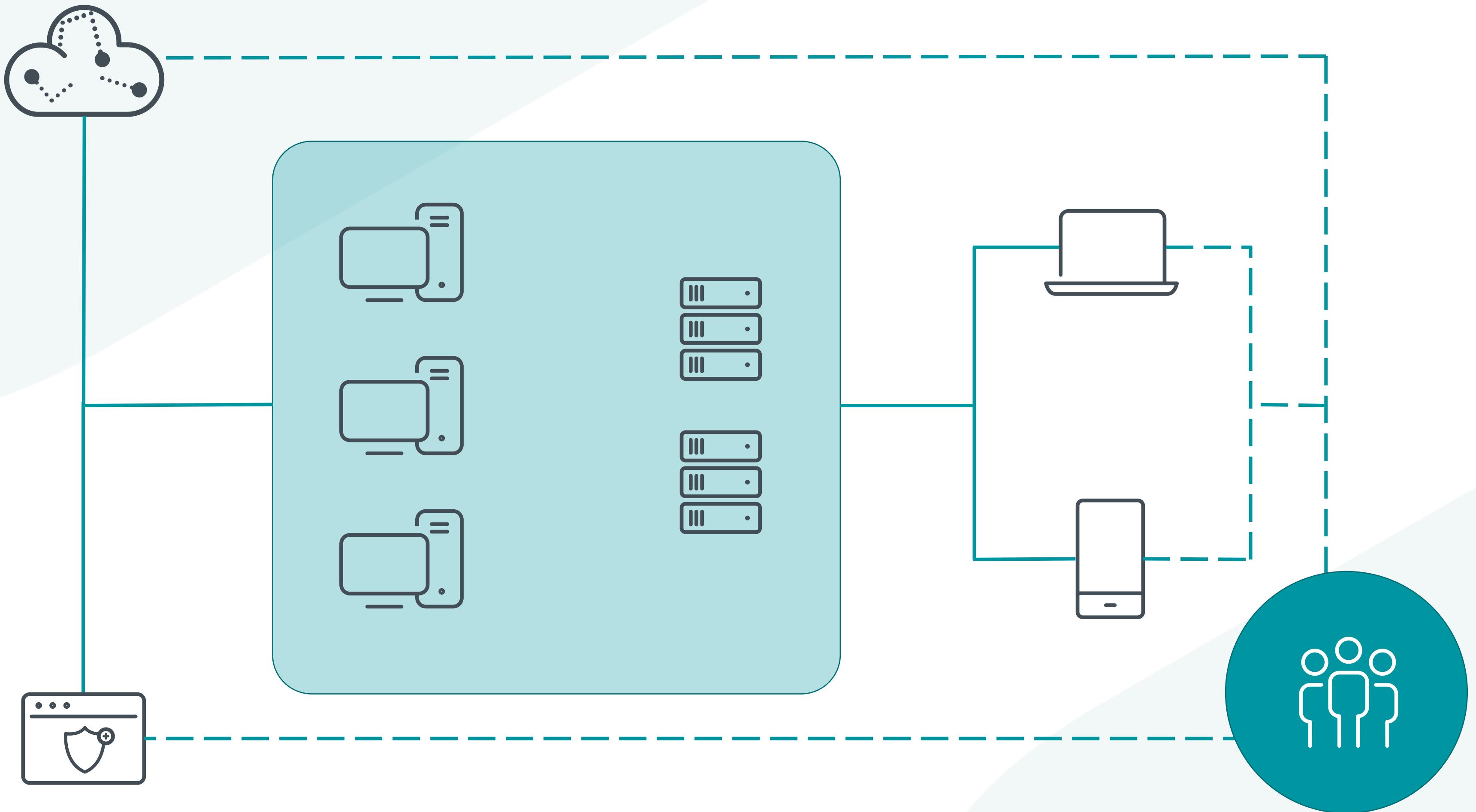
- ✓ Alojar códigos maliciosos
- ✓ Propagación de amenazas, de manera interna y externa
- ✓ Suplantación de identidad





Mecanismos de protección

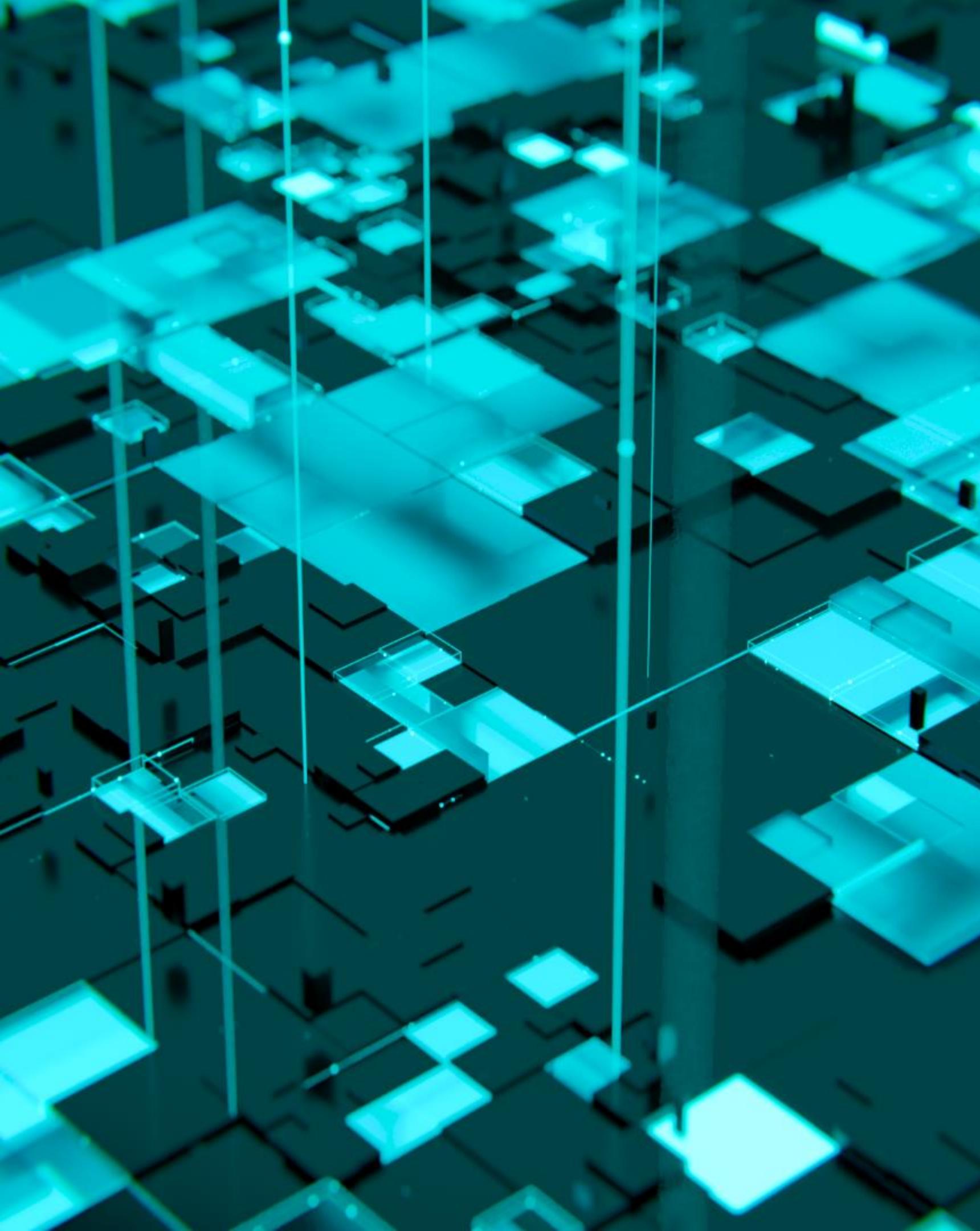
- ✓ **Protección contra códigos maliciosos – Microsoft 365 y Google Workspace**
- ✓ **Tecnologías adicionales para la detección de amenazas avanzadas o 0-day**



Compliance

Compliance

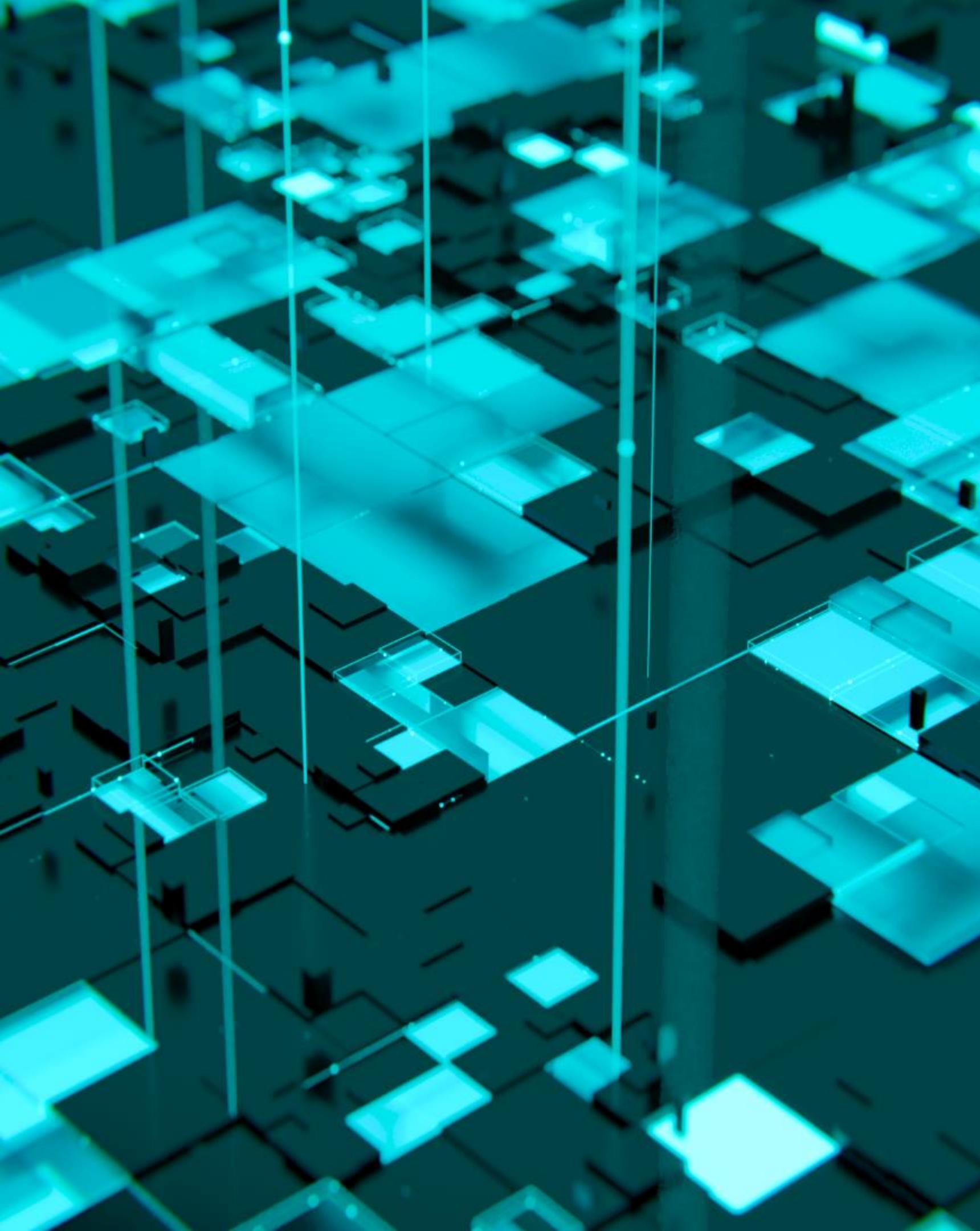
- ✓ Busca promover la cultura de cumplimiento a través de la capacitación y difusión sobre la importancia de cumplir con las leyes, reglamentos y normatividad interna que le resulten aplicables, evitando con ello sanciones, pérdidas económicas, reputacionales, entre otras. (Hard Law y Softlaw).



CNPP

Artículo 421. Ejercicio de la acción penal y responsabilidad penal autónoma

Las personas jurídicas serán penalmente responsables, de los delitos cometidos a su nombre, por su cuenta, en su beneficio o a través de los medios que ellas proporcionen, cuando se haya determinado que además existió inobservancia del **debido control en su organización**. Lo anterior con independencia de la responsabilidad penal en que puedan incurrir sus representantes o administradores de hecho o de derecho



Ley Federal de protección de datos personales en posesión de los particulares.

Artículo 19.- Todo **responsable** que lleve a cabo tratamiento de datos personales deberá establecer y mantener **medidas de seguridad administrativas, técnicas y físicas** que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Conclusión

El cumplimiento normativo de las empresas (en este caso para Datos Personales y Derechos de Autor), ofrece la oportunidad de mejorar la eficiencia y la precisión en la gestión de amenazas, vulnerabilidades y riesgos.

Hoy con la Inteligencia Artificial podemos apoyarnos en hacer más eficientes estos procesos, sin embargo, siempre debe de venir acompañada con la Ciberseguridad en todas sus vertientes, hoy en día todos estamos expuestos en este mundo digital por lo que hoy más que nunca debemos apostar por la Debida Diligencia.

Gracias.



**SECURITY
DAYS2024**





Break time



¡Ya estamos
de regreso!



CÓDIGO QR VIRTUAL





Fátima Rodríguez

*Ethical Hacker | Auditor ISO27001 | Analista Forense
Cybersecurity Intelligence Analyst | Red Team*



Leyes de protección de datos

Un aliado más que enemigo

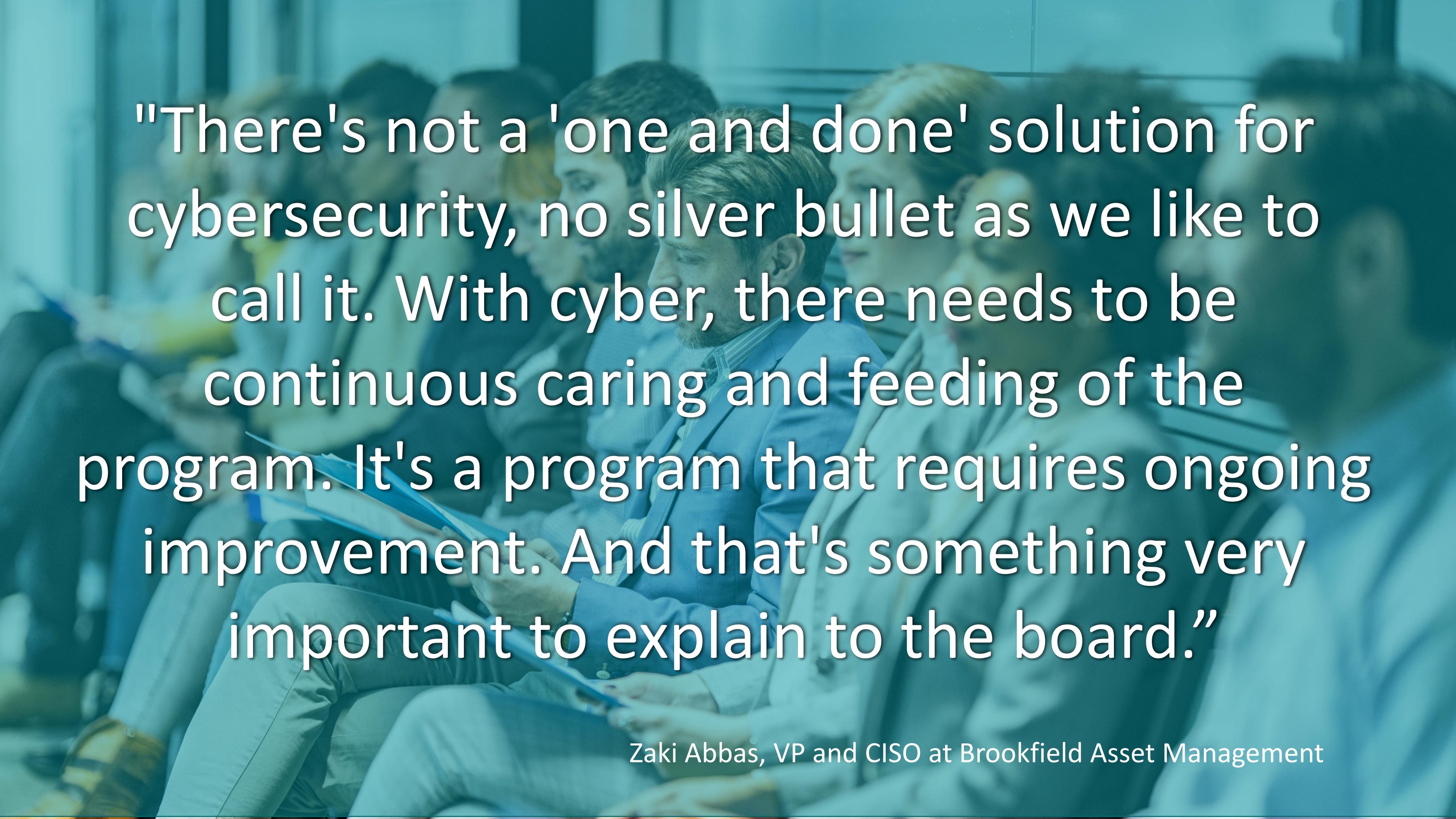
Fátima Rodríguez Giles

Ethical Hacker | Auditor ISO27001 | Analista Forense

Cybersecurity Intelligence Analyst | Red Team



SECURITY
DAYS 2024



"There's not a 'one and done' solution for cybersecurity, no silver bullet as we like to call it. With cyber, there needs to be continuous caring and feeding of the program. It's a program that requires ongoing improvement. And that's something very important to explain to the board."

Zaki Abbas, VP and CISO at Brookfield Asset Management

Argentina – Ley de Protección de Datos Personales N° 25.326 (LPDP).

Conforme el Artículo 9 LPDP, el responsable o usuario del archivo de datos, debe adoptar aquellas medidas técnicas y organizativas que: 1. Resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado. 2. Permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

México - Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).

Establecer una relación de las medidas de seguridad con las que cuente el responsable para asegurar la protección de los datos personales.

El responsable deberá actualizar las medidas de seguridad para su mejora continua, o en caso de alguna modificación sustancial en el tratamiento o vulneración/afectación de datos personales

Brasil - Ley General de Protección de Datos de Brasil (“LGPD”)

Los agentes del tratamiento adoptarán medidas de seguridad, técnicas y administrativas que puedan proteger los datos personales de accesos no autorizados y situaciones accidentales o ilícitas de destrucción, pérdida, modificación, comunicación o cualquier forma de tratamiento inadecuado o ilícito.

Uruguay – Ley N° 18.331: Protección de Datos Personales y acción de Habeas Data

La ley recepta el principio de seguridad de los datos mediante el cual el responsable o usuario de la base de datos debe adoptar las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales. Dichas medidas tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. En cuanto a medidas de seguridad, el Artículo 3 del Decreto N° 64/2020 dispone que los responsables y encargados del tratamiento, deberán adoptar las medidas técnicas y organizativas necesarias para conservar la integridad, confidencialidad y disponibilidad de la información, de forma de garantizar la seguridad de los datos personales.

Ecuador - Ley Orgánica de Protección de Datos Personales (“LOPDP”)

El responsable o encargado deberá implementar un proceso de evaluación continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole, que podrán incluir:

1. Anonimización, seudonomización o cifrado de datos personales.
2. Medidas dirigidas a mantener la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios

Chile – LGPD – N° 19.628

En el tratamiento de los datos personales, el responsable debe garantizar estándares adecuados de seguridad, protegiéndolos contra el tratamiento no autorizado o ilícito, y contra su pérdida, filtración, daño accidental o destrucción. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la naturaleza de los datos.

El responsable establecerá controles y medidas adecuadas para preservar el secreto o confidencialidad. Este deber subsiste aún después de concluida la relación con el titular.

Argentina – Ley de Protección de Datos Personales N° 25.326 (LPDP).

Conforme el Artículo 9 LPDP, el responsable o usuario del archivo de datos, debe adoptar aquellas medidas técnicas y organizativas que: 1. Resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado. 2. Permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

México - Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).

Establecer una relación de las medidas de seguridad con las que cuente el responsable para asegurar la protección de los datos personales.

El responsable deberá actualizar las medidas de seguridad para su mejora continua, o en caso de alguna modificación sustancial en el tratamiento o vulneración/afectación de datos personales

Brasil - Ley General de Protección de Datos de Brasil (“LGPD”)

Los agentes del tratamiento adoptarán medidas de seguridad, técnicas y administrativas que puedan proteger los datos personales de accesos no autorizados y situaciones accidentales o ilícitas de destrucción, pérdida, modificación, comunicación o cualquier forma de tratamiento inadecuado o ilícito.

Uruguay – Ley N° 18.331: Protección de Datos Personales y acción de Habeas Data

La ley recepta el principio de seguridad de los datos mediante el cual el responsable o usuario de la base de datos debe adoptar las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales. Dichas medidas tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. En cuanto a medidas de seguridad, el Artículo 3 del Decreto N° 64/2020 dispone que los responsables y encargados del tratamiento, deberán adoptar las medidas técnicas y organizativas necesarias para conservar la integridad, confidencialidad y disponibilidad de la información, de forma de garantizar la seguridad de los datos personales.

Ecuador - Ley Orgánica de Protección de Datos Personales (“LOPDP”)

El responsable o encargado deberá implementar un proceso de evaluación continua y permanente de la eficiencia, eficacia y efectividad de las medidas de carácter técnico, organizativo y de cualquier otra índole, que podrán incluir:

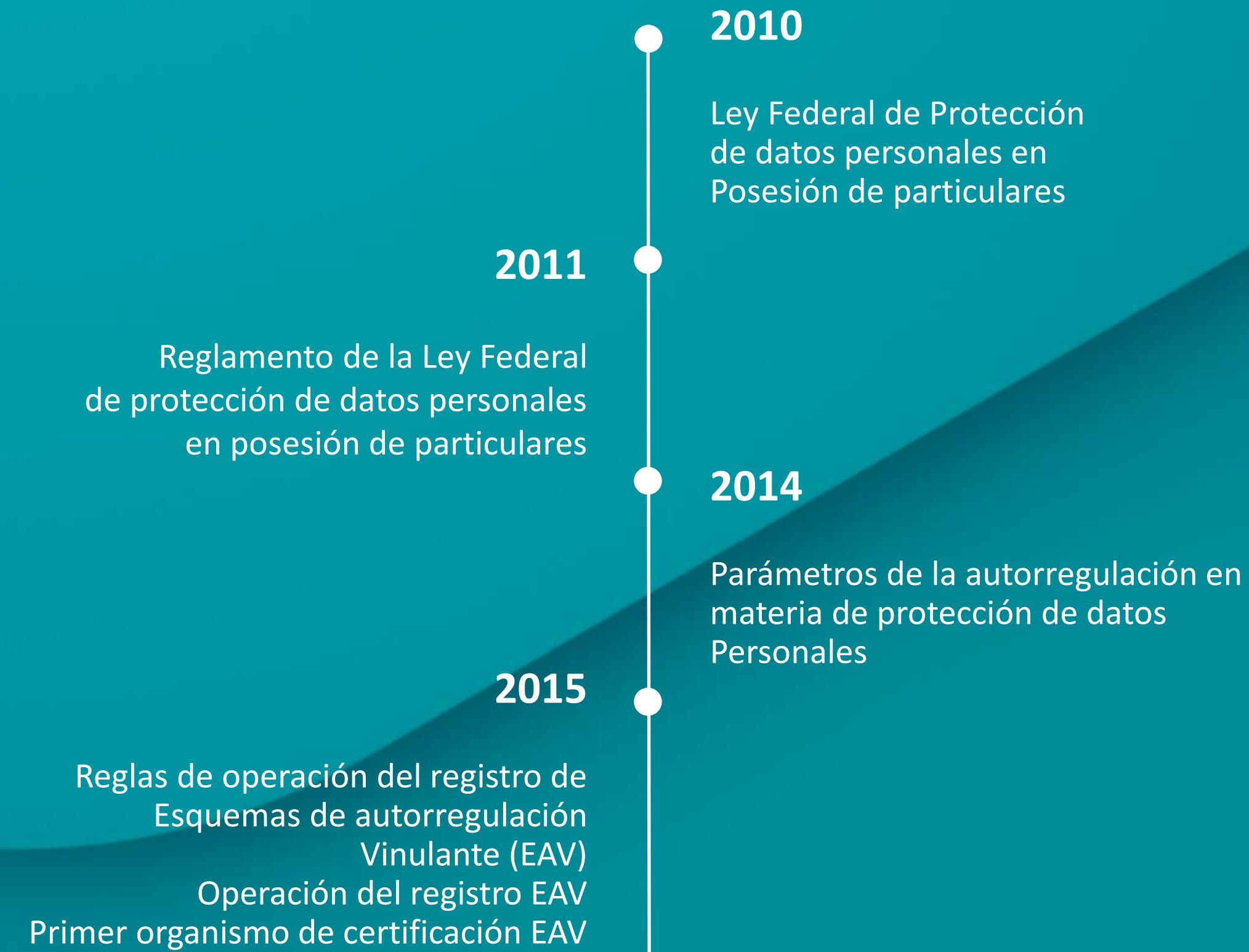
1. Anonimización, seudonimización o cifrado de datos personales.
2. Medidas dirigidas a mantener la confidencialidad, integridad y disponibilidad permanentes de los sistemas y servicios

Chile – LGPD – N° 19.628

En el tratamiento de los datos personales, el responsable debe garantizar estándares adecuados de seguridad, protegiéndolos contra el tratamiento no autorizado o ilícito, y contra su pérdida, filtración, daño accidental o destrucción. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la naturaleza de los datos.

El responsable establecerá controles y medidas adecuadas para preservar el secreto o confidencialidad. Este deber subsiste aún después de concluida la relación con el titular.

Protección de datos en México



Protección de datos en México



Vulneraciones de los datos personales



Protección de los datos

Información



Consentimiento



Licitud



Proporcionalidad



Calidad



Finalidad



Lealtad



Responsabilidad



¿cómo podemos ejercer los principios contenidos en los artículos 6o. y 16 de la LFPDPPP Y LGPDPPSO, respectivamente?

Artículo 16. El respeto de la protección de datos personales, derechos humanos, propiedad industrial, propiedad intelectual, quedan amparados conforme a las leyes en la materia durante el cumplimiento de esta ley.

¿Cómo se integra el uso de datos en las tecnologías emergentes?



SECURITY
DAYS 2024

Consentimiento



Mínimo uso indispensable

Infraestructura crítica



Ética y transparencia



Vigilancia externa



Gestión de amenazas

Consentimiento



Mínimo uso indispensable



Infraestructura crítica



Ética y transparencia



Vigilancia externa



Gestión de amenazas

Consentimiento



Mínimo uso indispensable



Infraestructura crítica



Ética y transparencia



Vigilancia externa



Gestión de amenazas

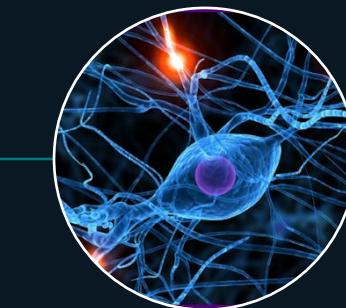


Consentimiento



Mínimo uso indispensable

Infraestructura crítica



Ética y transparencia



Vigilancia externa



Gestión de amenazas

Consentimiento



Mínimo uso indispensable



Infraestructura crítica



Ética y transparencia



Vigilancia externa



Gestión de amenazas

Consentimiento



Mínimo uso indispensable

Infraestructura crítica



Ética y transparencia



Vigilancia externa



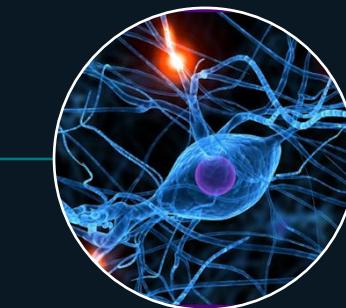
Gestión de amenazas

Consentimiento



Mínimo uso indispensable

Infraestructura crítica



Ética y transparencia



Vigilancia externa



Gestión de amenazas

¿Cómo se regula el uso de datos en las tecnologías emergentes?



SECURITY
DAYS 2024

El 25 de noviembre del 2021, la UNESCO, preocupada por el desarrollo exponencial de la inteligencia artificial en la actualidad, lanzó el primer Acuerdo Mundial sobre la Ética de la Inteligencia Artificial:

“Este marco ético define valores y principios comunes que guiarán y garantizarán un desarrollo saludable de esta tecnología. Afirma que todos los individuos deberían poder acceder a sus registros de datos personales o incluso borrarlos y prohíbe explícitamente el uso de sistemas de inteligencia artificial para la calificación social y la vigilancia masiva”.





SECURITY
DAYS 2024

Iniciativas Vigentes

16/04/2024

Iniciativa: Se reforman los artículos 5, 11, 17, 24; se adiciona un último párrafo al artículo 4; se adiciona un último párrafo al artículo 13; se adiciona una fracción XI al artículo 14; y sea adiciona un artículo 114 Bis de la Ley Federal del Derecho de Autor

Tema: Protección de derechos de autor e inteligencia artificial

28/11/2023

Iniciativa: Se adiciona una nueva fracción VIII Bis al artículo 11 de la Ley General en Materia de Humanidades, Ciencias, Tecnologías e Innovación.

Tema: Impulso de Investigación y Desarrollo de Conocimiento sobre Inteligencia Artificial

27/02/2024

Iniciativa: Reforma y adiciona los artículos 21 y 24 de la Ley Federal del Derecho de Autor

Tema: Derechos de Autor

Iniciativas Vigentes

28/11/2023

Iniciativa: Expide la Ley que Regula el Uso de la Inteligencia Artificial.

Tema: Expide Legislación

05/03/2023

Iniciativa: Reforma y adiciona los artículos 20 Ter y 20 Quáter de la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia

Tema: Delitos

20/02/2024

Iniciativa: Se adiciona el capítulo III y los artículos 211 Ter y 211 Ter 1, al Código Penal Federal

Tema: Delitos

Desafíos en la regulación de ciberseguridad y datos a nivel nacional



SECURITY
DAYS 2024

Ciberseguridad en México

4 mill.

de ciberataques
al día

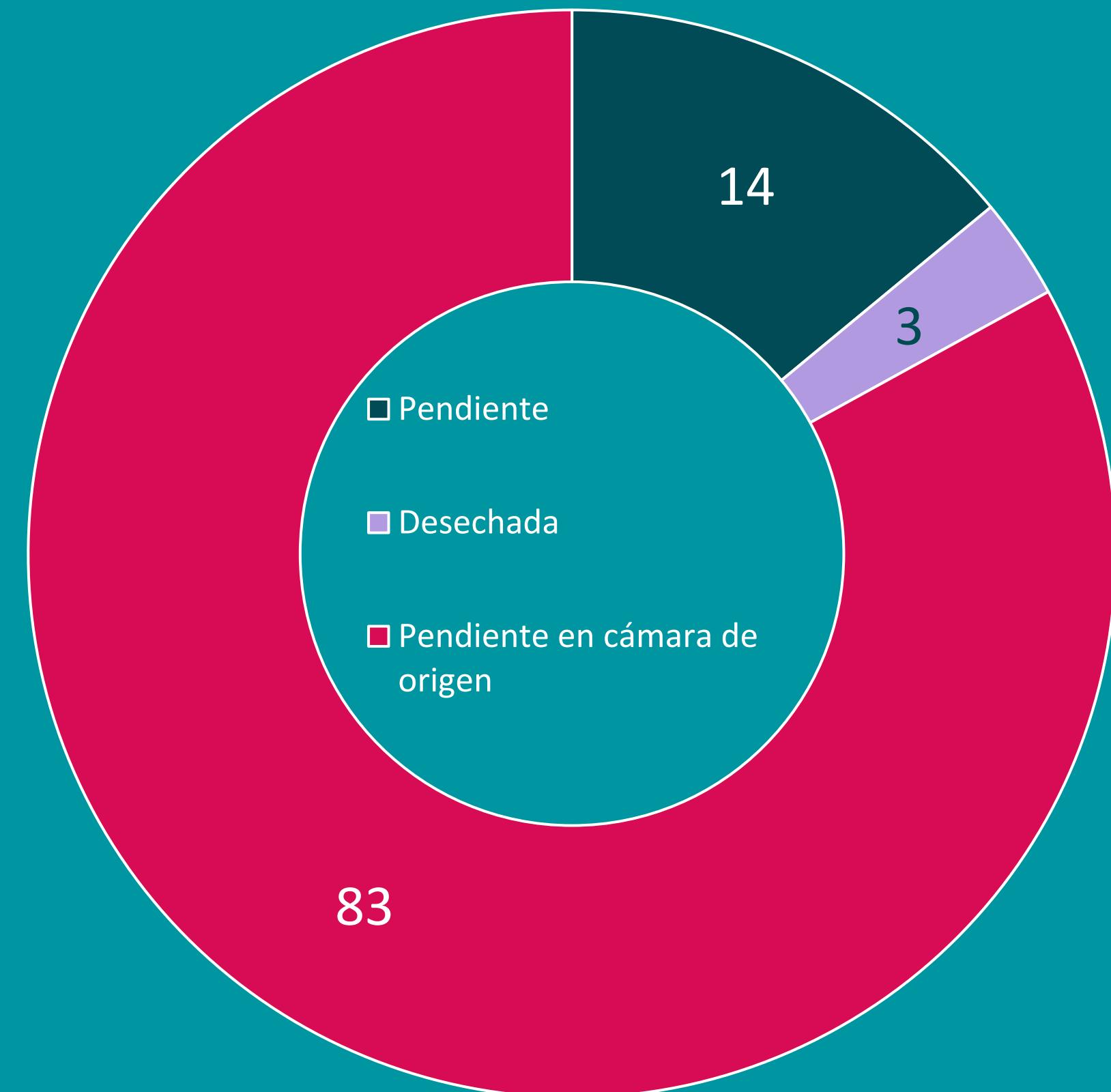
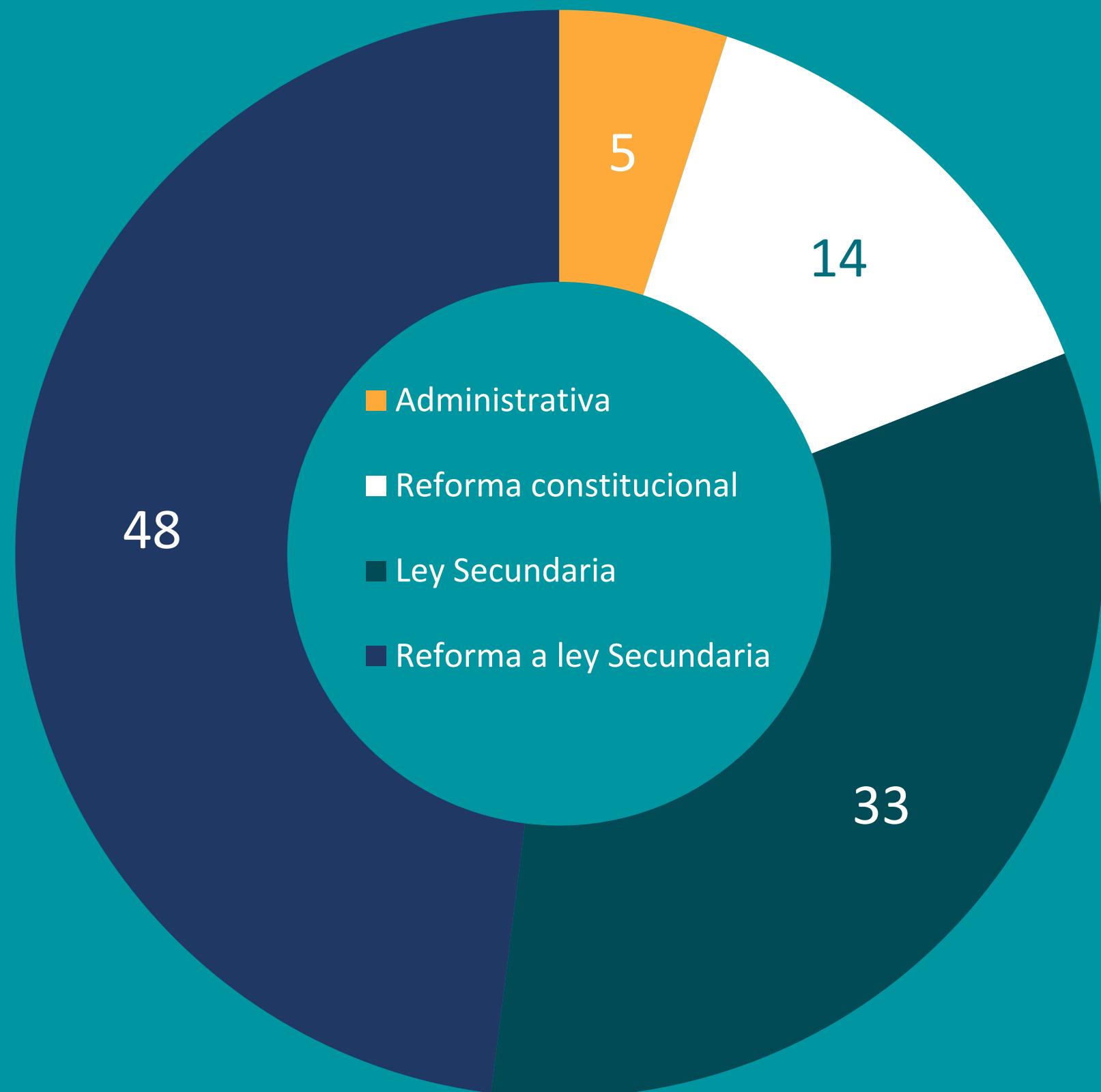
20-30%

Les cuesta a las
MiPyMes

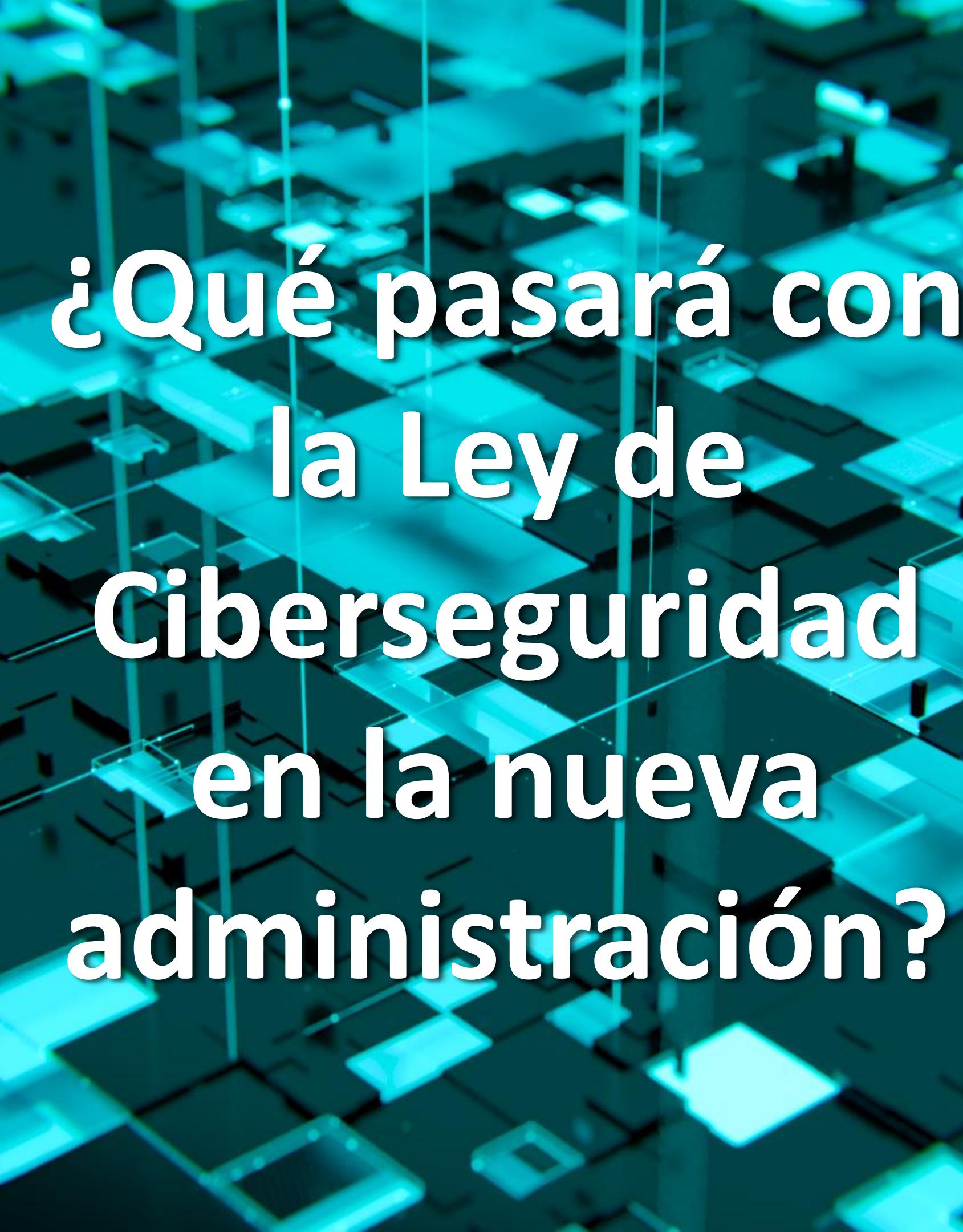
11

Iniciativas
pendientes

Iniciativas de Ley



Fuente: Abogada



¿Qué pasará con la Ley de Ciberseguridad en la nueva administración?

- No hay una norma jurídica aprobada, a pesar de que fue un compromiso del sexenio pasado
- Tanto para la aplicación de una ley como para el desarrollo de un Centro especializado en IA y Ciberseguridad se requiere talento humano escaso en México y el mundo.
- La más actual que está en revisión aún requiere de una revisión, sobre todo en la parte técnica.

Una solución milagrosa

Proteger los datos como el oro corporativo



SECURITY
DAYS 2024

Piso preventivo

Leyes Federal
y General de
Protección de
datos

Infraestructura crítica

Iniciativa de
Ley Federal de
Ciberseguridad

Derechos Humanos

Iniciativa de
Ley Federal de
Ciberseguridad

Iniciativa
Regulación de
la inteligencia
Artificial

Instituciones regulatorias

Manejo de riesgos

Leyes Federal y
General de
Protección de
datos

Multas/Sanciones

Transparencia

vulneraciones

Iniciativa
Federal para
Regular el uso
de la IA

Organismos
de
protección

Iniciativa de
Ley Federal de
Ciberseguridad

Privacidad y derechos

Un aliado más que un enemigo



Tecnología



Gestión



Procesos

POST EVENT

03 diciembre - virtual

06 diciembre - presencial



**SECURITY
DAYS2024**



Gracias.



**SECURITY
DAYS2024**





CÓDIGO QR VIRTUAL





Laura Canales
Pre-Sales ESET México

Master en Seguridad en TIC & Master en Ciberinteligencia

La cultura de ciberseguridad la construimos entre todos

LAURA CANALES

PRE-SALES ENGINEER ESET MÉXICO

Master en Seguridad en TIC & Master en Ciberinteligencia



**SECURITY
DAYS2024**

“Cuando creíamos que teníamos todas las respuestas, de pronto, nos cambiaron las preguntas”

Factores de cambios externos



Nuevas Regulaciones

- 1. Protección de datos:** Debemos asegurar la protección de datos sensibles y personales, garantizar la **confidencialidad, disponibilidad e integridad de la información.**
- 2. Evaluación de riesgo y auditorias:** Contemplemos realizar evaluaciones de riesgo en **sistemas, procesos, planes de seguridad interna.** Considerando los cambios en las auditorías externas del sector que debemos cumplir.
- 3. Responsabilidad y Gobernanzas:** Diseñar claramente las **responsabilidades del nuestro equipo y roles** involucrados en la seguridad de la información. Acompañar con planes vigentes de procesos actualizados.

Vida laboral digital

1. Formatos Híbridos:

Cambio en la dinámica laboral, nuevas reglas de convivencia donde **el colaborador cuenta con movilidad para su sector de trabajo.**

2. Flexibilidad y Autonomía:

Debemos asegurar la protección de datos sensibles y personales, **garantizando la libertad del colaborador.**

3. Herramientas colaborativas:

La forma de trabajo comunitario se realiza sobre plataformas colaborativas, las cuales **resguardan información sensible y clave para la organización.**

Ataques de robo de información

VANGUARDIA MX

MÉXICO COAHUILA SALTILLO OPINIÓN ECONOMÍA SHOW DEPORTES VIDA UTILIDAD EXPERTOS PREMIUM Nuestro

Fallas en el sistema de Coppel crean rumor sobre posible hackeo a sus servidores, ¿Qué información personal recopila su app?

INFORMACIÓN / 18 abril 2024



México

INTERNACIONAL · MÉXICO · OPINIÓN · SOCIEDAD · ECONOMÍA · CIENCIA / MATERIA · TECNOLOGÍA · CULTURA · DEPORTES · GENTE Y ESTILO DE VIDA

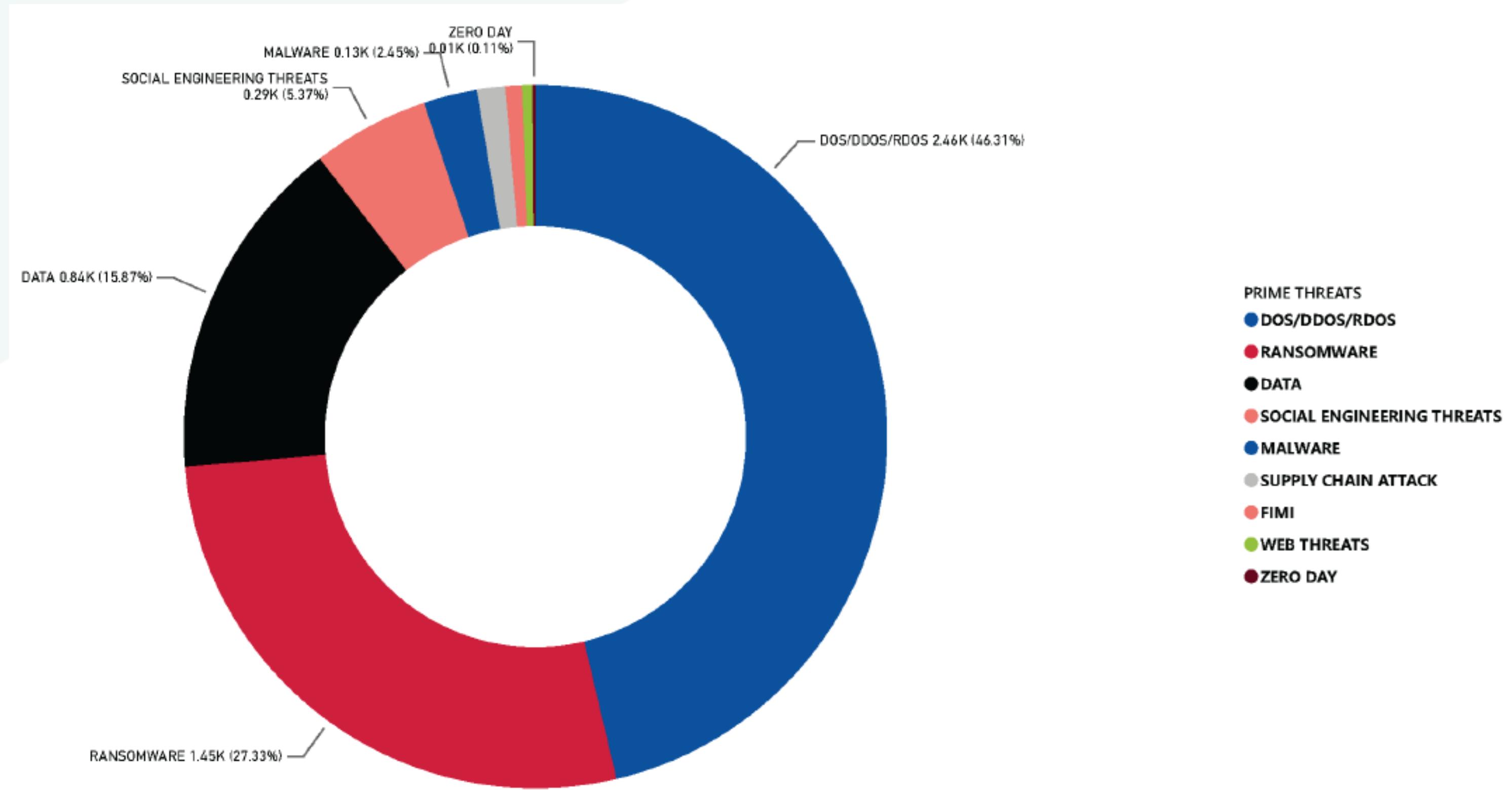
VIOLENCIA CONTRA PERIODISTAS >

La filtración de datos de los periodistas que cubren la ‘mañanera’ se hizo a través del usuario de un antiguo trabajador del Gobierno

Las autoridades aseguran que el robo se realizó desde una dirección IP en España, pero desconocen quién lo hizo ni sus motivos

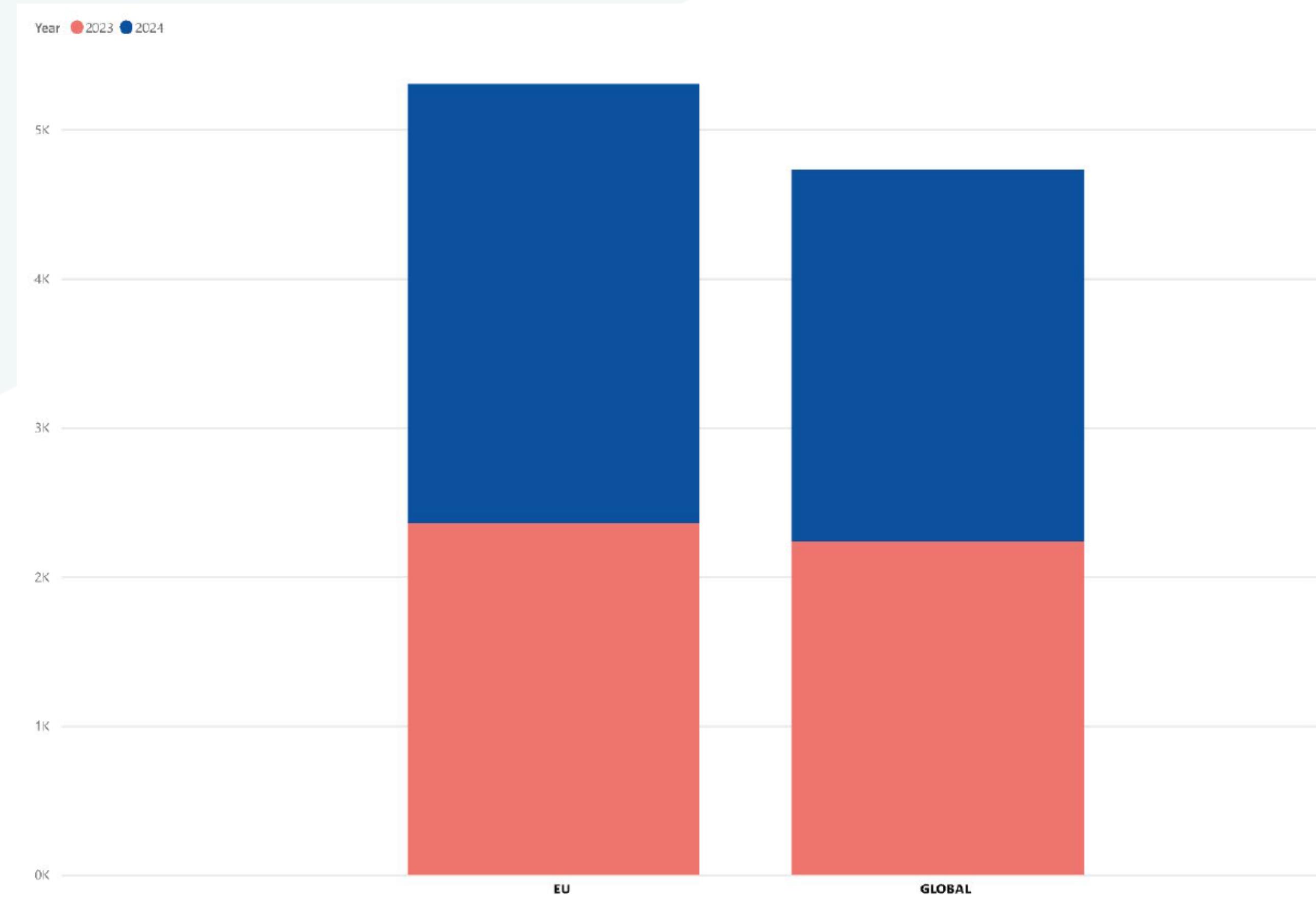


Número de amenazas por grupo

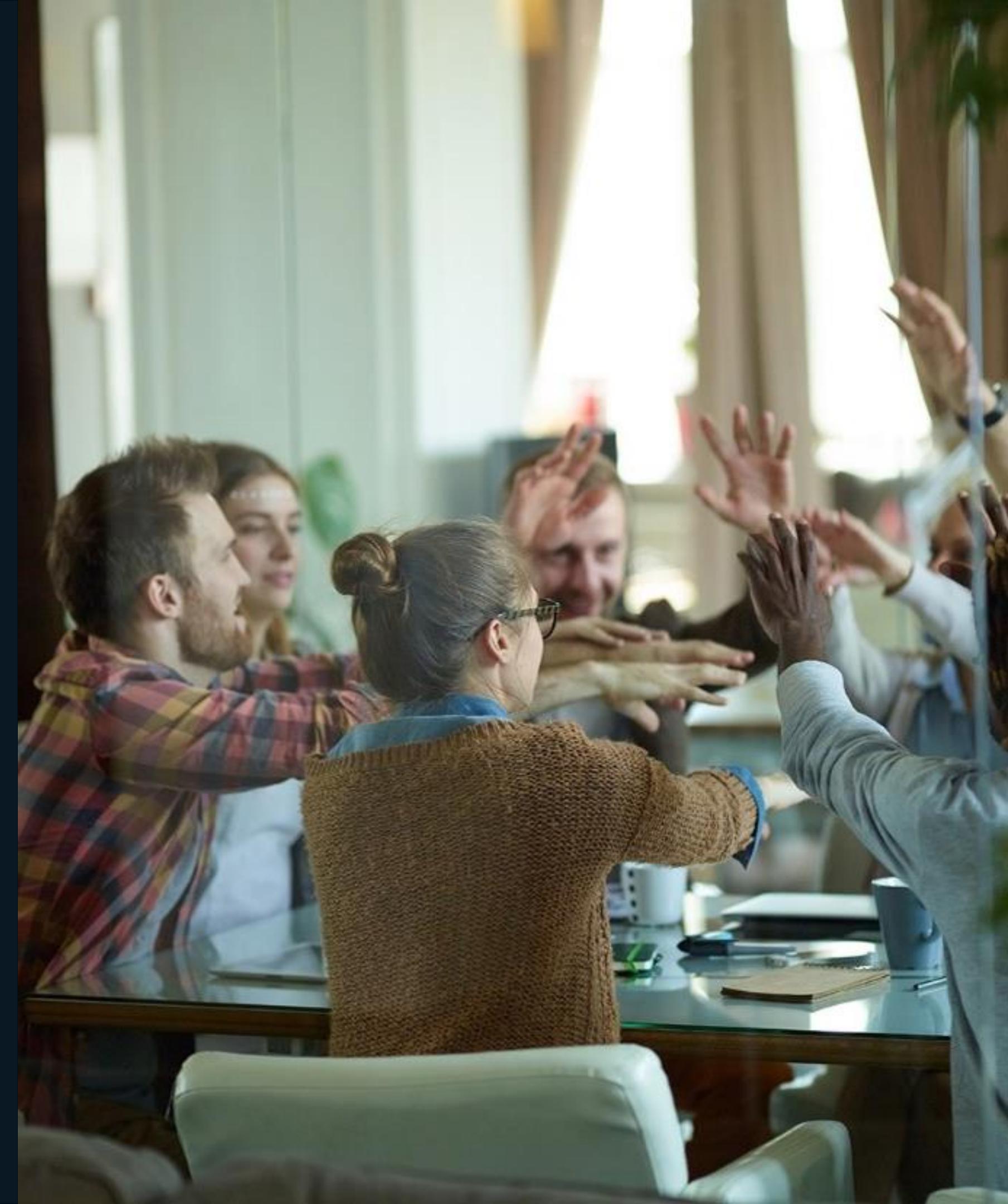


* Fuente: ENISA THREAT LANDSCAPE 2024 | Septiembre 2024

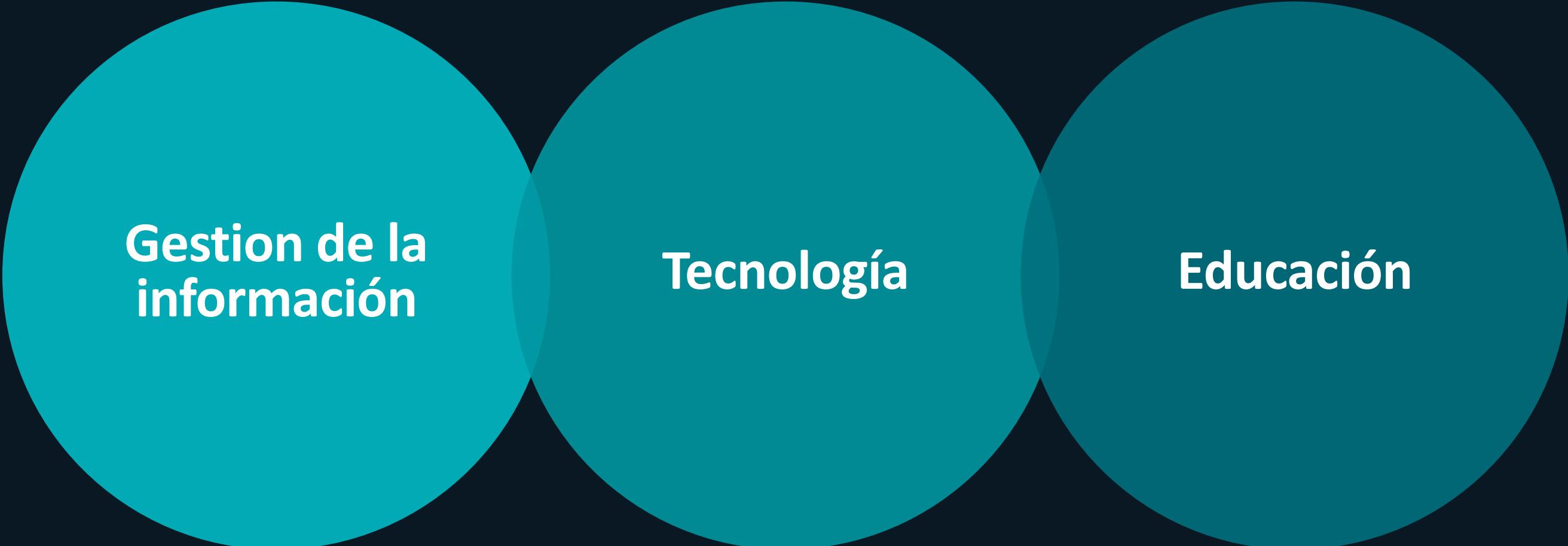
Eventos globales y de la UE (Julio 2023 – Junio de 2024)



Consolidemos la cultura de ciberseguridad



La cultura es transversal a la organización



Gestión de la información

Tecnología

Educación

Gestión de la información

- ✓ Procesos de información dentro de la organización
- ✓ Plan de contingencia
- ✓ Administración centralizada
- ✓ Continuidad del negocio



Tecnología

- ✓ Protección antimalware
- ✓ Patch Management
- ✓ Doble factor de autenticación
- ✓ Cifrado
- ✓ Sandbox en la nube
- ✓ Protección de herramientas colaborativas
- ✓ Servicios profesionales:
 - Análisis de vulnerabilidades
 - Ethical Hacking
 - CISO as a Service
 - MDR



Seguridad
por capas

Educación

- ✓ Plan integral de concientización.
- ✓ Acompañamos a cada colaborador con sus metricas, para evaluar seguimiento.
- ✓ Capacitaciones lúdicas + workshops presenciales.
- ✓ Campañas controladas de phishing.



Incorporamos
hábitos de
seguridad

“El verdadero problema de la
humanidad es el siguiente: tenemos
emociones del Paleolítico,
instituciones medievales y tecnología
propia de un dios. Y eso es
terriblemente peligroso”



-Edward Osborne Wilson

Gracias



**SECURITY
DAYS2024**



ESPA^OCIO DE PREGUNTAS

¡SORTEO!





SECURITY DAYS 2024

CICLO DE EVENTOS DE
SEGURIDAD DIGITAL

Progress. Protected.

¡GANADOR SORTEO!

GIFTCARD AMAZON
\$2,000.00MXN

GANADOR: XXXX

¡GANADOR SORTEO!

GIFTCARD AMAZON
\$2,000.00MXN

GANADOR: XXXX

iSORTEO!



SECURITY
DAYS 2024

¡GANADOR SORTEO!

GIFTCARD AMAZON
\$2,000.00MXN

PRESENCIAL

¡GANADOR SORTEO!

GIFTCARD AMAZON
\$2,000.00MXN

PRESENCIAL



SECURITY DAYS 2024

CICLO DE EVENTOS DE
SEGURIDAD DIGITAL

Progress. Protected.



Gabriela Rodríguez

Sales Manager ESET México

