ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

PROCESO DE
INVESTIGACIÓN DE AMENAZAS

2025

Si bien un rol importante de un **Equipo de Respuesta a Incidentes** es (como dice su nombre) apoyar en la respuesta ante incidentes, el trabajo de **prevención de incidentes y ciberataques** cobra cada vez mayor relevancia.

Concientización

Normativa

Capacitaciones

Investigación

Íconos de https://flaticon.com

Proceso de Investigación de Amenazas

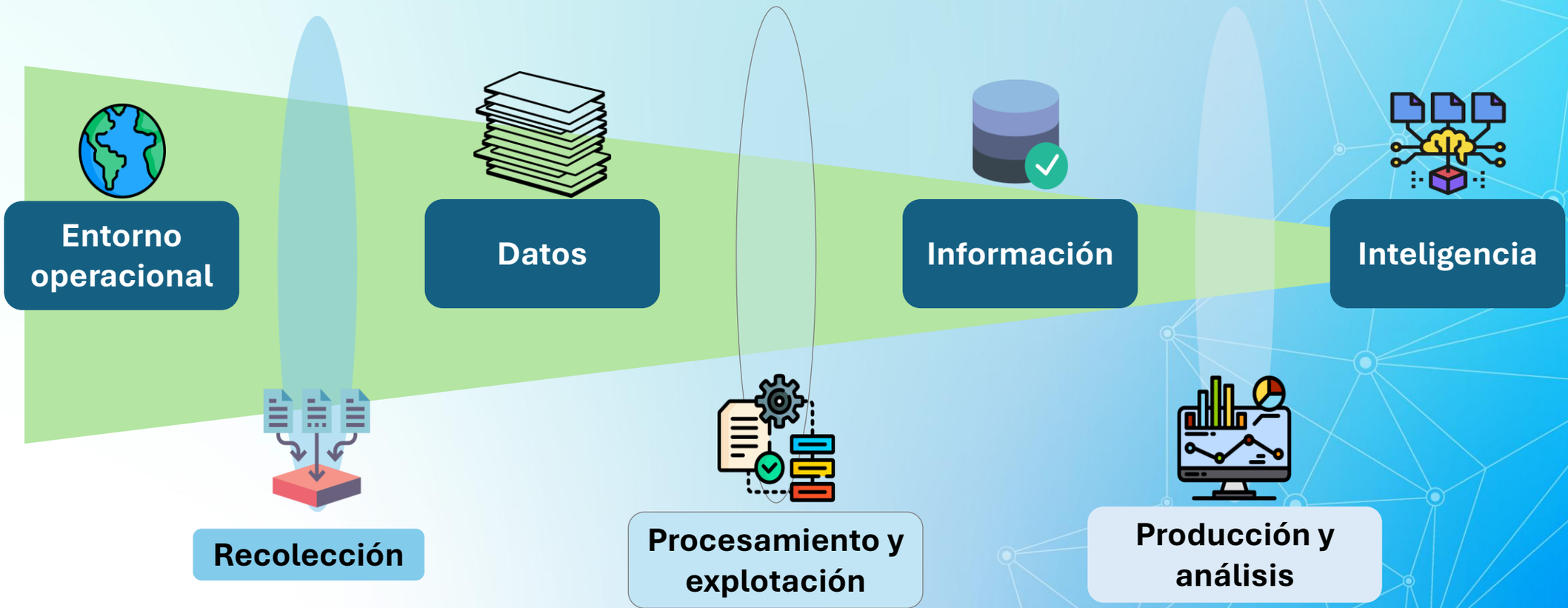
Su objetivo es **comprender el panorama de amenazas de nuestra región,** a partir de información de incidentes de ciberseguridad y ciberataques recopilada tanto interna como externamente.

Se busca entender **el cómo y el por qué de la ocurrencia de incidentes y ciberataques,** para disminuir su probabilidad de ocurrencia en el futuro.

Íconos de https://flaticon.com

CONCEPTOS DE
INVESTIGACIÓN DE AMENAZAS

Datos, información e Inteligencia



Íconos de https://flaticon.com

Proceso de investigación de amenazas

FUNCIONES DE UN EQUIPO DE **INVESTIGACIÓN DE AMENAZAS**

Funciones y Capacidades

Administración de Infraestructura

Manejo de Bases de Datos

Administración de servidores

Desarrollo de Software y scripting

Habilitación de interoperabilidad de información

Mantenimiento de plataformas de info pública (MISP)

Análisis de Amenazas

Análisis y procesamiento de datos

Funciones proactivas

Recolección/Análisis de fuentes públicas

Clasificación/validación de incidentes

Generación de alertas e informes

Funciones reactivas

Análisis Forense

Análisis de Malware

Procesamiento de logs y eventos de sistema

Productos y entregables

Informes de Inteligencia

Buenas prácticas y normas técnicas

Intercambio de Indicadores de Compromiso

Alertas dirigidas

Íconos de https://flaticon.com

HERRAMIENTAS DE
INVESTIGACIÓN DE AMENAZAS

Herramientas y marcos de trabajo comunes

ANCI
AGENCIA NACIONAL DE CIBERSEGURIDAD

Definiciones comunes

EPSS
Exploit Prediction Scoring System

MITRE ATT&CK™

CVE

CWE

CVSS
COMMON VULNERABILITY SCORING SYSTEM

Herramientas *Open Source*

OpenCTI

MISP
Threat Sharing

Integraciones e infraestructura

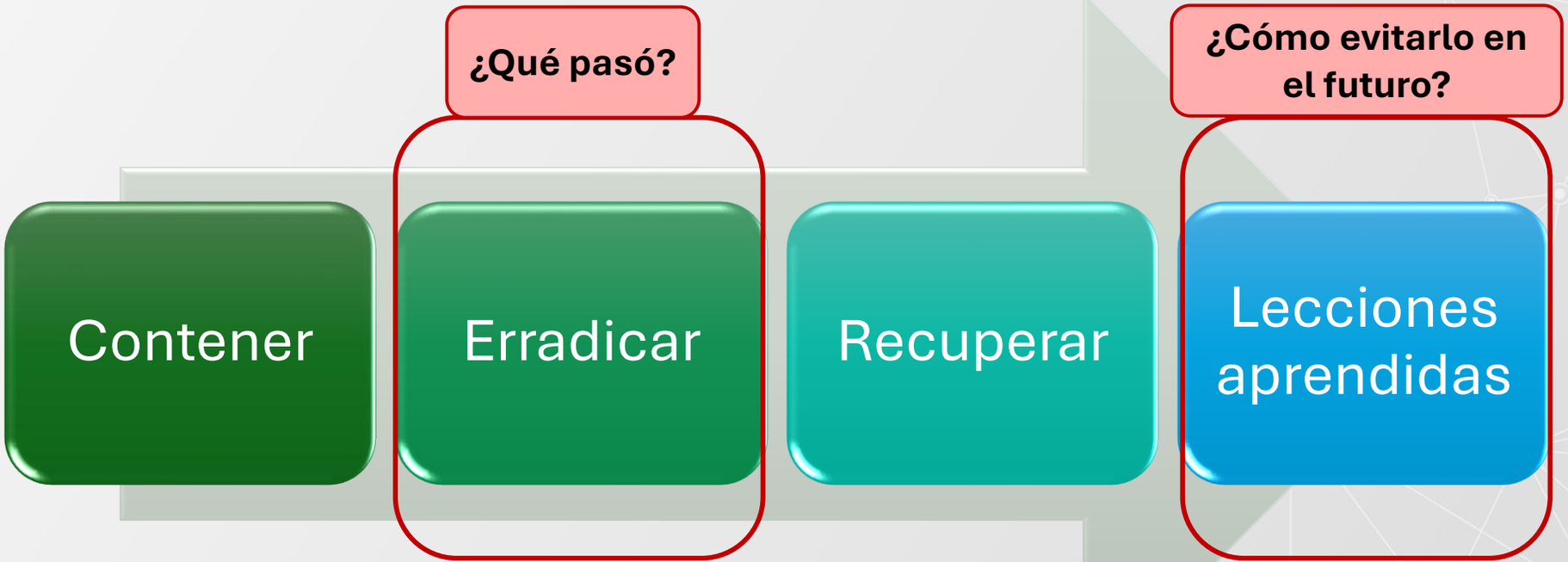
n8n

PostgreSQL

INVESTIGACIÓN DE AMENAZAS
DURANTE UN INCIDENTE

Proceso de Respuesta ante Incidentes

(Ver charla marzo 2025 ANCI)



¿Qué datos son útiles en el proceso de inv. de amenazas para apoyar la respuesta ante incidentes?

ANCI
AGENCIA NACIONAL DE CIBERSEGURIDAD

Carpetas de logs y eventos	THOR Lite, CHAINSAW X	Para determinar acciones del atacante
Accesos a herramientas de seguridad	kaspersky, FORTINET	Para contar con respaldo de logs
***Dumps* de memoria**	LiME, VOLATILITY	Para recopilar información del atacante
Carpetas de archivos temporales	 , BASH THE BOURNE-AGAIN SHELL	En busca de un archivo importante
Muestras de Malware	GHIDRA, 	Para entender mejor los pasos de cifrado

La profesionalización de los procesos de **investigación de amenazas** puede derivar en **normas y recomendaciones a medida del panorama de amenaza de la región a la que pertenece**, permitiendo el uso eficiente los recursos necesarios para protegerse en el ciberespacio y disminuyendo los costos económicos y sociales asociados a incidentes de ciberseguridad.

Concientización

Normativa

Capacitaciones

Investigación

Íconos de https://flaticon.com

ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

anci.gob.cl