UxTIC

Philippe Boland

Analista geopolítico

Gestor de la Red de Universidades por las TIC - UxTIC. Actualmente cofundador de la Cámara de Comercio Blockchain Token Partner.

philippe@enredo.org
TW: @enredo
https://www.linkedin.com/in/boland/

enREDo

DNS Abuse

Abuso del sistema de nombres de dominio:
Retos y estrategias de mitigación

ICANN

UxTIC
Red de Universidades

Red RIBCi
Red Iberoamericana de Blockchain y Ciberseguridad

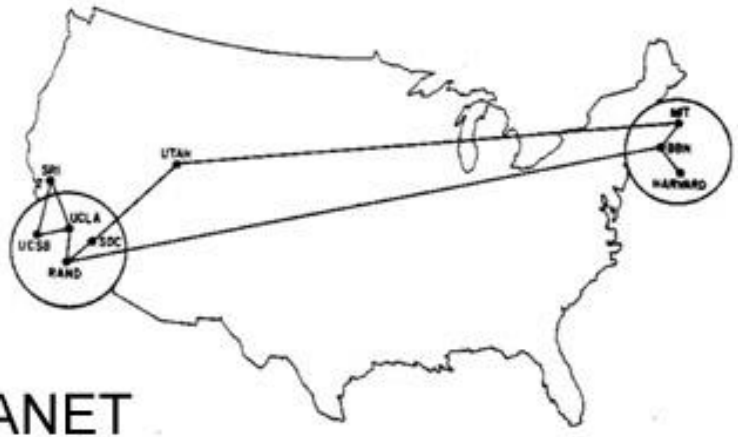
CYTED

UdeCataluña

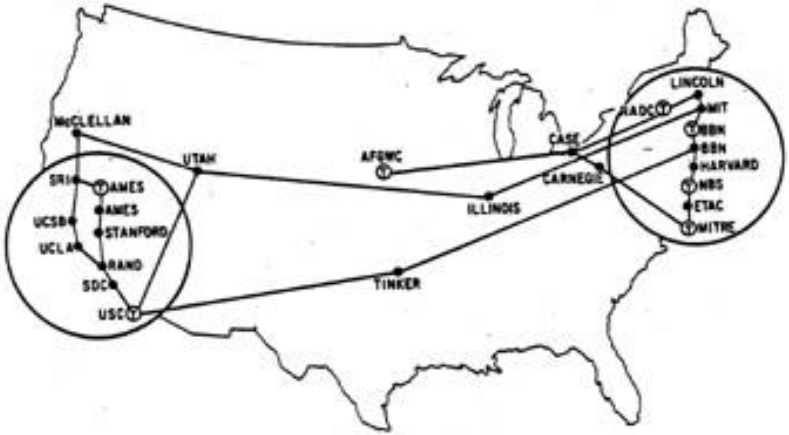
LACRALO
ICANN

1969

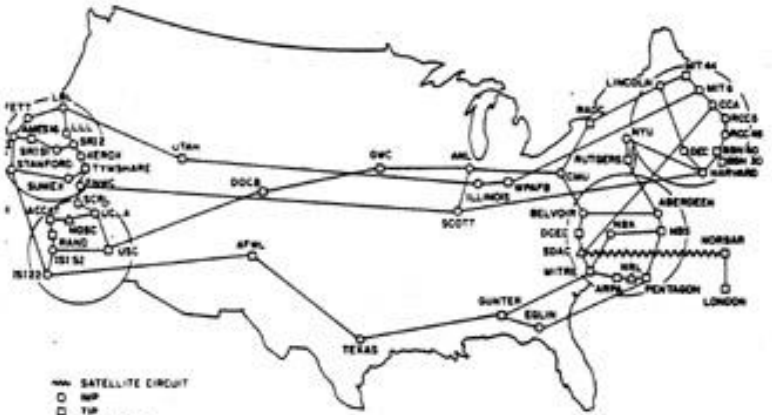
ARPANET



1970



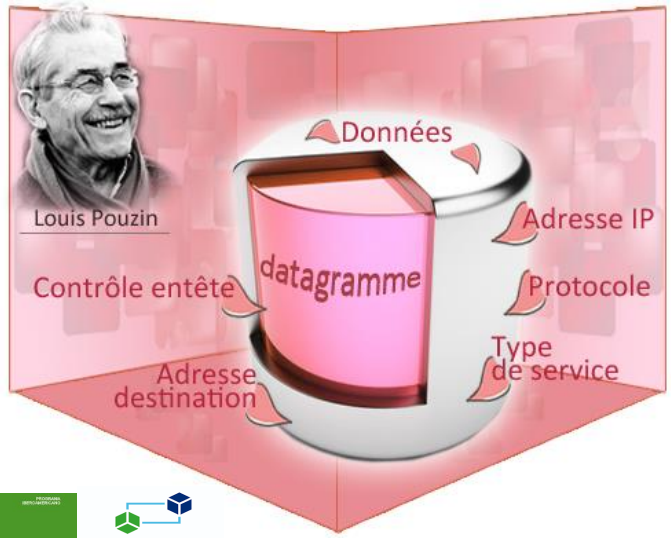
1972

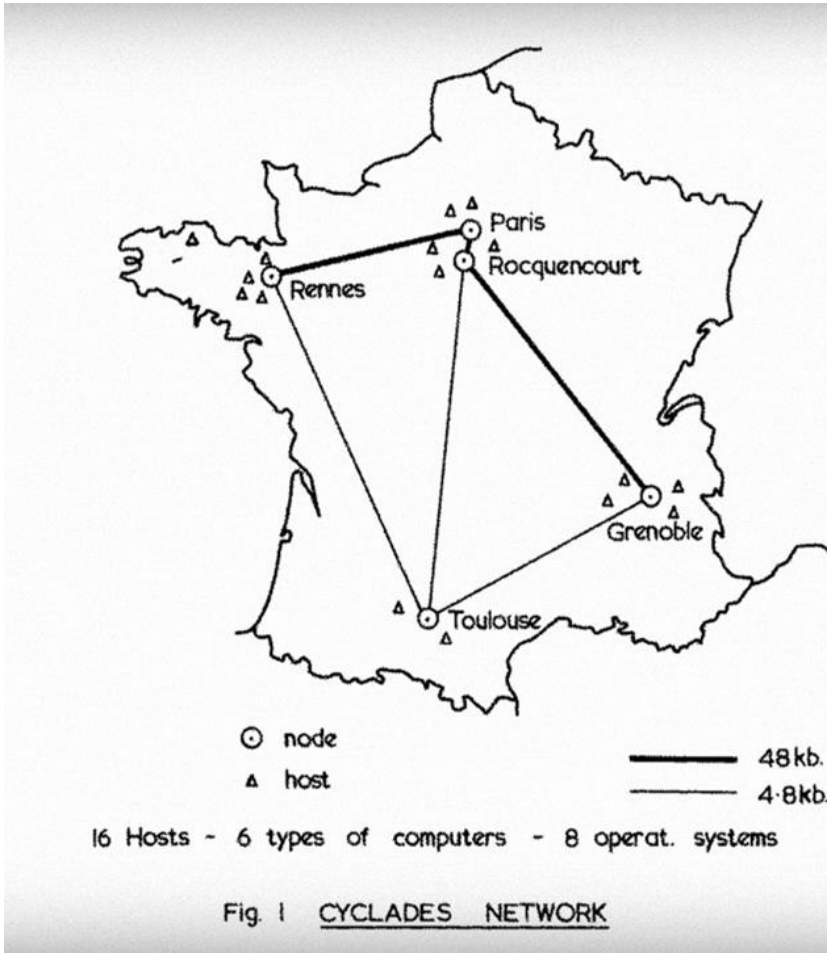


1977

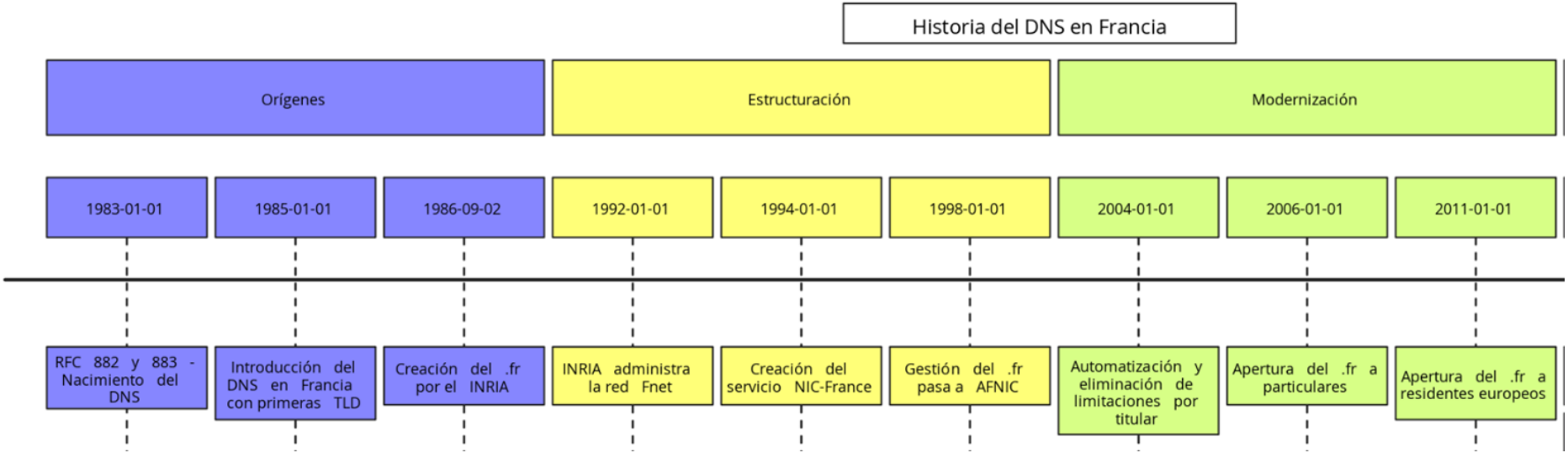
1972-78
Red experimental

Délégation à l'Informatique, Louis Pouzin ; Inventor del datagrama
Interconexión de 20 universidades y centros de investigación



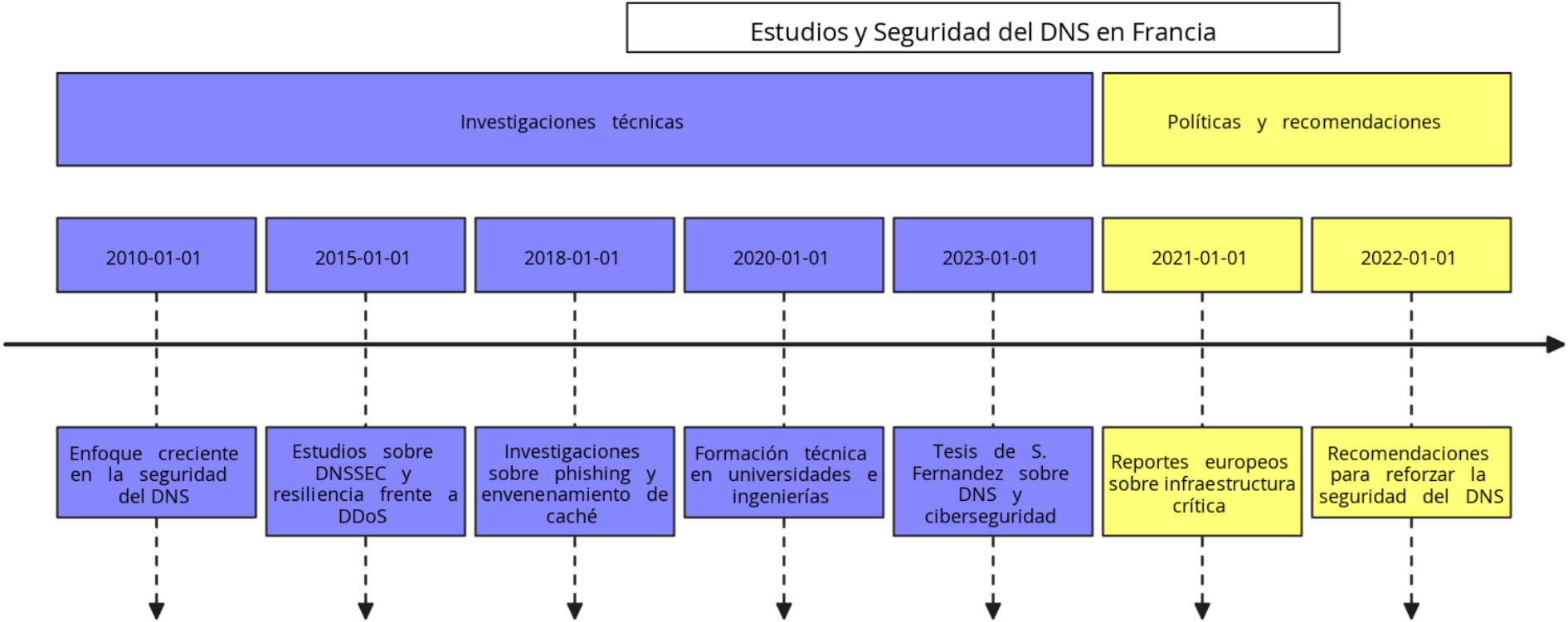


CYTED
Red RIBCi
Red Iberoamericana de Blockchain y Ciberseguridad



El DNS (Domain Name System) se diseñó a principios de los años 80 para sustituir al archivo hosts.txt, que se estaba volviendo inmanejable a medida que Internet se expandía.

Las primeras normas se establecieron en los documentos RFC 882 y 883, y posteriormente en los documentos 1034 y 1035.


Estudios y Seguridad del DNS en Francia
Investigaciones técnicas
Políticas y recomendaciones
2010-01-01
2015-01-01
2018-01-01
2020-01-01
2023-01-01
2021-01-01
2022-01-01
Enfoque creciente en la seguridad del DNS
Estudios sobre DNSSEC y resiliencia frente a DDoS
Investigaciones sobre phishing y envenenamiento de caché
Formación técnica en universidades e ingenierías
Tesis de S. Fernandez sobre DNS y ciberseguridad
Reportes europeos sobre infraestructura crítica
Recomendaciones para reforzar la seguridad del DNS

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

ESPACE PRESTATAIRE | MON ESPACE | A

ASSISTANCE ET PRÉVENTION DU RISQUE NUMÉRIQUE AU SERVICE DES PUBLICS

NOUS SOMMES #CYBERENGAGÉS
CYBER MOIS
01 OCT – 31 OCT
ÉDITION 2025

VOUS INFORMER | NOS SERVICES | À PROPOS | VOUS ÊTES VICTIME ? ASSISTANCE EN LIGNE 17CYBER

NOS MISSIONS PRÉVENIR

Cybermalveillance.gouv.fr a pour missions d'assister les particuliers, les entreprises, les associations, les collectivités et les administrations victimes de cybermalveillance, de les sensibiliser au risque cyber, de les informer sur les menaces numériques et les moyens de s'en protéger.

DES SERVICES POUR :

PARTICULIERS | PROFESSIONNELS | COLLECTIVITÉS

CYTED
Red RIBCi
Red Iberoamericana de Blockchain y Ciberseguridad

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

17 CYBER
Mon assistance en ligne

En cas d'urgence, **appelez le 17 ou le 112** ou envoyez un **SMS au 114** en cas de difficulté à parler ou entendre

17 CYBER
Mon assistance en ligne

Victime de cybermalveillance ? Nous vous guidons pour agir.

Un service proposé par la Police Nationale, la Gendarmerie Nationale et Cybermalveillance.gouv.fr

Faire le diagnostic de votre situation

Vous avez besoin d'aide pour identifier votre problème ?

Répondez à quelques questions pour déterminer l'attaque dont vous êtes victime.

Démarrer le diagnostic

Vous connaissez déjà votre problème?

Consultez nos recommandations pour votre problème (ex : hameçonnage, piratage, virus informatique etc.)

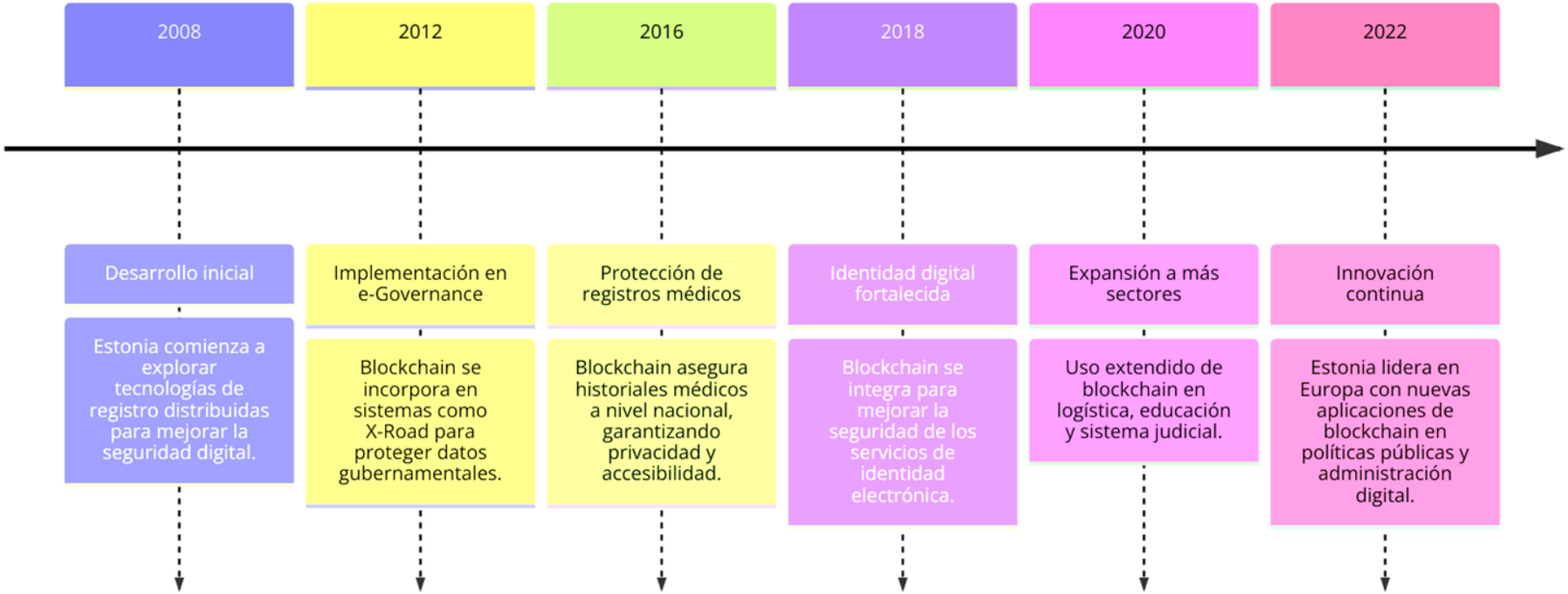
Voir les recommandations

CYTED
CIENCIA Y TECNOLOGÍA PARA EL DESARROLLO

Red RIBCi
Red Iberoamericana de Blockchain y Ciberseguridad

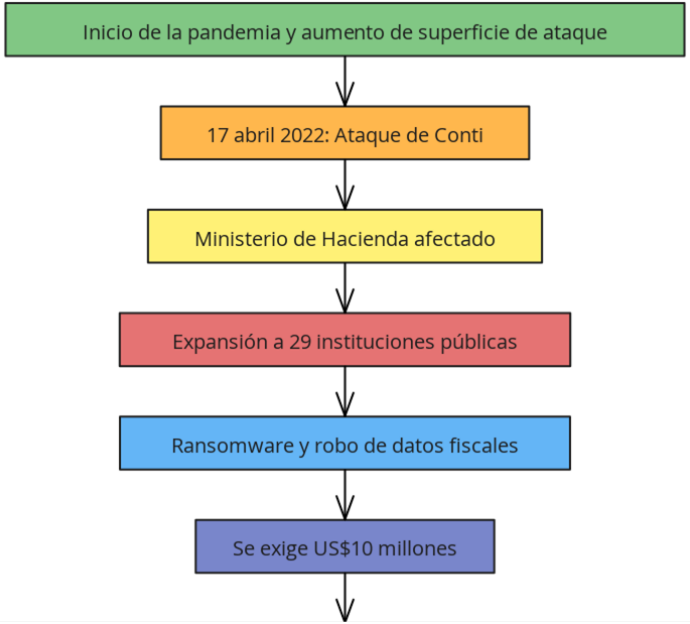
Relación con el sector defensa

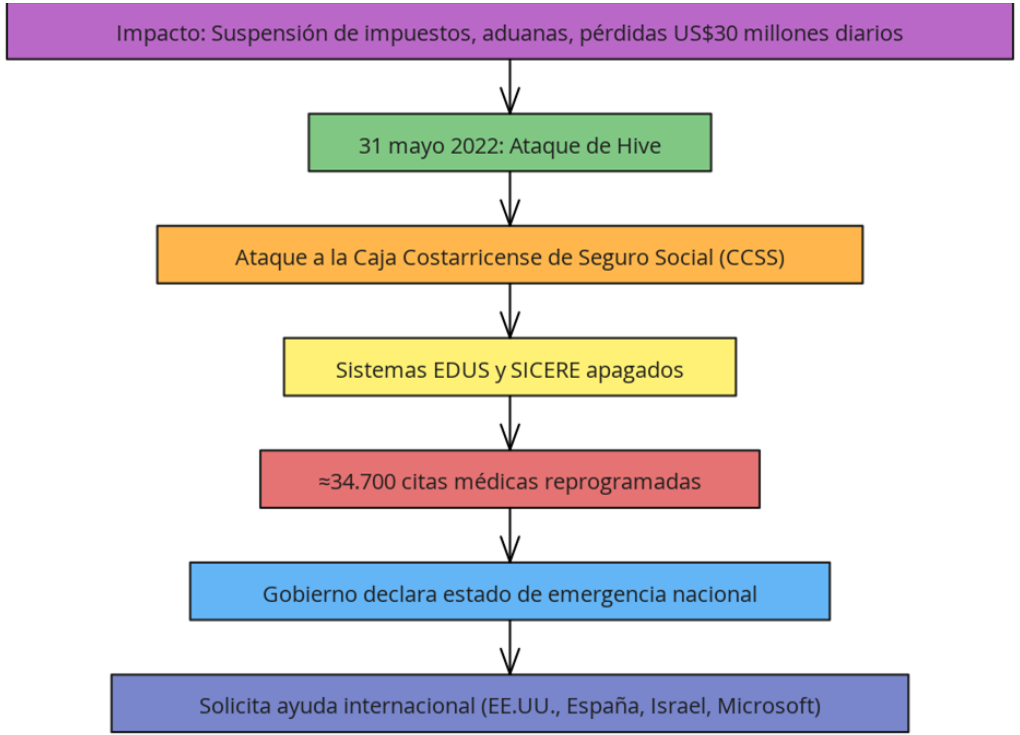
Estonia



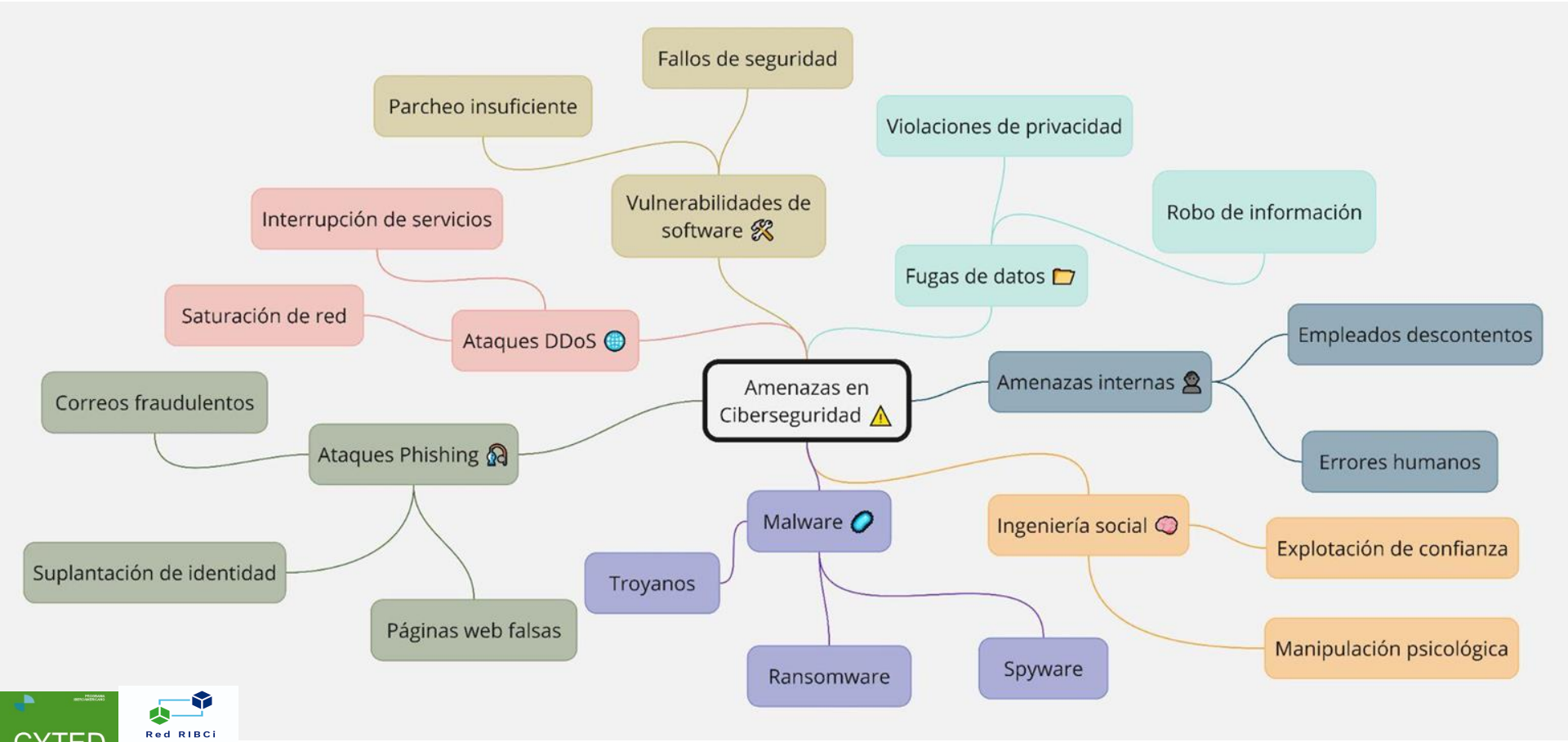
:.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf

Costa RICA


Inicio de la pandemia y aumento de superficie de ataque
17 abril 2022: Ataque de Conti
Ministerio de Hacienda afectado
Expansión a 29 instituciones públicas
Ransomware y robo de datos fiscales
Se exige US$10 millones

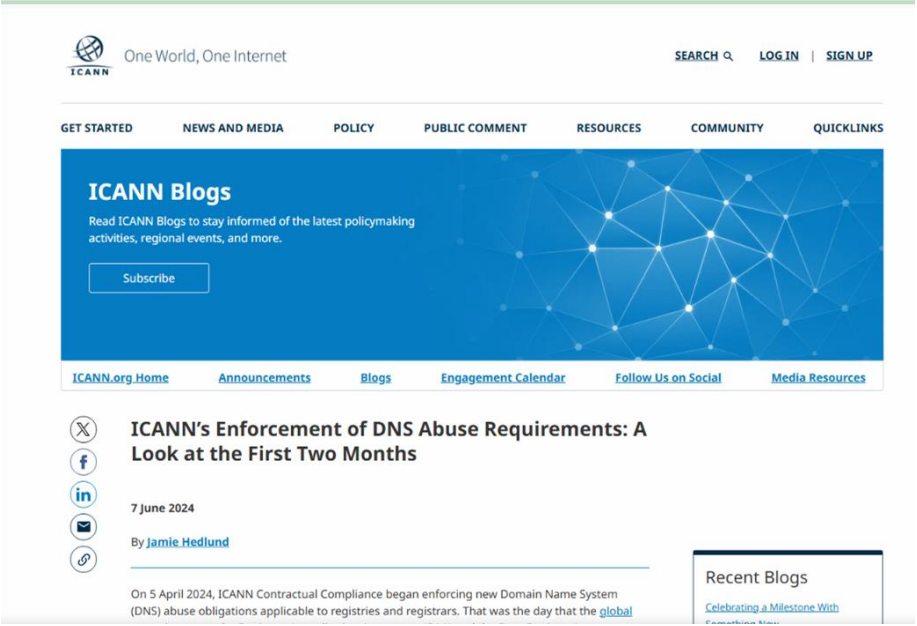

Impacto: Suspensión de impuestos, aduanas, pérdidas US$30 millones diarios
31 mayo 2022: Ataque de Hive
Ataque a la Caja Costarricense de Seguro Social (CCSS)
Sistemas EDUS y SICERE apagados
≈34.700 citas médicas reprogramadas
Gobierno declara estado de emergencia nacional
Solicita ayuda internacional (EE.UU., España, Israel, Microsoft)

Principales amenazas



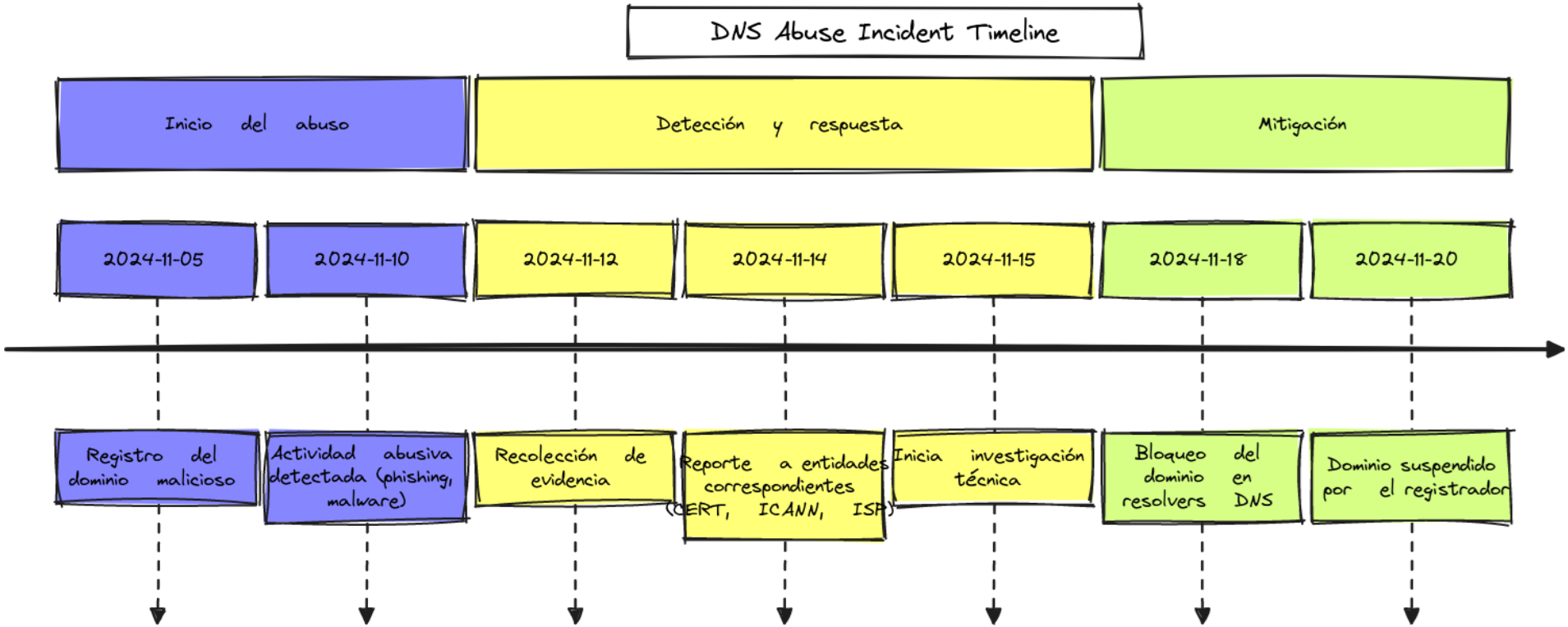
Combatir las amenazas asimétricas y mantener una situación táctica informada y predictiva

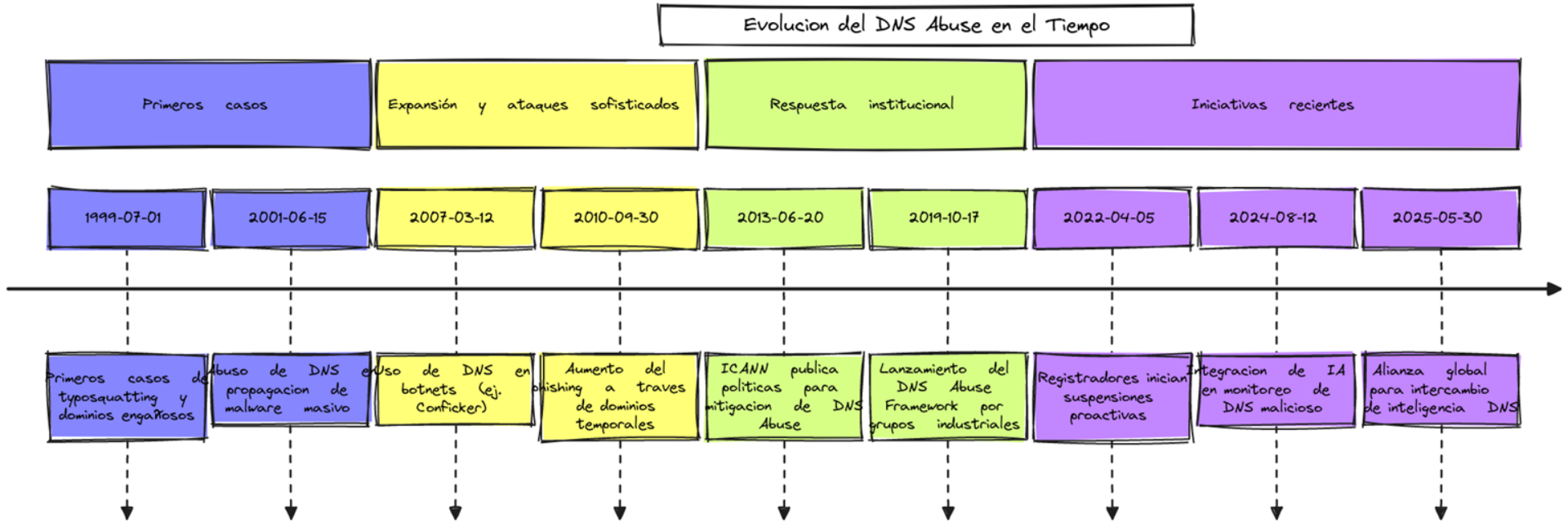
7 Junio 2024

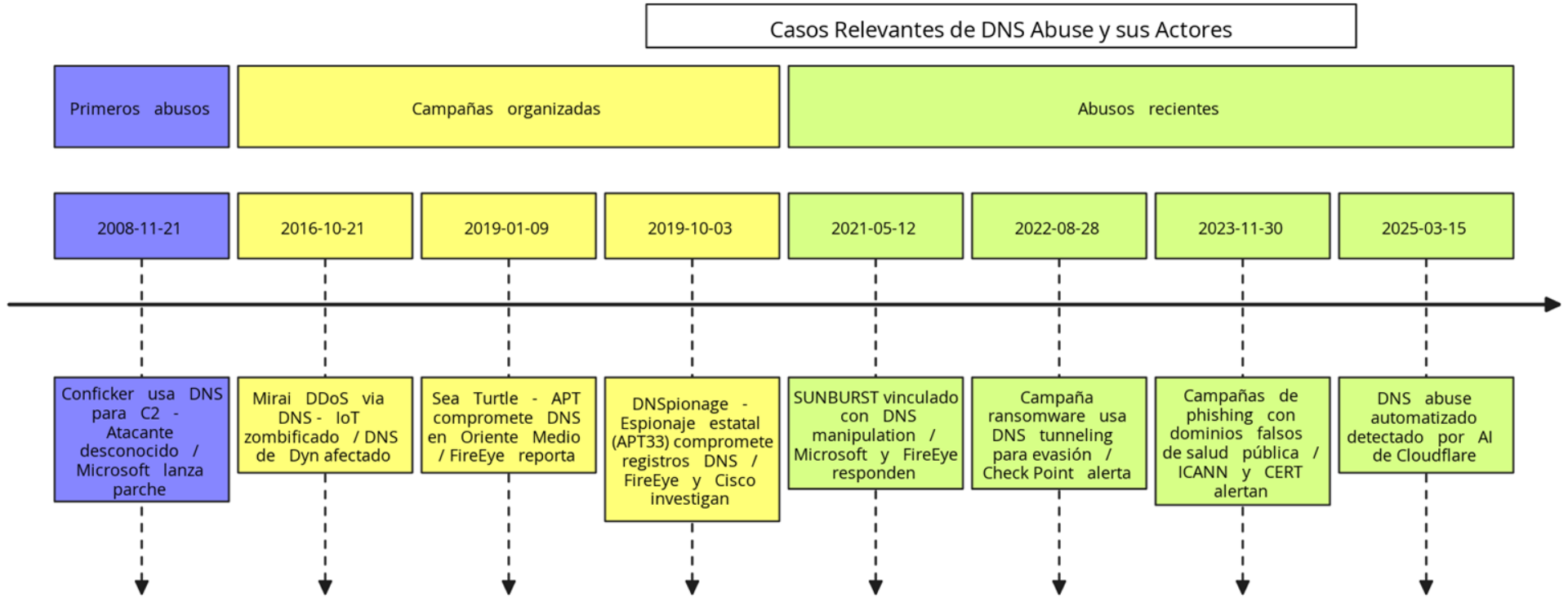


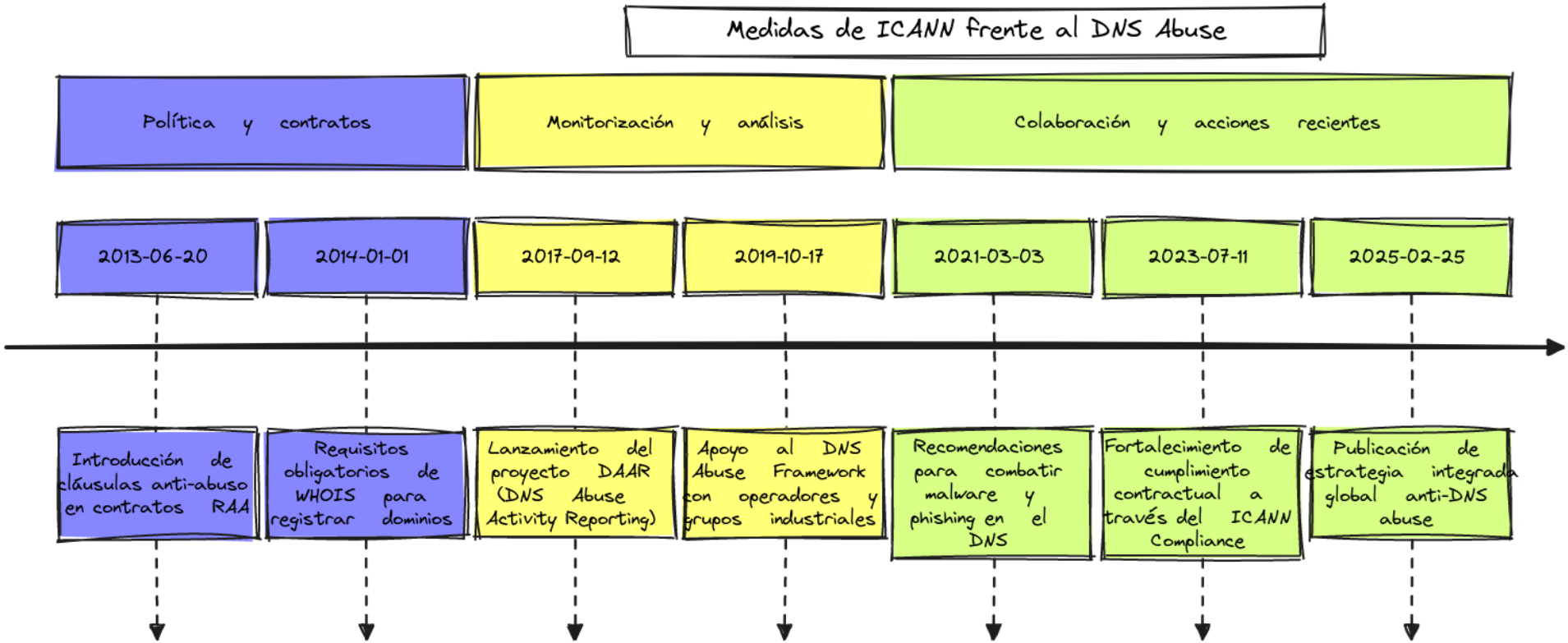
Desde el 5 de abril de 2024, ICANN comenzó a hacer cumplir nuevas obligaciones contractuales relacionadas con el abuso del DNS, tanto para registradores como para registros.

Estas obligaciones provienen de las enmiendas globales al Registrar Accreditation Agreement (RAA) y al Base Registry Agreement (RA).








Medidas de ICANN frente al DNS Abuse
Política y contratos
Monitorización y análisis
Colaboración y acciones recientes
2013-06-20
2014-01-01
2017-09-12
2019-10-17
2021-03-03
2023-07-11
2025-02-25
Introducción de cláusulas anti-abuso en contratos RAA
Requisitos obligatorios de WHOIS para registrar dominios
Lanzamiento del proyecto DAAR (DNS Abuse Activity Reporting)
Apoyo al DNS Abuse Framework con operadores y grupos industriales
Recomendaciones para combatir malware y phishing en el DNS
Fortalecimiento de cumplimiento contractual a través del ICANN Compliance
Publicación de estrategia integrada global anti-DNS abuse

Recepción de denuncias

ICANN habilitó **nuevos formularios de quejas** sobre abuso de DNS accesibles globalmente.

En **abril y mayo 2024** se recibieron **1.558 quejas**, pero:

- **1.382** se cerraron por ser **no procesables**:
  - Principalmente por no haber sido remitidas previamente al registrador o registro.
  - También por ser duplicadas o referirse a **ccTLDs** (fuera del alcance de ICANN).
- El resto dio lugar a:
  - **38 investigaciones a registradores**.
  - **2 investigaciones a registros**.

Tipos de abuso detectado

Phishing fue el tipo más común, a veces acompañado de:

- Infracción de marcas.
- Falsificación.
- Spam usado para distribuir malware o phishing.

Los dominios maliciosos suplantaban:

- Instituciones gubernamentales.
- Entidades financieras.
- Servicios de parqueo y movilidad.
- Cadenas hoteleras y comerciales, entre otros.

Quiénes reportaron

- 13 investigadores de seguridad.
- 9 representantes de entidades suplantadas.
- 7 abogados de propiedad intelectual.
- **Ningún caso** fue iniciado por autoridades públicas o policiales locales.

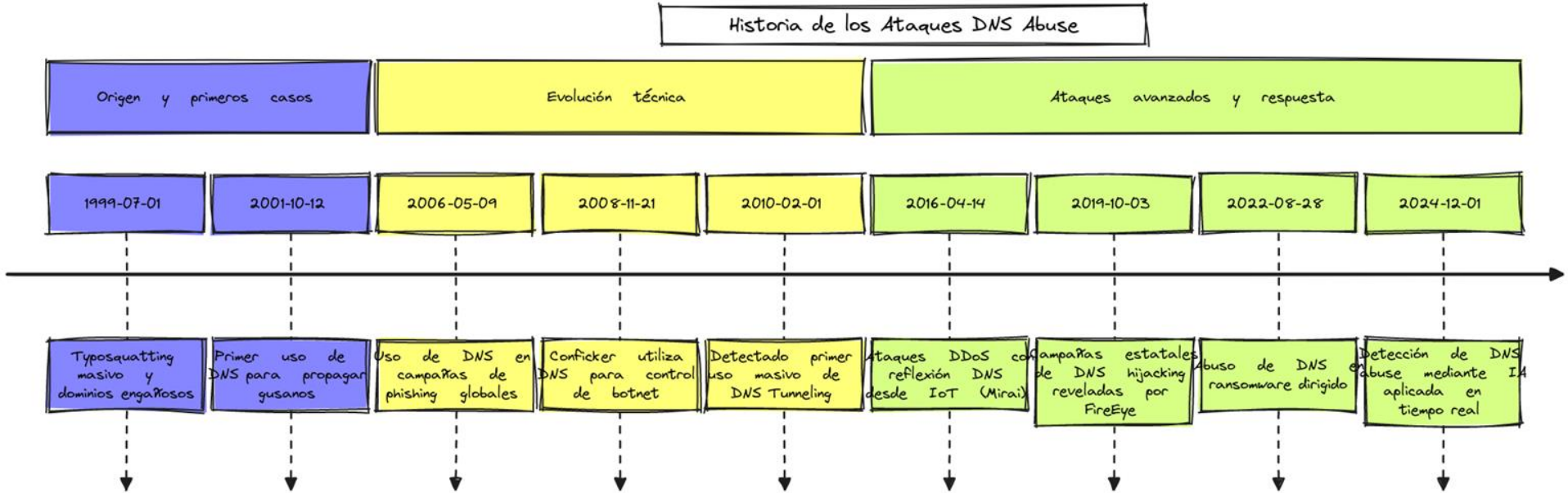
Medidas tomadas

- **2.528 dominios maliciosos suspendidos** por registradores.
- **328 sitios de phishing deshabilitados** en subdominios, cuando se determinó que el dominio principal estaba comprometido.
- Algunos registradores están revisando y **mejorando sus propios procesos internos** de respuesta a abusos.

¿Qué se entiende por DNS Abuse?

DNS Abuse (abuso del Sistema de Nombres de Dominio) se refiere al uso malicioso o indebido de servicios de nombres de dominio para facilitar actividades dañinas en Internet.

No se trata solo de un mal uso técnico, sino de un peligro directo para la seguridad digital, la privacidad de los usuarios y la confianza en Internet.



La definición adoptada por ICANN se centra en cinco categorías claras de abuso técnico.

⚠ Tipos comunes de abuso del DNS

Phishing (suplantación de identitád): Creación de dominos falsós that imitan sitos legitimos (como bancos, universidades, plataformas de usuarios a robár passareñas, datos bancarios o información sensibie.

Malware (software malicioso): Dominios utilizados far distribuir programas dañinos que infectan computadoras o redes, aisea vara para espionaje, sequestrado (ransomware) or control remoto de dispositivos.

Botnets: Netes de computadoras infectadas ton controllada por un atacante. Los dominios abusivos actúan amo “centros de mando y C&C) fara coordinar ataques distribuldos (DDoS) o campanhas de spam.

Spam técnico: Uso massivo de dominios para enviar correos no nsolicitados, muchas vezes coilences a sitios perigprosos. Esto affècta la réputación de dominios legitimos y congeston ā el tràfico digital.

Child Abuse Material / Illegal Content (Contenido ilegal): Algunos dominios son utlizados para joi, distribuir oo facilitar el acceso a material llegal o ꝺ ltamente dáñino. Aunque esta categoria cae entécnica

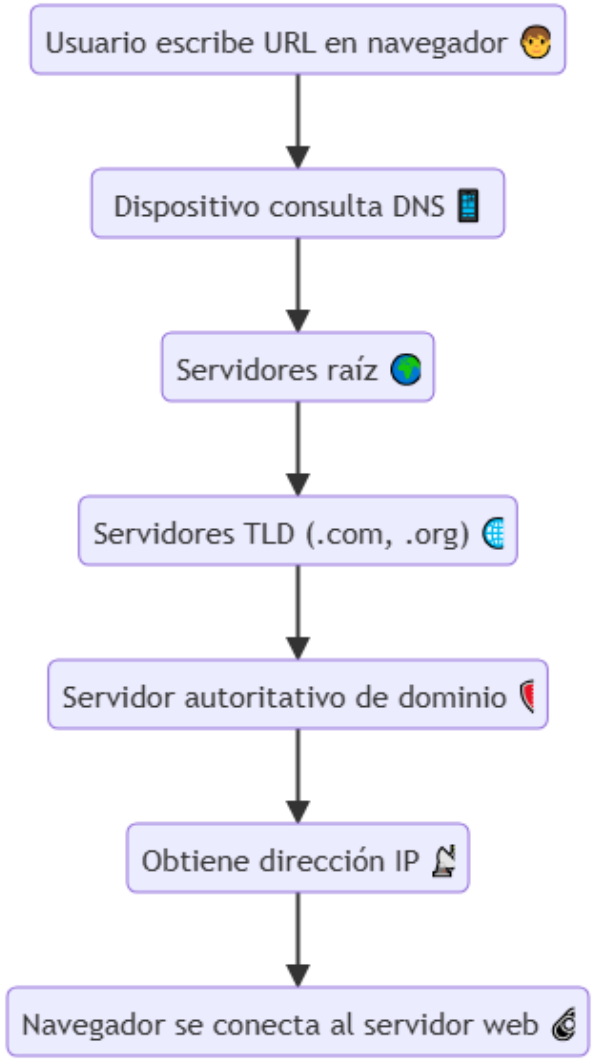
Otros usos problemáticos (más allá del abuso técnico)

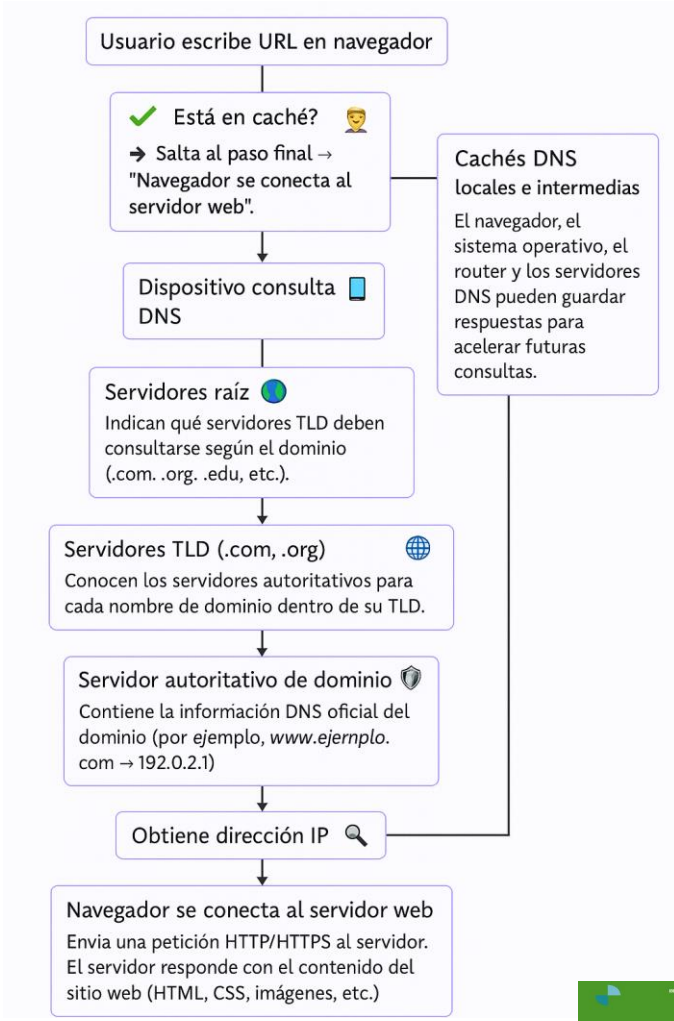
⚠️ **Typosquatting:** registrar dominios con errores tipográficos de dominios populares (por ejemplo, gooogle.com) para engañar al usuario

🔑 **Domain hijacking:** robar el control de un dominio legítimo mediante ingeniería social o explotación de vulnerabílidades

🖥️ **DNS tunneling:** uso del DNS como canal encubierto para transferir datos maliciosos o evadir controles de red

🖥️ **Otros usos problemáticos** (más állá del abuso técnico)
Envria de contenos a ringos peigoroisos


Usuario escribe URL en navegador
Dispositivo consulta DNS
Servidores raíz
Servidores TLD (.com, .org)
Servidor autoritativo de dominio
Obtiene dirección IP
Navegador se conecta al servidor web


Usuario escribe URL en navegador
Está en caché?
→ Salta al paso final → "Navegador se conecta al servidor web".
Cachés DNS locales e intermedias
El navegador, el sistema operativo, el router y los servidores DNS pueden guardar respuestas para acelerar futuras consultas.
Dispositivo consulta DNS
Servidores raíz
Indican qué servidores TLD deben consultarse según el dominio (.com. .org. .edu, etc.).
Servidores TLD (.com, .org)
Conocen los servidores autoritativos para cada nombre de dominio dentro de su TLD.
Servidor autoritativo de dominio
Contiene la información DNS oficial del dominio (por ejemplo, www.ejernplo.com → 192.0.2.1)
Obtiene dirección IP
Navegador se conecta al servidor web
Envia una petición HTTP/HTTPS al servidor. El servidor responde con el contenido del sitio web (HTML, CSS, imágenes, etc.)

¿Por qué es preocupante el DNS abuse para las universidades?

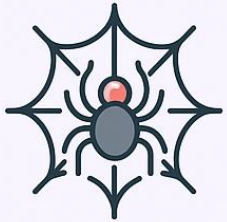
Phishing

Ataques de suplantación de identidad pueden comprometer datos financieros y credenciales de estudiantes, profesores y personal.

Malware

Software malicioso puede infectar redes universitarias, afectando la infraestructura de TI y robando información confidencial.

Botnets

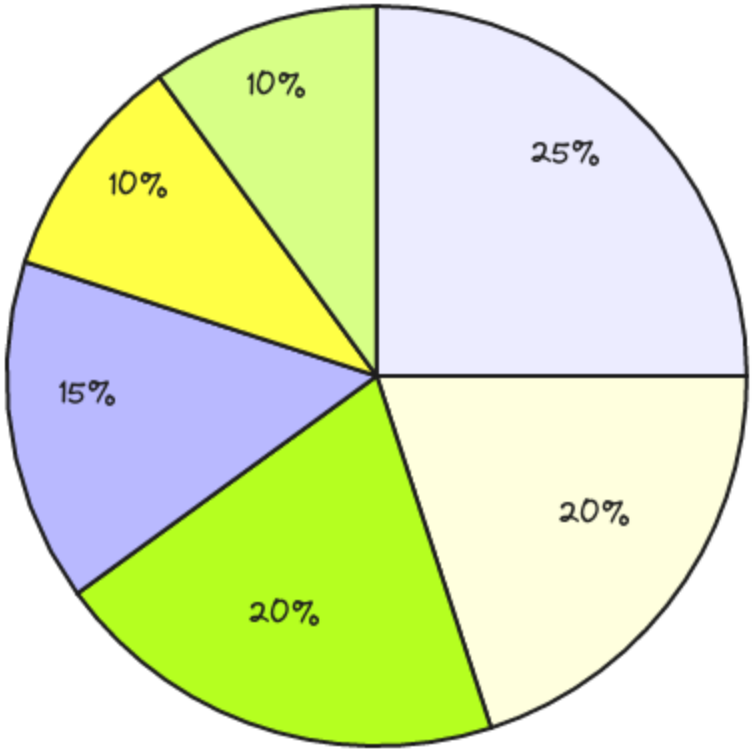


Redes de computadores infectadas pueden ser utilizadas para lanzar ataques DDoS dirigidos contra los recursos en iinea de las universidades.

Reputación

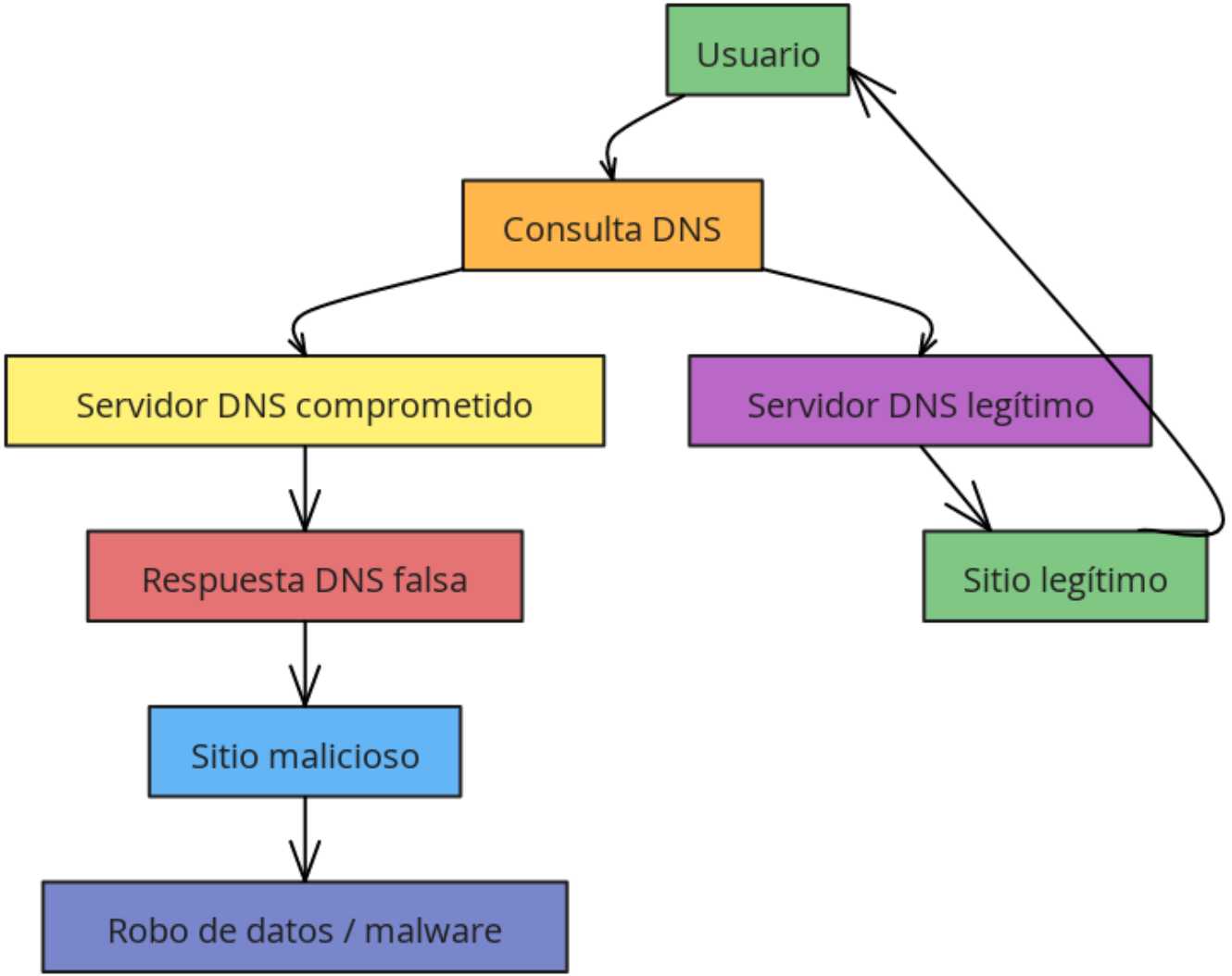
El abuso del DNS y el contenido liegal relacionado puéden danar la reputacion de las instituciones académicas y erosionar la confianza

Tipos de Ataques DNS

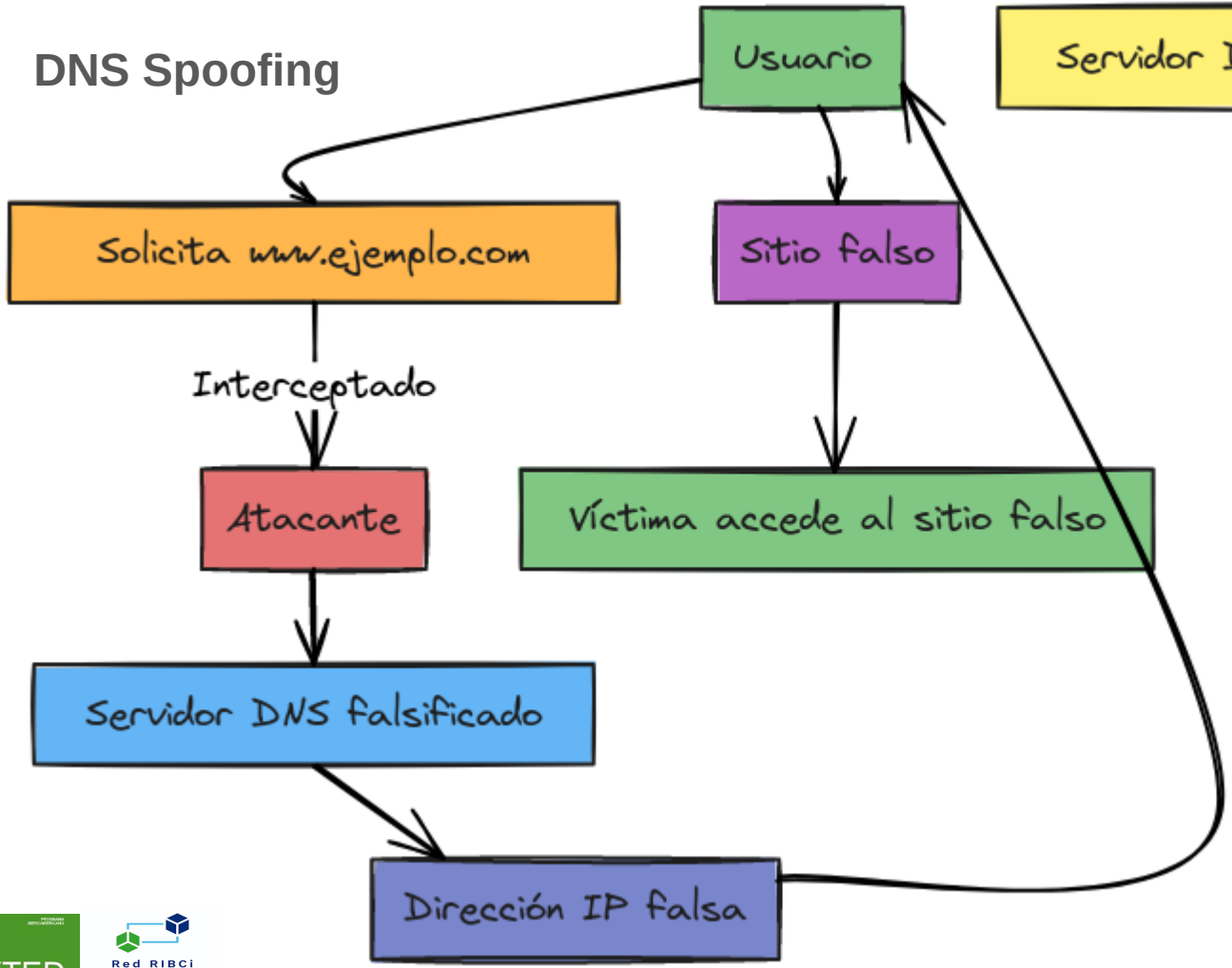


- DNS Hijacking [25]
- DNS Spoofing [20]
- Amplification Attacks [20
- Cache Poisoning [15]
- Tunneling [10]
- Domain Lock-up [10]

DNS Hijacking



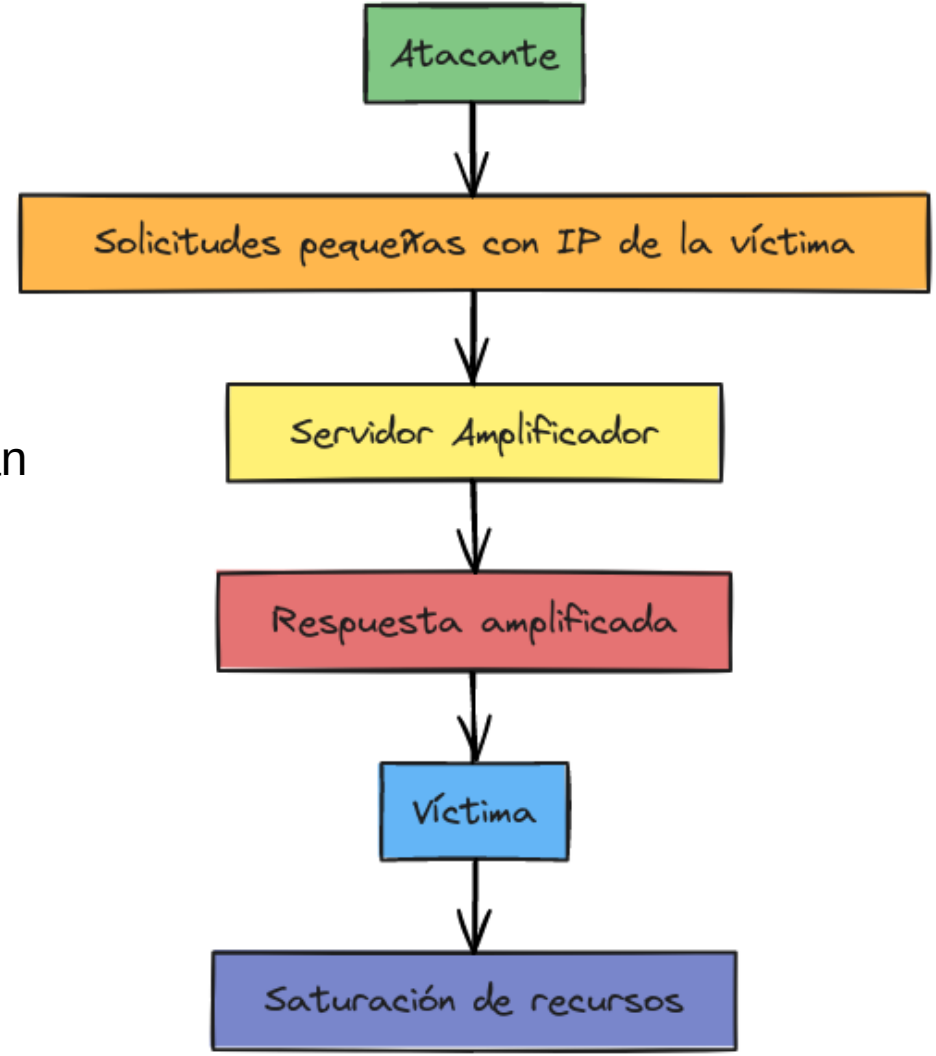
DNS Spoofing



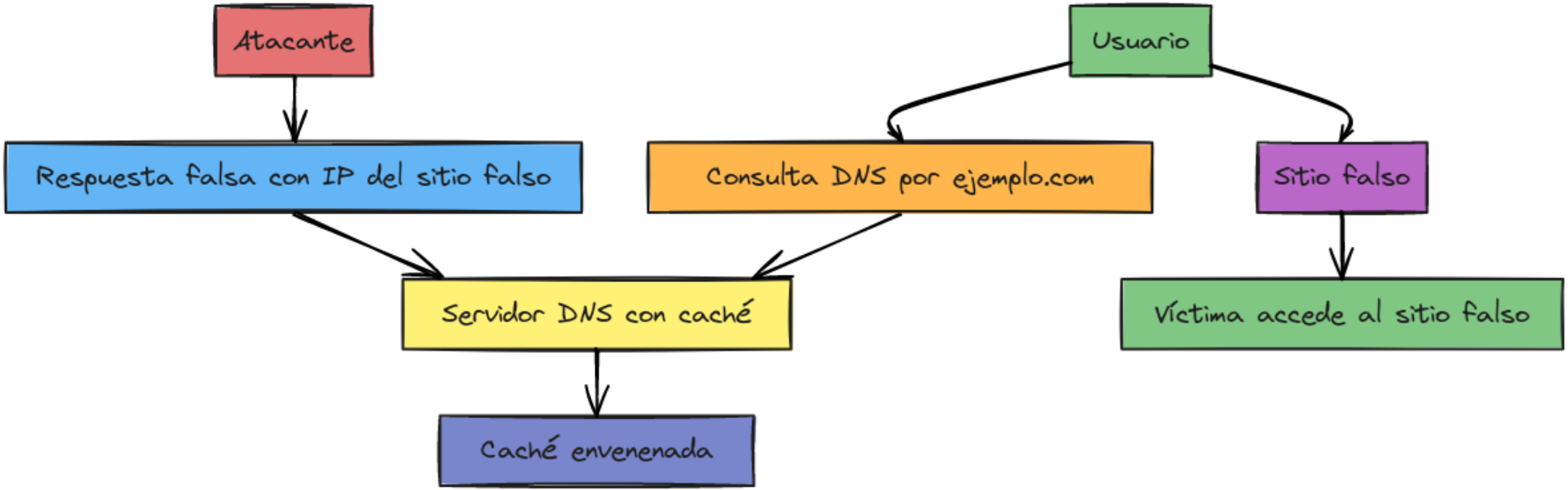
Flujo de acciones desde una solicitud legítima hasta una respuesta manipulada por un atacante

Amplification Attack

Comunes en ataques DDoS y aprovechan servicios vulnerables para multiplicar el tráfico hacia la víctima.



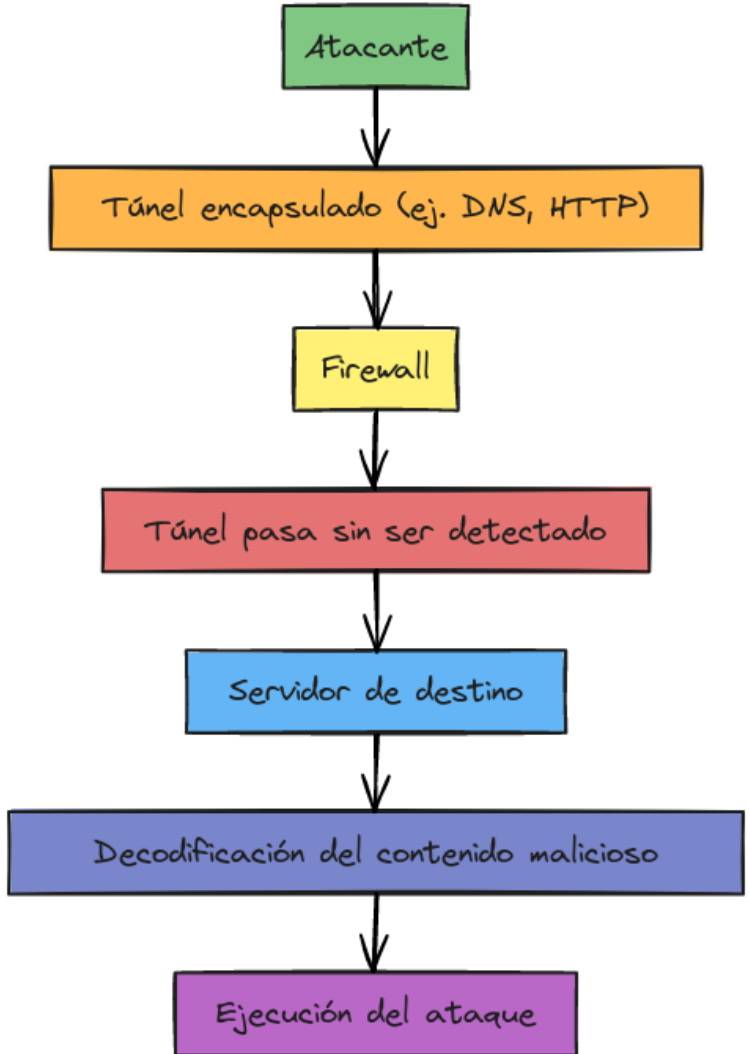
Cache Poisoning



Un ataque en el que un actor malicioso introduce respuestas falsas en la caché de un servidor DNS o de proxy para redirigir tráfico.

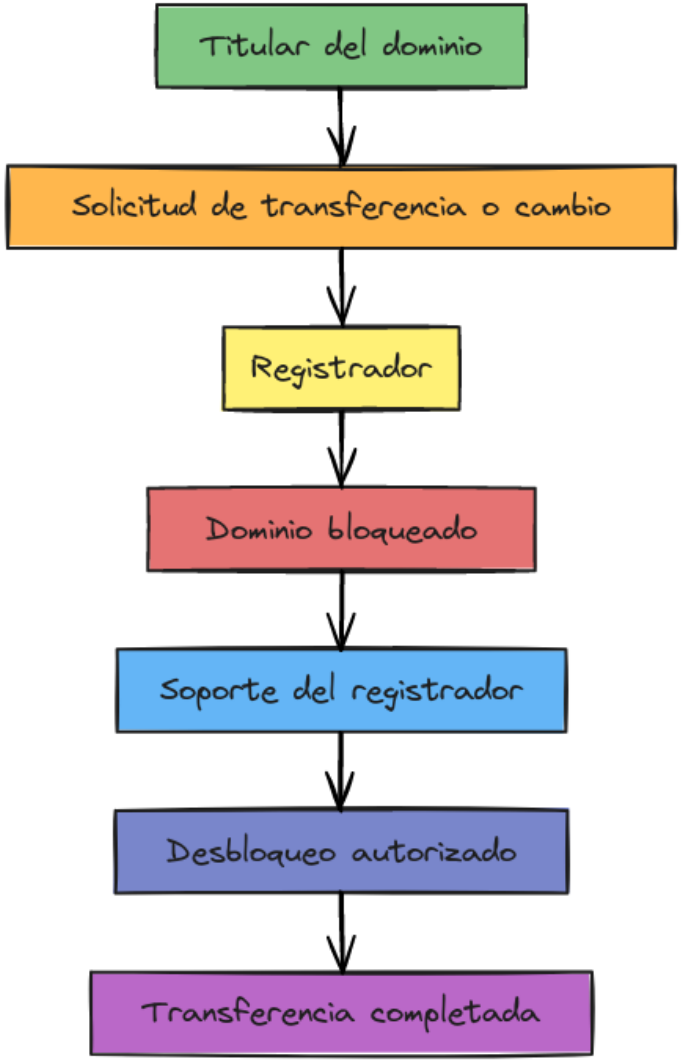
Tunneling Attack

Encapsula tráfico malicioso dentro de protocolos legítimos para evadir filtros o firewalls.

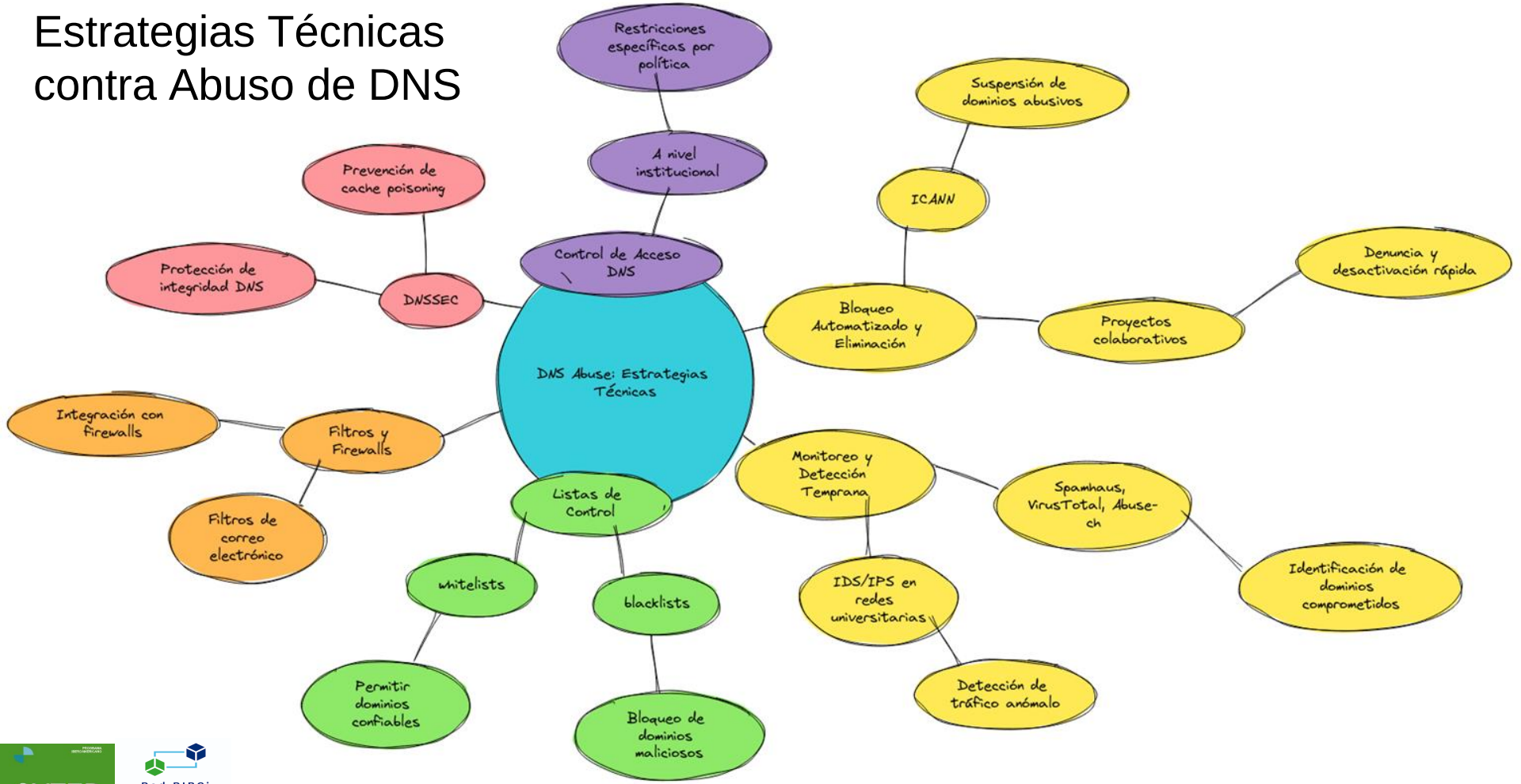


Domain Lock-Up

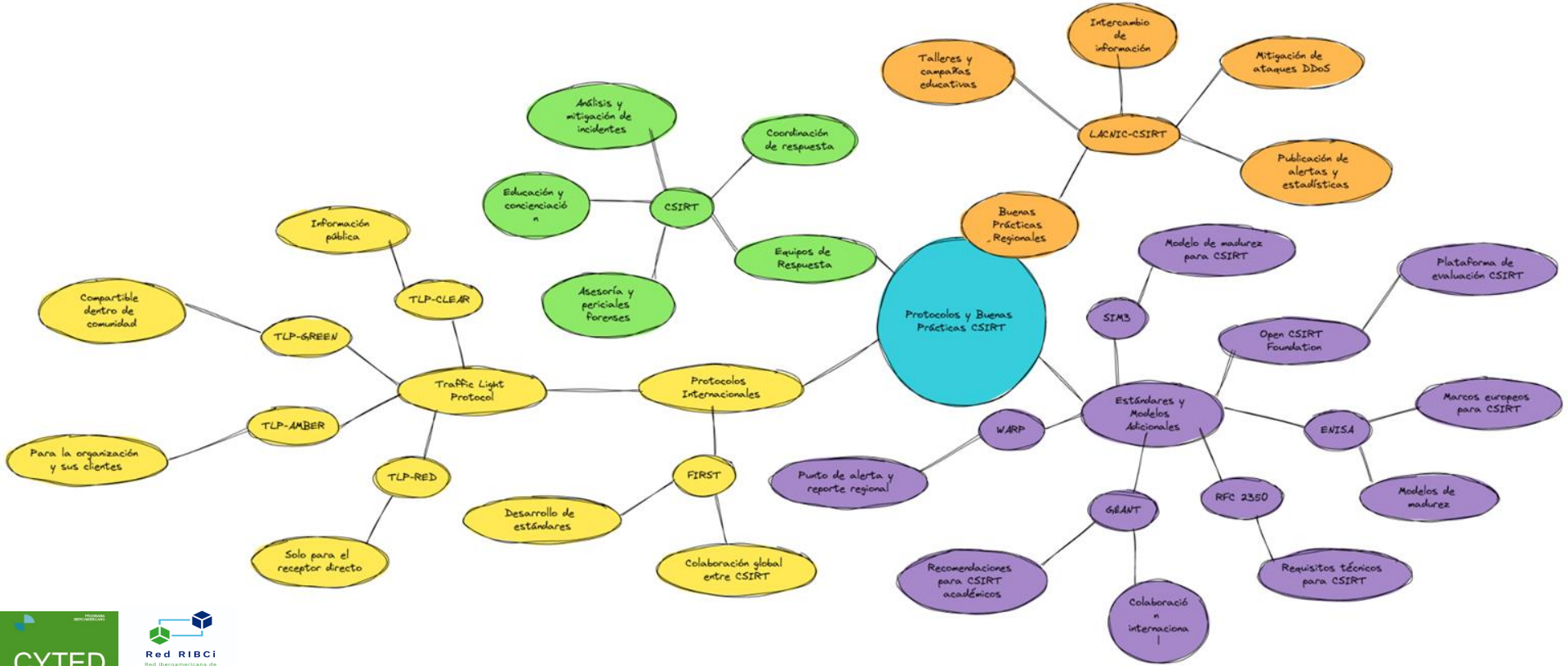
Suele referirse a la retención o secuestro de un dominio, impidiendo transferencias o cambios debido a controles maliciosos, errores de configuración o abuso contractual.



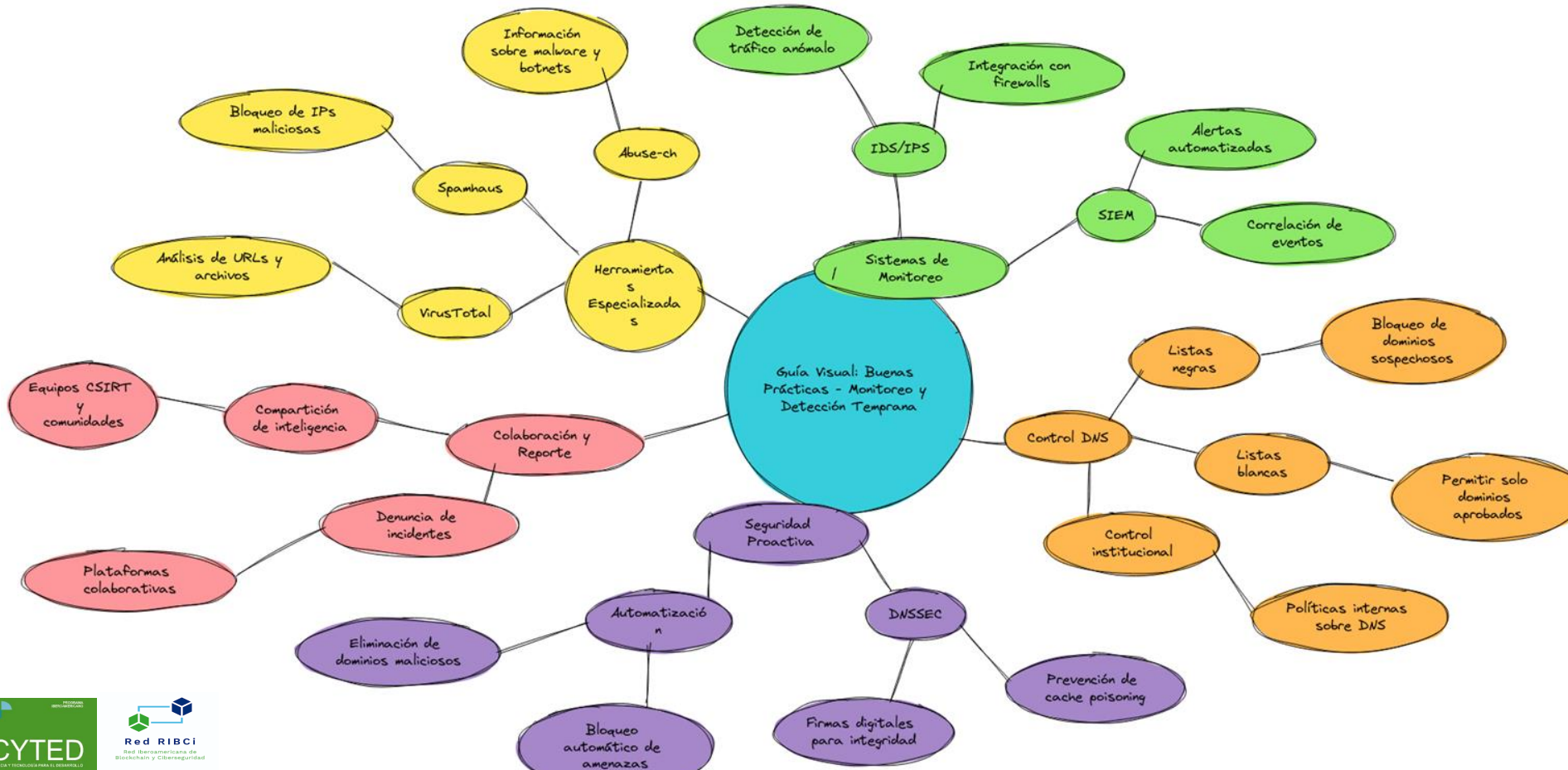
Estrategias Técnicas contra Abuso de DNS

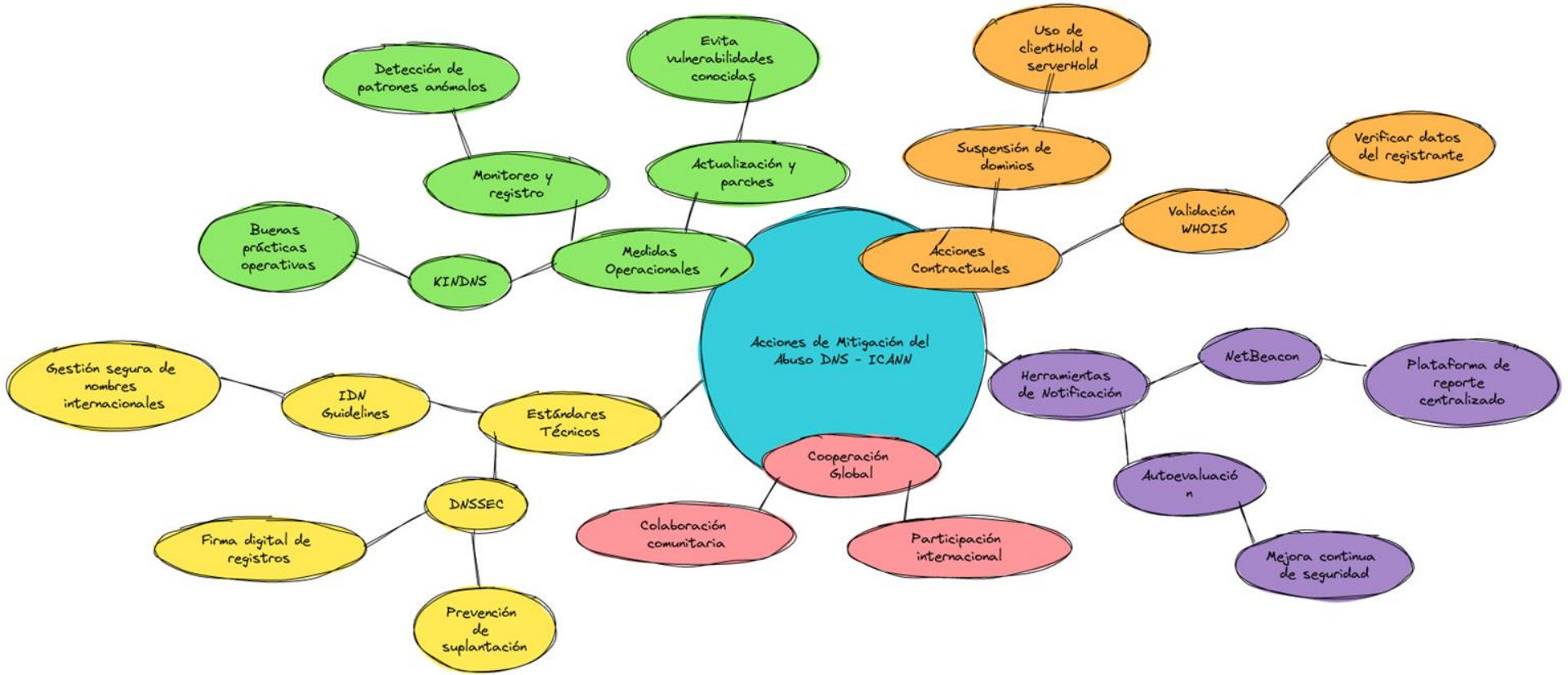


Protocolos, Estándares y Buenas Prácticas para CSIRT



Buenas Prácticas - Monitoreo y Detección Temprana:





¿Para qué sirve el OSINT en la detección y mitigación del DNS Abuse?

- https://sites.google.com/view/cibercol/cybercol?authuser=0

CYTED

Red RIBCi
Red Iberoamericana de Blockchain y Ciberseguridad

Identificar dominios maliciosos o sospechosos

Mediante OSINT, se puede:

- Verificar si un dominio ha sido **reportado por phishing, malware, spam o botnets**.
- Consultar **blacklists** (listas negras) en tiempo real.
- Analizar si un dominio ha sido **registrado recientemente** y está relacionado con campañas fraudulentas.

Investigar la propiedad y registro de dominios (Whois)

OSINT permite examinar los datos de registro de un dominio:

- **Nombre del registrante** (si no está privado)
- Fecha de creación y expiración
- Registrar (empresa proveedora)
- Servidores de nombre asociados (DNS)

Esto es clave para:

- Detectar dominios “frescos” creados para campañas de abuso
- Identificar patrones sospechosos (múltiples dominios registrados por el mismo contácto)
- Investigar casos de typosquatting o domain hijacking

Herramientas:

- Whois.domaintools.com
- ICANN WHOIS Lookup

Mapear relaciones y comportamientos de redes maliciosas

Con técnicas OSINT más avanzadas, se puede:

- Rastrear múltiples dominios que comparten la **misma IP o DNS**.
- Visualizar redes de **dominios relacionados o controlados por un atacante**.
- Establecer correlaciones entre ataques a diferentes instituciones educativas, gubernamentales o sociales.

Herramientas: RiskIQ PassiveTotal - DNSdumpster - Shodan

Fortalecer la ciberinteligencia institucional

- OSINT permite a las universidades hacer **monitoreo proactivo** de intentos de suplantación de su dominio.
- Facilita **informes de inteligencia cibernética** para la toma de decisiones técnicas y de gobernanza.
- Empodera a estudiantes y docentes con capacidades reales de análisis y respuesta.

Prevenir y educar

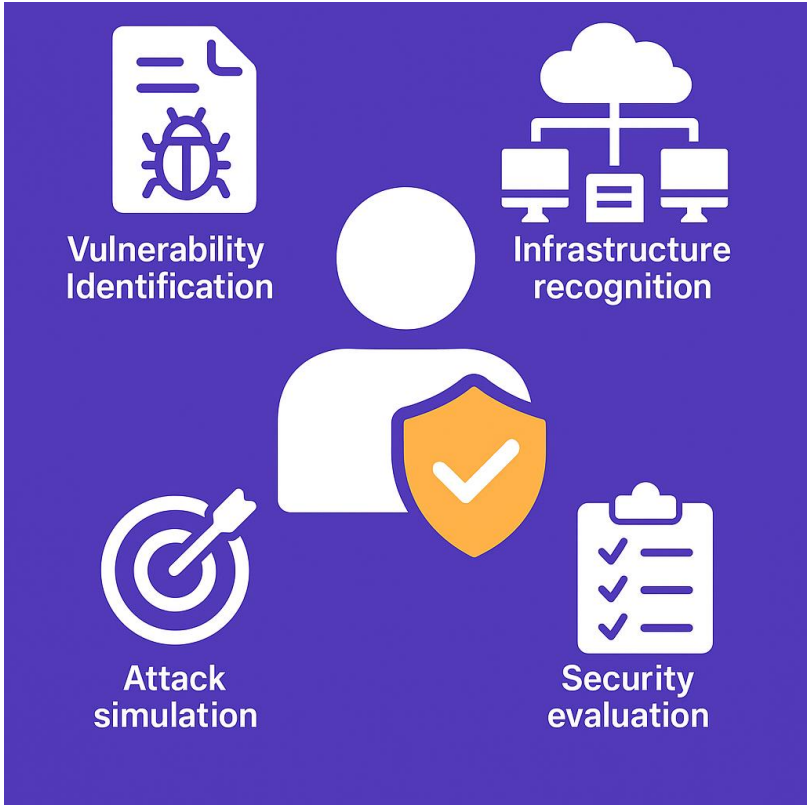
- OSINT no solo es para especialistas. Puede ser una **herramienta pedagógica** para enseñar a detectar sitios falsos, analizar URLs y generar conciencia.

- Ideal para cursos de **ciberseguridad, periodismo digital, ciencia de datos o relaciones internacionales**.

Kali GPT- AI Assistant For Penetration Testing on Kali Linux

Pentesting

En el contexto del pentesting (pruebas de penetración), analizar el abuso de DNS (DNS abuse) sirve para identificar y explotar vulnerabilidades relacionadas con el sistema de nombres de dominio, lo que permite evaluar la seguridad de la infraestructura digital de una organización y prevenir ataques reales.



Identificación de Vulnerabilidades:

El pentester utiliza técnicas para descubrir si existen configuraciones inseguras en el servidor DNS, como nombres de servidor expuestos, transferencias de zona desprotegidas, o registros mal configurados que pueden ser explotados por atacantes para realizar ataques de DNS hijacking, spoofing, poisoning o tunneling.

Reconocimiento de Infraestructura:

Herramientas como `dnsenum` permiten descubrir subdominios y servidores ocultos mediante consultas DNS, lo que ayuda a mapear la infraestructura y encontrar posibles puntos de entrada para ataques más avanzados.

Simulación de Ataques:

El pentester puede simular ataques comunes como:

- DNS Hijacking: Redirigir el tráfico a servidores controlados por el atacante.
- DNS Poisoning/Spoofing: Manipular las respuestas DNS para engañar a los usuarios y desviarlos a sitios maliciosos.
- DNS Tunneling: Utilizar el protocolo DNS para exfiltrar datos o evadir firewalls.

Evaluación de Controles de Seguridad:

Se verifica si existen mecanismos de protección como DNSSEC, bloqueos de dominio (registry/registrar lock), monitoreo de cambios de registros DNS y autenticación multifactor para cuentas de gestión DNS.

DNSSEC (Domain Name System Security Extensions o Extensiones de Seguridad del Sistema de Nombres de Dominio) es un conjunto de extensiones que añaden una capa de seguridad adicional al protocolo DNS tradicional. Su objetivo principal es garantizar la autenticidad e integridad de los datos DNS, asegurando que las respuestas recibidas provengan realmente del servidor autorizado y no hayan sido modificadas en tránsito

Cumplimiento de directrices y mejores prácticas:

El pentesting ayuda a asegurar que la organización sigue las directrices de ICANN y las mejores prácticas de ciberseguridad para mitigar el abuso de DNS

CYTED

Red RIBCi
Red Iberoamericana de Blockchain y Ciberseguridad

Colmena DAO

Colmena DAO se presenta como una solución integral que busca transformar la apicultura y meliponicultura en una herramienta para enfrentar los desafíos ambientales y sociales de la región andina, combinando tecnología avanzada con un enfoque de inclusión social.

El proyecto

Participa

Apicultores e meliponicultor Interesados

Banco de proyectos de apicultura y

enREDo

UxTIC

Gracias