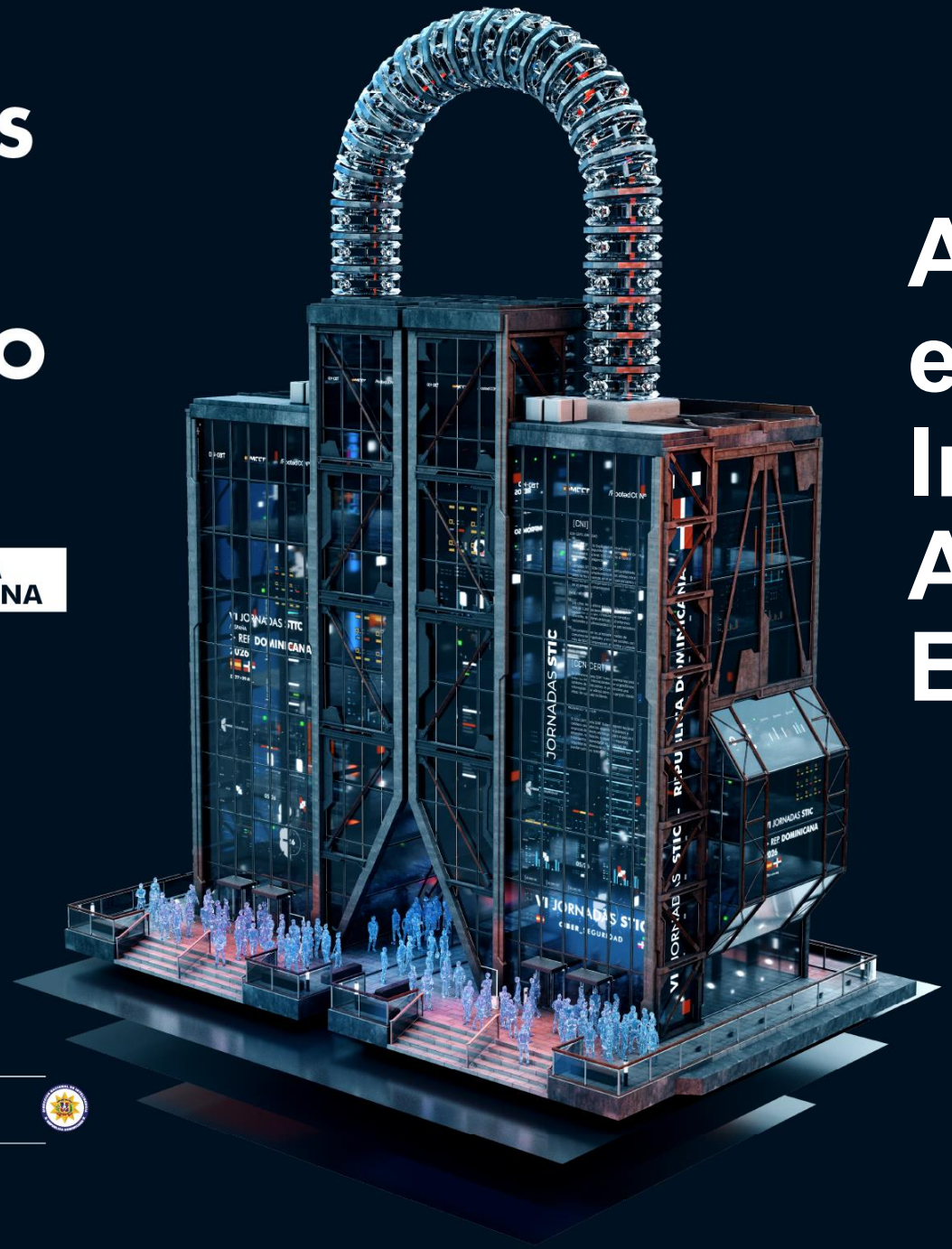
VI JORNADAS STIC & CONGRESO ROOTED_ CON

REPÚBLICA DOMINICANA

UN **ESCUDO DIGITAL** CONTRA LAS **CIBER_ AMENAZAS**

DEL **27** AL **29** **MAYO 2026**

#STIC**DOMINICANA**



Armando un equipo de Inteligencia de Amenazas: El caso chileno

ORGANIZADO POR:

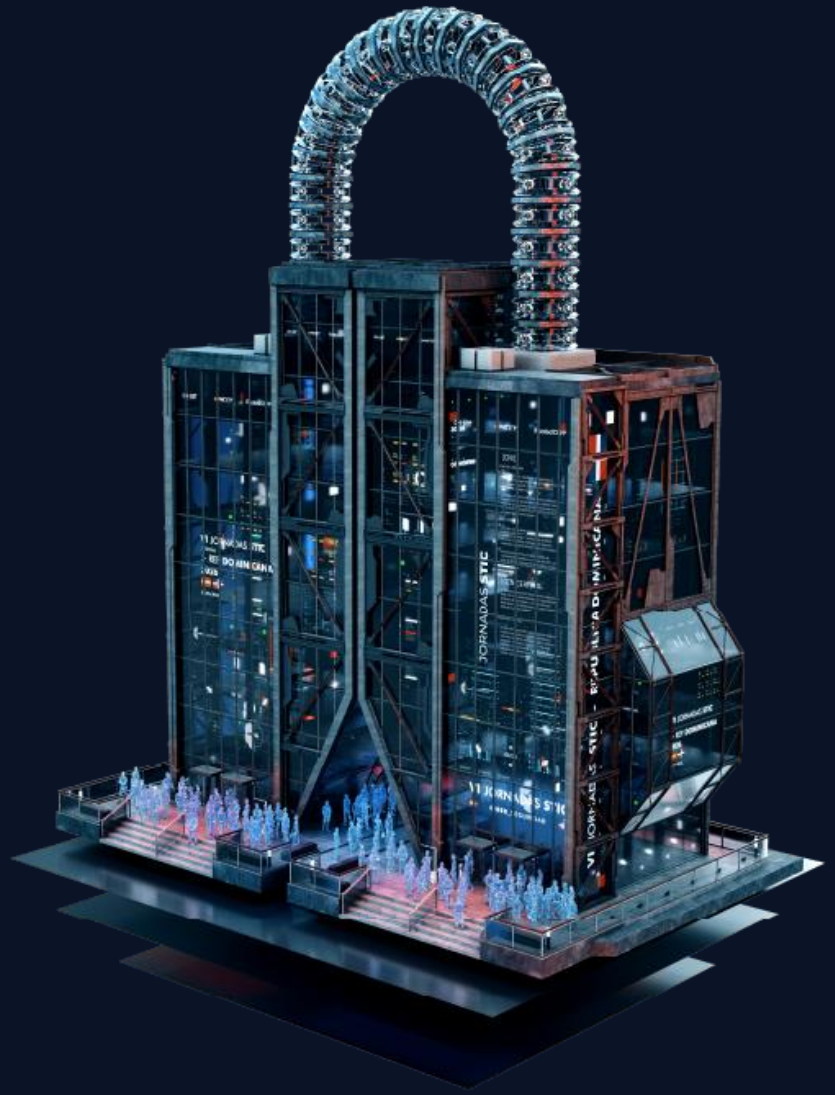
CCN · MCCE · /RootedCON

CON EL APOYO INSTITUCIONAL DE:

OEA · BID

ANCI
AGENCIA NACIONAL DE CIBERSEGURIDAD

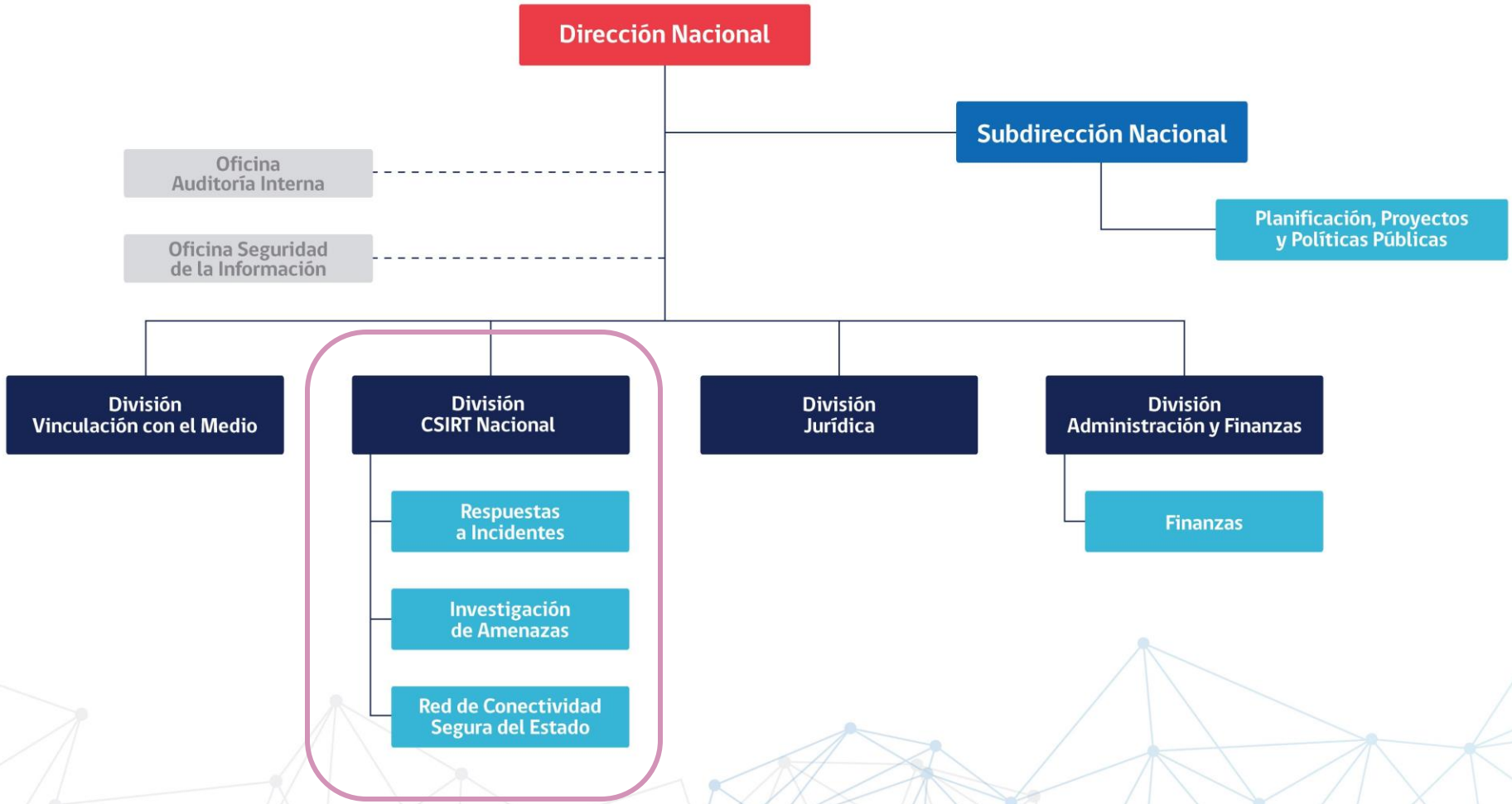
ÍNDICE



1. La Agencia Nacional de Ciberseguridad
   - El CSIRT Nacional
2. Armando un equipo de Inteligencia de Amenazas
   - Personas
   - Fuentes
   - Refinamiento
   - Almacenamiento y Diseminación
   - Herramientas
3. Productos
4. Recomendaciones

La Agencia Nacional de Ciberseguridad

De las cuatro divisiones, la División CSIRT Nacional es la más numerosa.



Cosas que cambian y que se mantienen

Más constituyentes, obligación de reportar, secreto del reporte, misma cantidad de especialistas

CSIRT Equipo de Respuesta ante Incidentes de Seguridad Informática		CSIRT NACIONAL
Reporte **solo de instituciones públicas**	→	Reporte obligatorio de Servicios esenciales (públicos y privados) → Más información de primera fuente
Publicación anual de estadísticas de incidentes	→	Toda información de la Agencia es secreta por defecto → Publicar información es más complejo, pero igual de necesario
~1.000 Constituyentes (Solo públicos)	→	~60.000 Constituyentes (Servicios esenciales) → Número de instituciones crece considerablemente
Publicación de guías y ciberconsejos para ciudadanía	→	Se mantiene, pero como deber de la Agencia → Enfoque en ciberseguridad de ciudadanos

Objetivo: aprovechar mayor flujo de datos para ser un "CSIPT".
Prevenir antes que responder

¿Por qué necesitamos Inteligencia de Amenazas?

No damos abasto apagando incendios, necesitamos prevenirlos. ¿Cómo lo hacemos?

Dominio Público, basado en Joint Chiefs of Staff
http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf

Enfoque científico: "Investigación de Amenazas"

- Replicabilidad y documentación
- Validación entre pares
- Dar herramientas a la comunidad

Público Objetivo: Todas las personas

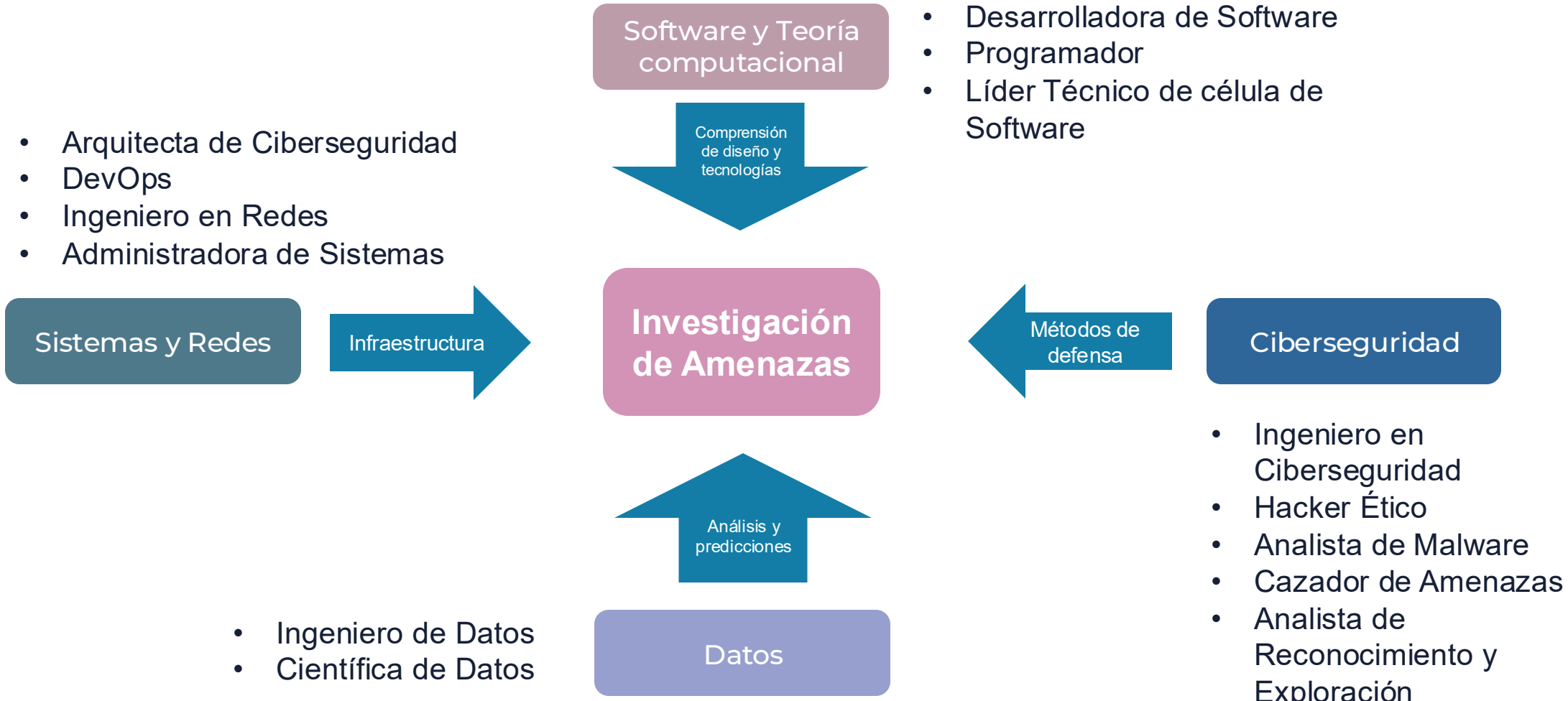
- Varios niveles de confidencialidad
- Muchas formas de comunicar

Cinco decisiones importantes

- Personas y Capacidades
- Fuentes de Información
- Refinamiento
- Almacenamiento y Diseminación
- Herramientas

Personas y Capacidades

Cuatro perfiles técnicos complementarios



- Desarrolladora de Software
- Programador
- Líder Técnico de célula de Software

- Arquitecta de Ciberseguridad
- DevOps
- Ingeniero en Redes
- Administradora de Sistemas

- Ingeniero en Ciberseguridad
- Hacker Ético
- Analista de Malware
- Cazador de Amenazas
- Analista de Reconocimiento y Exploración

- Ingeniero de Datos
- Científica de Datos

Fuentes de Inteligencia

Abiertas, Internas, Comerciales y Ciudadanas

Abiertas

Primarias

Sitios web y RRSS

- Cuentas en X/Mastodon
- Foros en Dark Web
- Data Leak Sites en TOR
- Canales de *Telegram*

Escaneos activos

- Escaneos en capa de red, protocolo y aplicación

Agregadas

Plataformas gratuitas

- Ransomware.live
- Cymru/Shadowserver (sujeto a aprobación)
- CSIRTAmericas (sujeto a aprobación)

Cerradas

Internas

Portal ANCI

- Fecha y hora de cada incidente
- Efectos Observables
- Actualizaciones periódicas
- Posibilidad de colaborar en recuperación

Ciudadanas

Reportes Ciudadanos

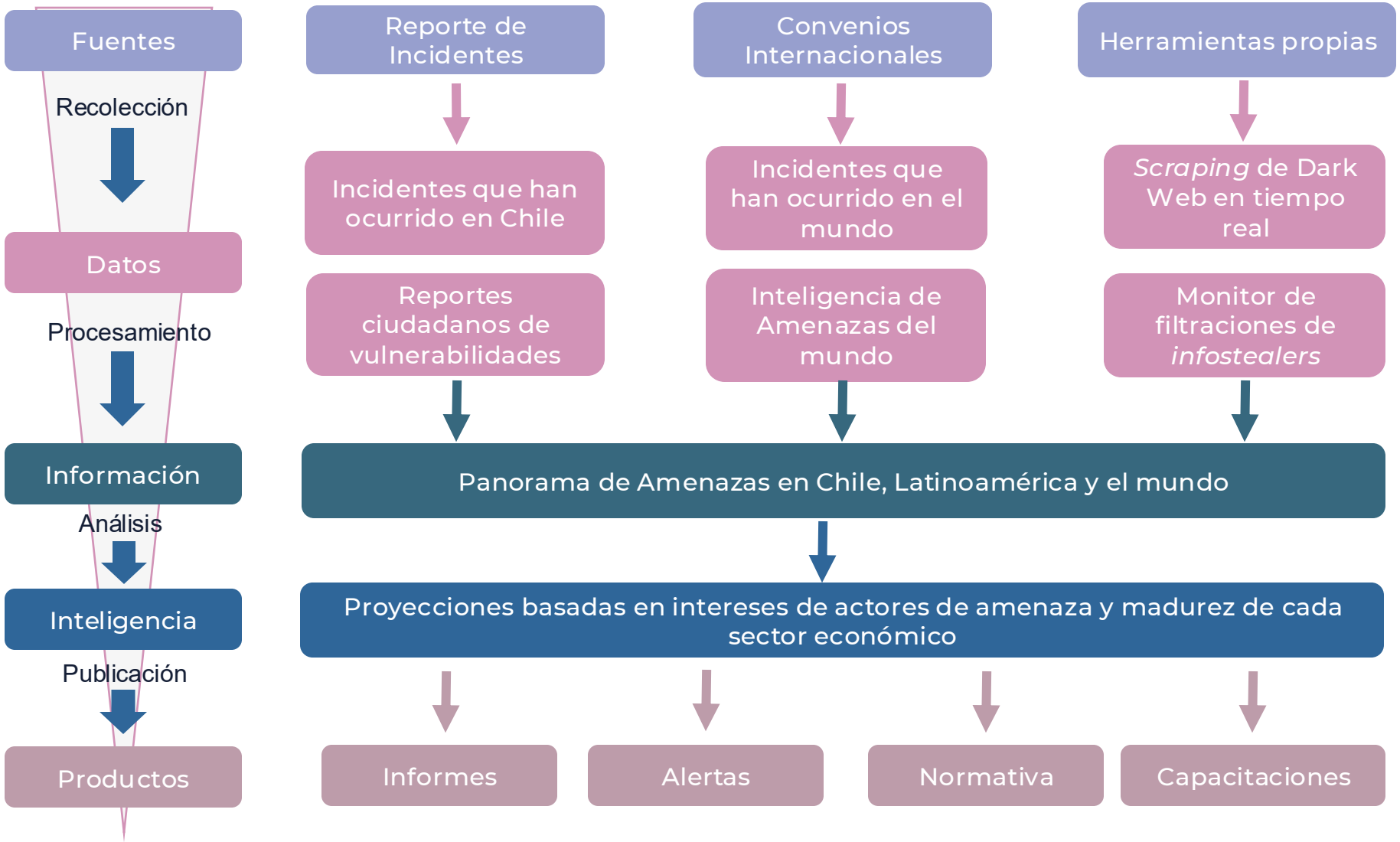
- Vulnerabilidades no explotadas ni conocidas masivamente
- Datos de actores de amenaza

Comerciales

Plataformas de pago

- IntelligenceX
- Shodan.io
- VirusTotal

Refinamiento: de datos a productos



Almacenamiento y Diseminación de DII

Centralización y distribución de información

Almacenamiento: **Guardar lo esencial que pueda ser necesario referir en el futuro**

- Instituciones
- Incidentes
- Versiones de productos
- Dominios Gob.cl
- Identificadores de red
- Actores de Amenaza
- Investigaciones

Diseminación: **Compartir toda información que ayude a prevenir incidentes, sin delatar víctimas**

- Informes de Inteligencia
- Cuadros de mando con datos centralizados
- OpenCTI
- MISP
- APIs y RSS

Herramientas comunicacionales y técnicas

Tablas, informes, desarrollos propios, automatizaciones y plataformas de información a medida para crear y procesar datos, analizar información y diseminar inteligencia

Definiciones comunes

EPSS Exploit Prediction Scoring System

MITRE ATT&CK

CWE

CVSS COMMON VULNERABILITY SCORING SYSTEM

Herramientas *Open Source*

OpenCTI

MISP Threat Sharing

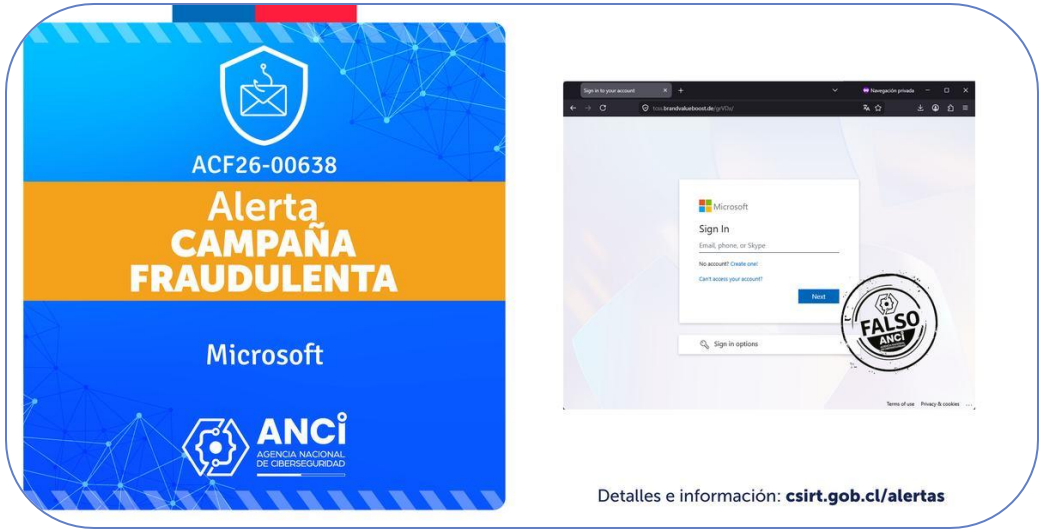
Integraciones e infraestructura

n8n

PostgreSQL

Productos: Alertas y datos de Filtraciones

Generando feeds de inteligencia internos



Alertas

- En Página web https://csirt.gob.cl/alertas
- Dirigidas a contacto de ciberseguridad en Portal

Informes Periódicos

https://csirt.gob.cl/articulo/informe-de-investigacion-de-amenazas-2025

Recolección activa de credenciales en Telegram

- Sistema automático de monitoreo
- Validación ciudadana en https://ciberlupa.anci.gob.cl
- Envío de credenciales potencialmente filtradas a contacto de ciberseguridad

Productos: *Ciberconsejos* y los 9 básicos

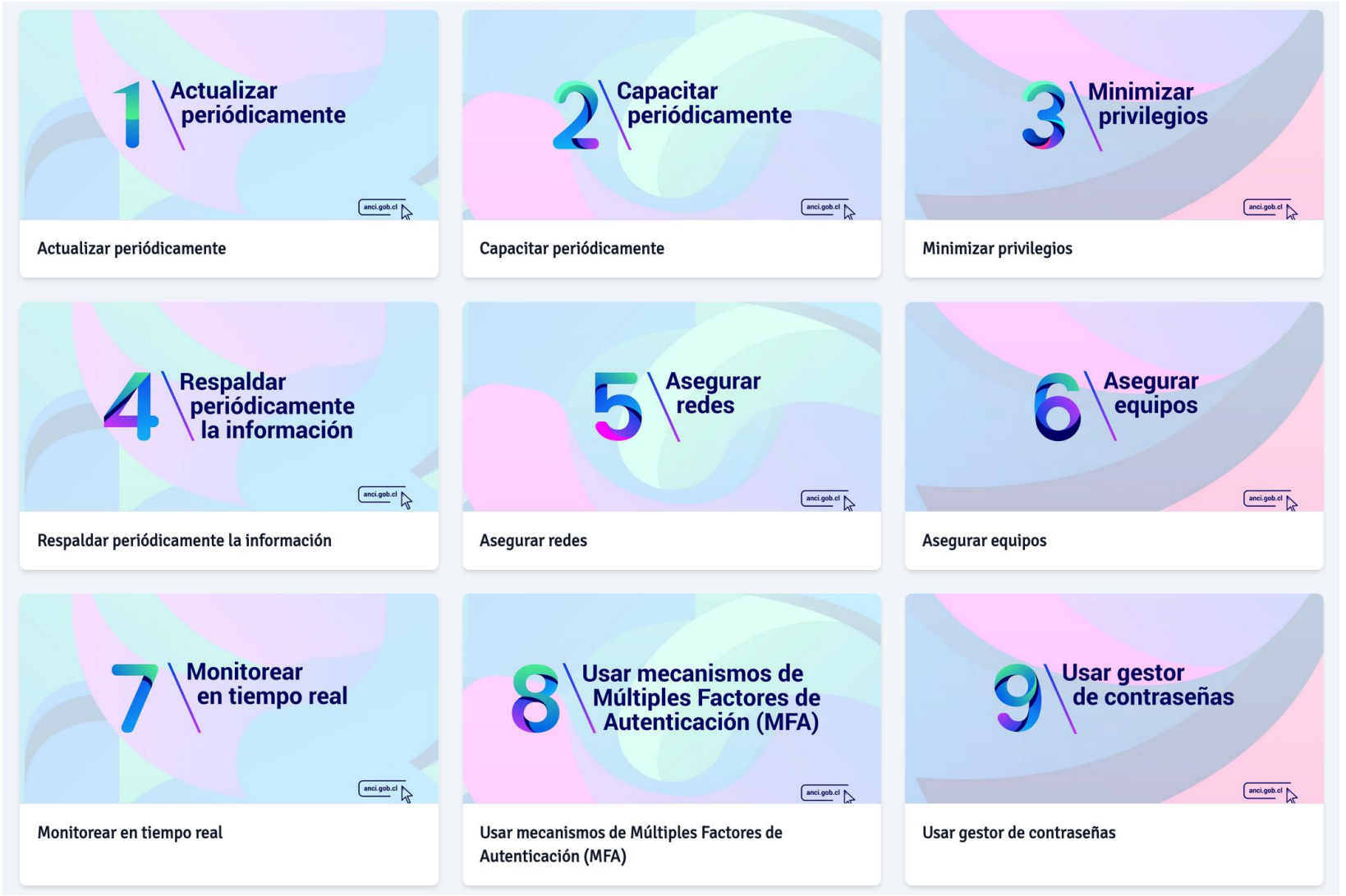
Basados en datos de acceso inicial de incidentes reportados

Elaboramos cursos, guías y material de difusión asociado a cada básico

Compartimos material para ciudadanía: Ciberconsejos

Mascota: **Ciberpudú**

https://instagram.com/ancichile



https://anci.gob.cl/9basicos

Recomendaciones para otras instituciones

Sugerencia secuencial para partir con un equipo pequeño y de bajo costo

1. Obtener fuentes abiertas o ciudadanas
2. Automatizar usando herramientas de código abierto
3. Analizar periódicamente datos recibidos
4. Comprometerse a escribir periódicamente predicciones y validarlas continuamente
5. Crear productos en orden de importancia

Las fuentes públicas primarias pueden ser de muy buena calidad, **pero para recolectarlas es necesario aprender a automatizar**

Si la legislación de tu país lo permite, **aprovecha el conocimiento colectivo de las comunidades de investigadores de ciberseguridad.**

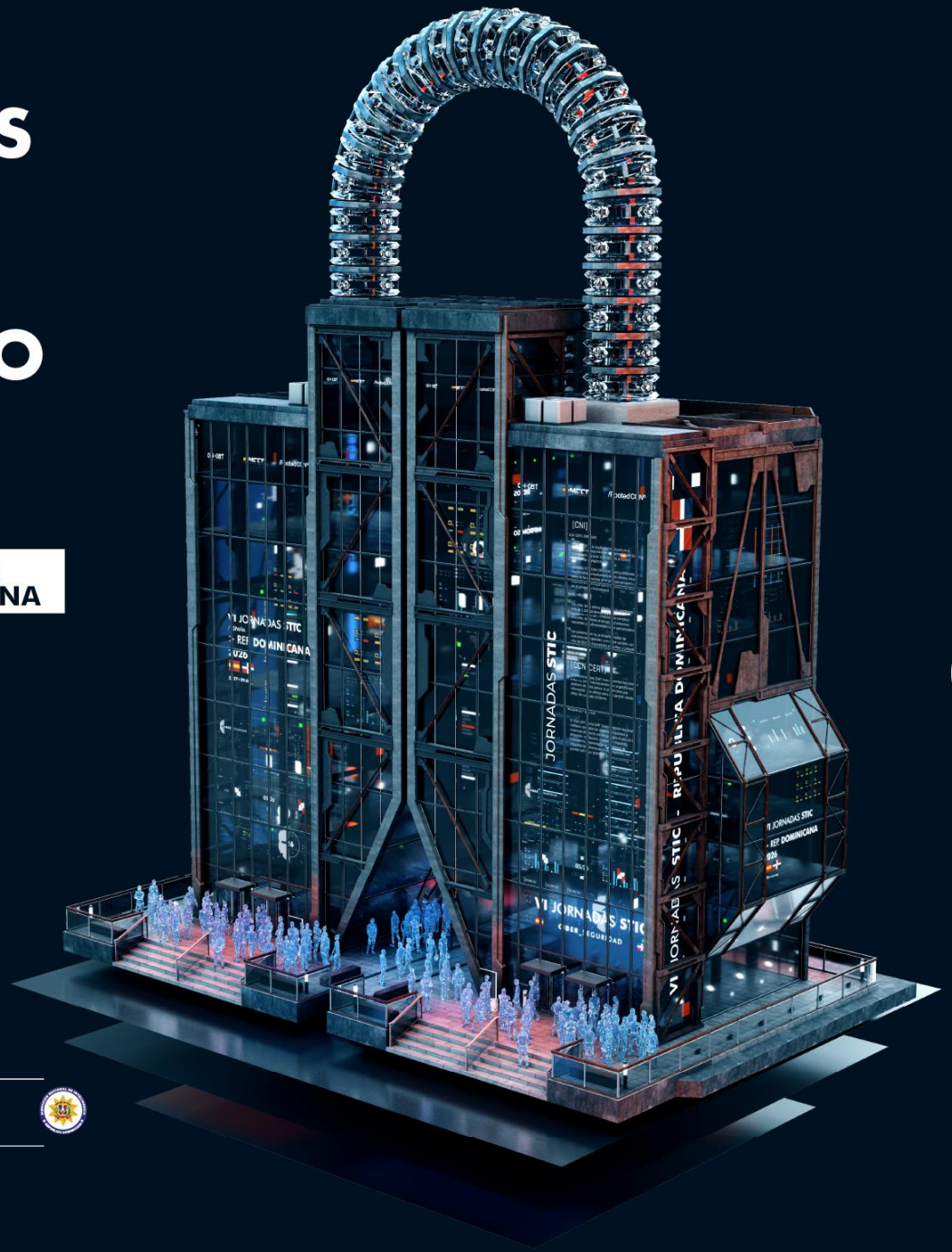
VI JORNADAS STIC & CONGRESO ROOTED_ CON

REPÚBLICA DOMINICANA

UN **ESCUDO DIGITAL** CONTRA LAS **CIBER_ AMENAZAS**

DEL **27** AL **29** **MAYO 2026**

#STIC**DOMINICANA**



ANCI
AGENCIA NACIONAL DE CIBERSEGURIDAD

international@anci.gob.cl

https://anci.gob.cl

https://csirt.gob.cl

ORGANIZADO POR:

CCN · MCCE · RootedCON · Policía Nacional

CON EL APOYO INSTITUCIONAL DE:

OEA · BID