Proyecto de CSIRT de Gobierno y nueva institucionalidad

Cristian Bravo Lillo, Ph.D. - cbravol@interior.gob.cl

Director CSIRT de Gobierno, Coordinación Nacional de Ciberseguridad

Noviembre de 2023

Ministerio del Interior y Seguridad Pública

Gobierno de Chile

¿En qué estamos en Chile en ciberseguridad?

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Este es el plan

Política Nacional de Ciberseguridad 2023-2028

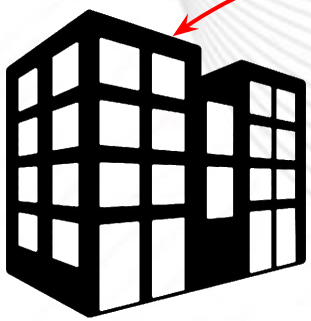
que es coordinado y supervisado por

Comité Interministerial sobre Ciberseguridad

es secretaría ejecutiva del

Coordinación Nacional de Ciberseguridad

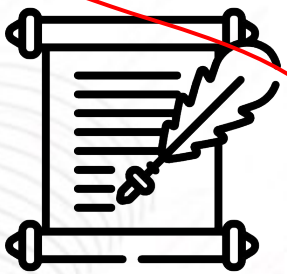
se transformará en



(Futura) Agencia Nacional de Ciberseguridad

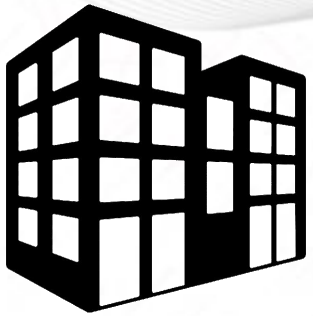
que crea la gobernanza de ciberseguridad en Chile

Esta es la base legal



Proyecto de Ley Marco de Ciberseguridad

¿Qué papel va a cumplir la Agencia?



Agencia Nacional de Ciberseguridad

1. CSIRT de Gobierno → **CSIRT Nacional**
2. Red de Conectividad del Estado → **Red de Conectividad Segura del Estado**

¿Cómo (demonios) vamos a hacer eso?

Ministerio del Interior y Seguridad Pública
Gobierno de Chile

BID
Banco Interamericano de Desarrollo

La CNC propuso al BID tomar un componente del préstamo BID (~US$27 millones) y renovar la infraestructura de la Agencia y del CSIRT.

Estamos trabajando desde junio en:

1. Fortalecer el equipo de trabajo
2. Formalizar los procesos del CSIRT
3. Generar una plataforma tecnológica nueva para la Agencia (y CSIRT)
4. Crear una comunidad de ciberseguridad de gobierno

Proyecto de Ley Marco de Ciberseguridad

- **Título 2: Obligaciones de ciberseguridad**
  - **Párrafo 1: Servicios esenciales y operadores de importancia vital**
    - Artículo 4. Ámbito de aplicación.
    - Artículo 5. Operadores de importancia vital.
    - Artículo 6. Procedimiento de calificación de los operadores de importancia vital.
  - **Párrafo 2: Obligaciones de ciberseguridad**
    - Artículo 7. Deberes generales. → Todas las organizaciones
    - Artículo 8. Deberes específicos de los operadores de importancia vital.
    - Artículo 9. Deber de reportar.

Esquema progresivo

Servicios Esenciales

Operadores de Importancia Vital

- Título 1: Disposiciones generales
  - Artículo 1. Objeto.
  - Artículo 2. Definiciones.
  - Artículo 3. Principios rectores.
- Título 2: Obligaciones de ciberseguridad
  - Párrafo 1: Servicios esenciales y operadores de importancia vital
    - Artículo 4. Determinación de los servicios esenciales e identificación de los operadores de importancia vital.
  - Párrafo 2: Obligaciones de ciberseguridad
    - Artículo 5. Deberes generales.
    - Artículo 6. Deberes específicos de los operadores de importancia vital y para la protección de los servicios esenciales.
    - Artículo 7. Deber de reportar.
- Título 3: De la Agencia Nacional de Ciberseguridad
  - Párrafo 1: Objeto, naturaleza y atribuciones
    - Artículo 8. Agencia Nacional de Ciberseguridad.
    - Artículo 9. Atribuciones.
  - Párrafo 2: Dirección, organización y patrimonio
    - Artículo 10. Dirección de la Agencia.
    - Artículo 11. Atribuciones del Director o Directora Nacional.
    - Artículo 12. Del patrimonio de la Agencia.
    - Artículo 13. Nombramiento de autoridades.
    - Artículo 14. Del personal de la Agencia.
    - Artículo 15. Prohibiciones e inhabilidades.
  - Párrafo 3: Consejo Multisectorial sobre Ciberseguridad
    - Artículo 16. Consejo Multisectorial sobre Ciberseguridad.
    - Artículo 17. Funcionamiento del Consejo.
    - Artículo 18. De las causales de cesación.
  - Párrafo 4: Red de Conectividad Segura del Estado
    - Artículo 19. Red de Conectividad Segura del Estado.
  - Párrafo 5: Equipo Nacional de Respuesta a Incidentes de Seguridad Informática
    - Artículo 20. Equipo Nacional de Respuesta a Incidentes de Seguridad Informática.
- Título 4: Otras instituciones intervinientes
  - Artículo 21. CSIRT Sectoriales.
  - Artículo 22. Facultades especiales.
  - Artículo 23. Incidentes de efecto significativo.
  - Artículo 24. Centros de Certificación Acreditados.
- Título 5: Del Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional
  - Artículo 25. Equipo de Respuesta a Incidentes de Seguridad Informática de la Defensa Nacional.
  - Artículo 26. De las funciones del CSIRT de la Defensa Nacional.
  - Artículo 27. De los Equipos de Respuesta a Incidentes de Seguridad Informática Institucionales de la Defensa Nacional.
  - Artículo 28. Deber de reporte al CSIRT de la Defensa Nacional.
- Título 6: De la reserva de información en el sector público en materia de ciberseguridad
  - Artículo 29. De la reserva de información.
  - Artículo 30. Extensión de la obligación de reserva.
  - Artículo 31. Deber de reserva de la Agencia.
  - Artículo 32. Sanciones.
- Título 7: De las infracciones y sanciones
  - Artículo 33. De las infracciones.
  - Artículo 34. Procedimiento administrativo por infracción de ley.
  - Artículo 35. Procedimiento de reclamación judicial.
  - Artículo 36. Responsabilidad administrativa del jefe superior del organismo público.
  - Artículo 37. Responsabilidad del funcionario o funcionaria infractor.
  - Artículo 38. Agravante especial.
- Título 8: Del Comité Interministerial de Ciberseguridad
  - Artículo 39. Comité Interministerial sobre Ciberseguridad.
  - Artículo 40. De los integrantes del Comité.
  - Artículo 41. De la secretaría ejecutiva.
  - Artículo 42. De la información reservada.
  - Artículo 43. Del reglamento.
- Título 9: Órganos autónomos constitucionales
  - Artículo 44. Regímenes especiales.
- Título 10: De las modificaciones a otros cuerpos legales
  - Artículo 45.
  - Artículo 46.
  - Artículo 47.
  - Artículo 48.
- Título 11: Disposiciones transitorias
  - Artículo primero. Entrada en vigencia y personal.
  - Artículo segundo.
  - Artículo tercero.
  - Artículo cuarto.
  - Artículo quinto.
  - Artículo sexto. Renovación de los miembros del Consejo Multisectorial sobre Ciberseguridad.
  - Artículo séptimo.
  - Artículo octavo. Sobre los servicios esenciales.

Art. 7: Deberes generales

Aplicar medidas neces venir, reportar y resolver incidentes → gestión de riesgos

Serán diferenciados, según tipo de institución.

Implementar **protocolos y estándares** establecidos por Agencia y por regulación sectorial respectiva

Cristian Bravo Lillo, Ph.D. - cbravol@interior.gob.cl - noviembre de 2023

Art. 8: Deberes específicos de OIV

a. Implementar un sistema de gestión de seguridad (SGSI)
b. Mantener registros de acciones (logs)
c. Implementar planes de continuidad operacional (BCP)
d. Revisar y realizar ejercicios de simulación (TTX)
e. Contener incidentes de ciberseguridad
f. Contar con certificaciones que especifique reglamento
g. Informar a comunidad de incidentes que expongan datos sensibles o cuando sea necesario para evitar un incidente
h. Capacitar de forma continua
i. Designar un encargado de ciberseguridad

Art. 9: Deber de reportar

¿Qué se debe reportar? → ciberataques e incidentes "significativos":

a. **Alerta temprana**: en 3 horas
b. **Evaluación inicial, gravedad, impacto, e IoC** (si existen): en 24 horas para OIV, en 3 días para el resto
c. **Informe final**: en 15 días

Hablemos del elefante en la sala

- Contarle al resto de un hackeo “se siente mal”. Uno siente que lo hizo pésimo, y que todo el mundo lo está observando.
- **Cuando uno observa un hackeo de otro, uno aprende mucho**.

Los hackeos son cuento de todos los días. Nadie está mirando especialmente, y nadie se alegra de que a otro lo hackeen.

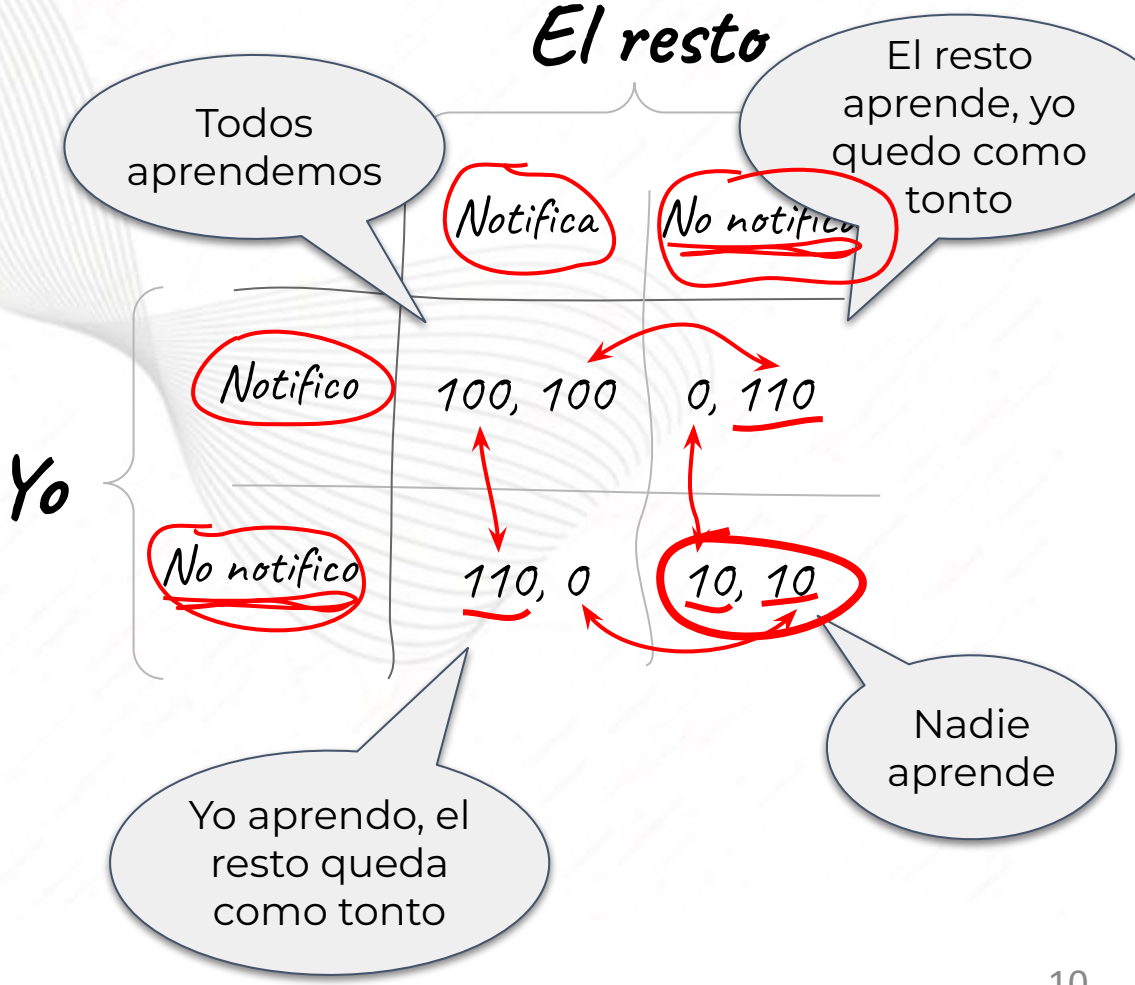
En una comunidad técnica, cuando uno puede “observar” el hackeo de otro, uno sí aprende mucho.

“Notificar, o no notificar”

Aprendizaje:
- *“Veo” el hackeo de otro:* **+100**
- *No veo nada:* **+0**

Percepción:
- *Si me hackean, “quedo como tonto”:* **+0**
- *Si parece que no me han hackeado, parezco OK (aunque en realidad igual me van a hackear)* **+10**

La estrategia dominante de todos es no notificar, a pesar de que notificar es mejor para todos.

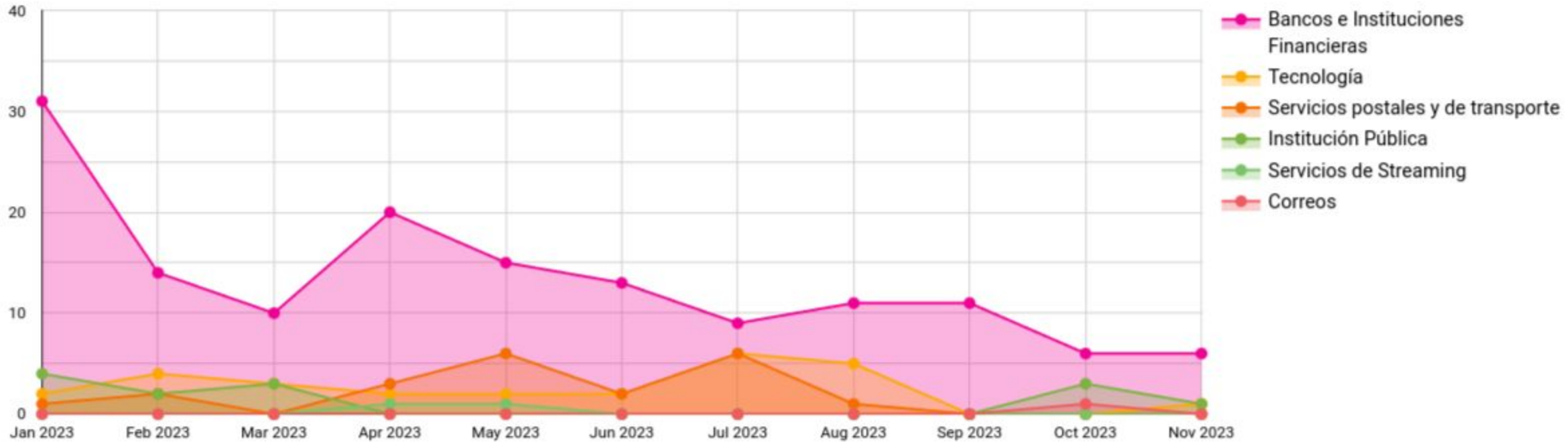


Ministerio del Interior y Seguridad Pública

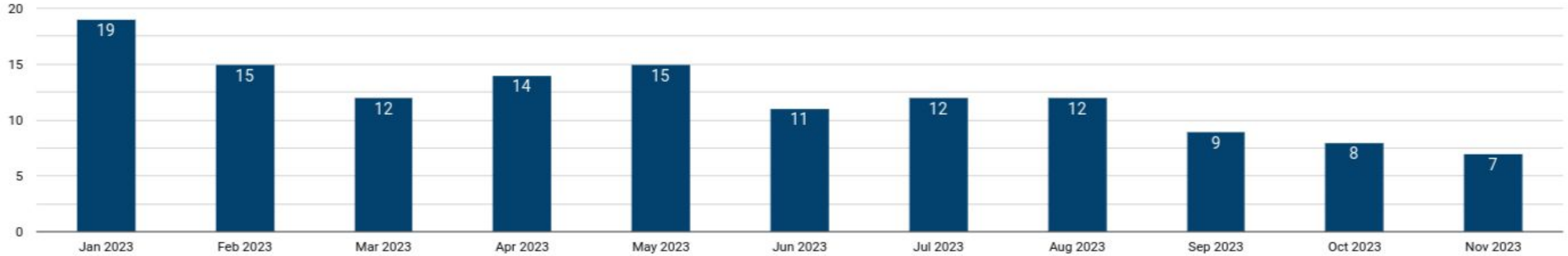
Gobierno de Chile

¿En qué estado estamos hoy en el Gobierno?

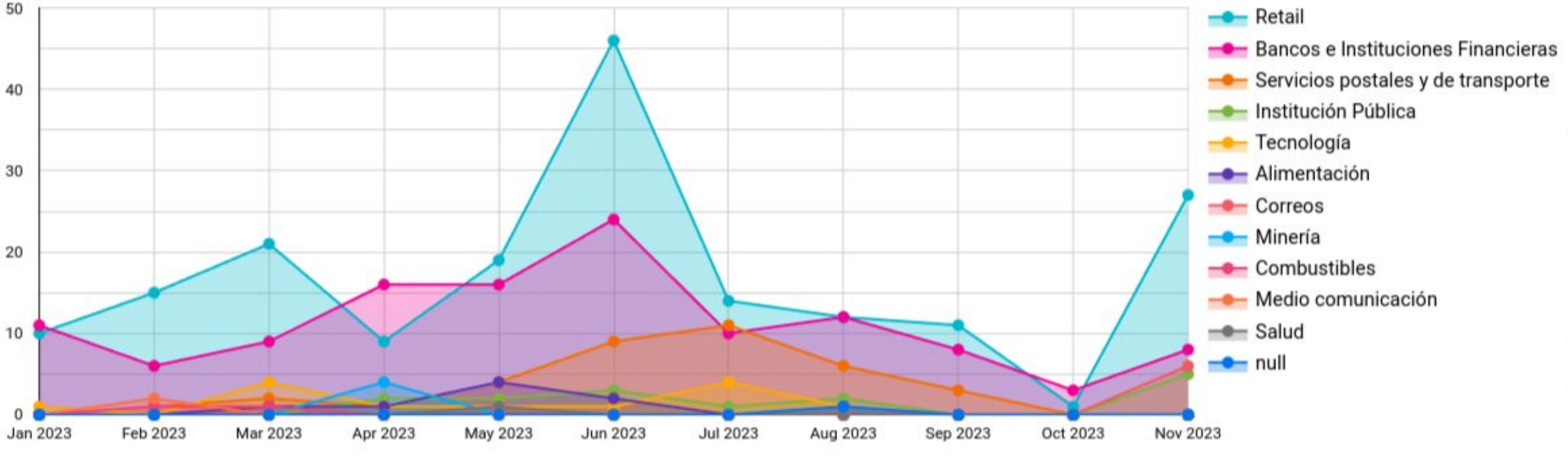
Casos de phishing observados por o reportados al CSIRT en 2023



Número de reportes de phishing del CSIRT en 2023



Suplantación de web en 2023 (observadas por el CSIRT)

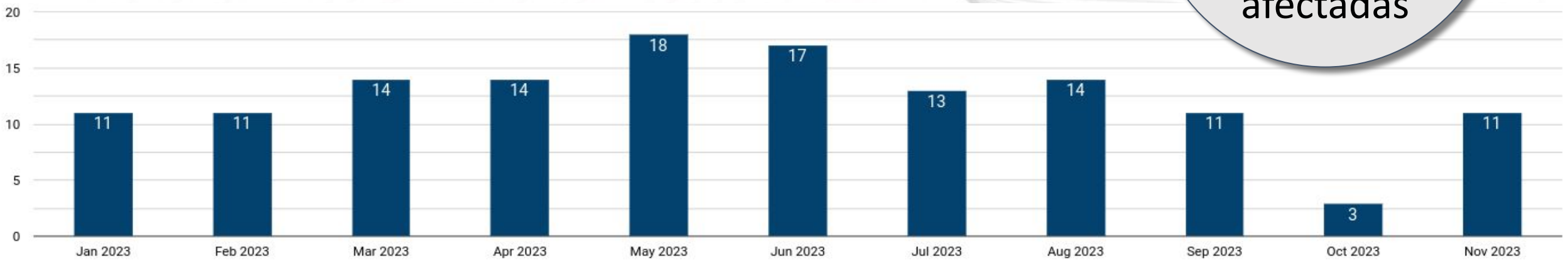


Número de reportes de suplantación del CSIRT de Gobierno en 2023

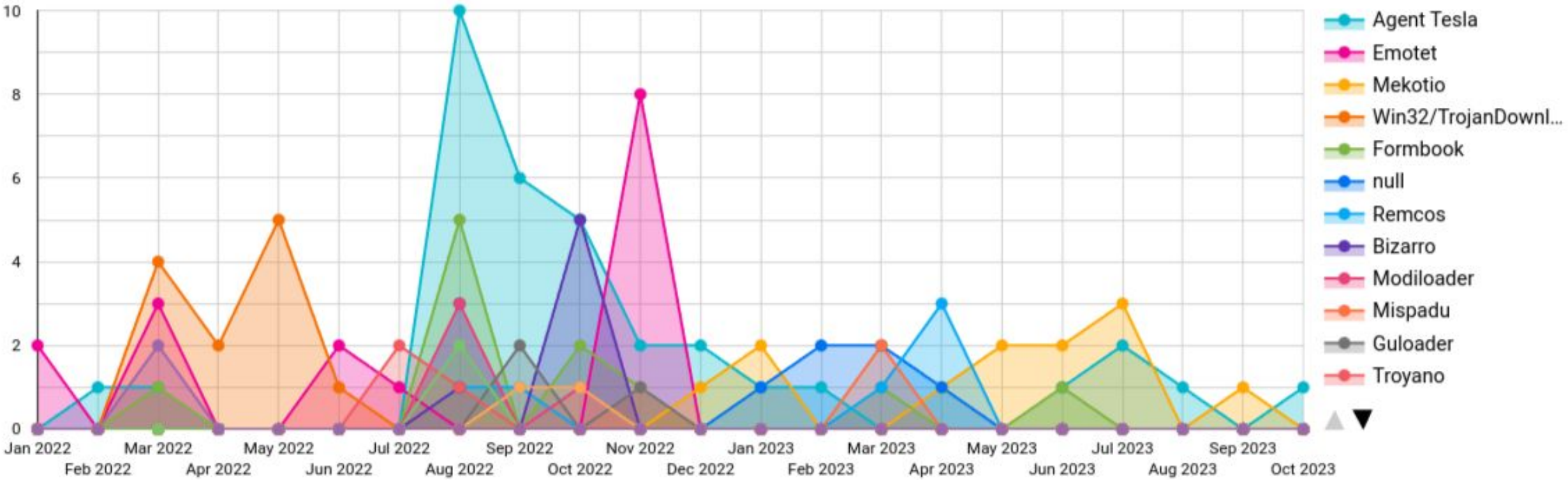
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

104

instituciones afectadas



Malware observado en 2022 y 2023



Nuestros servicios

- **Apoyo a respuesta a incidentes**
  - Diagnóstico
  - Análisis de malware
  - Comunicación política
  - Mediación con proveedores
- **Escaneo de vulnerabilidades**
  - Automático sobre lista de recursos
  - De exploración
  - A pedido
  - Monitoreo continuo de sitios en RCE
- **Pentesting (a pedido)** 

- **Información y estadísticas** 

- **Auditoría y apoyo normativo** 

- **Entrenamiento y concientización** 

- **Inteligencia de amenazas** 

¿Cómo me comunico con el CSIRT?

incidentes@interior.gob.cl para notificar incidentes, solicitar ayuda, reportar problemas y requerir escaneos.

csirt-comunicaciones@interior.gob.cl para información general, servicios, capacitaciones, eventos o actividades sobre ciberseguridad.

csirt-legal@interior.gob.cl para requerimientos legales o judiciales.

¡Muchas gracias!

Cristian Bravo Lillo, Ph.D. - cbravol@interior.gob.cl

Director CSIRT de Gobierno, Coordinación Nacional de Ciberseguridad

Noviembre de 2023

Ministerio del Interior y Seguridad Pública

Gobierno de Chile