



Panorama de las amenazas en Chile

PRIMER SEMESTRE 2026

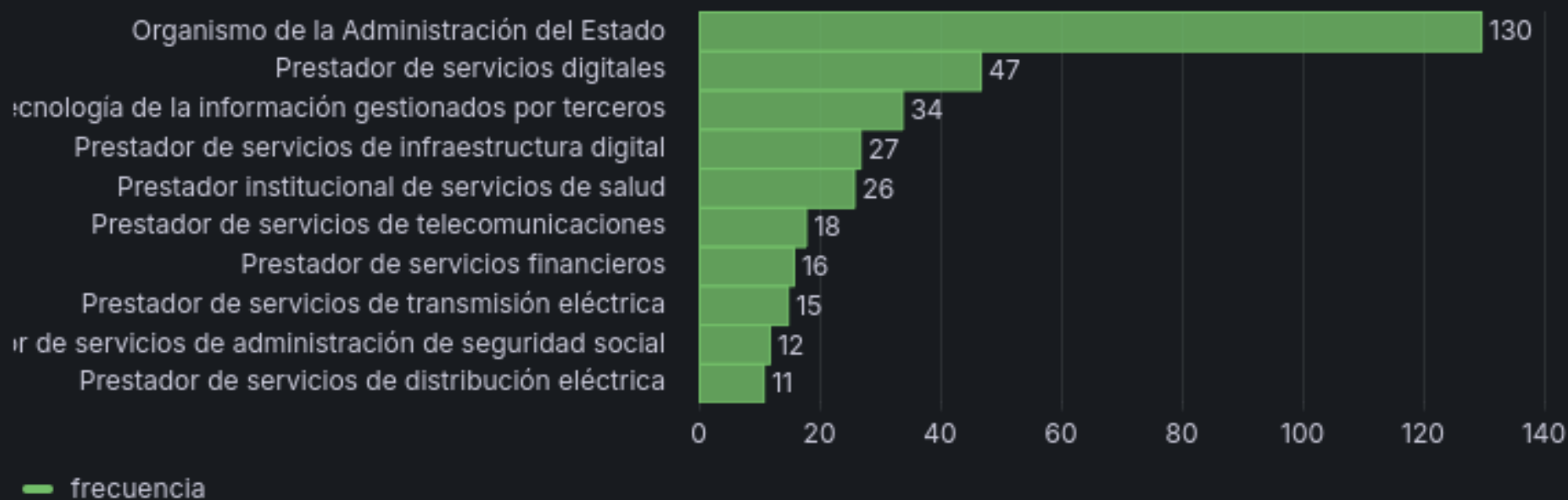


Reporte de incidentes

Entre enero y junio del 2026 recibimos 324 reportes.

~54 ciberataques de efecto significativo por mes.

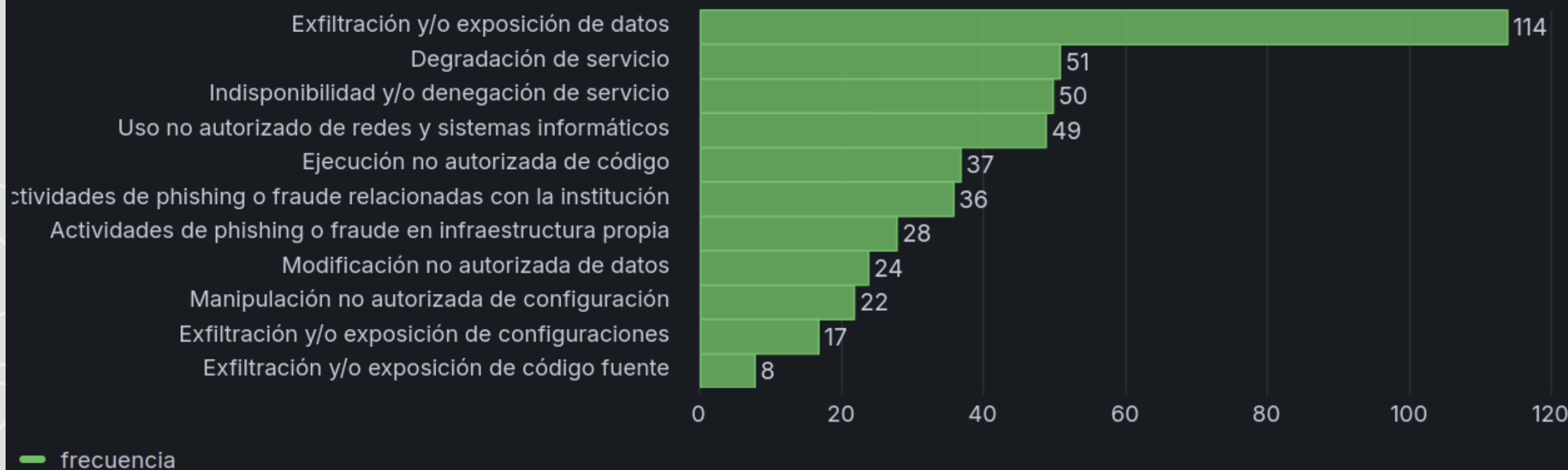
Principales sectores afectados



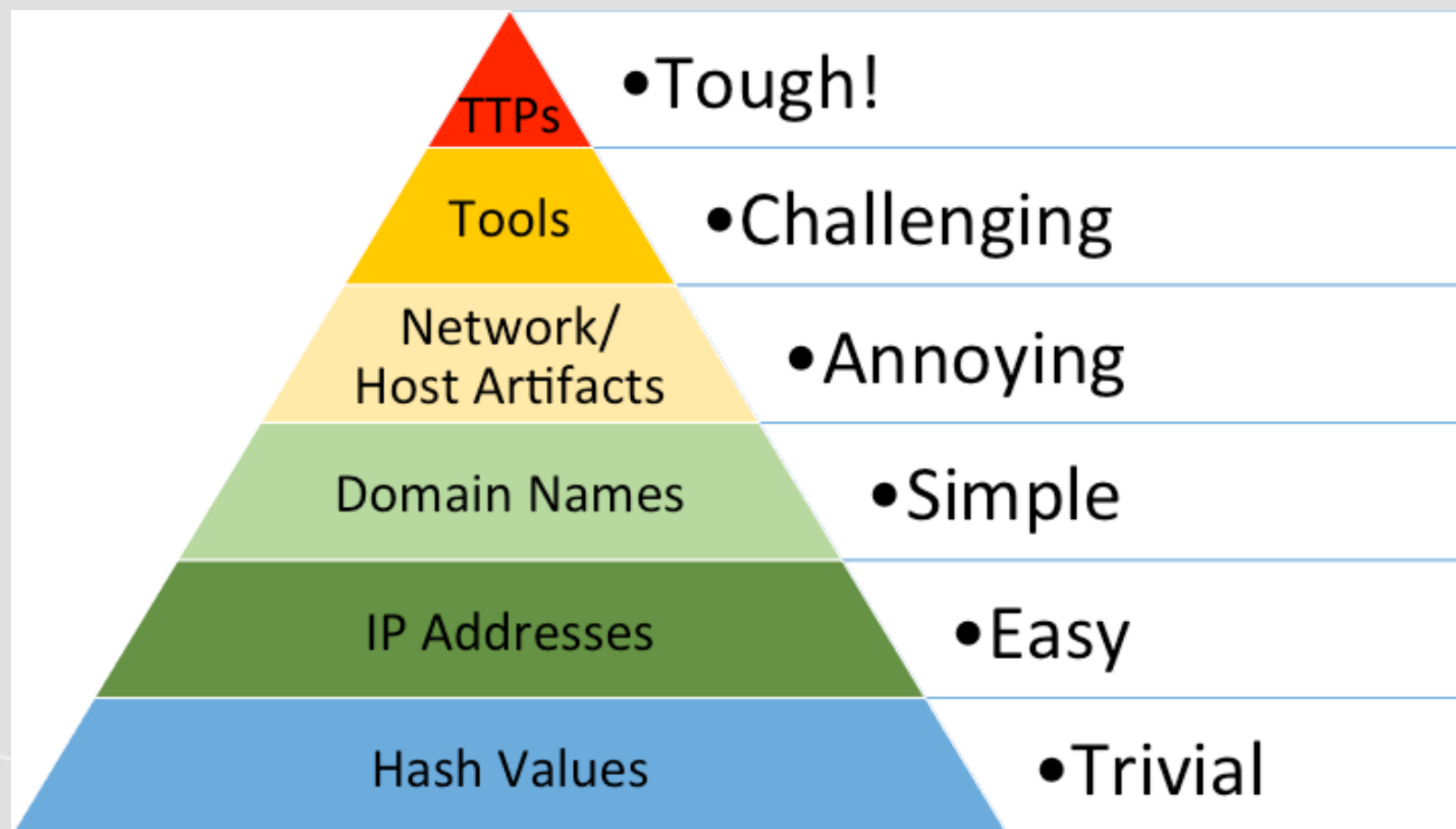
Reporte de incidentes

Entre enero y junio del 2026

Áreas de impacto reportadas



Metodología de análisis



[TA0001] Acceso Inicial

Técnicas que utilizan varios vectores de entrada para ganar su punto de apoyo inicial dentro de una red.



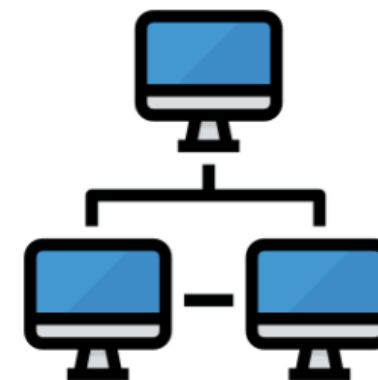
[T1078] Valid accounts



[T1190] Exploit Public-Facing Application



[T1566] Phishing



[T1566] External remote services

Análisis de amenazas: **Filtraciones**

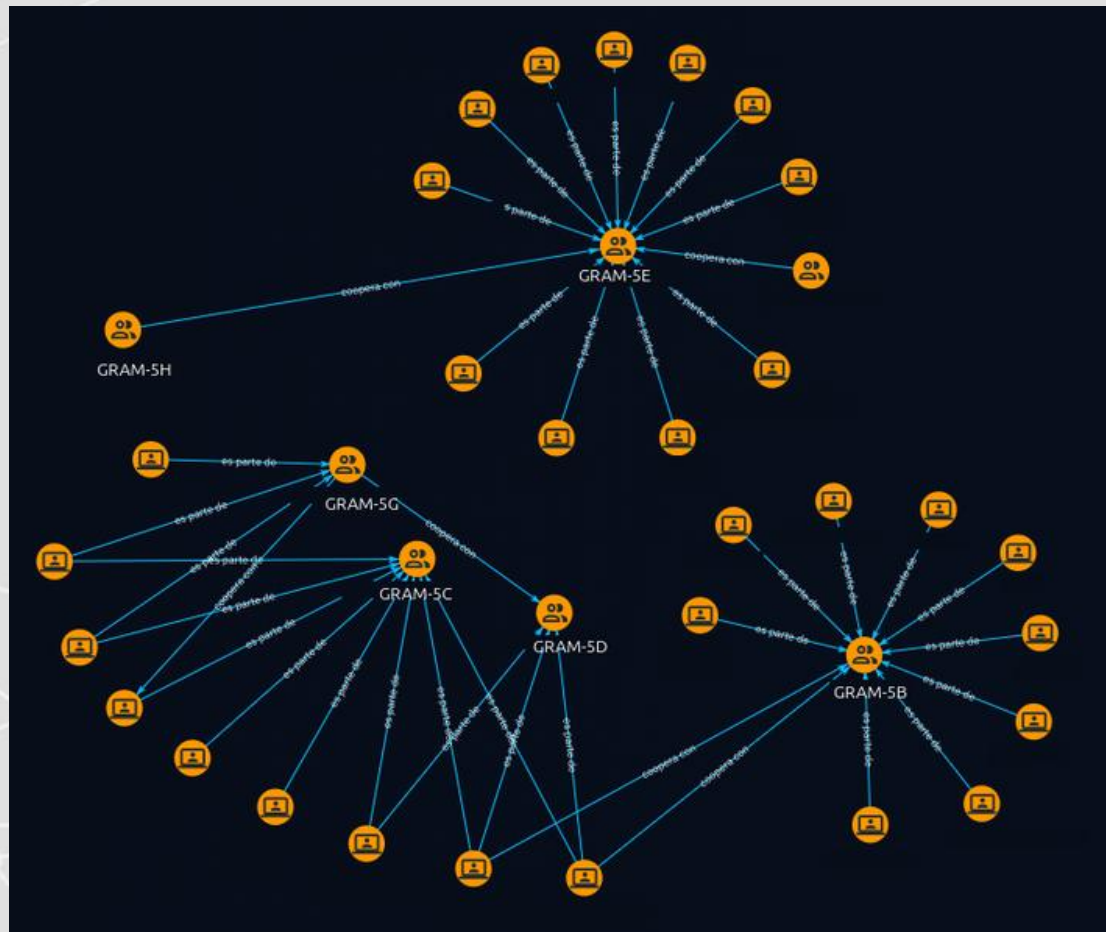


Análisis de amenazas: Filtraciones

GRUPOS DE AMENAZA

- GRAM-5B
- GRAM-5C
- GRAM-5D
- GRAM-5E

Afectación comprobada: 47 incidentes



- 📌 Especializados en la exfiltración de información
- 📌 Integrantes latinoamericanos
- 📌 Preferencia por atacar al sector público
- 📌 Mensajes hacktivistas
- 📌 Mediáticos
- 📌 Cooperan entre sí

[TA0001] Acceso Inicial

Técnicas que utilizan varios vectores de entrada para ganar su punto de apoyo inicial dentro de una red.



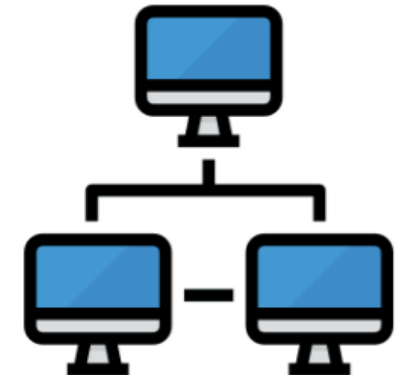
[T1078] Valid accounts



[T1190] Exploit Public-Facing Application



[T1566] Phishing



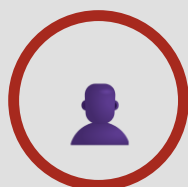
[T1566] External remote services

ACCESO INICIAL

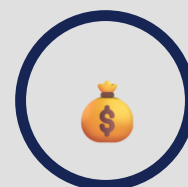
[T1078] Valid accounts



**Equipo se infecta con
malware**



**Usuario se ingresa con
credenciales válidas**



**Corredor de acceso
inicial las vende**



**Nuevo atacante las
utiliza**

Filtraciones previamente publicadas

ACCESO INICIAL

[T1078] Valid accounts

Técnica utilizada en el 78% de los incidentes confirmados.

El 26% de los incidentes confirmados consistieron solamente en esto.

EXFILTRACIÓN

[T1567] Exfiltration Over Web Service

Exfiltración desde:

- 📌 sistemas críticos, operacionales, de soporte y legacy
- 📌 ambientes de producción o de desarrollo

EXFILTRACIÓN

[T1567] Exfiltration Over Web Service

Exfiltración de:

- 📌 información relacionada con una organización desde sistemas de sus proveedores, clientes y usuarios
- 📌 información en tiempo real desde API deficientemente monitoreadas

EXFILTRACIÓN

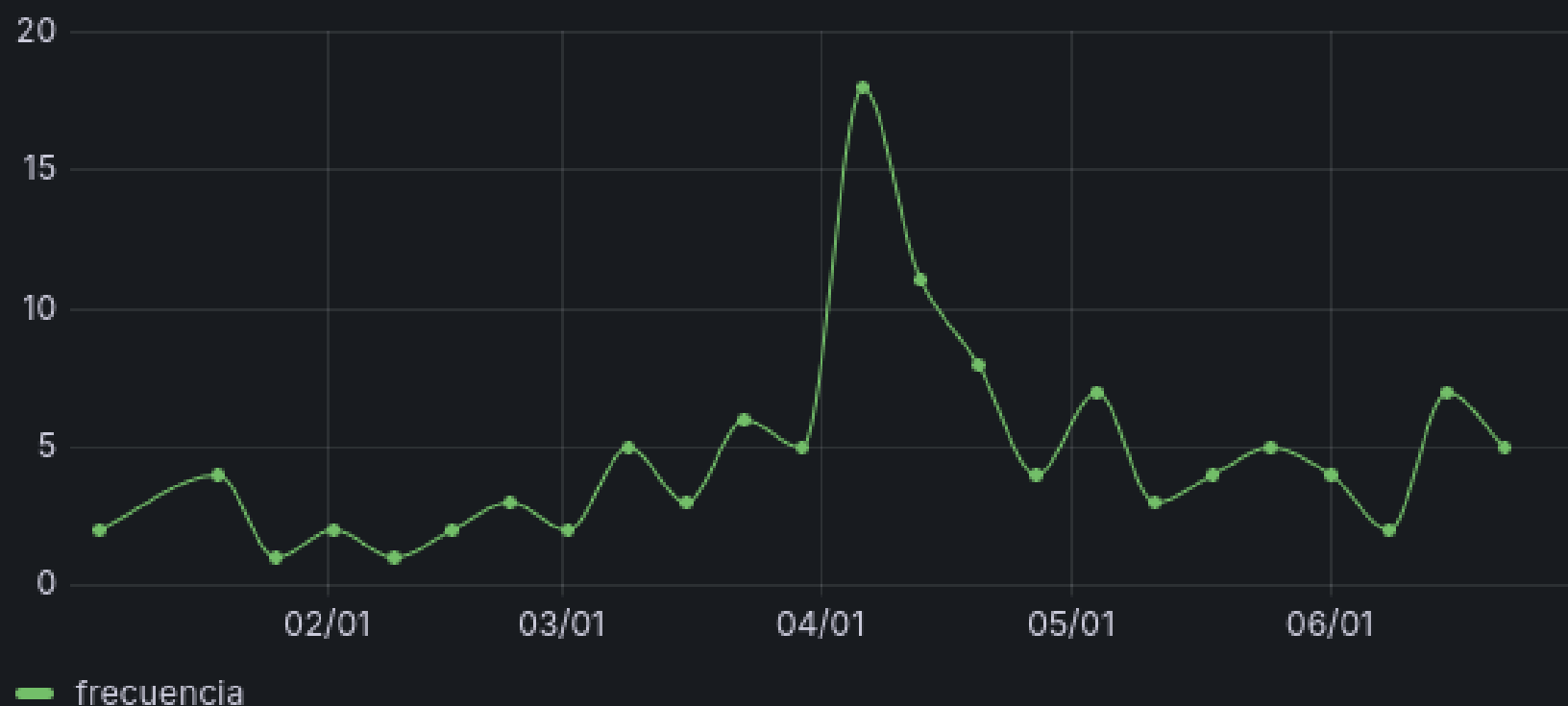
[T1567] Exfiltration Over Web Service

Técnica utilizada en el 43% de los incidentes confirmados, siempre con acceso inicial mediante [\[T1078\] Valid Accounts](#).

Pese a que para algunos casos se comprobó que los incidentes se dieron tal como lo señalaban los atacantes, fue justamente en la exfiltración de datos donde se encontraron más diferencias entre lo publicado y la realidad.

Medidas de contención y mitigación

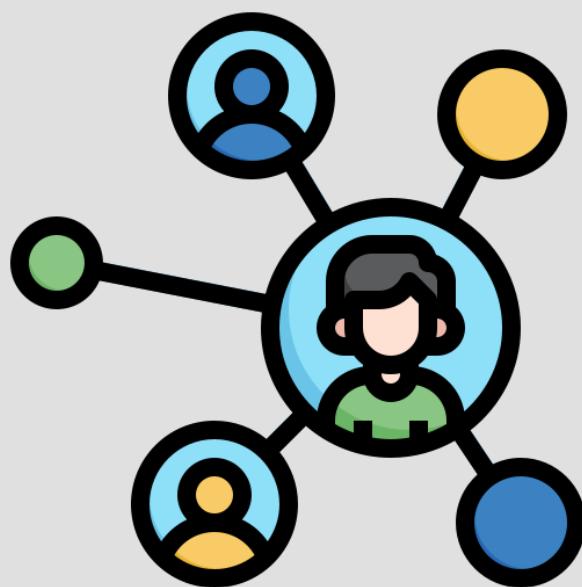
Variación de "Exfiltración y/o exposición de datos" en el tiempo



Recomendaciones

Rotación de credenciales filtradas y revisión de equipos.



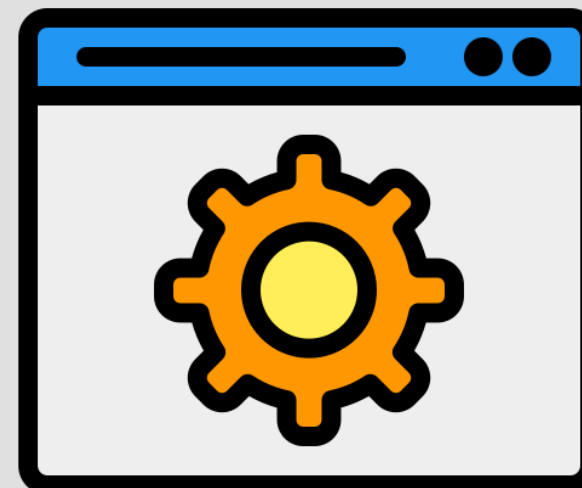


Recomendaciones

2FA y restricción de servicios a redes autorizadas.

Recomendaciones

Correcta gestión de
cuentas y separación de
entornos.



WWW.ANCI.GOB.CL/9BASICOS/

 1 / Actualizar periódicamente Actualizar periódicamente	 2 / Capacitar periódicamente Capacitar periódicamente	 3 / Minimizar privilegios Minimizar privilegios
 4 / Respalidar periódicamente la información Respalidar periódicamente la información	 5 / Asegurar redes Asegurar redes	 6 / Asegurar equipos Asegurar equipos
 7 / Monitorear en tiempo real Monitorear en tiempo real	 8 / Usar mecanismos de Múltiples Factores de Autenticación (MFA) Usar mecanismos de Múltiples Factores de Autenticación (MFA)	 9 / Usar gestor de contraseñas Usar gestor de contraseñas

Se puede vulnerar un sistema sin explotar una vulnerabilidad



Muchas gracias

