La seguridad de un Estado digital, hacia una detección participativa

20 años
Fundación Karisma

«Lo esencial es invisible a los ojos».

Antoine de Saint-Exupéry

Stéphane Labarthe
Consultor de la Fundación Karisma

Fundación Karisma

Bogotá, Colombia
Marzo 2023

Diagramación y diseño:
Nicolás Vargas H.

<K+LAB>

En un esfuerzo para que todas las personas tengan acceso al conocimiento, Fundación Karisma está trabajando para que sus documentos sean accesibles. Esto quiere decir que su formato incluye metadatos y otros elementos que lo hacen compatible con herramientas como lectores de pantalla o pantallas braille. El propósito del diseño accesible es que todas las personas, incluidas las que tienen algún tipo de discapacidad o dificultad para la lectura y comprensión, puedan acceder a los contenidos.
Más información sobre el tema: http://www.documentoaccesible.com/#que-es.

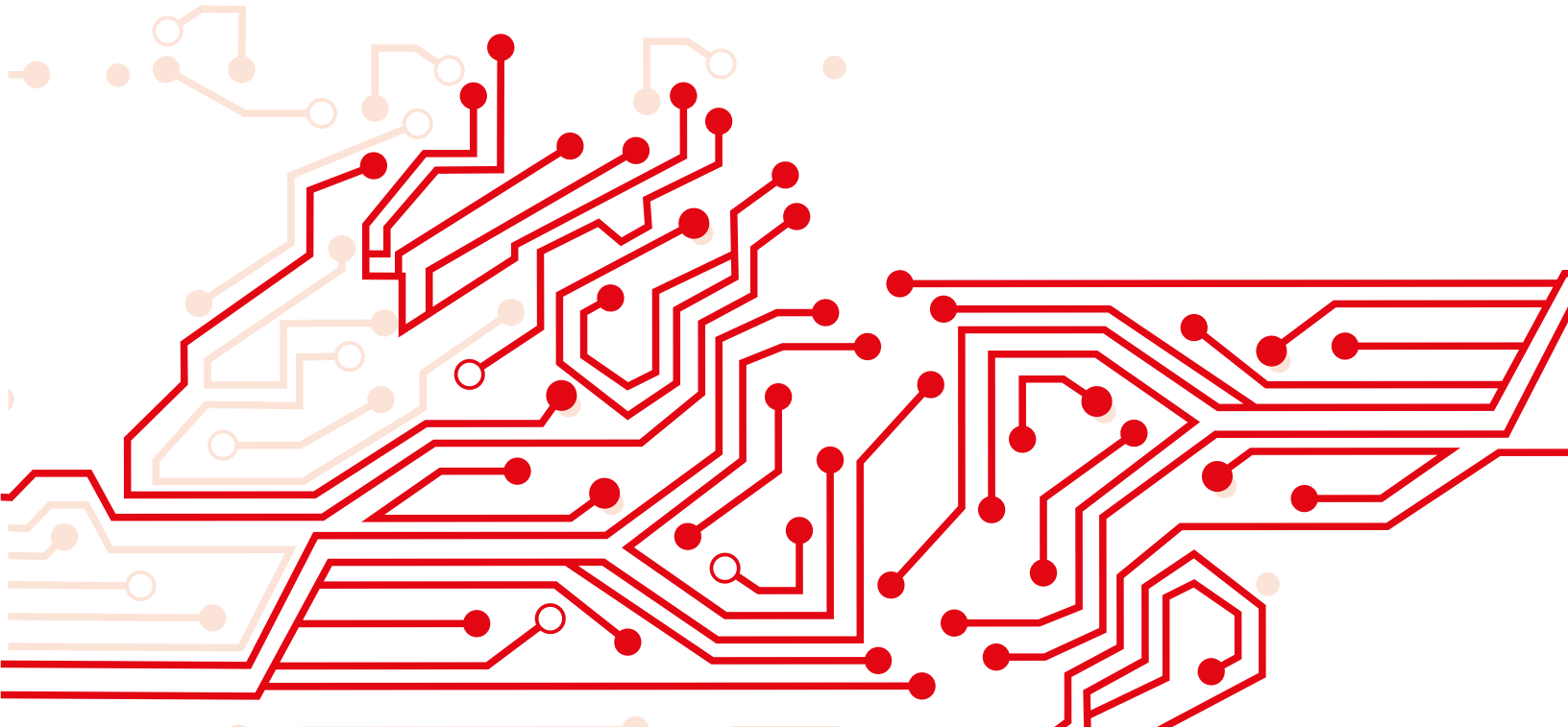
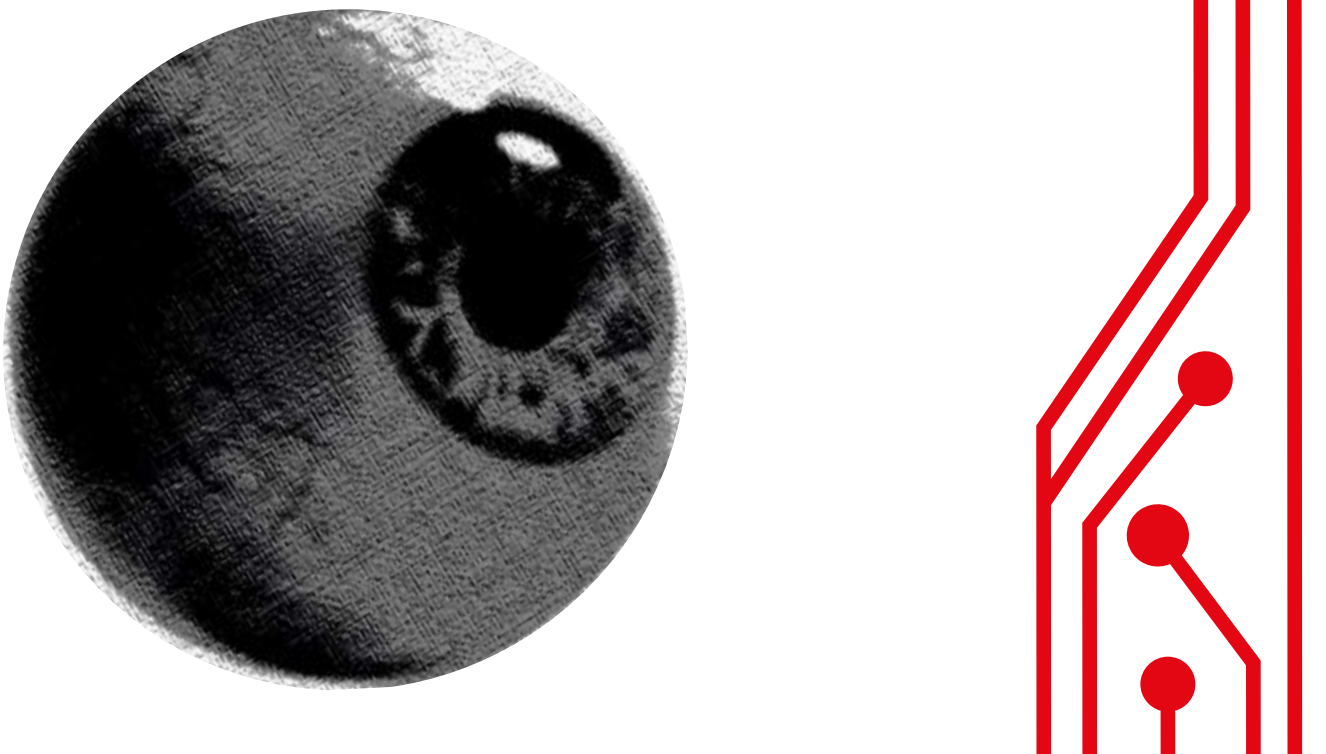


Tabla de contenido.



Nota previa:

El texto que se publica aquí es la traducción al español con algunos pequeños añadidos del artículo "Sécurité d'un État digital, vers une détection participative" escrito originalmente en francés en mayo del 2021 y publicado en octubre de 2022 en la compilación «L'État digital» que incluye otras contribuciones[1]. La publicación de esta traducción cuenta con la autorización de la editora Berger-Levrault. Este trabajo se hizo a raíz del coloquio del mismo nombre, co-organizado por la Universidades de París Panthéon-Assas y la Fundação Getulio Vargas (FGV) de Rio de Janeiro. Las presentaciones correspondientes se pueden ver y escuchar en el sitio web del evento[2].

Ha pasado un año y medio entre la escritura inicial y esta traducción, por lo que algunos datos podrían estar desactualizados. Sin embargo, se hizo un esfuerzo para complementar y poner al día el texto original cuando se identificaron novedades importantes. Así mismo, las secciones que están entre paréntesis angulares son nuevas adiciones y actualizaciones que no aparecen en el original francés. Las notas al pie con número y letra fueron también añadidas.

1 El libro cuenta con 18 contribuciones incluyendo esta. De Colombia se pueden mencionar los artículos «El informe Going Digital in Colombia: recomendaciones de la OCDE y Estado digital en Colombia» de Felipe Calderón-Valencia profesor en la Universidad de Medellín, y «La implementación de los medias digitales en los procedimientos administrativos en el sistema jurídico colombiano» de Ciro Güecha Medina, en la época decano de la Universidad libre de Bogotá. [traducción de los títulos nuestra]

2 *https://cyberbrics.info/digital-state-etat-digital/*

La transición hacía un Estado digital en el cual la casi totalidad de los documentos y de los servicios están disponibles en una forma digital implica un aumento exponencial de los datos almacenados e intercambiados. Los sistemas de información subyacentes que conllevan estos datos y los servicios asociados se vuelven un mecanismo central que sostienen las funciones vitales del Estado. Su seguridad se convierte naturalmente en una condición central para la viabilidad de esta transición hacía un «Estado digital». Pero la complejidad creciente de estos sistemas vuelve su protección y la detección de sus debilidades más difícil. Esta detección de las vulnerabilidades de los sistemas y lo que las nuevas normativas europeas llaman los «incidentes de seguridad» y las «violaciones de la seguridad de los datos» son, sin embargo, fundamentales porque constituyen el primer eslabón de su seguridad y de la confianza que los ciudadanos le pueden entregar. Hasta ahora, la idea dominante para el Estado ha sido contar con las capacidades internas de sus entidades, sumándole unidades administrativas con una función preventiva o restaurativa. Este artículo sostiene que esta forma clásica de acercarse al problema ya no es suficiente y que la capacidad de detección de los riesgos digitales tiene que apoyarse en toda la sociedad, incluyendo las universidades, la sociedad civil, los usuarios, los expertos técnicos e incluso lo que los medios de comunicación llaman de manera confusa los «hackers»[3]. Se trata entonces de pasar de un enfoque cerrado a un enfoque abierto y participativo, cómo ya lo empezaron a hacer algunos actores estatales o privados. A lo largo de este artículo usaremos el término «investigador» para estas personas externas susceptibles de desempeñar este papel de detector.

Este análisis apunta en primer lugar a explicar la importancia de la detección y aclarar los tipos de eventos que se pueden detectar (para no limitarse a las vulnerabilidades como lo suelen hacer las publicaciones en este tema), las evoluciones normativas y las rutas de divulgación existentes. Después se pondrán en evidencia las barreras que todavía hay que cruzar para acercarse a una detección participativa, en particular la necesidad de disminuir los riesgos legales a los cuales se puede exponer un investigador de seguridad digital cuando desempeña este papel de «detector». Finalmente se analizarán las evoluciones normativas y organizacionales en curso que ya son un comienzo de cambio y se tratará de extenderlas a algunas recomendaciones para los gobiernos y los investigadores. Este trabajo cruza dimensiones técnicas, legales y organizacionales del problema.

Este artículo se basa en parte en el «Estudio sobre las rutas de divulgación en seguridad digital» que se realizó y se publicó en octubre del 2019 con la Fundación Karisma[4] y también en una publicación de la Organización para la Cooperación y el Desarrollo Económicos (OCDE)[5] a la cual nuestra Fundación ha participado a través del CSISAC[6]

3 Es importante mencionar que el término «hacker» se suele confundir de manera errónea con el de «cibercriminal». En seguridad digital, se trata de «un experto en informática que usa sus conocimientos en seguridad digital para buscar y [eventualmente] explotar sus debilidades.» (https://fr.wikipedia.org/wiki/Hacker), traducción nuestra). Los cibercriminales sólo son un pequeño subconjunto de los hackers, que realizan este tipo de acciones con el fin de hacer daño o de lucrarse.

4 Labarthe S., «Estudio sobre las rutas de divulgación en seguridad digital», Fundación Karisma, 2019 (https://stats.karisma.org.co/aportes-para-un-entorno-seguro-y-confiable/).

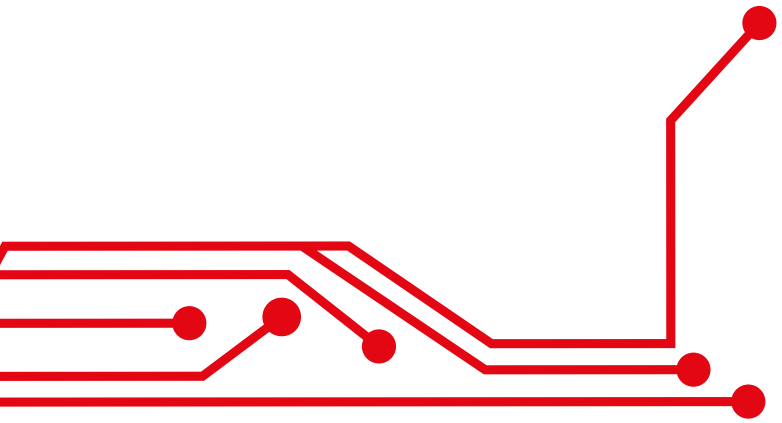
5 OECD, «Encouraging vulnerability treatment, Responsible management, handling and disclosure of vulnerabilities», 2021 (https://one.oecd.org/document/DSTI/CDEP/SDE(2020)3/FINAL/en/pdf).

6 Civil Society Information Society Advisory Council que es la voz de la sociedad civil en la OCDE y del cual Fundación Karisma es miembro (https://csisac.org/).

El primer estudio se apoyaba en trabajos y publicaciones de la Agencia Europea de Seguridad Digital (ENISA), de agencias estatales de Estados Unidos y también de la Electronic Frontier Foundation[7] que se mencionan más adelante. Por otra parte la alimentó también mi experiencia concreta en estas áreas, tanto del lado del Estado como receptor de estos incidentes cuando trabajé en la agencia francesa de protección de datos (Commission Nationale de l'Informatique et des Libertés, CNIL), como del lado de la sociedad civil como detector o a veces intermediario entre los investigadores y las entidades involucradas. Una parte importante del trabajo que se hizo con Fundación Karisma estos últimos años tiene que ver con el análisis de la información y transparencia, con respecto a la privacidad y de la seguridad digital de sitios web y aplicaciones del Gobierno Colombiano. Estos análisis se hicieron para el beneficio de la sociedad civil y de los ciudadanos. En este marco, detectamos vulnerabilidades, incidentes y fugas de datos personales y tuvimos que informar a las entidades del Estado involucradas, a veces hostiles con este tipo de auditoría no solicitada.

Es de estas experiencias que salieron dos hallazgos originales reflejados en la presentación del coloquio y en este artículo: por una parte la necesidad de no limitarse a la cuestión de la detección y divulgación coordinada de las solas vulnerabilidades genéricas, y por otra parte la creación de una propuesta de categorización de los riesgos legales a los cuales se exponen los que detectan, analizan y a veces revelan estos problemas, en función de la metodología de investigación técnica usada.

Es imposible hacer un análisis exhaustivo de un tema tan amplio y complejo, en el cual los contextos administrativos, políticos y legales –y por lo tanto los riesgos– cambian de un país a otro. Sin embargo, hay algunos patrones comunes y para este análisis se tomarán ejemplos que provienen de Europa, Francia en particular, de Estados Unidos y de América Latina, Colombia en particular.



7 Rodríguez, K., «Protecting Security Researchers' Rights in the Americas», Electronic Frontier Foundation, 2018 (www.eff.org/wp/protecting-security-researchers-rights-americas).

A- Detección y clasificación de los eventos de seguridad: lo que está en juego

1. La detección: un pilar de la seguridad

Tanto en seguridad física como en seguridad digital se suelen considerar tres pilares: la detección, la protección y la capacidad de reacción frente a un evento no deseado.

El primero, muchas veces, se descuida y, de todas formas, se vuelve cada vez más complejo. En efecto, detectar una vulnerabilidad o incluso un incidente o una fuga de de datos a tiempo se vuelve más difícil, sobre todo si las organizaciones cuentan únicamente con sus capacidades internas, incluso cuando estas son considerables[8]. No faltan ejemplos de casos en los cuales la entidad víctima, a pesar de sus capacidades internas, no pudo detectar a tiempo la o las vulnerabilidades que han sido explotadas ni la fuga de datos resultando de esta explotación. Vamos a citar sólo dos ejemplos, uno de la actualidad reciente y otro de nuestra propia experiencia.

En diciembre 2020, la compañía de ciberseguridad Fire Eye anuncia haber descubierto un ataque a la cadena de suministros de software de la plataforma Orion de SolarWinds[9]. El código malicioso involucrado tenía la capacidad de infectar los clientes cuando actualizaban sus sistemas. Este incidente constituyó un evento importante en el mundo de la seguridad digital porque las aplicaciones de SolarWinds permitían gestionar de manera centralizada grandes redes informáticas, perteneciendo por lo general a empresas multinacionales y a Estados. Los sistemas afectados incluían por ejemplo la empresa Microsoft, el Departamento de Estado y la Agencia Nuclear de Estados Unidos. El impacto fue aún más grande ya que las primeras versiones infectadas del software tenían fechas al menos de marzo 2020[10], lo que significa que este ataque a gran escala perduró durante más de nueve meses sin ser detectado.

8 En los sistemas y procesos internos «técnicos» permitiendo esta detección, se pueden mencionar los sistemas de detección de intrusión (I DS), los sistemas de monitoreo de los servidores y equipos, el análisis de los logs de los servidores, los sistemas anti-malware, etc. pero también la supervisión continua, las auditorías y las pruebas de penetración.

9 Fire Eye, «Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor, Threat research», 2020 (https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html)

10 CISA, «Active Exploitation of SolarWinds Software», 2020 (https://us-cert.cisa.gov/ncas/current-activity/2020/12/13/active-exploitation-solarwinds-software).

Otro ejemplo, que proviene de nuestra experiencia en la Fundación Karisma y que pudimos analizar directamente, concierne a una falla de seguridad que llevó a una fuga de datos personales en el sistema de visados del Estado colombano. Fue detectada inicialmente por una persona usuaria quien primero alertó la entidad estatal a cargo del sistema[11] pero sin resultado.

Finalmente fue revelada el 15 de enero del 2021 por el medio independiente colombiano La Silla Vacía, antes de su resolución, lo que aumentó los riesgos y las consecuencias para los más de 550.000 extranjeros cuyos datos personales estaban en juego[12]. Un segundo análisis del sitio web fue realizado después por la Fundación Karisma. Éste puso en evidencia otras vulnerabilidades y se transmitió cómo alerta al Ministerio de Relaciones Exteriores[13]. A pesar de que su explotación era bastante fácil[14], parece que esta vulnerabilidad había permanecido sin ser detectada durante al menos cinco años.[15]

Teniendo en cuenta la sensibilidad de los datos involucrados (copia digital de la visa con su categoría y todos los datos personales asociados), la facilidad de explotación de esta vulnerabilidad[16] y el largo tiempo de exposición antes de ser solucionada, es posible que cibercriminales, servicios de inteligencia o cualquier otro actor malintencionado la haya explotado en silencio para extraer los valiosos datos.

Para dar una cifra más general que proviene del análisis automático realizado por la empresa de ciberseguridad Veracode en más de 130.000 aplicaciones durante un año, el 24% de las aplicaciones escaneadas incluían una vulnerabilidad severa[17]. Si bien se volvió muy común decir que la seguridad al 100 % no existe, la existencia de vulnerabilidades críticas, de incidentes o incluso de violaciones de datos que permanecen en el tiempo puede tener consecuencias muy grandes para las personas víctimas. Mejorar su detección es, por lo tanto, fundamental e implica de todas las partes involucradas una humildad necesaria para reconocer la utilidad de ayudas externas.

11 La Cancillería, del Ministerio de Relaciones Exteriores de Colombia.
12 Duque, T., «Un bache de seguridad amenazó los datos de extranjeros y Cancillería no sabía», 2020 (La Silla Vacía, https://lasillavacia.com/bache-seguridad-amenazo-los-datos-extranjeros-y-cancilleria-no-sabia-79749)
13 Botero, C, «La importancia de reportar fallos en sistemas informáticos del Estado», El Espectador, 2021 (https://www.elespectador.com/opinion/columnistas/carolina-botero-cabrera/la-importancia-de-reportar-fallos-en-sistemas-informaticos-del-estado-column/).
14 El sistema se basaba en un código QR que contenía una URL permitiendo, para cada persona usuaria, acceder a su visa. La URL contenía en sus parámetros el número de visa y su sóla modificación permitía, sin necesidad de autenticación, acceder a las visas de otras personas usuarias.
15 Tuvimos en nuestra posesión una visa de más de cinco años con su código QR de consulta. La URL que contenía tenía exactamente la misma estructura y el mismo parámetro.
16 Se puede mencionar al respecto que los periodistas de La Silla Vacía pudieron fácilmente extraer 25 visas que muestran como ejemplo en su artículo, ocultando parcialmente los datos y las fotografías.
17 Veracode, «State of Software Security v11», 2021 (https://www.veracode.com/state-of-software-security-report).

2. Los cinco tipos de eventos que se pueden detectar

En general las publicaciones en este tema se limitan o se centran en las «vulnerabilidades» (ver definición más adelante). Es el caso de los informes de la ENISA y de la OCDE ya mencionados y que usamos para este trabajo. Esto se explica en parte porque este tema de la detección y divulgación responsable y coordinada en seguridad digital fue durante mucho tiempo impulsado por los proveedores de soluciones, los gigantes del mundo digital, naturalmente preocupados por detectar y corregir las vulnerabilidades de sus sistemas, en relación con sus clientes y usuarios. Aquí, se quiere ampliar la reflexión a cinco tipos de eventos que el Estado debe estar en capacidad de detectar para poder garantizar la seguridad de sus sistemas de información. Además de ser necesaria para un acercamiento completo hacia la problemática y enfocado hacía el ciudadano, esta lista se conecta con las nuevas obligaciones de las normativas europeas en cuanto a la notificación de los incidentes y de las violaciones de la seguridad de los datos. No siempre existe un consenso en la categorización de los eventos, pero se ofrecen aquí definiciones que provienen de entidades de referencia a nivel internacional. Las traducimos y las adaptamos a veces ligeramente para más claridad y simplicidad.[18]

a - Las vulnerabilidades «genéricas»

Ellas tienen que ver con una categoría de equipos, programas y servicios en línea. Según la definición de la ENISA que ella misma se basa en la norma ISO27147, se trata de «un error de concepción o de implementación, o de una debilidad que posee un equipo, un programa, una red, un protocolo o un servicio en línea, y que puede ser explotado incluso para comprometer la seguridad del sistema».[19] Este tipo de vulnerabilidad, la tiene que corregir normalmente el constructor/proveedor, cada entidad/persona usuaria teniendo después que asegurar de la instalación del correctivo (que puede ser automática o no) en los componentes involucrados de sus sistemas. Cuando se publican, las vulnerabilidades se suelen registrar en bases de datos públicas,siendo la más conocida la lista «CVE» del MITRE.[20]

Un ejemplo de este tipo de vulnerabilidad es la «CVE-2021-26855» que afectó a los servidores de correo electrónico Microsoft Exchange.

18 A pesar de que la Agencia de ciberseguridad francesa (ANSSI) haya dado una definición de estos términos directamente en francés en Internet ((https://www.ssi.gouv.fr/entreprise/glossaire/) [y que la versión original de este artículo haya sido escrito en francés] se eligieron en general otras definiciones. Por otra parte no se decidió adoptar la clasificación del informe de la OCDE ya mencionado respecto a las vulnerabilidades (code vulnerabilities y system vulnerabilities) porque buscamos tener un espectro más amplio y menos específico que el de este informe.

19 ENISA, «Economics of Vulnerability Disclosure», 2018, p. 9-10 (https://www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure).

20 Common Vulnerabilities and Exposures (https://cve.mitre.org/).

b - Las vulnerabilidades propias a un sistema específico de una entidad

A veces llamadas vulnerabilidades de activos o fallas de seguridad (security flaw en inglés). La Agencia de Ciberseguridad de Estados Unidos (CISA)[21] da de ellas una definición clara y sencilla: «una característica o una debilidad específica que hace una organización o un activo (como una información o un sistema de información) vulnerable a una amenaza intencional o accidental»[22]. Se puede resaltar que la existencia de una vulnerabilidad genérica en un sistema específico de una entidad constituye una falla de seguridad.

Un ejemplo es la primera versión de la aplicación CoronApp, desarrollada e implementada por el Estado colombiano en el contexto de la pandemia de covid-19, que usaba el protocolo inseguro de transferencia hipertexto (HTTP) para transmitir los datos personales de las personas usuarias. Esto la hacía vulnerable a escuchas pasivas, por ejemplo.[23]

c - Los incidentes de seguridad

La norma ISO27001[24] define un incidente de seguridad digital como «un evento o una serie de eventos de seguridad digital, no deseados o no esperados y que tienen una probabilidad significativa de comprometer las actividades y de amenazar la seguridad de la información». En algunos sectores, dependiendo de los países, puede ser obligatorio notificar a las autoridades estatales competentes un incidente de seguridad. Por ejemplo en Estados Unidos es el caso en el sector financiero y en Europa para lo que llaman los «servicios esenciales del Estado».[25]

Un ejemplo de esto es el incendio en el centro de datos de la empresa francesa OVHcloud en marzo de 2021.

21 Cybersecurity and Infrastructure Security Agency (CISA) (https://www.cisa.gov/).
22 CISA, «Cybersecurity Glossary», 2021 (https://niccs.cisa.gov/about-niccs/cybersecurity-glossary).

23 Velásquez A. y Labarthe, S., «CoronApp, Medellín me Cuida y CaliValle Corona al laboratorio - O cómo se hackea CoronApp sin siquiera intentarlo», 2020 (https://web.karisma.org.co/coronapp-medellin-me-cuida-y-cali-valle-corona-al-laboratorio-o-como-se-hackea-coronapp-sin-siquiera-intentarlo/).

24 ISO/IEC, «ISO/IEC27001 : 2013. Information technology — Security techniques — Information Security Management Systems — Requirements», 2013 (https://www.iso.org/standard/54534.html). [Esta norma ha sido actualizada en octubre 2022 (https://www.iso.org/standard/82875.html)]

25 Los servicios esenciales del Estado, definidos por la directiva europea «NIS», se reparten en siete sectores: energía, transporte, bancos, infraestructuras de mercados financieros, salud, suministro y distribución de agua potable e infraestructuras digitales. NIS Directive, 2016 (EU 2016/1148).

d - Las violaciones de la seguridad de los datos personales

El reglamento general de protección de datos (RGPD) de Europa las define como «toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos»[26]. Es importante darse cuenta que, según esta definición, las violaciones de seguridad de los datos personales incluyen las violaciones de su confidencialidad pero también de su integridad[27]. Por lo tanto, el incendio en el centro de datos de la empresa OVHcloud en marzo del 2021, por causa del cual 120.000 servidores no han podido ser restablecido prontamente y quedaron «totalmente o parcialmente impactados»[28], constituye un incidente del cual resultó una violación de la seguridad de los datos personales, para las entidades que perdieron datos de este tipo.[29] Este evento tuvo una importancia particular para el Estado francés porque OVHcloud es una empresa de «cloud soberano», certificada por la agencia francesa de ciberseguridad (ANSSI) para albergar datos y servicios de las administraciones del Estado, incluyendo los que son sensibles.[30]

Otro ejemplo es la fuga de datos personales que impactó a 220 millones de personas en enero de 2021 en Brasil.[31]

26 Reglamento (UE) 2016/679 del Parlamento europeo y del Consejo del 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD) (https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES), artículo 4, definición 12. [En el RGPD el término francés es «violation de données personnelles» que literalmente significa «violación de datos personales» y en inglés es «personal data breach». Sin embargo, en la versión española del texto, es «violación de la seguridad de los datos personales». En Colombia también se usa «violación de datos personales» en la ley de protección de datos. En este artículo, se emplea de manera indistinta una o otra formulación, que sea para datos personales o para otro tipos de datos.]

27 La violaciones de la disponibilidad no entran aquí mientras no haya destrucción, pérdida o alteración de estos datos y por lo tanto violación de su integridad.

28 OVH, «Dernières informations sur notre site de Strasbourg», 2021 (https://www.ovh.com/fr/news/presse/cpl1785.dernieres-informations-notre-site-strasbourg).

29 CNIL, «Incendie OVH : faut-il notifier à la CNIL ?», 2021 (https://www.cnil.fr/fr/incendie-ovh-faut-il-notifier-la-cnil).

30 ANSSI (2020), «Décision de qualification du service d'informatique dans le nuage OVH – Private Cloud» (https://www.ssi.gouv.fr/uploads/2020_2965_np.pdf).

31 PSAFE, «Vazamento em massa expõe número de CPF de milhões de brasileiros, alerta Psafe», 2021 (https://www.psafe.com/blog/vazamento-expoe-numero-de-cpf-de-milhoes-de-brasileiros-alerta-psafe/).

e - Las violaciones de la seguridad de otro tipo de datos

Se trata en particular de las violaciones de la seguridad de los datos definidas por lo que las normativas europeas llaman los servicios esenciales del Estado, ya mencionados más atrás.[32]

Se puede ilustrar esta noción con un ejemplo sencillo más cercano de la persona usuaria: si la ausencia de cifrado del disco duro de un computador portátil que contiene datos personales es una vulnerabilidad, su robo constituye un incidente de seguridad, y el acceso a los datos personales que contenía, por parte de un tercero no autorizado, es una violación de la seguridad de estos datos.

También se puede observar que, desde un punto de vista puramente técnico, estos cinco tipos de eventos no son siempre distinguibles. Por ejemplo, las violaciones de la seguridad de los datos personales a veces se consideran como incidentes de seguridad, como lo muestra la clasificación del CISA que se presenta en la parte C. Sin embargo, tomando en cuenta las dimensiones legales y organizacionales, esta clasificación puede ser más adaptada, en particular para los países que cuentan con una ley de protección de datos personales.

B- Metodologías de detección y riesgos legales asociados

Buscar y descubrir vulnerabilidades, incidentes o violaciones de la seguridad de los datos en un sistema de información externo conlleva todavía, en muchos países, riesgos legales importantes para el investigador, incluso si lo hace con un enfoque «ético» y buenas intenciones. El informe de la OCDE del 2021 menciona varios ejemplos de investigadores que han tenido que enfrentar amenazas y procesos legales.[33] Nosotros mismos, en la Fundación Karisma, cuando empezamos nuestro trabajo de análisis de sitios webs y aplicaciones, hemos recibido reacciones hostiles de parte del Gobierno, incluyendo amenazas de pleito. El hecho de estar en capacidad de presentar y justificar que nuestros análisis son no intrusivos, reproducibles, legales y éticos nos ha permitido, con el tiempo, construir un diálogo más constructivo con el Estado colombiano.[34]

32 Se hubieran podido reagrupar las categorías del d y del e, porque desde un punto de vista técnico son similares. Sin embargo, desde un punto de vista jurídico y organizacional, no es el caso. La categoría del e, depende de las normativas vinculadas con la protección de los datos personales y de las autoridades de protección de datos personales.

33 OECD, «Encouraging vulnerability treatment, Responsible management, handling and disclosure of vulnerabilities», op. cit., p. 53 y 54.

34 Ibid., p. 71.

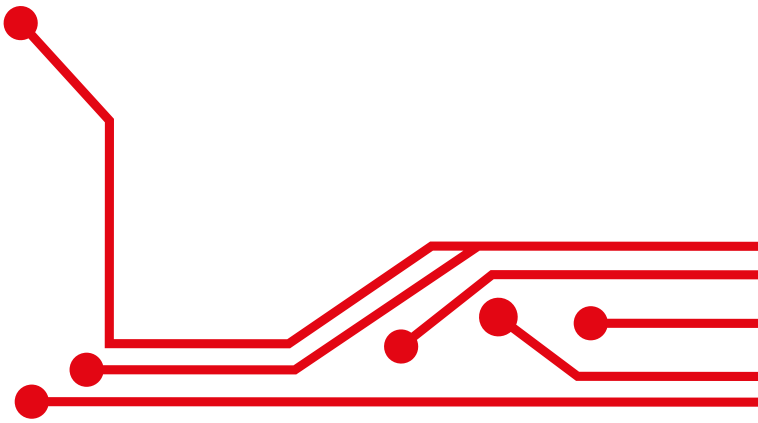
Es por esto que nos parece importante insistir en las metodologías técnicas de análisis y en los riesgos legales asociados a cada una de ellas. Este cruce entre metodologías técnicas de análisis y riesgos legales proviene de nuestra experiencia, de diálogos y de análisis realizados con juristas y expertos técnicos, en particular de la CNIL y de la Fundación Karisma.

1. Clasificación de los métodos de análisis

Esta categorización de los riesgos legales para el investigador que descubre la vulnerabilidad, el incidente o la violación de datos, y eventualmente la reporta, depende en parte de la metodología técnica usada y si esta es más o menos intrusiva. Que sepamos, esta clasificación técnico-jurídica no había sido realizada antes de la publicación de nuestro estudio sobre las rutas de divulgación[35] y constituye por lo tanto un primer ensayo que sin duda se tendrá que profundizar. Obviamente, esta clasificación puede variar en función de las normativas de cada país y son por ende únicamente las grandes líneas comunes que intentamos dibujar aquí, dando algunos ejemplos en ciertas legislaciones nacionales particulares. Partimos de la hipótesis según la cual el investigador de vulnerabilidad, de incidente o de violación de datos no tiene un vínculo contractual con la entidad responsable del sistema de información involucrado, y nos situamos fuera del contexto de programas de recompensas (bug bounty) que abordamos en la parte C. Se puede tratar de un investigador externo a la organización, de un «hacker», de un miembro de una ONG, de una persona usuaria del sistema, etc. También asumimos que esta persona tiene «buenas» intenciones y practica lo que se suele denominar «hacking ético». En esta clasificación identificamos seis familias de metodologías de análisis:

a - Análisis pasivo y búsqueda no intrusiva de informaciones públicas

Este tipo de análisis (estático) incluye la observación de la parte visible del sistema, la consulta de los términos y condiciones, políticas o cualquier otro documento público vinculado con él. También puede incluir observaciones técnicas como el exámen de un código fuente público, el análisis del certificado criptográfico del sitio web o de la aplicación, el análisis de direcciones IP de servidores a través de los registros públicos, etc.



35 Labarthe S., «Estudio sobre las rutas de divulgación en seguridad digital», Fundación Karisma, op. cit..

b - Análisis de flujos de datos saliendo de/entrando a un dispositivo de la persona usuaria («cliente»), sin descifrar los datos

A veces llamada «captura de paquetes», este tipo de análisis (dinámico) se suele hacer desde un programa instalado en el dispositivo cliente[36] o desde un dispositivo externo (computador por lo general) que actúa entonces cómo un intermediario entre el dispositivo del usuario y el servidor web o de aplicación.

c - Análisis de flujos de datos saliendo de/entrando a un dispositivo de la persona usuaria («cliente»), descifrando los datos

Este tipo de análisis (dinámico) apunta a capturar y descifrar los flujos de datos para estar en capacidad de analizar su contenido. En general se trata del protocolo HTTPS[37] que es el protocolo de comunicación más usado en Internet para cifrar los datos y autenticar las comunicaciones. Es importante notar que los programas que permiten realizar este tipo de análisis[38] suelen funcionar creando dinámicamente falsos certificados criptográficos que permiten al programa o al dispositivo intermediario hacerse pasar por el/los servidor(es) final(es)[39] ante el dispositivo cliente.

d - Solicitudes activas e inusuales activas a un sistema pero sin intrusión

Esto puede incluir, por ejemplo, desde «escaneo de puertos» hasta solicitudes repetidas del tipo «denegación de servicio». Es importante tener en cuenta que este tipo de acción puede ser detectada por la entidad encargada del sistema analizado –cuando se trate de un servidor informático en particular– y que puede, en ciertos casos, alterar su funcionamiento o su disponibilidad.

36 En general un teléfono inteligente, una tableta o un computador, pero también puede incluir otros tipos de dispositivos conectados.

37 HyperText Transfer Protocol Secure de su sigla en inglés, en español «protocolo seguro de transferencia de hipertexto». Consiste en la encapsulación del protocolo estándar HTTP en el protocolo cifrado SSL o su sucesor TLS.

38 Se puede mencionar por ejemplo los programas de código abierto MITM proxy y OWASP ZAP o el programa propietario Charles Proxy.

39 Esto necesita tener el control del dispositivo cliente analizado para poder instalar en él un certificado raíz del programa, el cual firmará estos «falsos certificados».

e - Ingeniería inversa de un programa, de un servicio en línea o de un dispositivo (hardware) con o sin elusión

Este tipo de análisis puede incluir la reconstrucción o el acceso a un código fuente no público, la copia y la difusión parcial o total de código fuente o de elementos técnicos, pero también el hecho de sobrepasar medidas de protección («elusión») para poder tener acceso a él o a funcionalidades normalmente no accesibles a la persona usuaria. Dos ejemplos concretos pueden incluir la de-compilación de un programa propietario o el jailbreak de un iPhone.

f - Explotación efectiva de una vulnerabilidad e intrusión en un sistema (cuando el investigador entra en el sistema, el servidor)

Al contrario de lo que se podría pensar, es muy fácil dar el paso y entrar en esta categoría porque es muy tentador de querer verificar la realidad de una vulnerabilidad o de una fuga de datos que parece estar aquí. El investigador es curioso por naturaleza… Además, hasta el simple hecho de hacer clic en una URL indexada por un motor de búsqueda, pero que llevaría a una parte del sistema que no debería ser accesible permite, en ciertos casos, «entrar en la casa» sin estar autorizado a ello.

2. Las tres principales familias de riesgos legales

Aquí retomamos las tres familias de riesgos legales identificadas en el informe de la ENISA,[40] inicialmente pensado para la detección de una vulnerabilidad, pero que se puede también extender a la detección de incidentes o de violaciones de la seguridad de datos.

a - Una infracción a leyes penales relacionadas con sistemas informáticos o protección de la información

En Francia, se pueden mencionar los artículos 323-1 hasta 323-8 del Código Penal, relacionados con las «violaciones a sistemas de tratamientos automatizados de datos». El Código contempla multas desde 30.000 hasta 300.000 € y hasta diez años de prisión para las intrusiones en sistemas informáticos, el hecho de obstaculizar su funcionamiento o el hecho de «extraer, de tener en su posesión, reproducir, suprimir o modificar de manera fraudulenta los datos que contiene» (art. 323-3, traducción propia).

40 ENISA, «Good Practices on Vulnerability Disclosure: From Challenges to Recommendations», 2015 (www.enisa.europa.eu/publications/vulnerability-disclosure).

La únicas excepciones previstas en esta serie de artículos se aplican a los oficiales habilitados del Estado en ciertas condiciones (art. 323-8). También existen casos específicos de protección para ciertos tipos de informaciones como las que tienen que ver con la defensa nacional.[41] En Colombia, se puede mencionar la ley de delitos informáticos que estipula penas muy severas sin contemplar excepciones y se aplica en particular al acceso no autorizado a un sistema, protegido o no por medidas de seguridad.[42]

Las metodologías de la categoría f de nuestra lista («explotación efectiva de una vulnerabilidad e intrusión en un sistema») exponen sin duda el investigador a este tipo de riesgos legales. Las metodologías de la categoría d («solicitación activa de un sistema fuera de un uso normal, pero sin intrusión») también, porque son susceptibles de obstaculizar el funcionamiento o la disponibilidad del sistema.

b - Una infracción a las leyes de propiedad intelectual así como a los términos y condiciones de los contratos, licencias y políticas de uso

Las metodologías de la categoría e de nuestra lista (ingeniería inversa) pueden entrar en esta categoría en la medida en la cual suelen implicar acceder, copiar y difundir parcialmente o totalmente el código fuente o elementos técnicos propietarios del programa o del sistema, lo que en general no está permitido por las leyes de derechos de autor. Este riesgo no aplica en el caso de programas publicados con licencias libres.

El otro riesgo tiene que ver con el hecho de que técnicas de esta familia pueden implicar sobrepasar medidas de protección, lo que está prohibido por ciertas leyes y por muchos contratos, y/o acuerdos de términos y condiciones. Sin embargo, estas cuestiones vinculadas con la propiedad intelectual pueden tener excepciones, son extremadamente complejas y dependen de numerosos detalles en cada caso específico.[43] En otro contexto, el juicio reciente de la Corte suprema de Estados Unidos que dió la razón a la empresa Google frente a Oracle para el uso de Java en el sistema operativo Android[44], muestra también la complejidad de las cuestiones de derechos de autor en el mundo digital. Por esto, este artículo no apunta en tratar esta cuestión en detalle, sino solamente a resaltar la existencia de esta problemática.

41 C. pénal., art. 413-11.

42 Ley n° 1273, 2009 (https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf). [Este pequeño «o no» amplía mucho el espectro de aplicación que podría abarcar casos cómo el clic en la URL indexada mencionada en el 1-f.]

43 Warusfel, B et Dhenne M., «La propriété intellectuelle face à l'ingénierie inverse», 2016, Propriétés intellectuelles, Institut de Recherche en Propriété Intellectuelle, p. 20-32 (https://hal-univ-paris8.archives-ouvertes.fr/CRJP8/hal-01852555).

44 Supreme Court of the United States, «GOOGLE LLC v. ORACLE AMERICA, INC.», 2021, (https://www.supremecourt.gov/opinions/20pdf/18-956_d18f.pdf).

c - Infracción al arreglo internacional de Wassenaar

El arreglo de Wassenaar sobre «el control de las exportaciones de armas convencionales y tecnologías de doble uso»[45], se aplica en los casos en que entran en juego equipos de seguridad digital incluídos en la lista de tecnologías en cuestión.[46] El riesgo se limita por lo tanto al análisis de ciertas tecnologías muy específicas.

¿Hasta dónde ir?

Basándonos en nuestro análisis y experiencia previa, así como en trabajos metodológicos e intercambios con distintos abogados, consideramos que las metodologías a y b de nuestra lista (análisis pasivo y búsqueda no intrusiva de informaciones públicas y análisis de flujos de datos saliendo de/entrando a un dispositivo de la persona usuaria sin descifrar los datos) no conllevan riesgos legales intrínsecos y que pueden, por lo tanto, ser usadas por investigadores con un nivel de riesgo mínimo.

Sin embargo, existen algunos riesgos residuales periféricos en cuanto a la segunda, aunque no vinculados con la metodología técnica en sí misma. El principal riesgo que ha sido identificado, tanto en mi trabajo en la CNIL cómo en la Fundación Karisma tiene que ver con el análisis de sitios webs y aplicaciones cuando hay que completar formularios con datos personales para analizar los flujos de datos generados por el envío de estas informaciones.[47] En efecto, esto puede necesitar introducir datos ficticios. Es por esta razón que, en Francia, la ley de protección de datos personales[48] ha sido completada de la manera siguiente, para que los mismos oficiales de investigación de la agencia de protección de datos (CNIL) no estuvieran en riesgo de cometer un delito cuando hacen controles e investigaciones en línea de sitios webs y aplicaciones: «Para los controles e investigaciones en línea de servicios de comunicación destinados al público, los miembros y oficiales mencionados en el primer párrafo del I pueden realizar toda operación en línea necesaria a su misión con una identidad ficticia» (art. 19). Para el trabajo con la Fundación Karisma, con el fin de minimizar este riesgo y con la preocupación de ser transparentes y éticos, llenamos los formularios con datos vinculados con la fundación. Además informamos de manera previa a las entidades involucradas sobre este punto, del contexto de nuestros análisis y de la necesidad de no tomar en cuenta los datos completados [esto puesto que en ciertos casos puede haber consecuencias. En el caso de la aplicación colombiana de seguimiento de covid-19, por ejemplo, se hubiera podido generar una «falsa alerta de salud»].

45 Wassenaar, «On Export Controls for Conventional Arms and Dual-Use Goods and Technologies», 1995 (https://www.wassenaar.org/es/).
46 Ibid.
47 En particular saber si se hacen vía un protocolo seguro, saber a qué servidores son enviados los datos, etc.
48 Loi «informatique et libertés» n°78-17, 6 janv. 1978, mod.

Siguiendo con el tema de los análisis de sitios webs y aplicaciones[49], nos hemos voluntariamente limitado a las metodologías a y b durante mucho tiempo. En los análisis más recientes de aplicaciones para teléfonos inteligentes, hemos tomado la decisión de ir hasta la metodología c (análisis de flujos de datos saliendo/entrando de un dispositivo de la persona usuaria, descifrando los datos). Esta metodología es muy eficiente y muchas veces exitosa pero quizás se sitúe en la «zona gris» de esta lista. Por esta razón queremos hacer una parada aquí sin dar un veredicto definitivo sobre la cuestión de su legalidad.

Empecemos por por contar dos anécdotas vinculadas con dos empresas multinacionales de primer plano en el mundo digital que han mostrado actitudes distintas en esta cuestión. Primero, la empresa Apple quien, en un documento titulado «Charles Proxy Logs (macOS and iOS)»[50], explica a los desarrolladores de aplicaciones para su almacén en línea (App store) cómo usar el programa de intercepción de paquetes Charles Proxy para realizar este tipo de análisis. Casi se podría decir que se trata de una incitación implícita a que los desarrolladores de aplicaciones potencialmente hagan este tipo de análisis sin riesgo, o al menos de un reconocimiento de que esto se puede hacer.[51] Ahora, otro ejemplo que va en la dirección opuesta, más prudente, es el de otra empresa multinacional del mundo digital para la cual hice en el pasado un trabajo que me llevó a usar esta metodología. La empresa en cuestión querría analizar los flujos de datos generados por una de sus aplicaciones y en particular los que eran destinados a sus socios publicitarios. Estos flujos eran generados por la ejecución del código fuente que ellos le entregaban y que la empresa añadía a su aplicación pero sin poder controlar su funcionamiento.[52] El objetivo de este análisis era saber si los socios publicitarios respetaban el consentimiento de las personas usuarias antes de rastrearlos vía cookies o otros tipos de rastreadores. Explicamos a la empresa en cuestión que descifrar estos flujos implicaría la generación de falsos certificados criptográficos asociados a los nombres de dominios de sus socios y que no sabíamos si esto abarcaba riesgos legales en este contexto. Después de analizar la cuestión con su servicio jurídico e identificar riesgos débiles, pero que existían en cuanto a los artículos del Código penal ya mencionado y a la propiedad intelectual, la empresa pidió que se hiciera el análisis pero después de haber modificado todos los contratos con sus socios publicitarios. Añadió una cláusula para que consintieran a que fueran auditados y descifrados los flujos de datos generados por la ejecución de su código fuente.

49 La metodología ha sido presentada en las conferencias RightsCon (2017, 2018 y 2019, respectivamente en Bruselas, Toronto y Túnez) y en el NPDEV (2019 en Oakland en California).

50 Apple, «Charles Proxy Logs (macOS and iOS)», 2020 (el acceso a este documento necesita tener una cuenta «business» Apple).

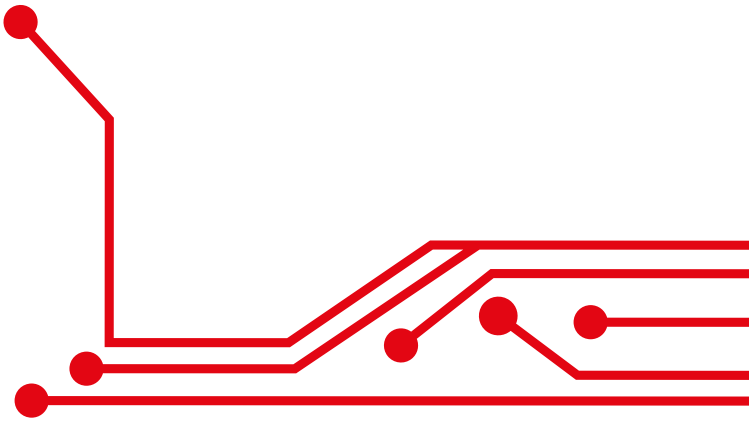
51 Hay que resaltar que una aplicación contiene por lo general código fuente propio y código fuente de terceros cuya ejecución puede generar flujos de datos hacia servidores externos. Estos flujos serán por lo tanto también descifrados en el análisis.

52 De hecho, no estar en capacidad de controlar el código fuente entregado por terceros y añadido a una aplicación o a un sitio web es una cuestión real, tanto en términos de protección de datos cómo en términos de seguridad digital. No sólo esto puede ser la causa de vulnerabilidades sino también de fugas de datos muchas veces no detectadas. Este tema se aborda en un artículo publicado en el sitio web de la Fundación Karisma (Labarthe S., «Fugas de datos por rastreo publicitario», 2019, https://archive.org/details/fugadedatosporrastreopublicitario).

En efecto, como ya se mencionó, los programas que permiten implementar esta metodología generan dinamicamente falsos certificados criptográficos para «hacerse pasar» por el servidor web ante el dispositivo cliente, lo que podría violar leyes sobre la propiedad intelectual. Por otra parte, desde cierto punto de vista, este tipo de análisis «penetra» en lo que podría considerarse cómo una extensión del sistema de la entidad, el flujo cifrado que conecta el dispositivo al servidor.[53] Desde otro punto de vista, si estos análisis se hacen desde una red privada y controlada, se podría decir que el análisis se ubica en la salida del dispositivo del investigador y en todos casos dentro de su red. En ningún caso el análisis genera una intrusión e incluso una escucha pasiva del tráfico al nivel del servidor de la entidad propietaria o encargada del sistema. En cuanto a la generación de de falsos certificados, se hace únicamente al interior del dispositivo del investigador y sólo «engaña» su propio dispositivo. Finalmente, el análisis se hace con un objetivo ético: estudiar los flujos entrando y saliendo de su dispositivo para detectar defectos relacionados con la seguridad digital y la privacidad de una aplicación o de un sitio web. Desde este punto de vista el riesgo parece, por lo tanto, limitado.

[Para concluir con esta metodología de análisis, se puede mencionar una última cosa. Hoy en día ciertas aplicaciones usan una protección adicional llamada certificate pinning que consiste en incluir informaciones del o de los certificados criptográficos directamente en el código fuente de la aplicación. Sobrepasar/eludir esta protección implica modificar el código fuente de la aplicación. Por lo tanto, sobrepasar de esta forma el certificate pinning, en el caso de programas propietarios, podría tener implicaciones y riesgos en cuanto a las leyes de propiedad intelectual y a los términos y condiciones de los contratos, licencias y políticas de uso, pero dejaremos esta nueva cuestión para profundizar en otro momento.]

En conclusión, es muy importante que los investigadores y analistas, quienes muchas veces tienen perfiles técnicos y no siempre están al tanto de los riesgos legales que implican sus investigaciones, estén muy atentos al momento de elegir la metodología que vayan a usar. También tienen que estar en capacidad de justificar lo que hayan hecho.



53 En realidad este «canal» cifrado virtual que conecta el dispositivo del usuario al servidor informático de la entidad encargada del sistema se ubica «entre los dos», de ahí la complejidad del asunto.

C- De la detección hacia la divulgación coordinada y participativa: evoluciones y recomendaciones

1. Las evoluciones recientes de las normativas: de Europa a Estados Unidos

Las barreras legales que ponen los investigadores en situaciones de incertidumbre jurídica hacen que, cuando vulnerabilidades, incidentes o violaciones de datos se descubren, pocas veces se notifique y se divulguen de una manera coordinada, que permita solucionar efectivamente del problema e informar adecuadamente a las partes involucradas. Se quedan entonces sin resolver y alimentan a veces un mercado negro alrededor del cual gravitan cibercriminales y servicios de inteligencia, como lo resalta el informe de la ENISA.[54] Pocos países implementaron iniciativas que permitan superar estas barreras, pero queremos mencionar aquí el comienzo de algunos cambios interesantes.

Francia y Holanda han sido pioneros en Europa para empezar a levantar poco a poco el tabú y los riesgos legales a los que se enfrentan los investigadores de vulnerabilidades, incidentes y violaciones de datos. En Francia al artículo 40 del Código de procedimiento penal que obliga a los funcionarios y las autoridades públicas a denunciar crímenes y delitos de los cuales tuvieran conocimiento. Sin embargo, se creó una excepción que se aplica cuando una «persona de buena fé transmite a la sóla Agencia nacional de ciberseguridad (ANSSI) información sobre la existencia de una vulnerabilidad relativa a la seguridad de un sistema de tratamiento automatizado de datos»56a. En ese caso específico el funcionario ya no tiene la obligación de denunciarlo como un crimen, y por el contrario sí tiene la obligación de no revelar la identidad de la persona que identificó y comunicó a la ANSSI la vulnerabilidad. Es un paso grande que pocos países han dado y que disminuye el riesgo jurídico para los investigadores que notifican vulnerabilidades ante la ANSSI. Sin embargo, se puede resaltar que las infracciones a leyes penales ya mencionadas permanecen y que ninguna excepción a las infracciones mismas ha sido añadida. Sólamente desapareció la obligación para los funcionarios de la ANSSI de denunciarlas. El riesgo para el investigador ha disminuido, pero sigue existiendo.

54 ENISA, «Economics of Vulnerability Disclosure», op. cit., p. 10.

56a [Esta nota al pie no aparece en el original francés.] Loi pour une République numérique, 2016, art. 47.

En Holanda, el enfoque que ha sido adoptado es otro: no crear o modificar leyes sino limitar los casos de pleitos. El fiscal general de la nación ha enviado instrucciones a sus servicios: reconociendo que la noción de «hacking ético» no existe en la legislación del país, les pidió tomar en consideración «motivos éticos» para determinar si se violaron leyes penales.[55]

En Estados Unidos, un proyecto de ley de diciembre 2017[56], obligaría al departamento de seguridad interior (Department of Homeland Security) a presentar ante el Congreso un informe que describa las políticas y procedimientos desarrollados para coordinar la divulgación de vulnerabilidades.[57] Por otra parte, el Departamento de Justicia publicó en 2017 recomendaciones para implementar sistemas de divulgación coordinada para los servicios en línea[58]. Más recientemente, en el 2020, el CISA publicó una directiva aplicándose a casi todas las instituciones federales y pidiéndoles crear políticas de divulgación coordinada.[59]

Por fin, en América latina, el tema es emergente. Colombia, que es el país que quizás más haya avanzado en este tema, empieza a incluirlo, sin todavía definirlo precisamente, a través de su nueva «política nacional de confianza y seguridad digital» que incluso se basó en parte en el estudio de la Fundación Karisma[60]. En efecto este documento menciona que:

«En sexto lugar, el Ministerio de Tecnologías de la Información y las Comunicaciones establecerá un procedimiento para la promoción y difusión del modelo de divulgación periódica de vulnerabilidades, con el fin de garantizar que las debilidades detectadas por un descubridor sean comunicadas en condiciones adecuadas para las partes y a su vez atendidas y subsanadas por las entidades, propietarios u operadores de infraestructuras críticas de manera oportuna. Lo anterior, dentro de un marco de divulgación responsable. Esta acción iniciará en marzo de 2021 y finalizará en agosto de 2021.»[61]

[No encontramos que se haya hecho y publicado este modelo de divulgación periódica de vulnerabilidades desde la escritura de este artículo.]

55 ENISA, «Good Practices on Vulnerability Disclosure: From Challenges to Recommendations», op. cit., p.52.
56 En el momento de la escritura de este artículo, el proyecto está en segunda lectura en el Senado. [En el momento de la traducción en español de este artículo, ha sido presentado otra vez pero todavía no ha sido aprobado por el Senado.]
57 https://www.congress.gov/bill/115th-congress/house-bill/3202
58 US Department of Justice, «A Framework for a Vulnerability Disclosure Program for Online Systems», 2017 (version 1.0) (www.justice.gov/criminal-ccips/page/file/983996/download).

59 CISA, «Develop and Publish a Vulnerability Disclosure Policy», 2020 (https://cyber.dhs.gov/assets/report/bod-20-01.pdf).
60 CONPES, «Política nacional de confianza y seguridad digital [de Colombia]», 2020. [Para más detalles sobre la evolución de estas políticas en Colombia, recomendamos el comunicado de prensa relacionado, en el sitio web de Fundación Karisma: (https://web.karisma.org.co/comunicado-de-prensa-nuevo-reporte-de-la-ocde-reconoce-el-trabajo-de-karisma-en-la-construccion-de-una-ruta-para-la-divulgacion-de-vulnerabilidades-en-colombia/)]
61 Ibid., p.35-36.

Estos ejemplos ya contienen varias ideas que convendría extender e implementar rápidamente, porque la tecnología avanza mucho más rápido que las legislaciones que la regulan. Sin embargo se puede notar que en ninguno de estos casos se creó un marco jurídico completamente seguro para el investigador. Las infracciones siguen existiendo y las excepciones para investigadores de buena fe todavía no han sido creadas. Es por lo tanto necesario ir mucho más lejos.

[El 15 de febrero del 2013, el Centro de Ciberseguridad de Bélgica (CCB) anunció la creación de una nuevo marco legal para acudir los reporte de vulnerabilidades en seguridad digital.]

2. La creación de rutas de divulgación coordinadas y el papel de las administraciones públicas existentes

a - La ubicación de la entidad receptora y la dimensión organizacional

Para ser eficientes, las evoluciones normativas tienen que estar asociadas a la creación de canales –estatales en particular– de recepción y de tratamiento de vulnerabilidades, de incidentes y de violaciones de datos que puedan ser detectadas por terceros.

En general, es es el papel de los centros de alertas y reacción a los ataques informáticos (CERT y CSIRT)[62], que pertenecen en general a entidades estatales, a grandes empresas o a universidades. La mayoría de los países tienen un CERT nacional que es el principal receptor de eventos de seguridad relacionados con los sistemas de información del Estado y de las autoridades regionales, departamentales o municipales según el país. En Europa, la existencia de un CERT nacional incluso se volvió una obligación con la directiva NIS.[63] Además existen también otras entidades públicas que pueden desempeñar este tipo de papel para sectores específicos. Es el caso de las autoridades de protección de datos personales en los países que disponen de una legislación en esta área. En Francia, en el sector de la salud las Agencias Regionales de Salud (ARS) reciben las notificaciones de incidentes de seguridad de este sector, complementando a la CNIL[64]. Estas entidades intermediarias y coordinadoras estatales desempeñan también un papel importante para asegurar que la divulgación se hace de manera coordinada y responsable. En lo ideal, van a incitar, e incluso ayudar, a la entidad encargada del sistema afectado a resolver el problema de seguridad identificado, proteger a quien lo detectó, y dejar un plazo para solucionarlo antes de hacerlo público para que contribuya a avanzar los conocimientos en seguridad digital.

62 De las siglas en inglés Computer Emergency Response Team y Computer Security Incident Response Team. Estos dos términos se pueden intercambiar.

63 NIS Directive, op. cit., art.9.

64 CNIL, «Notifications d'incidents de sécurité aux autorités de régulation : comment s'organiser et à qui s'adresser ?», 2020, (https://www.cnil.fr/fr/notifications-dincidents-de-securite-aux-autorites-de-regulation-comment-sorganiser-et-qui-sadresser).

Antes de ir más lejos, detengámonos un instante en una problemática organizacional central vinculada con esta cuestión: la ubicación del CERT nacional. En muchos países, por razones que tienen que ver con el papel histórico del Ministerio de Defensa en materia de seguridad digital, el CERT nacional depende directamente de él. Hasta se puede mencionar el caso patológico del Reino Unido donde el canal para reportar vulnerabilidades se ubica en el sitio internet de la Agencia Nacional de Ciberseguridad (National Cyber Security Centre [NCSC]). Esta agencia depende directamente del GCHQ, el servicio de inteligencia británico[65]. En Francia se podría decir que la situación está mejor, el CERT-FR[66] depende de la ANSSI, la cual depende del Secrétariat général de la Défense nationale, el cual depende del Primer Ministro. Sin embargo, en la práctica, los vínculos con los servicios de inteligencia permanecen, como lo demuestra el paso de Patrick Pailloux, ex director de la ANSSI, hacia la dirección técnica de la DGSE, el servicio de inteligencia exterior francés.[67] También en Colombia el CERT nacional (COL-CERT) depende del Ministerio de Defensa. [Entre el momento de escritura de este artículo y su publicación en español, esto cambió y el COLCERT (www.colcert.gov.co/) depende ahora del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), lo que es un cambio muy positivo.] Este tipo de dependencias crea problemas de dos tipos para la detección y la notificación eficiente de eventos de seguridad. Primero, la ausencia de confianza y hasta el miedo a represalias que pueda sentir el investigador pueden desincentivar el ejercicio de notificar hallazgos.. Segundo, como lo resalta el informe de la ENISA, hay un conflicto de interés obvio porque los servicios de inteligencia están interesados en poseer vulnerabilidades no públicas para usarlas en sus actividades ofensivas.[68]

Es por lo tanto fundamental que entidades receptoras tengan una independencia fuerte respecto a los Ministerios que realizan actividades de inteligencia. Sobre esto, se puede mencionar el ejemplo interesante de Japón, donde el CERT nacional (JP-CERT[69]) es una organización independiente sin ánimo de lucro.

Finalmente, podemos resaltar el papel creciente de organizaciones de la sociedad civil como intermediarios de confianzas entre el Estado y los ciudadanos, los defensores de derechos humanos, los periodistas, los hackers, etc. Un fenómeno nuevo en particular es la aparición de un CERT de la sociedad civil. La «Digital Security Helpline» de la fundación Access Now ha sido admitida en el 2019 como miembra del FIRST[70], la organización mundial que agrupa los CERT/CSIRT. Además el CIVICERT[71] ha sido invitado en el 2020 en el encuentro anual del FIRST para hacer una conferencia.[72]

65 Government Communication HeadQuarter (www.gchq.gov.uk/).
66 www.cert.ssi.gouv.fr/
67 Follorou, J., «Patrick Pailloux, nouveau patron de la «NSA à la française» [Patrick Pailloux, nuevo jefe de la «NSA francesa»], Le Monde, 21 de enero del 2014. https://www.lemonde.fr/technologies/article/2014/01/21/patrick-pailloux-prend-la-tete-de-la-direction-technique-de-la-dgse_4352081_651865.html
68 ENISA, «Economics of Vulnerability Disclosure», op. cit., p. 40.
69 https://www.jpcert.or.jp/english/about/
70 https://www.first.org/members/teams/access_now_digital_security_helpline
71 www.civicert.org. Fundación Karisma es parte del CIVICERT.
72 https://www.first.org/conference/2020/recordings

b - Las rutas de divulgación/notificación estatales

Como se menciona en nuestro estudio que, en este punto, se basa en parte en el informe de la ENISA del 2015, una ruta de divulgación/notificación de vulnerabilidades, incidentes y violaciones de datos tiene que funcionar junto con una política de divulgación que incluye cómo mínimo los elementos siguientes:

- la filosofía y objetivo de la ruta de divulgación;
- las garantías de protección y confidencialidad para la persona o la organización que reporta;
- el canal en sí mismo para reportar los eventos de manera fácil y segura. Puede, por ejemplo, incluir un formulario en línea seguro (HTTPS), una dirección de correo electrónico con su clave PGP, etc.;
- la información mínima que debería contener el reporte;
- los tipos de divulgaciones que no se pueden recibir y los que sí se pueden;
- las etapas del proceso y la línea de tiempo. Esto debe incluir el tiempo que tiene la entidad para hacer las correcciones antes que se haga la divulgación pública.

Desafortunadamente, las rutas de notificación estatales muy pocas veces incluyen todos estos elementos.

En Francia, la ANSSI ha creado un canal destinado a las personas que han descubierto una falla de seguridad, una vulnerabilidad o ciertos tipos de incidentes y desean notificarlo.[73] Sin embargo, la incompletud del canal (que no incluye las violaciones de datos), el hecho de que no incluya un formulario web,[74] y la poca comunicación sobre ello limita su eficacia real. Por otra parte, las modificaciones legislativas ya mencionadas han creado una protección relativa pero únicamente para el reporte de vulnerabilidades. ¿Qué pasa con la notificación de un incidente? ¿La persona también será protegida?

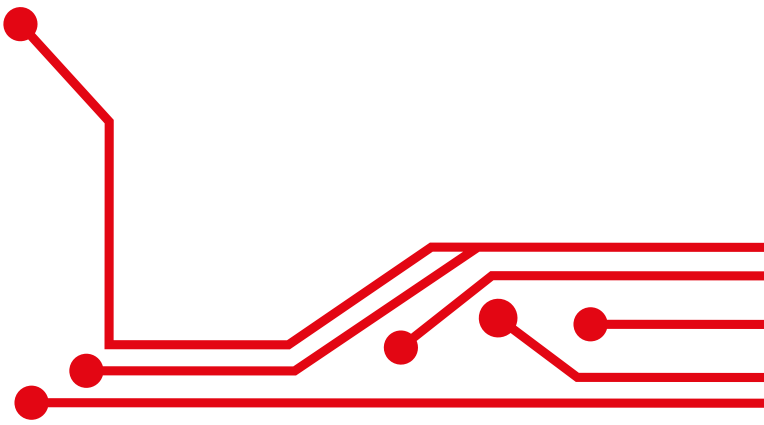
73 Página para hacer la notificación en el sitio de la ANSSI: www.ssi.gouv.fr/en-cas-dincident/vous-souhaitez-declarer-une-faille-de-securite-ou-une-vulnerabilite/. También existe un formulario para declarar un incidente de de seguridad especifícamente para los operadores de importancia vital (www.ssi.gouv.fr/uploads/2016/04/formulaire-declaration-incident-lpm_anssi.pdf). Se puede resaltar que no se trata de un formulario en línea sino de un archivo PDF que hay que completar, imprimir y mandar por vía postal a la ANSSI. [Desde la publicación inicial se han añadido URL en el sitio del ANSSI con formulario del mismo tipo para los casos específicos de los operadores de servicios esenciales y de los proveedores de servicios digitales aunque no estén pensados para que alguien exterior a la entidad lo detecté y lo reporte (www.ssi.gouv.fr/en-cas-dincident/).]

74 Las posibilidades son únicamente el correo postal, el teléfono [se quitó recientemente el FAX], el correo con cifrado PGP.

Para dar otro ejemplo, en Francia, la CNIL dispone de un servicio en línea para notificar una violación de seguridad. Sin embargo, como lo menciona la autoridad administrativa independiente en su sitio web, «este servicio en línea es únicamente para los responsables de tratamientos (organismos privados o públicos) deseando notificar a la Comisión una violación habiendo impactado los datos personales que tratan. Si usted es una persona particular y desea dejar una queja/denuncia a la CNIL, le agradecemos usar el servicio de quejas/denuncias en línea»[75]. Es por lo tanto en este caso el servicio de denuncias/quejas de la CNIL el que puede ser receptor, dando a la institución este papel coordinador en caso de descubrimiento de una vulnerabilidad, un incidente o una violación de la seguridad relacionada con datos personales. Pero el servicio en línea no dispone de una sección dedicada que permitiría señalar este tipo de eventos. Este tipo de herramientas debería, por lo tanto, ser completada y definida de una mejor manera.

Finalmente, ya sea en Francia o en Europa, este tipo de roles tienen que ser reforzados, bien definidos y ampliados. Además, el contacto y las relaciones entre las administraciones encargadas y toda la sociedad se debe desarrollar.

En Estados Unidos, la actualización de la página de notificaciones en el sitio web del CISA es un ejemplo interesante.[76] Primero incluye la posibilidad de notificar todos los eventos descritos en este artículo aunque la clasificación se haga de una manera distinta. En efecto, la página propone reportar incidentes, casos de phishing, de programas maliciosos (malware) o vulnerabilidades. La descripción de lo que puede constituir un incidente incluye las violaciones de datos. Al contrario, en nuestra clasificación, un caso de phishing o el descubrimiento de un programa malicioso constituye un incidente de seguridad. El hecho de poner a parte estos dos casos específicos tiene probablemente una motivación práctica de la agencia para poder analizarlos y encuentra hoy su justificación.[77] Finalmente, el hecho de haber creado un punto de entrada único, aunque después las notificaciones se hagan desde formularios webs distintos, simplifica las cosas para las entidades y las personas que las vayan a realizar.



75 CNIL, «Notifier une violation de données personnelles», 2018 (www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles).

76 https://www.cisa.gov/report

77 Quizás el día que los Estados Unidos adopten leyes federales en cuanto a la protección de datos personales, esta clasificación será modificada.

3. Del castigo hacia la recompensa: los programas bug bounty

Los programas de recompensa, más conocidos por su nombre inglés de bug bounty, han existido durante más o menos 20 años en empresas del mundo digital, antes de popularizarse en el sector público. El primer verdadero programa de este tipo es probablemente el que lanzó en 1995 la empresa Netscape, desarrolladora del programa de navegación del mismo nombre. El proyecto fue un logro y aproximadamente diez años después, este tipo de programas ya se había popularizado en el sector privado: Mozilla, Google, Facebook, etc., hasta la creación de empresas especializadas en su organización como YesWeHack[78] en Europa o HackerOne[79] en Estados Unidos[80]. El éxito creciente de este tipo de programa es un reconocimiento, que tiene su origen en el sector privado, de la necesidad de recurrir a la toda la sociedad, en particular a los expertos independientes, investigadores y hackers, para detectar problemas de seguridad.

Desde hace algunos años, las entidades públicas también empezaron a recurrir a este tipo de iniciativas. Se puede por ejemplo mencionar el caso del Departamento de Defensa de Estados Unidos y su programa Hack the Pentagon, lanzado en el 2016 y en cual todo tipo de actor era invitado a poner a prueba sus sistemas informáticos [en versiones simuladas a través de máquinas virtuales] para descubrir sus vulnerabilidades y reportarlas, a cambio de recompensas financieras, una revolución en la época. Después de la primera edición, el Pentágono reconoció públicamente que esta iniciativa le había permitido «identificar y resolver miles de vulnerabilidades de seguridad digital (más de 3600)»[81]. El experimento ha sido entonces repetido. Del lado de la Unión Europea, se lanzó en el 2018 el programa EU-FOSSA, cuyo objetivo era identificar vulnerabilidades, no directamente en sus sistemas, sino en una lista de programas de código abierto usados por la institución. Fue renovado al año siguiente, después de su éxito.[82] En Francia, después del lanzamiento de un programa que no era completamente abierto por el Ministerio de Defensa,[83] se tuvo que esperar hasta el 2020 y el bug bounty para la aplicación «StopCovid».[84]

78 www.yeswehack.com/

79 www.hackerone.com/

80 HackerOne, «History of Hacker-Powered Security», 2021 (https://www.hackerone.com/history-of-hacker-powered-security). [En el momento de la traducción de este artículo esta página ya no está en línea en el sitio de la empresa. Sin embargo se puede consultar una copia en el sitio web de Archive.org aquí: https://web.archive.org/web/20210301034100/https://www.hackerone.com/history-of-hacker-powered-security]

81 US Department of Defense, «Department of Defense Expands 'Hack the Pentagon' Crowdsourced Digital Defense Program», 2018 (https://www.defense.gov/Newsroom/Releases/Release/Article/1671231/department-of-defense-expands-hack-the-pentagon-crowdsourced-digital-defense-pr/).

82 https://joinup.ec.europa.eu/collection/eu-fossa-2/about

83 El Ministerio de Defensa Francés lanzó en 2019 y en 2020 un programa de tipo bug bounty pero la participación era limitada a los empleados del Ministerio y a reservistas operativos de ciberdefensa (https://www.defense.gouv.fr/actualites/articles/bug-bounty-2020-temoignages-des-reservistes-operationnels-de-cyberdefense). [El programa ha sido renovado cada año desde entonces (https://www.defense.gouv.fr/ema/actualites/resultats-du-bug-bounty-2022)]

84 El Ministerio de Defensa Francés lanzó en 2019 y en 2020 un programa de tipo bug bounty pero la participación era limitada a los empleados del Ministerio y a reservistas operativos de ciberdefensa (https://www.defense.gouv.fr/actualites/articles/bug-bounty-2020-temoignages-des-reservistes-operationnels-de-cyberdefense). [El programa ha sido renovado cada año desde entonces (https://www.defense.gouv.fr/ema/actualites/resultats-du-bug-bounty-2022)]

Estos programas de recompensas contrastan con el retraso de las legislaciones previamente mencionadas. Ofrecen una protección relativa a los investigadores vía un vínculo contractual –en general tripartito– entre el investigador, la entidad auditada y la empresa que organiza el bug bounty. Sin embargo, este marco protector no borra totalmente los riesgos legales mencionados previamente. Se puede mencionar el caso de un estudiante y de un investigador del Massachusetts Institute of Technology quienes ambos, después de haber encontrado vulnerabilidades críticas en los sistemas de votación de la misma empresa Voatz, han sido denunciado e incluso investigado por el FBI en el primer caso.[85]

4. Algunas recomendaciones como conclusión

Para concluir, hacemos algunas recomendaciones destinadas a las autoridades públicas y a las administraciones existentes:

a - Mejorar y completar los canales de notificación estatales existentes

Ya sea que los canales estén asociados a los CERT, a las autoridades de protección de datos o a cualquier entidad receptora de notificaciones, estos deben mejorarse y completarse. Todos los eventos de seguridad deben poder ser reportados y deben ser atendidos: vulnerabilidades genéricas y específicas (fallas de seguridad), incidentes y violaciones de datos que sean informaciones personales o de otro tipo. Es importante que estos canales tengan políticas de divulgación coordinada claras y completas (ver C, 2, b).

b - Crear un marco organizacional de confianza con los organismos estatales receptores de notificaciones

En particular es fundamental que los CERT nacionales y otras entidades con este papel puedan tener una independencia real respecto al Ministerio de Defensa y los organismos de inteligencia. Por otra parte, una relación de confianza tiene que construirse con los investigadores.

c - Minimizar los riesgos legales para los investigadores

Esto puede hacerse por medio de evoluciones legislativas, dándoles garantías con respecto a ciertas condiciones (como en Francia), la creación de excepciones a las infracciones posibles y/o una sensibilización de los fiscales para limitar los procedimientos legales en el caso de «hacking ético» (como en Holanda).

85 OECD, «Encouraging vulnerability treatment, Responsible management, handling and disclosure of vulnerabilities», op. cit., p. 53 y 54.

d - Desarrollar acciones de comunicación destinadas a los descubridores potenciales

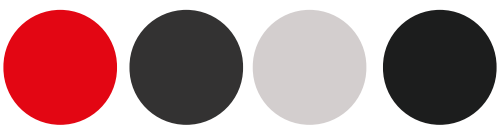
Se trata de investigadores universitarios, de la sociedad civil, de expertos independientes, de hackers, de usuarios de los sistemas, etc. La creación de guías y documentos de sensibilización relativos a este tema, así como la organización de programas de recompensas (bug bounty) son buenos ejemplos de lo que se puede hacer.

Añadamos para terminar tres recomendaciones para los investigadores:

Elegir una metodología de análisis cuyos riesgos sean aceptables en función del contexto de la investigación / del análisis. La parte B de este artículo puede ser útil;
Apoyarse, si se puede, en un organismo intermediario de confianza que ofrece garantías adicionales y ofrece una protección al investigador. Puede tratarse por ejemplo de una organización de la sociedad civil, de una Universidad, de un organismo estatal que ofrezca todas las garantías de confianza o de una empresa organizadora de programas bug bounty;
Más allá de los aspectos jurídicos, realizar los análisis de manera ética y transparente, en particular cuando impliquen completar formularios con datos personales (ver B, 2).

Agradecimientos:

Agradezco sinceramente a todas las personas que ayudaron a la redacción y revisión de este artículo, en particular Amalia Toledo para sus aportes jurídicos en el estudio que le sirvió de base, Carolina Botero y Pilar Sáenz de la Fundación Karisma por su apoyo y sus ideas, Benjamin Vialle de la CNIL para su revisión de fondo y Maryse Labarthe por sus correcciones de forma en la versión en francés.



20 años Fundación Karisma