Forense Digital para la rendición de cuentas

Daniel Bedoya
2025

SOCIALTIC PROTEGE.LA

¿Quién soy yo?

Él - Daniel Bedoya

Analista en seguridad digital

10+ años apoyando a la sociedad civil

Esfuerzos de respuesta a incidentes digitales

¿Qué hacemos en SocialTIC?

SOCIALTIC

Tecnología digital para el cambio social

PROTEGE.LA

DATÁVOROS

Respuesta a incidentes en Sociedad Civil

¿Por qué?	Tipos de ataques	¿Cómo se responde?
Periodistas, defensores DDHH exponen corrupción, abusos, etc.	Software malicioso, robo de cuentas, decomisos, campañas de desprestigio	Líneas de ayuda (servicios voluntarios). Enfoque en la recuperación, poder volver al trabajo.

Retos y dificultades

- No solo **ataques sofisticados**
  - exposición a **cibercrimen común**
- Recursos son **limitados**
- **Poca visibilidad** sobre redes y equipos
- La **prioridad la recuperación** lo más rápido posible

¿Qué podemos hacer para mejorar?

- Buenas prácticas de la industria:
  - Digital Forensics + Incident Response = **DFIR**
- Fortalecer **comunidades** de práctica
- Construir capacidades en **forense digital consentida**

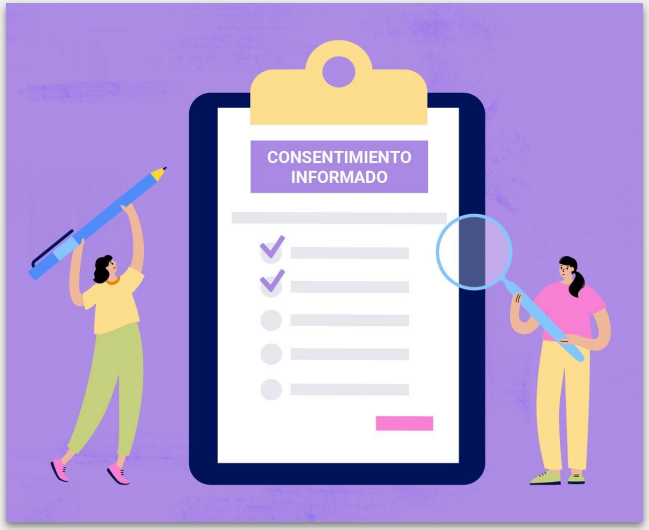
¿Qué es la forense digital consentida?

¿Qué es la forense digital?

Aplicación de **métodos científicos** y **técnicas de investigación** para la **recolección, preservación, análisis y presentación** de **evidencia digital** derivada de dispositivos electrónicos.[1]

Explainer - Introducción a la forense digital consentida para la defensa de los Derechos Humanos - SocialTIC Forensics

Acerca del consentimiento



Se refiere a la **voluntad entre dos o más personas para aceptar derechos y obligaciones**.

Acuerdo de acciones para facilitar la recolección, análisis, presentación y preservación de evidencia digital.

¿Cómo se ve la forense consentida en procesos de rendición de cuentas?

Algunos ejemplos relevantes

13 enero 2022

El Salvador: Amnistía Internacional verifica el uso del programa espía Pegasus para la vigilancia de periodistas

Una **investigación conjunta** de Access Now y Citizen Lab ha identificado el uso a gran escala del programa espía Pegasus de NSO Group contra periodistas y miembros de organizaciones de la sociedad civil en El Salvador. Expertos técnicos del Laboratorio de Seguridad de Amnistía Internacional han revisado el informe y verificado de forma independiente las pruebas forenses que demuestran el uso abusivo de Pegasus en el país.

https://www.amnesty.org/es/latest/news/2022/01/el-salvador-pegasus-spyware-surveillance-journalists/

Algunos ejemplos relevantes

Reportes de espionaje a periodistas y organizaciones de derechos humanos en México

[1] [2]

Jun 19, 2017 | Privacidad

R3D: Red en Defensa de los Derechos Digitales, junto con ARTICLE 19, oficina para México y Centroamérica, y SocialTIC, hemos documentado 76 nuevos intentos de infección con el malware Pegasus en contra de periodistas y defensores humanos en México. Estos ataques, ocurridos entre enero de 2015 y julio de 2016, se suman a los 12 intentos registrados en contra de científicos y activistas de la Alianza por la Salud Alimentaria en 2016.

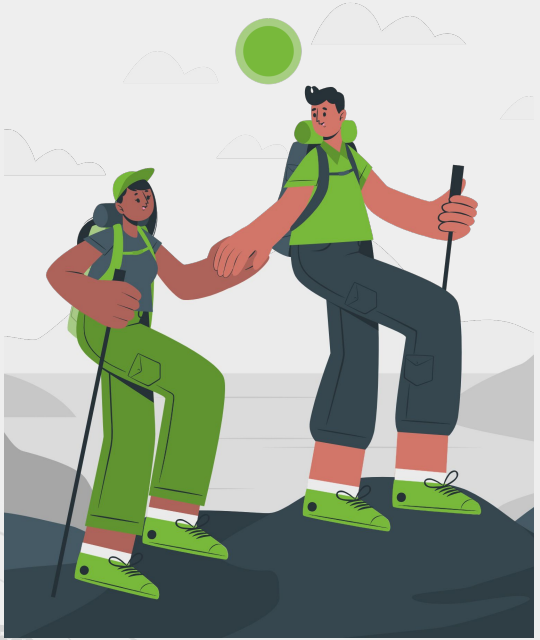
Ejército mexicano espió con Pegasus a dos personas defensoras de derechos humanos del Centro Prodh

- **Dos personas integrantes de la organización de derechos humanos fueron espiadas entre junio y septiembre de 2022 en coyunturas que involucran a las Fuerzas Armadas.**

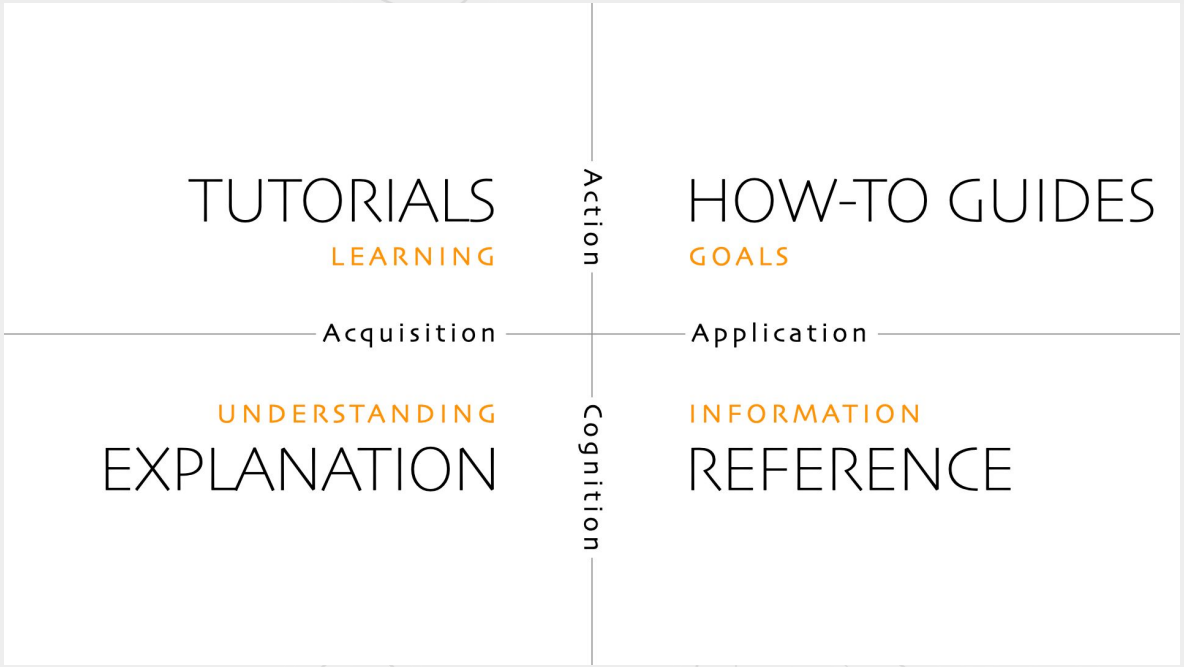
¿Cómo democratizar el acceso a la forense digital?

Una de nuestras propuestas...

- **Repositorio** de **documentación técnica** en forense consentida
- Compartir conocimientos para llevar a **más procesos de rendición de cuentas basados en evidencia**



¿Cómo se organiza?



https://diataxis.fr/

Breve demo

https://forensics.socialtic.org

¡Gracias!

seguridad@socialtic.org

@socialtic

SOCIALTIC

PROTEGE.LA