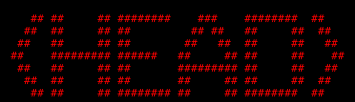
ESTUDIO SOBRE RUTAS DE DIVULGACIÓN EN SEGURIDAD DIGITAL

Fundación Karisma



Estudio sobre rutas de divulgación en seguridad digital

Fundación Karisma

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 en www.documentoaccesible.com/#que-es

Esta publicación fue realizada por la Fundación Karisma con el apoyo y financiación de Global Partners Digital.

Fundación Karisma

GLOBAL PARTNERS DIGITAL

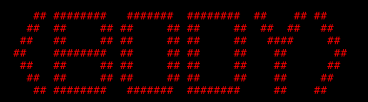
Autor
Stéphane Labarthe

Revisión
Carolina Botero
Pilar Sáenz
Amalia Toledo

Diseño editorial y gráfico
Cuántika Studio

Bogotá, Colombia
2019

Contenido



Resumen ejecutivo

El presente informe apunta a presentar, en el contexto de la seguridad digital en Colombia, la problemática de las vulnerabilidades, incidentes y violaciones de la seguridad de datos y explicar porque es hoy necesario implementar rutas de divulgaciones responsables, coordinadas y efectivas.

Después de una introducción al tema, hacemos un análisis de la situación en Colombia que muestra que las rutas de divulgación que puedan existir —en particular, el colCERT— no están adecuadamente adaptadas. Además, los riesgos legales para una persona que descubre alguna vulnerabilidad, falla o violación a la seguridad de los datos y quiere divulgarla son muy altos, elemento que resulta muy disuasivo.

Un mirada internacional, en particular de Europa y los Estados Unidos, demuestra que la situación, la legislación, y la implementación de rutas efectivas y hasta de programas de recompensas para las divulgaciones están cambiando las cosas poco a poco.

De estas experiencias y del análisis del contexto colombiano, destacamos 7 recomendaciones que deben permitir una construcción progresiva de estas rutas:

1. Apoyarse en estándares y experiencias internacionales.

2. Identificar las problemáticas y mejorar las rutas de divulgaciones existentes.

3. Construir políticas de divulgación.

4. Implementar rutas de divulgación de confianza.

5. Minimizar los riesgos legales para quien encuentra vulnerabilidades.

6. Desarrollar una comunicación que sensibilice sobre las divulgaciones responsables y coordinadas.

7. Crear una obligación de reporte de incidentes o violaciones de la seguridad de los datos en sectores específicos.

Esperamos que este informe y estas recomendaciones puedan constituir un aporte en el mejoramiento que está buscando el Estado colombiano para incrementar su capacidad de detección, por lo tanto, de resolución de los problemas en seguridad digital.

Introducción

Uno de los pilares de la seguridad digital en diferentes niveles para individuos, organizaciones y hasta para un país como Colombia es la detección de ataques, de vulnerabilidades, de incidentes y de violaciones de la seguridad de los datos personales y/o sensibles. ¿Cómo se mitigan o resuelven adecuadamente este tipo de problemas? ¿Cómo se implementan medidas de protección para evitar que ocurran?

Sabemos que hoy la seguridad digital abarca todas las componentes de una sociedad, desde los individuos, sus datos personales y sus derechos fundamentales hasta las actividades económicas y los servicios esenciales de un país como lo son la salud, la distribución de agua y electricidad o los sistemas de transporte. Estamos hablando de un asunto más que importante, un asunto vital.

Durante muchos años, la aproximación dominante sobre la seguridad digital —con su hija mayor la criptología o la ciencia de los secretos— era que se debía manejar exclusivamente o, al menos principalmente, desde el mundo militar y que era mejor hablar de este tema en círculos cerrados. En relación con la detección y divulgación en seguridad digital, en Colombia, esta óptica todavía se observa en el hecho de que los cuatro centros de respuestas a incidentes digitales del Estado están suscritos al Ministerio de Defensa. Esta visión está cambiando poco a poco en el país, en particular, a partir de la Política Nacional de Seguridad Digital de 2016, y el surgimiento de otros actores —como el Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC) o la Delegatura de Protección de Datos—, que están desempeñando un papel cada vez más importante.

Es importante acelerar este cambio. Ya en Europa y los Estados Unidos se están implementando transformaciones que buscan involucrar a todos los sectores de la sociedad y crear distintas rutas de alertas en seguridad digital. Desde la experiencia del Laboratorio de Seguridad y Privacidad de la Fundación Karisma (K+Lab) analizando y reportando vulnerabilidades, incidentes de seguridad digital y fugas de datos detectados, reconocemos que hay un largo camino que recorrer en este sentido.[1] Para Karisma, a pesar de las dificultades, el MinTIC ha sabido desempeñar un papel de intermediario que permite llegar a resultados que benefician a todas las partes involucradas.[2]

Esta posibilidad no ha existido para las personas que se identifican como parte de la comunidad técnica del país. En multiplicidad de veces, esta comunidad le ha manifestado a Karisma las dificultades que tienen para reportar al Gobierno vulnerabilidades e incidentes que detectan. Incluso han expresado sentir miedo de persecuciones legales, lo que muchas veces tiene como consecuencia que no divulguen los problemas encontrados, haciendo que persistan en el tiempo. Este informe ha sido presentado previamente a algunos miembros de la comunidad técnica con el fin de recibir observaciones y retroalimentación para mejorar el estudio.

Como se verá a lo largo del informe, el principal problema identificado, además de la falta de un marco jurídico que incentive la divulgación de vulnerabilidades o incidentes, es que el Estado no cuenta con un mecanismo de reporte que sea confiable, ni que permite desarrollar una coordinación para atender este tipo de eventos.

Estas son las motivaciones para este informe. Esperamos que pueda contribuir y alimentar la reflexión y la creación de rutas de divulgación adaptadas y eficientes en seguridad digital para construir un entorno digital más confiable.

---

1. Fundación Karisma (2018, 5 de marzo). *K+Lab, un espacio abierto*. Disponible en karisma.org.co/klab-un-espacio-abierto/

2. Véase, por ejemplo, la experiencia de Karisma con el análisis del sitio web de la Unidad de Atención y Reparación Integral a las Víctimas en *La corresponsabilidad en acción* (2017, 31 de agosto). Disponible en karisma.org.co/la-corresponsabilidad-en-accion/

Definiciones y presentación del problema

Cuando se habla de rutas de divulgaciones o alertas en seguridad digital, nos referimos a varias cosas distintas que a veces se mezclan de manera confusa. No ayuda que no exista acuerdo o denominador común entre las definiciones existentes; incluso las organizaciones internacionales de referencia (ej. ENISA, US CERT. etc.) usan conceptos diferentes. Por eso, es importante empezar este informe con algunas definiciones que servirán para plantear las distintas problemáticas que surgen cuando se esboza la creación de una ruta de este tipo en Colombia.

Definiciones

A continuación presentamos algunas definiciones de términos y siglas que se usarán a lo largo de este documento. Incluimos también su correspondencia en inglés y algunos comentarios para introducir el tema.

- **Vulnerabilidad *(vulnerability)***: Se pueden encontrar dos definiciones distintas de este concepto:

    1. La Agencia Europea de Protección de Datos (ENISA, por sus siglas en inglés) entiende que es un error de diseño o de implementación, o una debilidad que tiene un equipo (*hardware*), programa (*software*), red, protocolo o servicio en línea y que puede ser explotada para llegar incluso a comprometer la seguridad del sistema.[1]

        Cuando una vulnerabilidad no ha sido divulgada públicamente, se considera como una vulnerabilidad tipo día cero (*zero-day vulnerability*). A veces, se considera que una vulnerabilidad sigue siendo de tipo día cero mientras no se haya publicado un correctivo.

    2. El Equipo de Respuesta para Emergencias Informáticas de los Estados Unidos (US CERT, por sus siglas en inglés) precisa que es aquella característica o debilidad específica que hace a un activo (ej. información o sistema de información) vulnerable a una amenaza intencional o accidental.[2] A veces, a este tipo de vulnerabilidad también se le conoce como falla de seguridad (*security flaw*).

Ambas definiciones ofrecen elementos de distinción. La primera se refiere a una tecnología en particular, en consecuencia, afecta a todos los sistemas de información de organizaciones o personas que usen esta tecnología. Por ejemplo, la vulnerabilidad CVE-2018-8653 afecta a las versiones 9 al 11 de los navegadores *Internet Explorer*.[3] La compañía desarrolladora —en este caso, Microsoft— es la primera interesada en corregir o mitigar la vulnerabilidad una vez ha sido descubierta. Posteriormente, quienes deben tomar acciones son las organizaciones y personas que usan el navegador, actualizando a la versión corregida o tomando medidas de mitigación.[4]

La segunda definición concierne a los activos de una persona u organización (ej. un sitio web institucional). Puede que la falla de seguridad se deba al uso de un componente con una vulnerabilidad en

1. ENISA. (2018). *Economics of Vulnerability Disclosure*, pp. 9-10. Disponible en tinyurl.com/y3y98a8u. Esta definición, se basa en la norma ISO27147 y el FIRST. La ENISA también ha publicado una definición más específica y basada en el estándar *Information Technology Security Evaluation Criteria* (ITSEC) en su sitio web, indicando que una vulnerabilidad es «[u]na debilidad del *software*, *hardware* o servicio en línea que puede ser explotada (traducción nuestra)». Véase tinyurl.com/y5cvhe2k

2. Traducida y adaptada por nosotros de la definición del US CERT, disponible en niccs.us-cert.gov/about-niccs/glossary#V

3. Microsoft. (2018, 19 de diciembre). *CVE-2018-8653 | Scripting Engine Memory Corruption Vulnerability*. Disponible en portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8653

4. En ocasiones, cuando aún no se ha conseguido corregir completamente la vulnerabilidad y en espera de ello, se proponen medidas de mitigación, por ejemplo, que se desactive alguna funcionalidad, que se cierre algún puerto en el *firewall* de la red, etc.

el sentido de la primera definición (ej. un gestor de contenido o servidor web no actualizado), pero puede también que sea por otros motivos (ej. contraseña de administración débil, mala configuración, etc.).

Como veremos más adelante, el primer caso está bien documentado y las grandes compañías de desarrollo, al igual que los CERT y los Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT, por sus siglas en inglés), han definido rutas de divulgación y alertas, y hasta tienen programas de recompensas.

- **CERT y CSIRT**: Son grupos de trabajo encargados de responder a incidentes de seguridad digital. Los términos son hoy reconocidos como sinónimos.[5] Los CERT/CSIRT suelen pertenecer al Estado, a grandes empresas privadas y a universidades. Hay algunos que pertenecen a la sociedad civil e incluso son organizaciones sin ánimo de lucro. Existe una organización mundial que los reúne, el *Forum of Incident Response and Security Teams* (FIRST), con el fin de «fomentar la cooperación y la coordinación en la prevención de incidentes, estimular la reacción rápida a los incidentes y promover el intercambio de información entre los miembros y la comunidad en general».[6] En Colombia, al momento de escribir este informe, 11 CERT/CSIRT son miembros de esta organización. Sin embargo, el colCERT, que es el equipo nacional de respuesta, aún no pertenece al FIRST.[7]

- **Divulgación coordinada de vulnerabilidades (CVD o *Coordinated Vulnerability Disclosure*)**: Cuando una vulnerabilidad es descubierta, puede ocurrir una de tres posibilidades: (1) la divulgación completa (*full disclosure*), en la que la vulnerabilidad es publicada integralmente; (2) la ausencia de divulgación (*non-disclosure*), es decir, quien descubre la vulnerabilidad la vende o se queda con ella; o (3) la divulgación coordinada de la vulnerabilidad, en la que no se publica inmediatamente la vulnerabilidad, sino que se actúa junto con quien desarrolló el sistema afectado, su propietario y/o con lo que se conoce como un coordinador. Este último puede ser un CERT/CSIRT público o privado, una agencia nacional de seguridad digital, una agencia de protección de datos, el Estado mismo (por ejemplo, a través de un ministerio) o una entidad privada sin ánimo de lucro (ej. Access Now).

  El objetivo de esta divulgación coordinada es contribuir a la seguridad de los sistemas de información compartiendo conocimiento para llegar a una solución común y permitiendo así la resolución del problema antes de su divulgación.[8] Grandes empresas o

5. Véase la entrada de *Wikipedia* sobre «Equipo de Respuesta ante Emergencias Informáticas», disponible en en.wikipedia.org/wiki/Computer_emergency_response_team

6. Véase el sitio web de FIRST en www.first.org/

7. *FIRST Members Around the World*. (s.f.). Disponible en tinyurl.com/y2nbetf7

8. Definición adaptada de la que se encuentra en el informe del Centro Nacional de Ciberseguridad de Países Bajos: *Coordinated Vulnerability Disclosure: The Guideline*. (2018), p. 7. Disponible en https://tinyurl.com/y33jgokg

agencias de seguridad digital han creado políticas, guías y rutas de divulgación coordinada.

Algunas grandes empresas de tecnología y, más recientemente, organismos estatales han desarrollado programas de recompensas (*bug bounty programs*) en el seno de sus programas de divulgación coordinada para estimular a quienes encuentran vulnerabilidades a través del reconocimiento y/o dinero.[9] Es el caso de Mozilla, Facebook, Yahoo!, Google, Reddit, Square y Microsoft.

- **Vulnerabilidades y exposiciones comunes (CVE o *Common Vulnerabilities and Exposures*)**: Sistema mundial de exposición de vulnerabilidades operado por la corporación MITRE, sostenida por el Gobierno de los Estados Unidos.[10] Este sistema es la referencia mundial para la publicación de vulnerabilidades de tipo 1 —aquellas que afectan equipos, *software* o servicios en línea—, descripción de los riesgos asociados e información sobre los correctivos disponibles.

- **Alerta de seguridad (*security alert*)**: Vulnerabilidad con alto impacto o eventos que aumentan los riesgos digitales y que, por tanto, necesitan un aviso informativo importante (ej. vulnerabilidad muy grave como *HearthBleed*, campaña masiva de correos infectados).

  Es el papel de los CERT/CSIRT difundir este tipo de alertas en su misión de informar y prevenir. En Colombia, el colCERT sería la entidad encargada de cumplir esa función. Sin embargo, al momento de escribir este informe, la última actualización disponible en su página web es de septiembre 2017.[11]

- **Incidente de seguridad (*information security incident*)**: Evento o serie de eventos de seguridad digital inesperados o indeseados y que tienen una importante probabilidad de comprometer la seguridad de un sistema de información determinado (ej. robo de un computador portátil en una organización, *firewall* fuera de servicio).[12]

  En Europa y los Estados Unidos, ciertos sectores como el de telecomunicaciones, el financiero o el de salud tienen la obligación de información sobre los incidentes de seguridad a las autoridades de control.

- **Violación de la seguridad de los datos personales (*personal data breach*)**: El Reglamento General de Protección de Datos (RGPD) de la Unión Europea (UE) dio importancia a esta noción, definiéndola como «toda violación de la seguridad que ocasione la destrucción,

9. Véase la entrada de *Wikipedia* sobre «*Bug bounty program*» (programa de recompensas), disponible en en.wikipedia.org/wiki/Bug_bounty_program

10. Véase el sitio web del MITRE en www.mitre.org/centers/national-cybersecurity-ffrdc/who-we-are

11. Véase la página web «Alertas de seguridad» dentro del sitio web del colCERT en www.colcert.gov.co/?q=tags/alertas-de-seguridad

12. Definición basada en la norma ISO27001 (*Information technology — Security techniques — Information security management systems — Requirements*).

> 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».[13] Hay que resaltar que es una definición bastante amplia que no se limita a la confidencialidad de los datos y que el artículo 33 del mismo reglamento impone al responsable del tratamiento de notificar a la autoridad de control competente en 72 horas.

En Colombia, el sitio web del colCERT ofrece la posibilidad de reportar incidentes y vulnerabilidades.[14] Aunque no ofrece definición alguna, podemos concluir que este organismo considera ambas nociones.

Por último, la Ley de Protección de Datos colombiana (Ley 1581 del 2012) señala en su artículo 17 que se debe «[i]nformar a la autoridad de protección de datos cuando se presenten **violaciones a los códigos de seguridad** y existan riesgos en la administración de la información de los Titulares» (destacado nuestro). Hay que resaltar que el término «violaciones a los códigos de seguridad» es, *a priori*, mucho más limitado que una violación de la seguridad de los datos personales.[15] Sin embargo, es interesante notar que la Superintendencia de Industria y Comercio de Colombia ordenó a Facebook la adopción de una serie de medidas respecto a las violaciones de la seguridad de los datos personales equivalentes a las del RGPD de Europa:[16]

> 5. Facebook deberá desarrollar, implementar y mantener un programa de gestión y manejo de violaciones de seguridad en datos personales, que contemple procedimientos para informar sin dilación indebida a esta Autoridad de protección de datos y a los titulares de los mismos cuando se presenten incidentes que afecten la confidencialidad, integridad y disponibilidad de los datos.

13. Unión Europea. (2016). *Reglamento General de Protección de Datos*, Artículo 4(12). Disponible en tinyurl.com/yxbavxzv

14. Véase la página web «Reportar un incidente» en el sitio web del colCERT en www.colcert.gov.co/?q=contenido/reportar-un-incidente

15. Existe un proyecto de resolución de la Superintendencia de Industria y Comercio que permitiría hacer una interpretación más amplia a la definición de violaciones de códigos de seguridad de la información. Este proyecto probablemente explique, en parte, las exigencias adoptadas en contra de Facebook, que están alineadas con ella.

16. Resolución 1321 del 24 de enero 2019 de la Superintendencia de Industria y Comercio, Resuelve, artículo 1(5). Disponible en http://www.sic.gov.co/sites/default/files/files/Noticias/2019/Res-1321-de-2019.pdf

Introducción al problema

La falta de rutas de divulgación en seguridad digital debilita de manera importante la seguridad digital de organizaciones y Estados. La seguridad de grandes sistemas es muy compleja de manejar, incluso para entidades con una capacidad técnica interna muy fuerte y con equipos competentes dedicados a la seguridad digital. Es imposible asegurar un sistema al 100%. Por ello, es importante no rechazar ayudas externas de parte de la comunidad técnica, de la ciudadanía o de organizaciones de la sociedad civil que puedan detectar vulnerabilidades, incidentes o violaciones de la seguridad de los datos.

Para ilustrar esto no hay nada más que ver el ejemplo del Departamento de Defensa de Estados Unidos que, habiéndose caracterizado históricamente por ser una institución muy hermética, decidió abrir un programa de recompensa llamado *Hack the Pentagon*. Incluso reconoció públicamente que los aportes de este programa le han permitido «identificar y remediar miles de vulnerabilidades de seguridad digital» (traducción nuestra).[17]

Las rutas de divulgación pueden ser un componente clave que permita una mejor detección de los problemas de seguridad digital, constituyendo el primer paso indispensable antes de su mitigación y resolución.

Idealmente, estas rutas de divulgación no deberían limitarse a las vulnerabilidades del tipo 1, sino incluir de manera bien definida al menos estas cinco categorías:

1. **Vulnerabilidades que afecten una categoría de equipos, *software* o servicios en línea**. La divulgación concierne, en primer lugar, a quienes desarrollaran (ej. vulnerabilidad CVE-2018-14028 en el gestor de contenido WordPress 4.9.7).

2. **Vulnerabilidades de activos o fallas de seguridad** como un servidor web, un servidor de correo, etc., que pertenezca a una entidad bien definida (ej. vulnerabilidad en el servidor web del subdominio «muisca» de la DIAN).

3. **Incidentes de seguridad digital**. Un ejemplo sencillo sería el robo de computadores portátiles de una organización.

4. **Violaciones de la seguridad de los datos personales, que incluyen las fugas de estos mismos datos**. Por ejemplo, la fuga de datos personales de 57 millones de personas en Uber.[18] Como mencionamos antes, esta categoría tomó mucha importancia en Europa con la nueva obligación legal de notificación de los responsables de tratamientos. En Colombia, también existe una obligación similar, aunque todavía mucho más limitada, que están enfocada en la violaciones de códigos de seguridad.

5. **Violaciones de la seguridad de otros tipos de datos**. Generalmente, se trata de datos cuya

17. US Department of Defense. (2018, 24 de octubre). *Department of Defense Expands 'Hack the Pentagon' Crowdsourced Digital Defense Program* [Press Release]. Disponible en tinyurl.com/y4drp2ak

18. Una parte interesante de esta historia vinculada con el tema de este informe es que la empresa tuvo que pagar 148 millones de dólares por ocultar una fuga de datos de usuarios en 2016. *Véase* Uber pagará 148 mdd en EU por ocultar fuga de datos de usuarios. (2018, 26 de septiembre). *Expansión*. Disponible en tinyurl.com/yxn9cf64

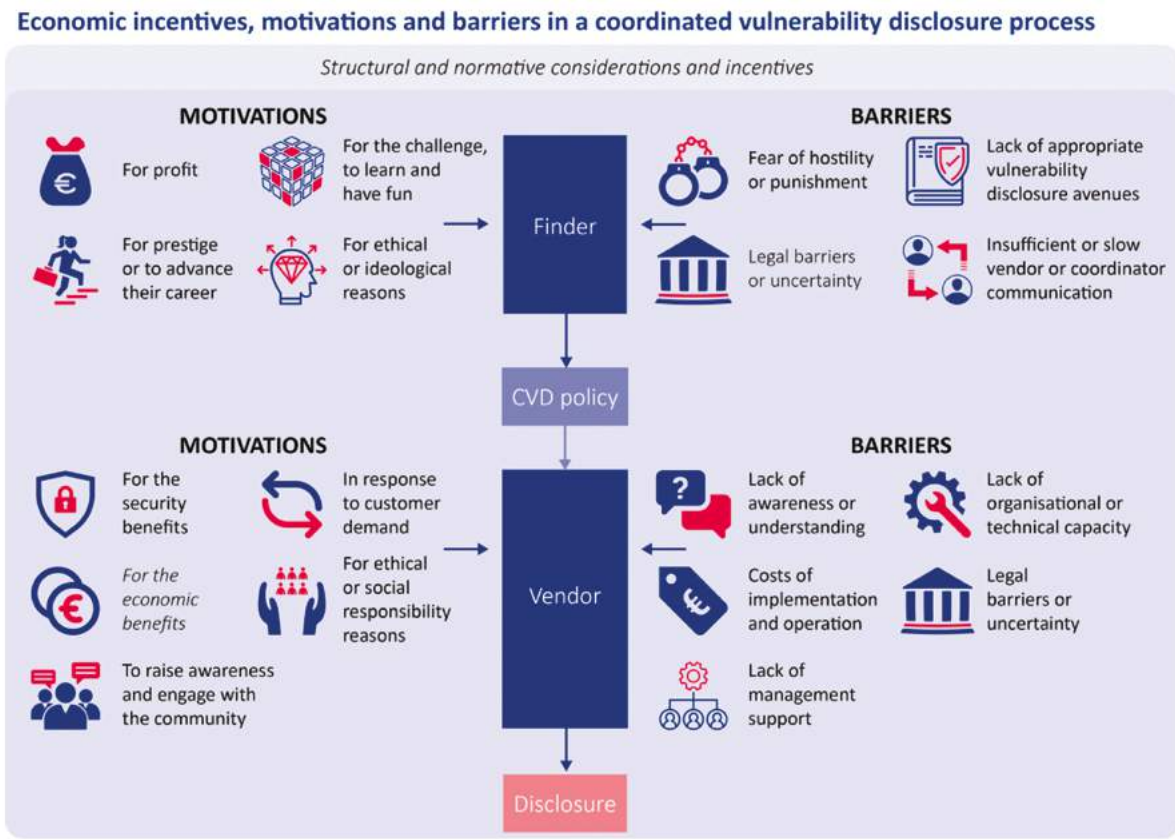
revelación, alteración o indisponibilidad puede tener consecuencias graves en ciertos sectores importantes como salud, telecomunicaciones o lo que se llama ahora en Europa servicios esenciales. En varios países, existen reglamentaciones y obligación de algunos sectores específicos de notificación a autoridades privadas o del Estado (ej. ciberataque que impide la disponibilidad de una red de un operador).

Las rutas de divulgación para la primera categoría están mucho mejor documentadas y desarrolladas gracias al fuerte impulso de empresas privadas, como Microsoft o Google, o coordinadores como los CERT/CSIRT.

No obstante, estas rutas aún se enfrentan con algunas barreras para su operatividad, entre ellas, las legales. En su reciente informe *Economics of vulnerability disclosure*, ENISA resume los incentivos económicos, motivaciones y barreras en los procesos de divulgación coordinada de vulnerabilidades (Fig.1):[19]

19. ENISA. (2018). *Economics of Vulnerability Disclosure*, p. 49. Disponible en https://tinyurl.com/y3y98a8u

(Fig.1)



Source: ENISA study on the economics of vulnerability disclosure

Aunque este esquema proviene de un informe que se centra en las vulnerabilidades del tipo 1, es fácilmente aplicable a los otros casos si se reemplaza al proveedor por la entidad cuyo sistema es objeto de una vulnerabilidad, de un incidente o de una violación de la seguridad de datos.

Como apuntamos a definir recomendaciones para que desde el Gobierno colombiano se trabaje en el desarrollo e implementación de rutas de divulgación adaptadas, hay que tener en cuenta algunas barreras importantes que desanimarían a una persona que encuentra un problema de seguridad digital a hacer una divulgación de la mejor manera:

- Miedo a una reacción hostil por parte de las autoridades o a sanciones legales;
- Barreras legales o ausencia de un marco jurídico seguro para quien descubre;
- Ausencia de una ruta de divulgación apropiada, con un política completa y bien definida; o
- Ausencia o insuficiencia de coordinación entre el Gobierno y las partes involucradas (ej. persona/entidad/compañía desarrolladora, entidad a quien pertenecen los activos involucrados, sociedad civil, etc.), lo que se traduce en una ausencia de acciones eficientes a pesar de la divulgación.

Estas barreras y las soluciones posibles se estudiarán en este documento, revisando los avances a nivel internacional.

Otro aspecto que vale la pena abordar son los efectos colaterales de no tener rutas apropiadas de divulgación como sería el reforzamiento de un mercado negro de vulnerabilidades de día cero; un mundo oscuro que alimenta mafias y entretiene a los servicios de inteligencia. El antes mencionado informe de ENISA describe muy bien este problema:

> La no divulgación puede ocurrir debido a una serie de razones. Individuos que encuentran vulnerabilidades pueden optar por no revelarlas a cambio de pagos, especialmente si se pueden lograr mayores pagos en el mercado negro en comparación con las vías de divulgación responsable. Otra área emergente de no divulgación está relacionada con las iniciativas del Gobierno para analizar, evaluar y seleccionar las vulnerabilidades a fin de mantenerlas en secreto con fines de seguridad nacional, a las que a veces se hace referencia como procesos de equidad de la vulnerabilidad. El razonamiento es que un gobierno puede desear no revelar información sobre vulnerabilidades particulares con el fin de explotar esas vulnerabilidades para la recopilación de información o para otras operaciones cibernéticas ofensivas (traducción nuestra).[20]

Cuanto más tarde se haga una divulgación responsable y una detección junto con la publicación de medidas de mitigación y resolución asociadas de la vulnerabilidad, más probable será su uso para fines oscuros. Por eso, es tan importante la creación e implementación efectiva de rutas de divulgación.

20. Ibid., p.10.

Metodologías de descubrimiento: de lo técnico a lo legal

Aspectos técnicos[1]

Para esta sección, consideramos la hipótesis de que las personas que buscan vulnerabilidades, incidentes o violaciones de la seguridad de los datos son externas y no tienen vinculación alguna con la entidad propietaria del sistema (ej. investigadora de seguridad, *hacker*, una ONG, etc.). También asumimos que tienen buenas intenciones, aunque no han firmado un contrato con la entidad propietaria del sistema que les autorice a hacer un test de penetración de sistemas (*pentesting*), ingeniería inversa o cualquier análisis intrusivo.

En el **descubrimiento de una vulnerabilidad**, ya sea de tipo 1 o 2, la persona puede haber usado varias metodologías técnicas, que clasificamos a continuación:

1. Análisis pasivo y no intrusivo con observación de un sistema desde el exterior (ej. análisis del certificado de seguridad de un sitio web, análisis de la dirección IP del servidor para determinar donde se ubica);

2. Solicitud activa del sistema fuera de un uso normal, pero sin intrusión (ej. escaneo de puertos de un servidor, solicitudes repetidas de tipo «DoS»);

3. Análisis inverso (*reverse engineering*) de un *software* o equipo. Este tipo de análisis puede incluir reconstitución del código fuente original e inteligible[2], copias, difusiones parciales de código fuente propietario, el traspaso de medidas de seguridad para acceder a funciones normalmente no accesibles (ej. *jailbreak* de un iPhone para obtener un acceso *root*), etc.

4. Análisis de flujo de datos de un equipo que le pertenece a la persona que busca vulnerabilidades con técnicas de «hombre en el medio» (*man in the middle*), pero sin ruptura de cifrado, con el objetivo de analizar, por ejemplo, el funcionamiento del equipo mismo, de su sistema operativo, de una aplicación instalada o de un sitio web.

5. Análisis de flujo de datos de un equipo propio con técnicas de «hombre en el medio» y con ruptura de cifrado (ej. HTTPS), usando una generacion de falsos certificados criptográficos con los mismos dominios que los usados

1. Estas categorías fueron definidas por nosotros como un ejercicio de clasificación técnica que puede conectarse con el análisis legal de este informe. No necesariamente se sustentan en una bibliografía extensa, por lo que podrían ser categorizaciones incompletas.

2. Por ejemplo, cuando se publica un *software* que no es libre, lo que se difunde es la versión compilada del programa. Hay herramientas que permiten descompilar para volver al código fuente, lo que puede ayudar a entender el funcionamiento interno del programa y, quizás, detectar vulnerabilidades. Hacer esto puede ser interpretado como una elusión de una medida tecnológica destinada a proteger el código fuente. Así el código fuente sea público —por ejemplo, el caso de funciones *javascript* de terceros usadas en los sitios web— puede ser «ofuscado», es decir, haber sido modificado por quien desarrolló el *software* de tal forma que fuese difícilmente entendible por un humano. Igual en este caso, hacer una desofuscación podría ser una «elusión» de esa medida de protección del código. Como se detalla más adelante, la elusión de medidas tecnológicas de protección puede ser una infracción penal en Colombia.

por los servidores web a los que la aplicación se conecta.[3]

6. Explotación de una vulnerabilidad o de una debilidad del sistema y su intrusión para comprobar que la vulnerabilidad es efectiva.

Si pensamos en una metáfora más familiar, es como querer comprobar la seguridad de una casa: mirar la casa desde el exterior estaría entre los métodos de la categoría 1, mientras que poner el pie más allá de los límites de la puerta de entrada o ventana caería en la categoría 6.

Otro punto importante que hace falta entender es que, incluso para las metodologías 1 a 5, la vulnerabilidad puede ser descrita de manera teórica o incluir lo que se llama una prueba de concepto (*proof of concept*) con eventual publicación de un código o un programa que permita usar la vulnerabilidad (*exploit code*).

Finalmente, se puede mencionar que el descubrimiento de vulnerabilidades —en particular, para el caso de servidores web— puede hacerse con herramientas automatizadas tercerizadas.[4] Estas técnicas entran en las categorías 1 y 2, aunque eventualmente podría caer en la sexta si se llegará después a usar la vulnerabilidad encontrada para entrar en el sistema y comprobar así su efectividad. En todo caso, pensamos que quien usa la herramienta automatizada es responsable por su uso, así sea en un servidor de tercero.

Para el descubrimiento de una **violación de la seguridad de los datos** desde el exterior, *a priori*, el conjunto de métodos que puede utilizarse son menos intrusivos:

1. Consulta de información pública;

2. Búsquedas avanzadas de datos personales o sensibles con los motores de búsqueda en internet; y

3. Acceso desde un perfil de usuario.

Sin embargo, el hecho de que la información esté disponible públicamente desde internet, por ejemplo, implica que acceder a estos datos o copiarlos pueda constituir una infracción.

Para el descubrimiento de **un incidente de seguridad**, se pueden usar todas las metodologías antes mencionadas.

3. Esto permite que el equipo que vaya a realizar la captura de flujo —posicionado entre el equipo que se vaya a analizar y el punto de acceso a internet— se haga pasar por el servidor web legítimo, que sea un servidor web clásico o un servidor web de aplicación. Varios programas como MITM proxy o ZAP permiten este tipo de captura y generan automáticamente los falsos certificados. Para que esto sea posible, hay que tener el control del equipo analizado (teléfono inteligente, tableta, computador) y añadir una nueva autoridad de certificación «nuestra» que vaya a firmar y «autenticar» estos falsos certificados.

4. Véase por ejemplo, esta pentest-tools.com/home

Riesgos legales

Como se menciona en el informe *Good Practices on Vulnerability Disclosure* de ENISA, en muchos países, varias de las técnicas antes descritas pueden constituir:[5]

1. Infracciones a leyes penales relacionadas con sistemas informáticos o protección de la información;

2. Infracciones a las leyes de propiedad intelectual; o

3. Infracciones al Acuerdo Internacional de Wassenaar sobre la exportación de armas convencionales y de tecnologías duales, en la medida en que se intervengan equipos de seguridad digital incluidos en la lista de tecnologías.[6]

En muchos países, particularmente en los Estados Unidos, hay riesgos legales asociados a las normas de propiedad intelectual y a los términos y condiciones en contratos, licencias o políticas de uso. Tienen que ver principalmente con las metodologías de ingeniería inversa o retroingeniería; de una parte, porque la divulgación de la vulnerabilidad implica generalmente acceder, duplicar y difundir una copia parcial del código fuente del programa o del sistema, lo que no está permitido por las leyes de derechos de autor. De otra, porque muchas veces las técnicas de ingeniería inversa implican sobrepasar medidas de protección o de seguridad digital («elusión») que está prohibido por leyes y por muchos contratos, términos y condiciones.

5. ENISA. (2015). *Good Practices on Vulnerability Disclosure: From Challenges to Recommendations*, pp. 50-52. Disponible en www.enisa.europa.eu/publications/vulnerability-disclosure

6. Arreglo de Wassenaar sobre Control de Exportaciones de Armas Convencionales y Productos y Tecnología de Doble Uso. Disponible en https://www.wassenaar.org/es/

Situación en Colombia

Marco legal-normativo y riesgos asociados

En Colombia hay al menos tres marcos legislativos o normativos que se puedan aplicar al contexto de este estudio:

- La Ley de Delitos Informáticos (Ley No. 1273 del 2009);
- La Ley de Protección de Datos (Ley No. 1581 del 2012); y
- La Ley de Propiedad Intelectual (Ley No. 23 de 1982, Decisión 351 de 1993 del Acuerdo de Cartagena y Ley 1915 de 2018).

Adicionalmente, cobra importancia en esta materia la Política Nacional de Seguridad Digital (CONPES n°3584 de 11 de abril 2016).

De todas las normas mencionadas, la Ley de Delitos Informáticos parece ser la barrera legal más importante a la divulgación de vulnerabilidades o alertas de seguridad. La misma crea un nuevo bien jurídico tutelado: la protección de la información y de los datos, adicionando nuevos delitos al Código Penal.[1] Precisamente, su objetivo es conservar los sistemas que usen las tecnologías de la información y las comunicaciones.

Algunos aspectos a destacar del conjunto de estos delitos: en primer lugar, sobresale que las penas económicas previstas por los delitos informáticos son las más altas del Código Penal, siendo la pena más baja 100 salarios mínimos mensuales legales vigentes. También se prevén penas de cárcel, la mínima siendo de cuatro años y, *a priori* y según interpretación del jurista Alexander Díaz García, sin posibilidad de modificar la medida de aseguramiento y sin tener beneficios como el de prisión domiciliaria.[2] Además, incluyen 8 circunstancias de agravación punitiva, entre las que está el hecho de que el sistema intervenido sea estatal u oficial (artículo 28H).

El principal problema de estas normas es que la mayoría de los delitos mencionados en esta ley no exigen la intención de cometer un daño, de tener un ánimo de lucro o un provecho cualquiera para aplicarse. Tampoco incluyen excepciones. Esta falta permitiría considerar casos como el de «*hacking* ético» u otras metodologías para detectar vulnerabilidades, incidentes o violaciones de la seguridad de los datos como hechos punibles.

A continuación presentamos los delitos informáticos que podrían aplicar a ciertas metodologías de descubrimiento de vulnerabilidades, incluso en caso de que exista buena intención. Aclaramos que, en esta investigación, no realizamos un análisis de condenas por delitos informáticos, por lo que solo hacemos una revisión de los elementos de los delitos frente a casos hipotéticos que creemos problemáticos.

> Artículo 269. Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido **o no** con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión

1. *Ley de Delitos Informáticos*. Ley No. 1273 de 5 de enero de 2009. Disponible en mintic.gov.co/portal/604/articles-3705_documento.pdf

2. Martínez, J.J. (2012, 30 de marzo). Colombia, el primer país que penaliza los delitos informáticos. *La Patria*. Disponible en tinyurl.com/yypt8fym

> de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes (destacado nuestro).

El uso, por ejemplo, del conjunto de metodologías de la categoría 6 de la lista de descubrimiento de vulnerabilidades mencionadas en este estudio, aquellas en las que se entra a sistemas informáticos, podría constituir una violación como la descrita en este artículo. El caso de que el delito mencione «sistema informático protegido o no» puede convertir en hecho punible el acceso no autorizado de una página interna que esté disponible por error y sea indexada por un motor de búsqueda. Aunque pueda parecer exagerado, el hecho de hacer clic en el enlace y entrar en ella, teóricamente, podría constituir un delito.

> Artículo 269C. Interceptación de datos informáticos. El que, sin orden judicial previa, intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Aunque no es evidente y existen zonas grises que añaden un nivel mayor de complejidad a este asunto, podría decirse que las metodologías de interceptación de flujo constituirán la comisión de este delito, a menos que se haga dentro de una red privada y con equipos propios de la persona que hace el análisis. Un caso sería aquel análisis de los flujos de datos WIFI entre el computador de una persona que busca vulnerabilidades y un punto WIFI ajeno. Además, las metodologías de la categoría 6 de la lista de descubrimientos de vulnerabilidades que buscan penetrar una red inalámbrica para testar su seguridad, sin lugar a dudas, podría constituir un delito de este tipo.

> Artículo 269D. Daño informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Las metodologías de las categorías 2 y 6 de descubrimiento de vulnerabilidades podrían ser un ejemplo de la comisión de este delito, pues solicitando activamente o realizando una intrusión en equipos que no se conocen perfectamente, siempre existe el riesgo de crear un daño informático.

> Artículo 269F. Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

En el caso de una explotación de una vulnerabilidad que permitiera entrar en un sistema con datos personales o el acceso a datos disponibles en internet e indexados por un motor de búsqueda, se podría aplicar este artículo. Sin embargo, este delito incluye la limitación «con provecho propio o de un tercero», lo que podría ser una disposición efectiva para minimizar este riesgo.

Otro problema que encontramos es el uso de la metodología de ingeniería inversa (metodología dentro de la categoría 3 de la lista de descubrimiento de vulnerabilidades) frente a los límites de la Ley de Propiedad Intelectual. Si bien en 2018 se introdujeron en esta legislación excepciones para los riesgos vinculados con la elusión de medidas tecnológicas (artículo 13) y para la reproducción temporal o difusión (artículo 16), no creemos que puedan ofrecer suficiente seguridad jurídica en el caso del uso de la ingeniería inversa.

En conclusión, los riesgos legales en Colombia son altos para cualquier persona que quiera divulgar vulnerabilidades, incidentes de seguridad digital o violaciones de la seguridad de los datos. Este contexto requiere mucha cautela y prudencia en la metodología que se utilice, lo que limita el descubrimiento de vulnerabilidades con la intención de mejorar los sistemas.

Rutas de divulgación en Colombia

Cualquier ruta de divulgación y alerta requiere de un coordinador identificado para que funcione. Por ello, nos dimos a la tarea de identificar entidades del Estado que pudieran desempeñar ese papel e implementar rutas:

- MinTIC
- Delegatura de Protección de Datos
- Centros de Respuesta a Incidentes del Estado (CERT/CSIRT):
  - » colCERT[3]
  - » Centro Cibernético de la Policía Nacional[4]
  - » Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional (CSIRT PONAL)
  - » Comando Conjunto Cibernético (CCOC)[5]

También existen CERT/CSIRT privados como el de la Cámara Colombiana de Informática y Telecomunicaciones (CSIRT-CCIT)[6] y CERT/CSIRT específicos a algunas empresas privadas

3. Véase el sitio web del colCERT en www.colcert.gov.co/

4. Véase el sitio web del Centro Cibernético de la Policía Nacional en caivirtual.policia.gov.co/

5. Véase el sitio web del Comando Conjunto Cibernético en www.ccoc.mil.co/

6. Véase el sitio web del CSIRT de la Cámara Colombiana de Informática y Telecomunicaciones en www.csirt-ccit.org.co/

establecidas en Colombia (Claro, ETB, Olimpia Digital, ShieldNow, ETEK International, DigiSOC y IT Security Services S.A.S).

En el sitio web del MinTIC no existe ninguna ruta de divulgación; mientras, en el sitio web de la Delegatura de Protección de Datos se encuentran los ítems de «Instaurar una queja» y «Denunciar una conducta». Aunque no son exactamente una ruta de divulgación, podrían ser usados para los casos de violaciones de la seguridad de datos personales. También es importante mencionar la existencia de un proyecto de resolución de la Superintendencia de Industria y Comercio relativa al procedimiento para el Registro Nacional de Bases de Datos (RNBD).[7] En el mismo se ofrece una definición completa de lo que se considera como un incidente de seguridad, incluyendo una interpretación amplia de lo que la Ley de Datos Personales llama «violación a los códigos de seguridad de información». Por otra parte, contiene la obligación de reportar estos incidentes de seguridad, siempre que involucren datos personales, a la Delegatura de Protección de Datos vía el RNBD (ver extractos del proyecto de resolución en Anexo).

Sobre los cuatro CERT/CSIRT públicos de Colombia, el colCERT es el único que cuenta con un botón para que cualquier persona pueda reportar vulnerabilidades e incidentes. Cuando se da clic, informa de la posibilidad de reportar estos eventos por correo electrónico.[8] El Centro Cibernético de la Policía Nacional ofrece en su sitio web la posibilidad de reportar un incidente informático, pero el botón es poco visible.[9] Además, requiere a la persona que va a reportar que cree una perfil muy detallado, lo que puede ser un disuasivo.[10]

En la *Guía para la gestión y clasificación de incidentes de seguridad de la información* del MinTIC, se señala al colCERT como la entidad receptora de reportes de incidentes en caso de que un componente de una infraestructura tecnológica «haya sido vulnerado o comprometido»; mientras, el Centro Cibernético de la Policía es el receptor en caso de que «se tenga evidencia de un incidente informático».[11] Para este último, se menciona únicamente un número de teléfono fijo como medio de contacto.

En relación con las rutas planteadas por el colCERT y por el Centro Cibernético de la Policía Nacional, al momento de preparar este informe, identificamos al menos 4 barreras para que una persona que encuentra vulnerabilidades divulge un «incidente o vulnerabilidad»:

1. El proceso es bastante complicado. Quien va a reportar un incidente tiene que enviar un correo cifrado después de completar un

7. *Proyecto de Resolución de la Superintendencia de Industria y Comercio para el establecimiento de procedimiento para el Registro Nacional de Bases de Datos*. Disponible en tinyurl.com/y6oseym6

8. Véase la página web sobre «Reportar un incidente» del sitio web del colCERT en www.colcert.gov.co/?q=contenido/reportar-un-incidente

9. Entendemos que el botón es poco visible por su posición (abajo de la página) y por problemas de contraste, dado que el texto es verde, un color que también se encuentra en la imagen de fondo.

10. Véase la página web sobre «Incidente informático» del sitio web del Centro Cibernético de la Policía en https://caivirtual.policia.gov.co/incidente-informatico

11. MinTIC. (2016). *Guía para la gestión y clasificación de incidentes de seguridad de la información*. Disponible en mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

formato bastante engorroso. Sería suficiente tener un formulario web seguro con información mínima obligatoria y complementos facultativos.

2. El sitio web del colCERT usa el protocolo HTTP, lo que no permite tener confianza en la identidad del sitio y es bastante sorprendente para un CERT nacional.

3. El colCERT no está en la lista de los CERT/CSIRT reconocidos internacionalmente ni está afiliado al FIRST. Esto reduce las posibilidades de cooperación y coordinación para la prevención y reacción ante incidentes, como también disminuye las oportunidades de intercambio de información y experiencias.

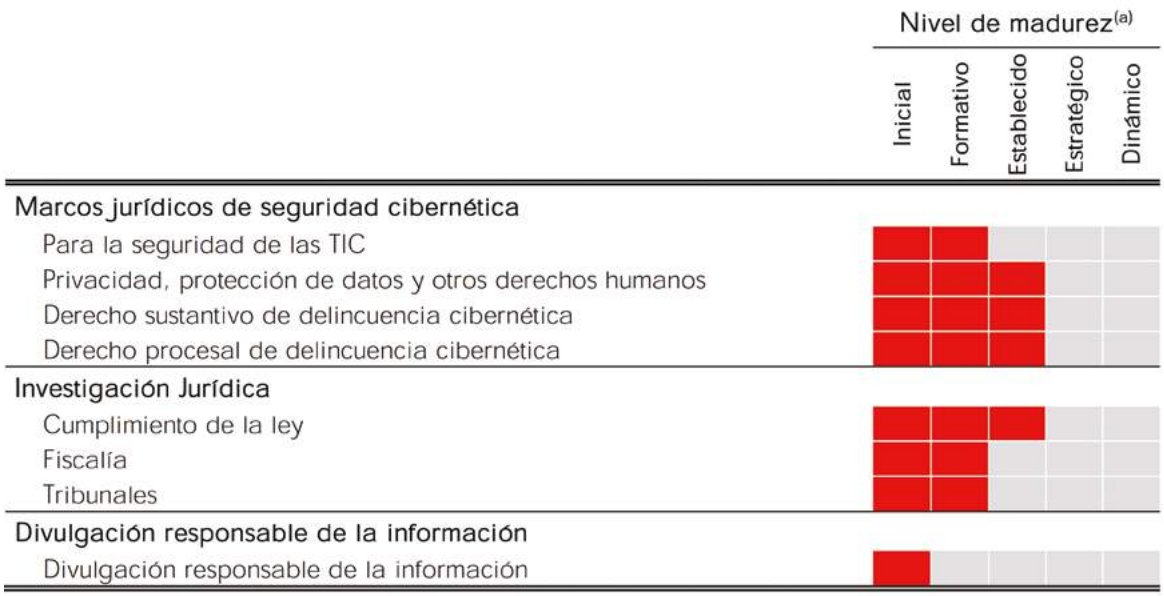
4. El colCERT y el Centro Cibernético de la Policía Nacional están vinculado al Ministerio de Defensa, lo que puede representar un desincentivo para muchos personas activistas, defensoras de derechos humanos o *hackers* éticos al momento de reportar una vulnerabilidad o incidente.

Es probable que lo anterior ofrezca algunas razones para que la Organización de Estados Americanos (OEA) considere que Colombia tiene un nivel de madurez inicial en temas de divulgación responsable de información **(Fig. 2)**:[12]

12. *Política Nacional de Seguridad Digital*. CONPES No. 3584 de 11 de abril de 2011. Disponible en tinyurl.com/y6ea4vu6

(Fig. 2)

Figura 2. Nivel de madurez del marco jurídico y reglamentario de seguridad cibernética en Colombia, 2015



Fuente: BID & OEA (2016).

Experiencia del K+Lab en el análisis de sitios web y aplicaciones del Gobierno colombiano

Desde 2016, el K+Lab de la Fundación Karisma ha realizado cuatro estudios que mostraron la necesidad de crear conciencia sobre la importancia y valor de las rutas de divulgación coordinada de vulnerabilidades. Se trata, precisamente, de un proyecto que tiene dos objetivos: (1) analizar la forma como importantes sitios web e incluso aplicaciones del Gobierno colombiano, o que cumplen funciones del Estado, protegen la seguridad y privacidad de las personas; y (2) retomar una queja persistente de miembros de la comunidad técnica de que no existe en Colombia un mecanismo para informar vulnerabilidades e incidentes, y que las respuestas de las directivas de la entidades o al colCERT ante los reportes son inexistentes o desobligantes, siendo tratados como amenaza.

Estos análisis se han realizado con el fin de demostrar que pueden hacerse y que, efectivamente, sirven para ayudar a mejorar la información, la privacidad y la seguridad digital de los sitios o aplicaciones para beneficio de la sociedad en general. También han servido para demostrar que sería útil contar con rutas de divulgación públicas y predecibles.

El ejercicio que desde Karisma se ha hecho siempre ha sido con métodos no intrusivos, documentado los procesos y hallazgo, e identificando la ruta adecuada para presentar los resultados, de modo que, sirvan para mitigar los hallazgos.

En orden cronológico, el K+Lab ha analizado la seguridad digital de lo siguientes sitios web:

- El sitio web para reporte de hurtos de celulares, imeicolombia.com.co;
- La Unidad para la Atención y Reparación Integral de las Víctimas (UNV);
- La Dirección de Impuestos y Aduanas Nacionales (DIAN), además de su aplicación; y
- El sitio web de TuLlave (Transmilenio).

Estos análisis han permitido descubrir los siguientes problemas:

- Vulnerabilidades que afectan sitios web y aplicaciones;
- Incidentes de seguridad; y
- Violación de la seguridad de los datos personales.

Los cuatro ejercicios mencionados han permitido confirmar que existen las barreras que ENISA describe para el contexto europeo y que antes hemos tratado.

La presentación de los reportes a las organizaciones responsables ha supuesto reacciones hostiles de diferente grado, en algún caso, incluso se ha mencionado la posibilidad de sanciones judiciales. Esto a pesar de haberse expresado claramente que las metodologías utilizadas son cuidadosas de mantenerse dentro del marco legal del país.

Ante la ausencia de un marco jurídico seguro para buscar vulnerabilidades, el K+Lab se ha soportado en buenas prácticas internacionales que incluyen entregar informes completos y documentados a los responsables de los sitios web o aplicaciones estudiadas. Esto también ha incluido el compromiso de que no se hará divulgación de las vulnerabilidades

identificadas. La metodología empleada y el hecho de que, efectivamente, ha servido para mitigar problemas importantes de seguridad digital ha servido para ir construyendo una relación de confianza en el proceso. Un éxito del proceso es haber identificado al MinTIC como un intermediario y facilitador para conectar con la entidades que han sido objeto del análisis. Esta relación ha servido para mitigar la reacción hostil de las entidades encargadas. Además, ubica al Ministerio como un ente coordinador y facilitador de la respuesta a los fallos identificados.

Sin embargo, la ausencia de una ruta de divulgación apropiada y con unas políticas definidas hacen que el modelo usado por Karisma no sea replicable por cualquier persona, mucho menos se puede decir que es un modelo escalable. El principal problema de esto es que el Estado no cuenta con un mecanismo de reporte que sea confiable, ni le permite desarrollar una coordinación para atender este tipo de eventos.

De los cuatro ejercicios realizados, no hay resultados que permitan hacer generalizaciones. El tiempo de respuesta para coordinar una reunión con la entidad que ha sido objeto del análisis va desde unos días hasta meses. La respuesta ha sido muy eficiente en algunos casos y mucho más lenta en otros, incluso después de haberse publicado los informes (en los que, en todo caso, nunca se divulgan las vulnerabilidades). Sin perjuicio de que en uno de los casos se hizo una presentación conjunta del ejercicio,[13] se puede afirmar que una vez se publica los resultados por parte de Karisma nunca se nos ha hecho una actualización de oficio sobre las acciones tomadas por la entidad. Tampoco se han hecho reportes públicos después de un tiempo para indicar lo que se hizo.

En suma, nuestra experiencia en esta área nos permite concluir que es necesario trabajar en la creación de una ruta de divulgación coordinada de vulnerabilidades porque:

1. No existe en Colombia un canal adecuado y de confianza para señalar problemas de seguridad digital;

2. Reportar problemas de seguridad digital trae beneficios a todas las partes involucradas, sobre todo, a la ciudadanía, que al final es la que se debe buscar proteger; y

3. Es importante contar con una entidad coordinadora y con un mecanismo oficial que indique no solo la ruta, sino el tipo de respuesta y seguimiento que se puede esperar.

13. En 2017, el MinTIC, la UNV y la Fundación Karisma hicieron una presentación conjunta que mostró la colaboración entre los tres organismos para mejorar la seguridad digital del sitio web de la UNV. Véase Fundación Karisma (2017, 31 de agosto) *La corresponsabilidad en acción*. Disponible en karisma.org.co/la-corresponsabilidad-en-accion/

Análisis de experiencias a nivel internacional

Europa y las nuevas obligaciones de notificación

Aunque el marco legal europeo no es muy favorable a las rutas de divulgación, existen prácticas y políticas que se han desarrollado, sobre todo, para responder a las obligaciones legales en materia de protección de datos. Más allá de sus particularidades, se puede aprender sobre ellas si lo que se busca es un camino para permitir el reporte de vulnerabilidades.

Marco general

En cuanto a la protección de datos personales, el RGPD introdujo en su artículo 33 nuevas obligaciones para los responsables y encargados del tratamientos de datos.[1] Es un cambio que se implementa con las autoridades de protección de datos de los Estados miembros de la Unión Europea.

Esta nueva obligación se suma a otras vinculadas con sectores específicos:

- La obligación de los **operadores de telecomunicación o internet** de reportar toda violación de datos personales a la autoridad competente y, eventualmente, a las personas afectadas.[2]
- La obligación de los **operadores encargados de la identificación electrónica y los servicios de confianza** de reportar toda «violación de la seguridad y pérdida de la integridad» en transacciones electrónicas.[3]
- La obligación de los **operadores de servicios esenciales**[4] de notificar «los incidentes que tengan efectos significativos en la continuidad de los servicios esenciales que prestan».[5] Adicionalmente, cada Estado miembro de la Unión Europea tiene la obligación de crear un CERT/CSIRT, que deberá ser responsable de desarrollar procedimientos claramente definidos de gestión de incidentes y riesgos.[6]
- La obligación de los **operadores de redes y servicios de comunicación electrónica** de reportar las violaciones a la seguridad o pérdidas de integridad.[7]

Estos últimos años, las obligaciones en Europa de notificar a los organismos competentes tanto las

1. Unión Europea. (2016). *Reglamento General de Protección de Datos*, Artículo 4(12). Disponible en tinyurl.com/yxbavxzv

2. Ibid., artículos 2 y 3.

3. Unión Europea. (2014, 23 de julio). *Reglamento No. 910 para la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior*, artículo 19. Disponible en tinyurl.com/y2fr7q2m

4. La Directiva Europea sobre la seguridad de las redes y sistemas de información, en su artículo 4(2)(a), define a un operador de servicios esenciales como «una entidad que presta un servicio esencial para el mantenimiento de actividades sociales o económicas cruciales». Además, la Directiva incluye una lista de tipos de operadores en su Anexo 2, clasificándolos en 7 sectores: energía, transporte, banco, infraestructuras de los mercados financieros, sector sanitario, suministro y distribución de agua potable, infraestructura digital. Véase Unión Europea. (2016, 6 de julio). *Directiva No. 1148 sobre las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información*. Disponible en tinyurl.com/y3grupjd

5. Ibid., artículo 14.

6. Ibid., artículo 9.

7. Unión Europea. (2009, 25 de noviembre). *Directiva No. 140 sobre las redes y los servicios de comunicaciones electrónica*, artículo 13 bis. Disponible en tinyurl.com/y5ohb3ds

violaciones de la seguridad de datos personales como de otros tipos de datos, o incidentes de seguridad en sectores específicos han ido aumentando. Como resultado, en varios países, se han creado rutas de divulgación dentro de las autoridades de protección de datos, de seguridad digital o en los CERT/CSIRT del Estado (en varios casos, estos CERT/CSIRT pertenecen a la autoridad nacional de seguridad digital).

Sin embargo, en pocos casos se ha resuelto el problema del riesgo legal en caso de que no sea el propio organismo el que descubra las violaciones de la seguridad de los datos, incidente o vulnerabilidad, sino una tercera persona como un investigador de seguridad digital, activista o una persona común.

A pesar de lo antes dicho, se puede resaltar la existencia de guías como las que ha publicado la ENISA en el tema de la divulgación coordinada de vulnerabilidades. Estos manuales promueven una divulgación coordinada y dan un marco más seguro sobre la forma en la que se pueden hacer. Ojalá los problemas que ponen en evidencias estas guías, a futuro, permitan evoluciones legislativas que creen marcos más seguro para las personas que buscan o encuentran con vulnerabilidades, incidentes y violaciones de la seguridad de los datos.

Reino Unido: la necesidad de separar actividades de inteligencia y seguridad digital

En el Reino Unido, todos los casos de violaciones de seguridad de los datos e incidentes mencionados previamente se pueden reportar en el sitio web de la Agencia Nacional de Protección de Datos (ICO o *Information Commissioner's Office*).[8] En el sitio se permite reportar los cuatro tipos de violaciones de la seguridad de los datos e incidentes definidos por la reglamentación europea que mencionamos antes. Esta centralización hacia una única entidad simplifica las cosas para las personas u organizaciones que buscan vulnerabilidades respecto a países como Francia, que tienen puntos de entradas múltiples. Por lo tanto, la gestión que hace el Reino Unido de la divulgación de incidentes y violaciones de la seguridad de los datos en sectores específicos nos parece adecuada. Nada en el formulario evita que cualquier persona informe de un hallazgo relacionado con violaciones de seguridad de datos e incidentes, por tanto, sirve tanto a entidades obligadas a hacer estos reportes como a cualquier otra persona. Además, esto estaría en línea con la norma de protección de datos de ese país.

En cuanto a las vulnerabilidades, el canal de denuncia es un formulario en el sitio web de la Agencia Nacional de Ciberseguridad (NCSC o *National Cyber Security Centre*).[9] Esta vía sufre de un problema organizacional importante y es que el NCSC es parte del servicio de inteligencia del país, el *Government Communications Headquarters* (GCHQ), situación muy similar a la vinculación de colCERT con el Ministerio de Defensa.

Lo anterior se suma a un posible problema creado en la sección 190 del *Investigatory Powers Act*,

8. Véase la página web de «*Report a Breach*» en el sitio web de la Agencia Británica de Protección de Datos en ico.org.uk/for-organisations/report-a-breach/

9. Véase la página web de «*Incident Management*» en el sitio web de la Agencia Británica Nacional de Ciberseguridad en www.ncsc.gov.uk/incident-management

legislación aprobada en 2016 que podría obligar a las personas investigadoras de seguridad a colaborar con el GCHQ en relación con la vulnerabilidad que hayan descubierto y no divulgado.[10] Esto tiene que ver con el problema de la capitalización y uso de vulnerabilidades de día cero por los servicios de inteligencia. Debido a que una agencia de inteligencia tiene interés en hacer investigaciones secretas, puede verse ante un dilema entre proteger a la ciudadanía o aprovechar esa vulnerabilidad para su beneficio. Poner a estos organismos en esa disyuntiva es problemático y, por eso, un Estado no debe ubicar la ruta de divulgación de vulnerabilidades en servicios de inteligencia, mucho menos hacer la ruta obligatoria para vulnerabilidades de día cero.

En resumen, el ejemplo del Reino Unido demuestra que no basta con que exista una rutas de divulgación bien concebida. También es importante que estas rutas estén coordinadas e implementadas por entidades que aporten confianza a las personas u organizaciones que buscan vulnerabilidades. Esto, además, debería incluir legislación protectora.

10. Lyden, J. (2017, 31 de mayo). UK surveillance law raises concerns security researchers could be 'deputised' by the state. *The Register*. Disponible en tinyurl.com/y8xz5qjj

Francia: hacia la protección legal de quien descubre

El caso de Francia es interesante, pues, ha mejorado las posibilidades de una divulgación coordinada de las fallas de seguridad y vulnerabilidades.[11] Se hizo de dos maneras:

1. A través de una modificación legislativa que introduce una excepción al artículo 40 del Código de Procedimiento Penal que obliga a los funcionarios públicos a denunciar delitos y crímenes.[12] La enmienda crea una excepción para «*las personas que actúen de buena fe y que transmitan a la única autoridad nacional de seguridad de los sistemas de información sobre la existencia de una vulnerabilidad relativa a la seguridad de un sistema de tratamiento automatizado de datos*» (traducción nuestra).

11. Las fallas de seguridad y vulnerabilidades (*failles de sécurité et vulnérabilités*) en Francia se aplican a los dos tipos de vulnerabilidades que hemos considerado al inicio de este informe, es decir, las que se refieren a un «un equipo (*hardware*), un programa o un servicio en línea» y las que se refieren a un activo, un sistema de una entidad específica.

12. *Loi pour une République numérique* n° 2016-1321 del 7 de octubre 2016.
Traducción nuestra: «Toda autoridad constituida, funcionario o servidor público que, en el ejercicio de sus funciones, tenga conocimiento de un delito o falta, estará obligado a notificarlo sin demora al fiscal y a transmitirle toda la información, las actas y los actos relativos a las mismas».
Texto original en francés: «*Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs*».

2. La introducción de una obligación a la Agencia Nacional de Sistemas de Información (ANSSI o *Agence Nationale de Sécurité des systèmes d'information*) de preservar «*la confidencialidad de la identidad de la persona que inició la transmisión y de las condiciones en que se llevó a cabo*» (traducción nuestra). La ANSSI es una agencia vinculada al Primer Ministro de Francia. Los canales propuestos para la divulgación son el correo postal o electrónico.[13]

Podemos notar que, aunque se entiende que el delito sigue existiendo, la ANSSI tiene ahora la obligación de no denunciar la comisión de un delito o falla que pudiera haber cometido la persona que buscó la vulnerabilidad (ej. intrusión en un sistema). En cuanto a la obligación de las organizaciones de reportar violaciones de la seguridad de los datos e incidentes de seguridad, existe un esquema bastante complejo que, según el tipo de datos, involucra una o varias de las agencias estatales que se mencionan a continuación (ver procesos de divulgación en Francia en Anexos):

- ANSSI;
- Agencia Nacional de Protección de Datos Personales (CNIL o *Commission Nationale de l'Informatique et des Libertés*); y
- Agencias regionales de salud (ARS) en los casos de datos de salud.

Finalmente, aunque en Francia la organización de las rutas de divulgación es un poco complicada, la reciente modificación de la ley, que introduce nuevas garantías para la persona que busca vulnerabilidades y fallas de seguridad, lo hace un caso interesante que podría servir de ejemplo.

Países Bajos: ruta de divulgación, el rol de la Fiscalía y una estrategia de comunicación

En los Países Bajos, el Centro Nacional de Ciberseguridad (NCSC o *National Cyber Security Centre*), desde 2013, se ha interesado en trabajar en procesos de divulgación coordinada de vulnerabilidades, creando guías para mejorar la seguridad digital.[14]

La última revisión de la guía recoge cinco años de experiencia de cooperación entre la comunidad técnica, el Gobierno, las empresas y el NCSC, que, además, ilustra la construcción de confianza que se ha generado. Esto se puede apreciar rápidamente con la aproximación comunicacional que adopta y que es evidente desde su primera página: una imagen cuya intención es tranquilizar a quienes buscan vulnerabilidades e invitarles a participar en los procesos de divulgación coordinada **(Fig. 3)**.

13. Suponemos que la decisión de la ANSSI de no optar por un formulario web es evitar hacerse cargo de una base de datos. Con ello, puede prevenir «ampliar la superficie de ataque» de su sitio web, que tiene mucho significado política y podría lastimar la imagen de la entidad de ocurrir un ataque. Véase el sitio web de la ANSSI informando sobre los medios para reportar fallas de seguridad y vulnerabilidades, disponible en tinyurl.com/jyxhjp6

14. NCSC. (2013). *Policy for Arriving at a Practice for Responsible Disclosure* (Disponible en tinyurl.com/y5wwokum) y NCSC, op. cit. (nota 10).

(Fig.3)

EL NCSC implementó una ruta de divulgación para las vulnerabilidades encontradas en sus propios sistemas, los del Gobierno o los de otro sistemas vitales.[15] La agencia se compromete a no perseguir a quien haya encontrado la vulnerabilidad en la medida en que se respete su política de divulgación, algo que es común en muchas rutas de divulgación coordinada.[16] También propone servir de intermediaria, preservando el anonimato de quien divulga, siempre que no exista una investigación legal al respecto.[17] Este acercamiento permite un primer nivel de garantía para la persona u organización que encuentra y alerta sobre una vulnerabilidad. El canal de comunicación propuesto para este proceso es el envió de un correo electrónico cifrado con PGP.

Otro punto interesante en el contexto holandés es que, si bien no se modificó el marco legal, el Fiscal General de la Nación envió instrucciones a todos sus departamentos sobre el tema de la divulgación coordinada de vulnerabilidades.[18] La orden reconoce que la noción de «*hacking* ético» no existe en la legislación del país, pero que pueden tomarse en concisderación «motivos éticos» para determinar si se violaron leyes penales. Así, identifica algunos aspectos a tener en consideración para determinar si una divulgación puede ser calificada como responsable y ética (ver comunicación de la Fiscalía General de los Países Bajos en Anexos).

En conclusión, el caso holandés es interesante en cuanto a la comunicación que se hizo, el buen ejemplo que dio su propia agencia, el canal de divulgación que se creó y la acción tomada por la Fiscalía General para dar cierta garantía jurídica a quienes buscan vulnerabilidades y están dispuestos a contar sobre ellas.

15. Ibid.

16. Véase la página web sobre «*Responsible disclosure*» en el sitio web del Gobierno de Países Bajos en tinyurl.com/yc7y4msn

17. Véase, por ejemplo, lo que se menciona al respecto en la guía: «El NCSC no comparte ningún dato personal a menos que esté legalmente obligado a hacerlo» o «El NCSC tratará los reportes de forma confidencial y no compartirá los datos personales de las partes informantes o de la organización receptora sin su consentimiento, a menos que se derive de una obligación legal» (traducción nuestra). NCSC. (2018). *Coordinated Vulnerability Disclosure: The Guideline*, p. 14. Disponible en https://tinyurl.com/y33jgokg

18. Véase ENISA. (2015). *Good Practices on Vulnerability Disclosure: From Challenges to Recommendations*, p. 52. Disponible en www.enisa.europa.eu/publications/vulnerability-disclosure

Estados Unidos: una progresiva apertura

A pesar de que la Primera Enmienda de la Constitución de Estados Unido tiende a proteger la divulgación de vulnerabilidades como una manifestación de la libertad de expresión, hay varios textos legislativos que se pueden oponer a ello:

- Ley de Derecho de Autor;
- Ley de Secreto Comercial;
- Ley de Patentes;
- Las disposiciones que impidan eludir medidas tecnológicas de protección, en el marco de la Ley de Derechos de Autor del Milenio Digital (DMCA o *Digital Millennium Copyright Act*);[19]
- Ley de Contratos para los casos de un programa relacionado con uno de estos tipos de contratos o términos y condiciones: acuerdo de licencia de usuario final (EULA o *End User License Agreement*), aviso de los términos de servicio (TOS o *Terms of Service Notice*), aviso de las condiciones de uso (TOU o *Terms of Use Notice*), acuerdo de confidencialidad (NDA o *Non-Disclosure Agreement*), acuerdo de desarrollo (*Developer Agreement*) o acuerdo de API (*API Agreement*);
- Leyes penales; y
- Ley de Fraude y Abuso Informático (*Computer Fraud and Abuse Act*).

Para un análisis legal detallado, recomendamos revisar el informe titulado *Coders' Rights Project Vulnerability Reporting FAQ* de la *Electronic Frontier Foundation* (EFF).[20] Vale resaltar que en este informe se identifican varios riesgos legales para quienes hacen investigación en seguridad digital y divulgan vulnerabilidades. Es por ello que se ofrecen algunas recomendaciones para limitar riesgos legales. Más allá de esa identificación, la EFF reiteró en otro informe de 2018 la necesidad de proteger a las personas que hacen investigación en seguridad digital y de desarrollar estándares que brinden seguridad jurídica.[21]

En la actualidad, está bajo consideración del Senado de los EEUU un proyecto de ley que, de aprobarse, obligaría al Secretario de Seguridad Nacional (*Homeland Security*) a presentar al Congreso un informe que describa las políticas y procedimientos desarrollados para coordinar la divulgación de vulnerabilidades.[22] También se puede destacar la existencia de un movimiento que busca facilitar la divulgación de vulnerabilidades. Así, la Unidad de Ciberseguridad del Departamento de Justicia publicó en julio de 2017 recomendaciones para implementar sistemas de divulgación coordinada.[23]

19. *Elusión de los sistemas de protección de derecho de autor*. 17 U.S. Code § 1201.

20. EFF. (s.f.). *Coders' Rights Project Vulnerability Reporting FAQ*. Disponible en tinyurl.com/mycbyle

21. Rodríguez, K. et al. (2018, 16 de octubre). *Protecting Security Researchers' Rights in the Americas*. Disponible en www.eff.org/wp/protecting-security-researchers-rights-americas

22. *Cyber Vulnerability Disclosure Reporting Act*. H.R.3202 — 115th Congress (2017-2018). Disponible en www.congress.gov/bill/115th-congress/house-bill/3202/text

23. US Department of Justice. (2017). *A Framework for a Vulnerability Disclosure Program for Online Systems*. Disponible en www.justice.gov/criminal-ccips/page/file/983996/download

De otra parte, existen rutas de divulgación del US CERT que distinguen muy claramente el tipo de casos que reciben:[24]

- Incidentes
- Indicadores y medidas defensivas
- *Phishing*
- *Malware*
- Vulnerabilidad de *software*
- Vulnerabilidad en un sitio web del Gobierno

La divulgación de los incidentes, indicadores y *malwares* se hace vía un formulario en línea seguro.[25]

Además, hay una ruta de divulgación para las vulnerabilidades de tipo 1 vía el CERT de Sistemas de Control Industrial (ICS-CERT o *Industrial Control Systems CERT*) del Departamento de Seguridad Nacional de los Estados Unidos.[26] A petición individual, se ofrece preservar el anonimato de quien divulga; en caso contrario, se informa la identidad al proveedor del producto afectado.[27]

En cuanto a los reportes de incidentes de seguridad y violaciones de seguridad de los datos, al igual que en Europa, existe legislación que impone la obligación de notificar y crear rutas de divulgación en dos sectores específicos:

- Salud, en donde existe la obligación de reportar violaciones de la seguridad de los datos personales y fallas de seguridad;[28] y
- Financiero, en el que las empresas públicas tienen la obligación de notificar a sus inversionistas ciertos riesgos e incidentes de seguridad digital.[29]

24. Véase la página web sobre «*Report Incidents, Phishing, Malware, or Vulnerabilities*» en el sitio web del US CERT en www.us-cert.gov/report

25. Véase la forma de reportar incidentes en www.us-cert.gov/forms/report

26. Véase la *Política de Divulgación de Vulnerabilidades* del US CERT en ics-cert.us-cert.gov/ICS-CERT-Vulnerability-Disclosure-Policy

27. Sobre este tema, la Política de Divulgación de Vulnerabilidades del US CERT señala que «[e]l nombre y la información de contacto de quien reporta vulnerabilidades se enviarán a los proveedores afectados, a menos que la persona solicite lo contrario». Ibid.

28. Véase US Department of Health & Human Services. (2013, 26 de julio). *Breach Notification Rule*. Disponible en tinyurl.com/jku75s2 y Federal Trade Commission. (2009). *Health Breach Notification Rule*. Disponible en tinyurl.com/y5t4gvwg

29. US Security and Exchange Commission. (2011, 11 de octubre). *CF Disclosure Guidance: Topic No. 2*. Disponible en www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Sector privado: del miedo a la cooperación hacia la entrega de recompensas

Finalmente, vale la pena recordar el programa de recompensas del Departamento de Defensa, antes mencionado, llamado *Hack the Pentagon*. Hace algunos años hubiera sido impensable que una entidad tan hermética como el Pentágono lanzará un programa de este tipo, pero reconociendo los beneficios del programa, el Departamento de Defensa anunció en octubre de 2018, dos años después de creado, su continuidad.

En el sector privado —en particular, las empresas de tecnología—, se han implementado desde hace varios años rutas de divulgación coordinadas de vulnerabilidades e incidentes de seguridad digital. No siempre ha sido así y todavía existen empresas que, por no estar familiarizadas con el tema, reaccionan con hostilidad y pánico frente a una divulgación de vulnerabilidad. Como lo menciona la investigadora Katie Monrsourris: «*Cuando los proveedores no tienen procesos y capacidad para recibir, investigar y comunicar vulnerabilidades de seguridad digital, muchas veces, la primera reacción es llamar a los abogados*» (traducción nuestra).[30] Un ejemplo de lo anterior le ocurrió al investigador de seguridad digital Mike Davis con la empresa Cyberlock. Davis descubrió una vulnerabilidad en las cerraduras digitales que notificó a esta empresa. La respuesta que recibió fue una carta firmada por los abogados de la organización en donde lo amenazaban con iniciar un proceso por violación a la DMCA.

Sin embargo, las grandes empresas ya están entendiendo que es en su interés desarrollar este tipo de programa. Microsoft lo explica así:

> Pedimos a la comunidad de personas investigadoras de seguridad que nos dé la oportunidad de corregir una vulnerabilidad antes de identificarla o publicarla, como hacemos nosotros mismos cuando descubrimos vulnerabilidades en los productos de otros proveedores. Esto sirve a los mejores intereses de todos al asegurar que los clientes reciban actualizaciones completas y de alta calidad para vulnerabilidades de seguridad, pero que no estén expuestos a ataques maliciosos

30. Moussouris, . (2015). Vulnerability Disclosure Deja Vu: Prosecute Crime Not Research. *Dark Reading*. Disponible en tinyurl.com/yxzppv6s

> mientras se hace la actualización. Después de proteger a los clientes, la discusión pública sobre la vulnerabilidad ayuda a la industria en general a mejorar sus productos (traducción nuestras).[31]

Para estimular y reforzar estas rutas de divulgaciones, muchas de estas empresas han desarrollado programas de recompensas (*bug bounty program*).[32] Netscape fue la primera empresa que implementó un programa de este tipo en 1995.[33] A pesar de que no todos en la dirección de la empresa estaban de acuerdo en lanzar este programa, se hizo con un presupuesto inicial de USD 50.000 y fue un gran éxito para la empresa, hoy relatado en varios libros.[34]

Más recientemente, otras empresas como Facebook o Yahoo! han aprendido de sus errores para implementar o mejorar estos programas de divulgación coordinada, eventualmente, asociados a recompensas. El caso de Facebook es interesante. Veamos.

En 2013, un investigador en seguridad digital llamado Khalil usó una vulnerabilidad que había descubierto en la red social para dejar una carta en el perfil de su fundador, Mark Zuckerberg. El investigador dijo que había intentado informar a Facebook vía su programa, pero que la falta de información y claridad de la respuesta lo llevo a actuar así. Después de este evento, Facebook mejoró su programa de recompensas, uno de los más innovadores en el sector en el que se entregan a las personas que reportan vulnerabilidades o fallas de seguridad un tarjeta bancaria VISA *White Hat* (*hacker* ético) como compensación.

Quizá como resultado de las acciones tomadas por el sector privado, varios Estados también han entendido que en el interés de su seguridad digital y de la ciudadanía es necesario lanzar programas de este tipo. Ya lo hace el Departamento de Defensa de Estados Unidos y parece que pronto la Unión Europa adoptará un programa de recompensas para *softwares* gratuitos y de código abierto.[35]

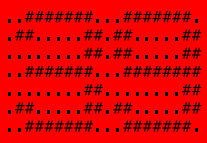
31. Microsoft. (s.f.). *Microsoft's Approach to Coordinated Vulnerability Disclosure*. Disponible en www.microsoft.com/en-us/msrc/cvd

32. Véase la entrada de Wikipedia sobre «*Bug Bounty Program*» en en.wikipedia.org/wiki/Bug_bounty_program

33. En 1983, Hunter & Ready implementó un iniciativa similar a lo que hoy se conoce como un programa de recompensa.

34. En específico, el Vicepresidente de Ingeniería se oponía al lanzamiento del programa de recompensas.

35. Reda, J. (2018, 27 de diciembre). *In January, the EU starts running Bug Bounties on Free and Open Source Software*. Disponible en juliareda.eu/2018/12/eu-fossa-bug-bounties/



Propuestas y recomendaciones

Estos últimos años Colombia ha hecho una apuesta por las herramientas digitales para transformar de manera positiva al país a través de una agenda nacional digital. Para lograr esto en un entorno de confianza y seguridad, se han ido creando marcos legales y normativos como la Ley de Protección de Datos o el CONPES de seguridad digital, además de que se han reforzado entidades como el MinTIC o los CSIRT sectoriales.

Sin embargo, queda mucho por hacer para crear rutas de divulgaciones y un marco adaptado y seguro que ofrezca garantía jurídica para las personas que buscan vulnerabilidades con fines de interés público. Nos parece fundamental seguir este trabajo de mejora de la seguridad digital del país y aumento de la confianza en el entorno digital.

Probablemente, este trabajo necesite de etapas y de fases de transición. A continuación hacemos una propuesta en este sentido.

1. Apoyarse en estándares y experiencias internacionales

Este documento contiene un mínimo de información para abordar el problema de las rutas de divulgación en seguridad digital, por lo que ofrece algunos lineamientos teóricos y prácticos. Sin embargo, para construir estas rutas es importante apoyarse en estándares y recomendaciones internacionales, en particular:

- Guías de ENISA;
- Normas ISO (ISO/IEC 29147:2018 y ISO/IEC 30111:2013), que aunque diseñadas para proveedores tienen contenidos que se puedan adaptar;
- Normas del *Internet Engineering Task Force* (IETF) sobre proceso responsables de divulgación de vulnerabilidades. Para el caso específico de los sitios web, es útil mencionar la propuesta de estándar presentada al IETF para ayudar a definir el proceso para que quienes trabajan investigación de seguridad digital puedan divulgar de forma segura las vulnerabilidades de seguridad encontradas;[1]
- Legislaciones europeas antes mencionadas relativas a las notificaciones de violaciones de la seguridad de datos e incidentes de seguridad digital en sectores específicos; y
- Modelos de rutas y políticas de empresas privadas de referencia en el sector.

Además, sería importante que todos los CERT/CSIRT, en particular, el colCERT, hagan parte del FIRST y pudieran contar con intercambios de experiencias y apoyos de otros CERT/CSIRT del mundo o de otras entidades internacionales.

1. Actualmente se ha propuesto como *Request for Comments* (RFC). Véase el sitio web de «security.txt» en securitytxt.org/

2. Fase de transición: identificar las problemáticas y mejorar las rutas de divulgaciones existentes

Es importante distinguir los diferentes tipos de eventos que pueden ser reportados, así se crean rutas de divulgación con entidades estatales diferentes:

1. Vulnerabilidades que afecten una categoría de equipos, *software* o servicios en línea.

2. Vulnerabilidades de activos o fallas de seguridad en una entidad determinada.

3. Incidentes de seguridad digital.

4. Violaciones de la seguridad de los datos personales, que incluyen, pero no se limitan, a las fugas de datos.

5. Violaciones de la seguridad de otros tipos de datos que presenten una sensibilidad particular.

El colCERT tiene una página web para reportar incidentes o vulnerabilidades que no provee información alguna que dé pistas sobre a qué se refiere exactamente. Adicionalmente, debería desarrollar una política clara y accesible al público que cubra los eventos 1, 2 y 3.

La Delegación de Protección de Datos podría encargarse del evento 4. No obstante, también necesita proveer información, crear la política y hacerse más accesible al público. El proyecto de resolución ya mencionado parece ir en este sentido.

En cuanto al evento 5, hay que señalar que es un tema no desarrollado en el país. Quizás pueda servir de inspiración para Colombia lo que se hizo en Europa con los sectores de salud, telecomunicación y los operadores de servicios esenciales, de manera que, puedan crearse un marco y unas rutas adaptadas.

La creación de estas rutas «centrales» no impide que ciertas entidades del Estado también tengan su propia ruta.

3. Construir políticas de divulgación

Esta recomendación se basa en parte en el mencionado informe *Good practice guide on vulnerability disclosure* de ENISA. De hecho, la información ahí desarrollada podría adaptarse al contexto colombiano y a la necesidad de no limitarse solo a las vulnerabilidades, sino también incluir incidentes y violaciones de la seguridad de los datos.

Una buena práctica es que las rutas de divulgación estén asociadas a **políticas de divulgación**. Con base en la investigación realizada, una política de este tipo debería incluir los siguientes elementos:

1. **Filosofía y objetivo** de la ruta de divulgación;
2. **Garantías de protección y confidencialidad** a la persona que reporta, siempre que respete el proceso;
3. **Canal** para reportar la vulnerabilidad/incidente/violación de la seguridad de los datos. Puede, por ejemplo, incluir un número de teléfono, una dirección de correo electrónico con una clave PGP, una URL de un formulario en línea seguro (HTTPS). En todo caso, es importante crear, dentro de las posibilidades, canales seguros;
4. **Información mínima** que debería contener el reporte;
5. **Tipos de divulgaciones que no se pueden recibir**, ya sea porque están fuera del contexto o porque se usaron métodos no permitidos para descubrir la vulnerabilidad/incidente/violación de la seguridad de los datos. Es importante dar una lista explícita y no cerrada con algunos ejemplos;[2]
6. **Etapas del proceso y línea de tiempo**. Esto debe incluir el tiempo que tiene la entidad para hacer las correcciones antes que se haga la divulgación pública. La práctica en otros países y en el sector privado muestra que ese tiempo suele variar de 45 (ej. US CERT, ICS-CERT[3]) a 90 días (ej. Google[4]).

En el sitio web del colCERT, solo hay información respecto a los puntos 3 y 4. El modelo seleccionado no genera la confianza necesaria en la comunidad a la que va dirigida.

2. Por ejemplo, metodologías que incluyeron ataques de tipo DDoS o de «fuerza bruta», ingeniería social, instalación de *malware*, modificación de la configuración del sistema, etc.

3. Véase la forma de reportar incidentes en www.us-cert.gov/forms/report

4. Google. (s.f.). *How Google handles security vulnerabilities*. Disponible en www.google.com/about/appsecurity/

4. Implementar rutas de divulgación de confianza

Como mencionamos, en Colombia, los cuatro CERT/CSIRT del Estado están vinculados con el Ministerio de Defensa, que también lleva a cabo actividades de inteligencia. Esto puede desalentar a muchas personas que quisieran divulgar, sean investigadoras de seguridad digital, activistas, personas comunes, etc.

Entre sus recomendaciones, la antes mencionada guía de la ENISA sugiere introducir una tercera parte neutral o mejorar los coordinadores existentes:

> En el análisis del equipo del proyecto, se considera conveniente contar con una tercera parte neutral a la que se pueda informar de las vulnerabilidades, especialmente porque algunas entidades pueden tener intereses creados que pueden entrar en conflicto con el interés general de un ecosistema seguro. Algunos de las personas entrevistadas expresaron sospechas de reportar vulnerabilidades a ciertos CSIRT Nacionales, ya que estos CSIRT son entidades gubernamentales que, debido al interés de la inteligencia nacional en las vulnerabilidades, pueden ser influenciadas por otros departamentos gubernamentales (traducción nuestra).[5]

Algunos países han logrado tener CERT/CSIRT nacionales realmente independientes. Es el caso del CERT de Japón (JP-CERT),[6] organización independiente y sin ánimo de lucro que es reconocida como uno de los tres CERT/CSIRT del mundo con más experiencia en coordinar divulgación de vulnerabilidades.[7]

En el caso de Colombia, la creación de un CERT/CSIRT independiente y neutro se podría contemplar a mediano o largo plazo. Mientras tanto, se podrían usar estructuras ya existentes que al menos no pertenecieran al Ministerio de Defensa para operar el canal de divulgación.

Recomendamos que se piense en el MinTIC y la Superintendencia de Industria y Comercio como las entidades que podrían operar el canal de divulgación mientras se cree un CERT/CSIRT independiente y neutro.

5. ENISA. (2015). *Good Practices on Vulnerability Disclosure: From Challenges to Recommendations*, p. 65. Disponible en www.enisa.europa.eu/publications/vulnerability-disclosure

6. Véase el sitio web del CERT de Japón en www.jpcert.or.jp/english/

7. ENISA, op. cit. (nota 5), p. 65.

5. Minimizar los riesgos legales para quien encuentra vulnerabilidades: de la Fiscalía al Congreso

Es necesario crear excepciones a los delitos informáticos relevantes, y ampliar las excepciones y limitaciones al derecho de autor para incluir la noción de *hacking* ético. Así, se podría proveer garantías jurídicas que protejan a quienes divulgan, respetando algunas reglas. Como se ha dicho antes, los riesgos legales y el miedo a la persecución judicial son una de las principales barreras que frenan o impiden una divulgación externa de vulnerabilidad/incidente/violación de la seguridad de los datos.

Sabemos que esto es un proceso que puede ser largo y complicado. Por ello, inspirándonos en las experiencias internacionales mencionadas en este informe, se podrían contemplar las siguientes posibilidades:

- Trabajar con la Fiscalía para que, como se hizo en Países Bajos, se definan criterios para que los «motivos éticos» pudieran ser tomados en consideración a la hora de determinar si se violaron leyes penales.

- Incluir garantías de confidencialidad en las rutas de divulgación e incluso, como se hizo en Francia, crear una obligación legal a la entidad que recibe y coordine la vulnerabilidad/incidente/violación de la seguridad de los datos (ej. el colCERT) de preservar el anonimato de la persona divulgadora, si así lo desea.

6. Desarrollar una comunicación que sensibilice sobre las divulgaciones responsables y coordinadas

La creación y difusión de una *Guía para la gestión y clasificación de incidentes de seguridad de la información* es un paso en este camino. Se podría trabajar en otro manual sobre divulgaciones responsables y coordinadas cuando se haya avanzado en la implementación de rutas de divulgación.

La creación de un programa de recompensas podría ser un eje de comunicación, además de un medio efectivo de encontrar vulnerabilidades en sistemas del Estado colombiano y así mejorar su seguridad.

También es importante que los CERT/CSIRT del Gobierno no sean entidades cerradas, sino que hagan un trabajo de sensibilización, de educación y de difusión de información clave a todas las partes interesadas. Por ejemplo, es importante que difundan las alertas y vulnerabilidades de seguridad digital.

7. Crear una obligación de reporte de incidentes o violaciones de la seguridad de los datos en sectores específicos

Como hemos mencionado antes, este tipo de obligación ya existe de manera limitada para los datos personales (violaciones de códigos de seguridad). Sin embargo, como parece haberlo hecho la reciente resolución de la Superintendencia de Industria y Comercio contra Facebook y como lo contempla el proyecto de resolución relativa al procedimiento para el RGBD, se podría extender esta obligación a las violaciones de la seguridad de los datos personales. Es importante que esta obligación quede recogida en un regulación para que no se preste a interpretaciones.

En cuanto a los otros sectores, es algo que se tendría que crear, pero parece muy importante porque la mayoría de los procesos «vitales» o «esenciales» de un país se basan, en parte y cada vez más, en tecnologías digitales. Su afectación puede tener consecuencias muy graves para la población, y todas las partes involucradas deberían ayudar a proteger y gestionar esos riesgos. El modelo europeo en relación con los servicios esenciales podría servir de referencia.

Bibliografía y referencias

Mucha de la bibliografía y de las referencias utilizadas aparecen en las notas a pie de páginas. A continuación se incluyen solo los principales informes, guías y leyes en los que nos apoyamos para este estudio.

Fuentes primarias

Protección de Datos Personales. Ley No. 1581 de 17 de octubre 2012.

Delitos Informáticos. Ley No. 1273 del 5 de enero 2009.

Derecho de Autor y Derechos Conexos. Ley 1915 del 12 de julio 2018.

Política Nacional de Seguridad Digital. CONPES No. 3854 de 11 de abril del 2016.

Superintendencia de Industria y Comercio. (2019, 24 de enero). *Resolución No. 1321*. Disponible en www.sic.gov.co/sites/default/files/files/Noticias/2019/Res-1321-de-2019.pdf

Unión Europea. (2016). *Reglamento General de Protección de Datos*, Artículo 4(12). Disponible en tinyurl.com/yxbavxzv

Fuentes secundarias

EFF. (s.f.). *Coders' Rights Project Vulnerability Reporting FAQ*. Disponible en tinyurl.com/mycbyle

ENISA (2019, 9 de enero). *Cooperation between CSIRTs and Law Enforcement: interaction with the Judiciary*. Disponible en www.enisa.europa.eu/publications/csirts-le-cooperation

ENISA. (2018). *Economics of Vulnerability Disclosure*. Disponible en tinyurl.com/y3y98a8u

ENISA. (2015). *Good Practices on Vulnerability Disclosure: From Challenges to Recommendations*, pp. 50-52. Disponible en www.enisa.europa.eu/publications/vulnerability-disclosure

FTC. (2019). *Data Breach Response: A Guide for Business*. Disponible en tinyurl.com/jey22z3

Information technology -- Security Techniques -- Vulnerability Disclosure. (2018). ISO/IEC 29147. Disponible en www.iso.org/standard/72311.html

Information technology -- Security Techniques -- Vulnerability Handling Processes. (2013). ISO/IEC 30111. Disponible en www.iso.org/standard/53231.html

MinTIC. (2016). *Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información*. Disponible en mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

National Cyber Security Centre. (2018). *Coordinated Vulnerability Disclosure: The Guideline*. Disponible en https://tinyurl.com/y33jgokg

Rodríguez, K. et al. (2018, 16 de octubre). *Protecting Security Researchers' Rights in the Americas*. Disponible en www.eff.org/wp/protecting-security-researchers-rights-americas

US Department of Justice. (2017). *A Framework for a Vulnerability Disclosure Program for Online Systems*. Disponible en www.justice.gov/criminal-ccips/page/file/983996/download

Anexos

Extractos de la Política Nacional de Seguridad Digital

Institucionalidad

El principal logro alcanzado por la política de ciberseguridad y ciberdefensa, fue el fortalecimiento de la institucionalidad en el tema. Lo anterior, fue posible por medio de la creación de nuevas instancias tales como el Grupo de respuesta a emergencias cibernéticas de Colombia (colCERT) del Ministerio de Defensa Nacional, el Comando Conjunto Cibernético (CCOC) del Comando General de las Fuerzas Militares de Colombia, el Centro Cibernético Policial (CCP) de la Policía Nacional de Colombia, el Equipo de respuesta a incidentes de seguridad informática de la Policía Nacional (CSIRT PONAL), la Delegatura de protección de datos en la Superintendencia de Industria y Comercio, la Subdirección técnica de seguridad y privacidad de tecnologías de información del Ministerio de Tecnologías de la Información y las Comunicaciones, el Comité de ciberdefensa de las Fuerzas Militares, y las Unidades cibernéticas del Ejército Nacional, la Armada Nacional y la Fuerza Aérea Colombiana.

Adicionalmente, en el marco del Documento CONPES 3701, se creó la Comisión Nacional Digital y de Información Estatal, mediante el Decreto 32 de 2013 del Ministerio de Tecnologías de la Información y las Comunicaciones. Instancia que tiene el objeto de ejercer la coordinación y orientación superior de la ejecución de funciones y servicios públicos relacionados con el manejo de la información pública, el uso de infraestructura tecnológica de la información para interacción con los ciudadanos, y el uso efectivo de la información en el Estado colombiano.

Extracto de la *Guía para la gestión y clasificación de incidentes de seguridad de la información* del MinTIC

4. En el evento de que algún componente de la infraestructura tecnológica (sitios Web, aplicaciones, servicios en línea, sistemas de información, entre otros) de la Entidad, haya sido vulnerado o comprometido, reportar en primera instancia al ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia) por medio de correo electrónico a: contacto@colcert.gov.co o al Teléfono: (+571) 2959897. En SEGUNDA instancia, adoptar las medidas y acciones necesarias para mitigar y resolver el incidente con el apoyo del personal encargado de la gestión de incidentes de la entidad, teniendo en cuenta la relevancia de ejecutar todos los procedimientos técnicos y operativos que faciliten la conservación (preservación) de las evidencias de naturaleza digital y soportes del incidente, fundamentales para tramitar su posterior judicialización ante la autoridad competente.

5. Cuando se tenga evidencia de un incidente informático, la entidad afectada se pondrá en contacto con el Cai Virtual de la Policía Nacional www.ccp.gov.co, Centro Cibernético Policial de la Policía Nacional al teléfono 4266900 ext. 104092, para recibir asesoría del caso en particular y posterior judicialización. Es importante aclarar que solamente, en caso de lograrse un contacto exitoso, y tras establecerse de común acuerdo que el incidente pone en riesgo la estabilidad, seguridad y resiliencia del sistema de nombres de dominio, así como de otras

entidades involucradas en el hecho, e incluso la reputación de la entidad, el responsable de la misma podrá solicitar, a través de un correo electrónico, se suspenda temporalmente el nombre de dominio mientras se gestiona internamente el incidente. Para el efecto, la comunicación deberá ser remitida desde cualquiera de las direcciones registradas en el WHOIS con destino al CCP de la Policía Nacional indicando motivo/situación detallada de afectación y solicitando de manera expresa asumiendo plena/total responsabilidad por las consecuencias técnicas/operacionales (sistema de correo, aplicaciones en línea bajo el dominio, etc.) de dicha acción solicitada. Dicho mensaje deberá incluir la información de contacto telefónico del remitente para realizar su respectiva validación y proceder de conformidad.

Extractos del proyecto de resolución de la Superintendencia de Industria y Comercio sobre la creación del procedimiento para el Registro Nacional de Bases de Datos

Artículo 3. Definiciones.

[...]

Incidente de seguridad. Violación a los códigos de seguridad de información del Responsable o del Encargado que generen riesgos en la administración de los datos personales de los Titulares. El incidente comprende, entre otros, la pérdida, el hurto, el acceso, la consulta, el uso, la divulgación, la modificación, la adulteración, la manipulación o la destrucción no autorizada o fraudulenta de información de una base de datos del Responsable o del Encargado del Tratamiento. También incluye un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a la Política de Seguridad del Responsable o del Encargado del Tratamiento.

[...]

Artículo 4. Forma de Inscripción. El registro de usuarios del sistema, la inscripción de las bases de datos, las actualizaciones voluntarias y obligatorias y los reportes de novedades de reclamos, incidentes de seguridad y eliminación de bases de datos se realizan en el portal web de la Superintendencia de Industria y Comercio.

[...]

Artículo 14. Reporte de incidentes de Seguridad. Para reportar los incidentes de seguridad, quienes están obligados a inscribir las bases de datos personales en el RNBD, pueden realizarlo a través de la opción que prevé el sistema del RNBD, por el aplicativo habilitado para tal fin en la página web de la Superintendencia de Industria y Comercio (SIC) en el micrositio de la Delegatura para la Protección de Datos Personales, o mediante cualquiera de los canales habilitados por la entidad para recibir comunicaciones, dentro de los quince (15) días hábiles posteriores al momento en que se detecta el incidente y se pone en conocimiento de la persona o área encargada de atenderlo.

Los Responsables y Encargados del Tratamiento que no se encuentren obligados a registrar sus bases de datos en el RNBD, deberán hacer el reporte de incidentes a través de los canales citados salvo la opción que prevé el RNBD, dentro del mismo término previsto en el párrafo anterior.

El reporte de incidente de seguridad debe especificar lo siguiente:

(i) Nombre de la (s) base (s) de datos afectada (s)

(ii) Ubicación de la bases de datos

(iii) Lugar o medio en que se encuentran los datos afectados (servidor de un proveedor de computación en la nube —cloud computing—, computador, memoria USB, servidor propio del Responsable o Encargado, página web, etc.)

(iv) Sitio, ciudad y país en donde se originó el incidente

(v) Resumen de los hechos relevantes alrededor del incidente

(vi) Causa(s) que generó (aron) el incidente según lo establecido en el Manual de Usuario del Registro Nacional de Bases de Datos —RNBD—

(vii) Tipo de incidente según lo establecido en el Manual de Usuario del Registro Nacional de Bases de Datos —RNBD—

(viii) Número de titulares de datos afectados por el incidente

(ix) Clase de datos personales comprometidos (datos privados, semiprivados, sensibles, públicos, de menores de edad, etc.)

(x) Fecha del incidente

(xi) Fecha en que se tuvo conocimiento del incidente

(xii) Comunicar si el Responsable o el Encargado cuentan con un protocolo o proceso documentado para gestionar incidentes de seguridad de la información

(xiii) Acciones correctivas efectuadas de forma inmediata para cesar o minimizar los efectos adversos del incidente en el tratamiento de los datos personales

(xiv) Planes de acción de mediano y largo plazo para prevenir la ocurrencia de futuros incidentes o, según el caso, evitar que se generen futuros riesgos en el tratamiento de los datos personales.

(xv) Manifestar si se ha informado del incidente a los titulares de los datos o a otras autoridades nacionales (Fiscalía General de la Nación, Policía Nacional, Procuraduría General de la Nación, Superintendencia Financiera) o extranjeras (otras autoridades de protección de datos)

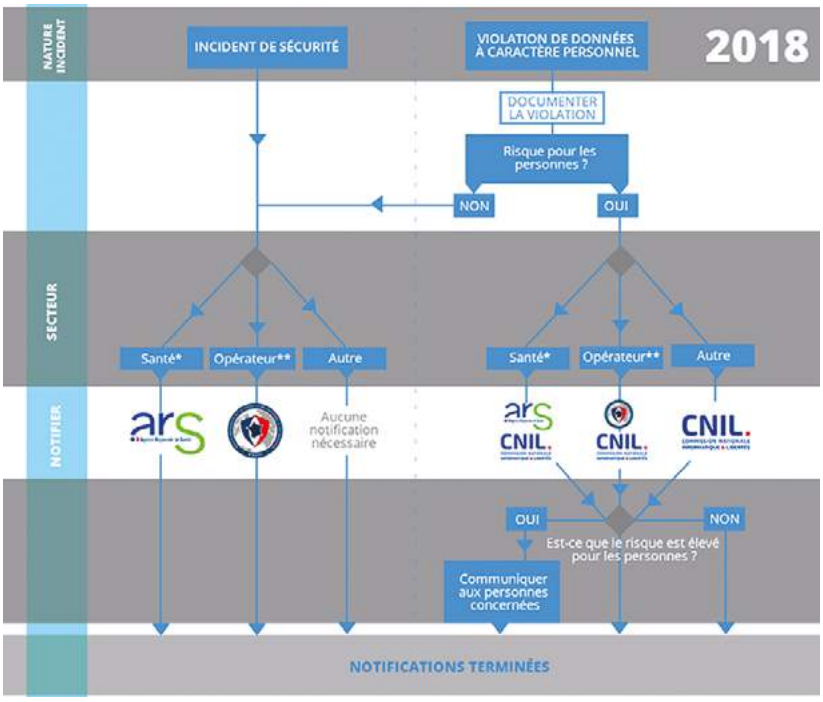
Parágrafo. Las personas jurídicas extranjeras que no tienen sucursal o representación jurídica en el país, y que por cualquier medio recolectan o tratan datos personales en el territorio Colombiano, deberá reportar los incidentes de seguridad de la forma y en el tiempo señalado mediante esta resolución. Esas entidades solo reportan los incidentes respecto de bases de datos que contengan información recolectada o tratada en Colombia.

Proceso de divulgación de incidentes de seguridad digital y violaciones de la seguridad de los datos personales en Francia

Según el tipo de evento (incidente de seguridad digital o violación de la seguridad de datos personales) y el sector involucrado (salud, operadores de importancia vital, otros), el esquema puede involucrar tres entidades:

- Agencias regionales de salud (ARS);
- Agencia Nacional de Seguridad Digital (ANSSI);
- Agencia Nacional de Protección de Datos Personales (CNIL).

En ciertos casos, como la violación de la seguridad de los datos con riesgo alto para las personas, se puede imponer el deber de informar a las personas «víctimas».



Sobre la comunicación de la Fiscalía General de Países Bajos para determinar si se trata de divulgación responsable

In short, the letter instructs public prosecutors to take the following aspects into consideration:

Did the suspect break criminal laws in the process of finding and reporting the vulnerability?

↓

Were the suspect's actions necessary within a democratic society, i.e. did they concern an important general interest?

↓

Did the suspect's conduct involve proportional actions (were the means chosen in proportion to the goal to be achieved)? In other words: how did the hacker gain access to the IT system? If any disproportional actions were carried out for this purpose, this will not constitute 'ethical' hacking.

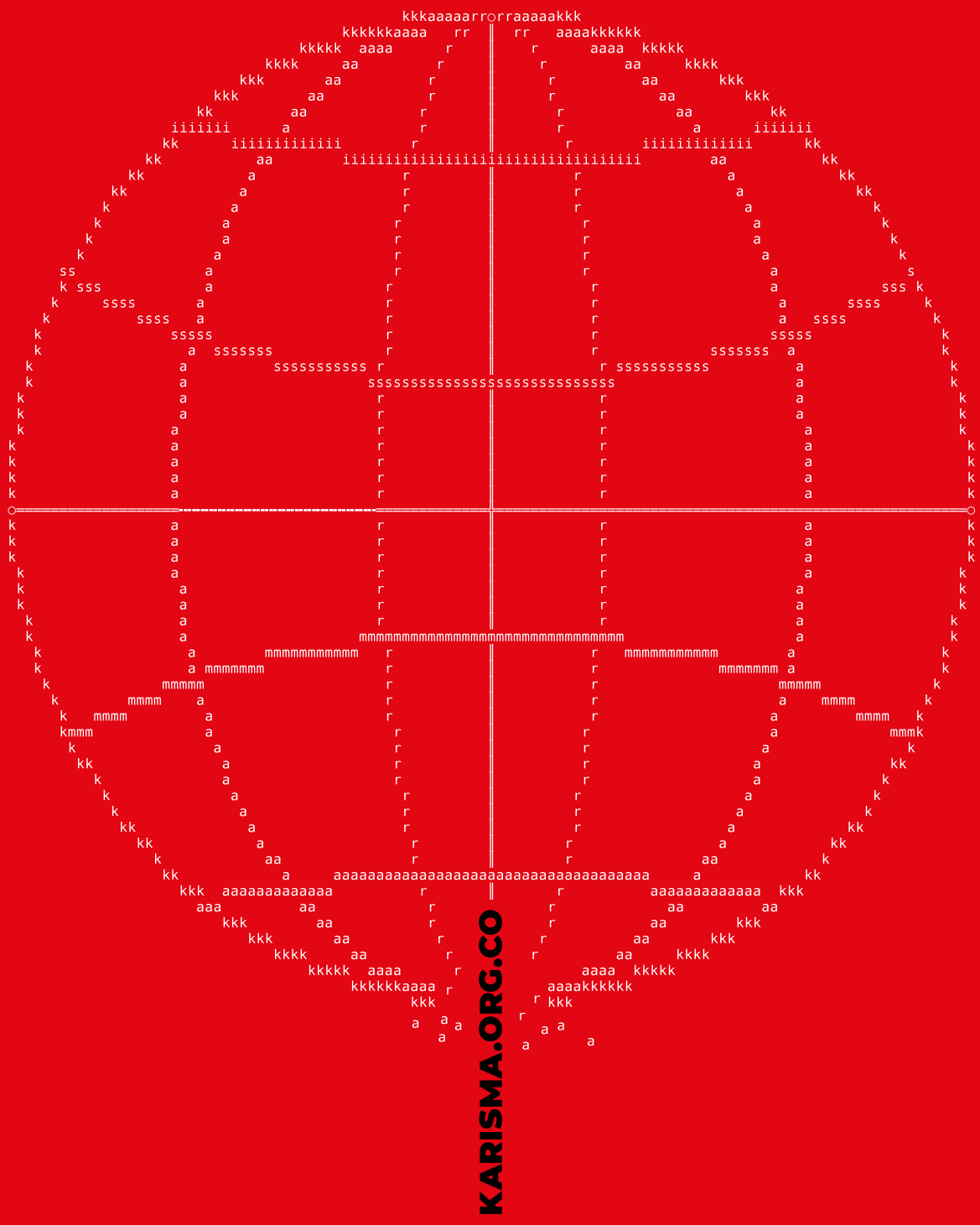
↓

Could the discloser have taken other possible actions? In other words: was the vulnerability immediately reported to the owner of the IT system or did the discloser fail to do so in order to erase his tracks or to manipulate, copy or delete data, for example? If any tracks were erased or data manipulated, copied or deleted, this will not constitute responsible disclosure.

Figure 21: Letter from the Dutch Public Prosecutor's office on responsible disclosure[206]

Fuente: ENISA (2015). *Good practices on vulnerability disclosure*, p 52.

En el documento ***Estudio sobre rutas de divulgación en seguridad digital*** se utilizaron las tipografías **Aleo** de Alessio Laiso y Kevin Conroy (para el cuerpo de texto) y **Raleway** de Matt McInerney (para titulares).


KARISMA.ORG.CO