REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 11 NÚM. 2 (2022) • PÁGS. 183-210 • DOI 10.5354/0719-2584.2021.65502
RECIBIDO: 25/11/2021 • APROBADO: 23/11/2022 • PUBLICADO: 31/12/2021

DOCTRINA

Estándar para activar la obligación de comunicar sobre ciberincidentes relevantes en instituciones públicas

Standard for triggering the obligation to communicate upon significant cyber incidents in public institutions

Clara-Luz Álvarez
Universidad Panamericana, México

RESUMEN Las instituciones públicas sufren constantemente ciberincidentes que pueden afectar la infraestructura crítica y el ejercicio de derechos de la ciudadanía. Informar a esta sobre cada ciberincidente sería impráctico, por lo que se propone un estándar para decidir en qué supuestos un ciberincidente sufrido por una institución pública debe comunicarse a la sociedad, y cómo debe ser la información para colmar el derecho a la información. Para ello se presenta el marco jurídico mexicano de ciberseguridad y de derecho a la información, sustentando la razón de por qué la atribución pública de ciberataques no sustituye al deber de informar a la sociedad. Finalmente, se analizan casos emblemáticos de ciberincidentes en instituciones públicas mexicanas aplicando el estándar propuesto.

PALABRAS CLAVE Ciberseguridad, derecho a la información, ciberincidentes, instituciones públicas, comunicación.

ABSTRACT Public institutions are constantly affected by cyber incidents capable of affecting critical infrastructure and the exercise of citizens' rights. Informing the citizens of every cyber incident would be unfeasible, therefore a standard is proposed to decide in which cases a cyber incident in a public institution must be communicated to society, and how they should be made aware in order to comply with the right to information. For this reason, the Mexican legal framework regarding cybersecurity and the right to information is presented, and thus sustaining the argument against considering public attribution of cyberattacks as a substitute to the obligation to inform society. Finally, emblematic cyber incidents in Mexican public institutions are analyzed according to the proposed standard.

KEYWORDS Cybersecurity, freedom of information, cyber incidents, public institutions, communication.

Introducción

Los ciberataques en América Latina han crecido significativamente en los últimos años (Banco Interamericano de Desarrollo y Organización de los Estados Americanos, 2020), siendo México uno de los países de la región con más ciberataques.[1] Estos afectan de manera permanente a las instituciones y en especial a los gobiernos (Castillo y otros, 2020; Jara y Jorquera, 2021).[2] En el caso de instituciones públicas mexicanas, de enero a junio 2021 el número de ciberataques a la Presidencia de la República fue de más de 78 millones y de más de 128 millones a la empresa estatal Petróleos Mexicanos.[3]

Si bien los ciberataques pueden producir diversas afectaciones,[4] también existen otros ciberincidentes de origen distinto al ciberataque. Para efectos de este artículo, los ciberincidentes son aquellos que causan interrupción, acceso no autorizado o cualquier falla que afecte a las redes, servicios, equipos e instalaciones asociados o vinculados a activos de tecnologías de la información y comunicaciones, pudiendo o no tener un origen en un ciberataque.[5]

El objetivo de este artículo es proponer un estándar para decidir en qué supuestos un ciberincidente sufrido por una institución pública debe comunicarse a la sociedad, e identificar si se colmó el derecho a la información tras un ciberincidente relevante con información oportuna, completa, comprensible y actualizándose la información según se vaya obteniendo. La hipótesis de la investigación que da origen a este artículo es que en ciberincidentes relevantes a instituciones públicas mexicanas

1. México sufre 299 ciberataques por segundo. Véase Hernan Diazgranados, «Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021», *Kaspersky Daily*, 31 de agosto de 2021, disponible en https://bit.ly/3PNxIr2.

2. Refieren Jara y Jorquera (2021) que «por el valor e importancia estratégica de esta información [datos personales en tratamiento por organismos del Estado], es posible especular que el riesgo de ocurrencia de ciberataques es más alto, en tanto dicha información puede ser de gran interés para terceros que deseen acceder a los datos personales tratados por los diferentes organismos públicos».

3. En *El Economista*, disponible en https://bit.ly/3YNDYTP.

4. Las consecuencias de los ciberataques de acuerdo con Jonathan (2020) pueden ser la degradación; la interrupción por pérdida de alguna capacidad cibernética; la corrupción, el cambio de la información, datos, protocolo o software que la inutiliza o la vuelve poco confiable; la usurpación o intrusión en el sistema; la intercepción de información; la exfiltración.

5. El ciberataque es considerado como aquella «acción ofensiva o maliciosa, externa o interna, con la intención de causar un efecto adverso en o a través del Ciberespacio». Disponible en https://bit.ly/3WFW8F9.

existe el deber jurídico de informar a la sociedad, salvo que encuadre en un caso de excepción justificada. Adicionalmente, se analizarán tres casos emblemáticos de ciberincidentes aplicando el estándar propuesto.

En primer lugar, se presenta el marco normativo de la ciberseguridad en México, país que recibió la calificación de 81,68 en el Global Cybersecurity Index.[6] Enseguida se exponen los fundamentos y argumentos jurídicos, doctrinarios y jurisprudenciales para sustentar el derecho a la información de la sociedad (dimensión colectiva), para conocer sobre ciberincidentes relevantes sufridos por instituciones públicas mexicanas.[7]

La siguiente sección es para exponer y destacar el estándar que activará la obligación de las instituciones públicas de comunicar sobre ciberincidentes relevantes, así como los requisitos que debe reunir la información que se proporcione. Con base en dicho estándar, se analizarán tres casos emblemáticos de ciberincidentes a instituciones públicas mexicanas que tuvieron amplia cobertura mediática y son instituciones con objetos muy distintos entre sí.

Finalmente, se presentarán las conclusiones, una recomendación y se perfilarán nuevas líneas de investigación vinculadas a la ciberseguridad y el derecho a la información.

Ciberseguridad y derecho a la información en México: Su marco normativo

Existen múltiples definiciones de lo que debe entenderse por ciberseguridad, además de que el resultado de lo que debe comprenderse por ciberseguridad puede variar según las circunstancias y las personas que la definan (Papakonstantinou, 2022).[8] Para efectos de este artículo, se toma como referencia la definición prevista en el marco del Reglamento sobre la Ciberseguridad de la Unión Europea (UE) que define la ciberseguridad como «todas las actividades necesarias para la protección de las redes y siste-

6. El GCI es elaborado por la Unión Internacional de Telecomunicaciones con base en las respuestas que los Estados miembro dan a 82 preguntas, dentro de cinco pilares, cada uno de veinte puntos máximo. México obtuvo la siguiente puntuación en los pilares: 14,70 sobre las estrategias nacionales y organizaciones que implementan la ciberseguridad (organizacional); 15,61 en medidas legales y de regulación sobre ciberdelitos y ciberseguridad (legal); 16,13 en relación a campañas de concientización, entrenamiento, educación e incentivos para el desarrollo de capacidades en ciberseguridad (desarrollo de capacidades); 17,34 respecto a la cooperación por alianzas entre instituciones, empresas y países (cooperación); 17,90 en la medición de la implementación de capacidades técnicas a través de instituciones nacionales o específicas de sector (técnico). Disponible en https://bit.ly/3I1GIqB.

7. Knight y Nurse (2020) señalan que la decisión de informar sobre un ciberincidente y el momento en que se comunica puede impactar a una institución, aun cuando la admisión de responsabilidad y el trabajar en las debilidades de seguridad pueden contribuir a restaurar la confianza de los consumidores.

8. Papakonstantinou (2022) propone distinguir la ciberseguridad como praxis y como estado (*state*), siendo la primera las medidas y acciones para lograr la ciberseguridad como estado y la ciberseguridad como estado sería la condición de estar protegidos y en un ambiente ciberseguro.

mas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas» (Parlamento Europeo y del Consejo de la Unión Europea, 2019).[9]

El marco normativo mexicano de la ciberseguridad está disperso en leyes, reglamentos, tratados, estrategias y otras disposiciones, siendo algunas genéricas y otras específicas a la seguridad de la información.[10] A continuación se presentan las normas de mayor relevancia para la ciberseguridad en México, para después presentar el fundamento jurídico de la obligación de las instituciones públicas de informar a la ciudadanía cuando los ciberincidentes sean de interés público, así como exponer excepciones a dicha obligación.

Ciberseguridad

La Constitución Política de los Estados Unidos Mexicanos (Constitución Mexicana) establece que la seguridad pública es una función del Estado mexicano en la cual tienen competencia de manera concurrente la Federación, las entidades federativas y los municipios,[11] mientras que la seguridad nacional está a cargo del titular del Poder Ejecutivo federal.[12] Al estar vinculada la ciberseguridad tanto a la seguridad pública como a la seguridad nacional, debe ser atendida por autoridades federales, estatales y municipales con base en sus respectivas competencias.

A nivel federal se han establecido diversos delitos relacionados con la ciberseguridad en el Código Penal Federal, como la modificación, destrucción y pérdida de información sin autorización, en sistemas o equipos informáticos protegidos por algún mecanismo de seguridad, ya sean estos del Estado, de instituciones financieras o de otras personas.[13] También se tipifica como delito cuando una persona provoque una vulneración de seguridad a las bases de datos bajo su custodia que contengan datos personales y lo haga con ánimo de lucro, delito previsto en la Ley Federal de Protección de Datos Personales en Posesión de Particulares.[14]

9. En el «Glosario de términos SEDENA-MARINA en materia de seguridad en el ciberespacio», se define la ciberseguridad como la «capacidad de un Estado-Nación y de todos los actores de la sociedad para generar y aplicar políticas públicas, legislación, normas, procedimientos y controles tecnológicos para la protección de Infraestructuras de Información Esenciales e Infraestructuras Críticas de Información». La crítica a esta definición es que omite referir a la protección a las personas ya sea como usuarios de redes y sistemas, o que pueden ser afectadas con motivo de un ciberincidente.

10. Existen diversas iniciativas de leyes de ciberseguridad en discusión en el Congreso de la Unión de la República Mexicana.

11. La República Mexicana se forma por 32 entidades federativas y 2.471 municipios y 16 demarcaciones territoriales en Ciudad de México. Disponible en https://bit.ly/3VBo8pH.

12. Artículos 21 y 89 fracción VI de la Constitución Mexicana.

13. Artículos 211 bis 1 a 211 bis 7 del Código Penal Federal.

14. Artículos 67 y 68 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares. Disponible en https://bit.ly/3WEf9b2.

Por su parte, la Ley de Seguridad Nacional[15] si bien no habla expresamente de la ciberseguridad ni de acciones encaminadas a procurarla y garantizarla, lo cierto es que múltiples acciones destinadas a la ciberseguridad (por ejemplo, sobre infraestructura crítica) estarían comprendidas dentro de aquellas para la integridad, estabilidad y permanencia del Estado Mexicano enumeradas dentro de la ley.

Las leyes sobre protección de datos personales también cuentan con ciertas normas aplicables a la ciberseguridad que, a pesar de no referir expresamente a esta porque se tratan de disposiciones genéricas, son plenamente aplicables tanto a archivos físicos que contengan datos personales como a sistemas informáticos.[16] Así, los sujetos obligados a la protección de datos personales deben establecer medidas administrativas, técnicas y físicas para la protección de estos, así como informar de vulneraciones a los titulares de los datos cuando dichas vulneraciones afecten significativamente sus derechos patrimoniales o morales.[17] Por lo que si un ciberincidente incluye vulneraciones de seguridad que afecten significativamente dichos derechos, entonces el sujeto obligado a la protección de estos deberá informar a las personas titulares de los datos personales comprometidos.

A nivel tratados internacionales vinculantes para México, está el Tratado entre los Estados Unidos Mexicanos, los Estados Unidos de América y Canadá (T-MEC) (2020) el cual enfoca la ciberseguridad al comercio electrónico y su importancia.[18] Con base en el T-MEC (2020), los países firmantes se obligan a desarrollar capacidades de sus CERT/CSIRT,[19] a fortalecer mecanismos para identificar y mitigar rápi-

15. Disponible en https://bit.ly/3Q2B8Gk.

16. Véase Ley Federal de Protección de Datos Personales en Posesión de los Particulares, disponible en https://bit.ly/3WEf9b2; y Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, disponible en https://bit.ly/3YP4En5.

17. A nivel federal existen 2 leyes que regulan la protección de datos personales, una respecto a particulares (Ley Federal de Protección de Datos Personales en Posesión de Particulares) y otra en relación a sujetos obligados que es un término amplio que abarca a instituciones públicas, partidos políticos, sindicatos, entre otros (Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados). La obligación de informar está prevista en los artículos 20 de la Ley Federal; disponible en https://bit.ly/3WEf9b2; y 40 de la Ley General mencionadas, disponible en https://bit.ly/3YP4En5.

18. Sobre ciberseguridad y tratados de libre comercio, véase Becerril (2019).

19. En la República Mexicana existen 11 CERT, 4 del sector público y 7 del sector privado. (Centro de Ciberseguridad IQSEC, 2021. Disponible en https://bit.ly/3hMKQ37; Gobierno de México-CERT-MX, 2021. Disponible en https://bit.ly/3BXpebh; Gobierno de México-CONACYT, 2021. Disponible en https://bit.ly/3WqXzYj; Global Cybersec, 2021. Disponible en https://bit.ly/3veeiSL; Mnemo, 2021, disponible en https://bit.ly/3jvTZO8; Netrix, 2021, disponible en https://bit.ly/3hNuVBM; Scitum, 2021, disponible en https://bit.ly/3PRIkoJ; TIC Defense, 2021, disponible en https://bit.ly/3juAjKs; TotalSec, 2021, disponible en https://bit.ly/3G1d9Dc; Universidad Autónoma de Chihuahua, 2021, disponible en https://bit.ly/3PTQ1ef; Universidad Nacional Autónoma de México, 2021, disponible en https://bit.ly/3veFArZ).

damente incidentes de ciberseguridad e intercambiar información. Adicionalmente, se obligan a procurar que el sector privado utilice un enfoque basado en riesgos que se estima más efectivo para atender los cambios constantes de las ciberamenazas (T-MEC, 2020: artículo 19.5). Salvo por lo del enfoque basado en riesgos referido, el Tratado Integral Progresista de Asociación Transpacífica establece compromisos similares al T-MEC (CPTPP por sus siglas en inglés) (CPTPP, 2018).

México no ha suscrito el Convenio de Budapest sobre ciberdelincuencia, ni tratados o convenios internacionales que sean específicamente sobre ciberseguridad o ciberdelincuencia (Secretaría de Relaciones Exteriores, 2021).[20]

La Estrategia Nacional de Ciberseguridad establece los objetivos, principios y ejes transversales en relación a la ciberseguridad del Estado mexicano. Dicha estrategia es muy general y se reconoce que es un instrumento vivo que deberá irse actualizando, lo cual no ha sucedido a la fecha. Esta estrategia no refiere a alguna obligación de comunicar a la ciudadanía sobre ciberincidentes relevantes.

Por su parte, la Estrategia Digital Nacional (Oficina de la Presidencia de la República, 2021b) considera a la seguridad de la información como un pilar, para lo cual se emitirán políticas generales sobre seguridad de la información e implementarán un protocolo homologado de gestión de incidentes en la administración pública federal. Derivado de esta estrategia, se encuentra también un acuerdo que buscará emitir políticas y disposiciones sobre seguridad de la información (Oficina de la Presidencia de la República, 2021a). Si bien en este acuerdo se establece la obligación de proveedores del gobierno federal de comunicar posibles incidentes de seguridad, ni la Estrategia Digital Nacional ni el acuerdo refieren a la comunicación a la sociedad sobre ciberataques.

El marco normativo de ciberseguridad en México no aborda expresamente una obligación de las instituciones públicas para comunicar a la ciudadanía cuando haya sucedido un ciberincidente. En consecuencia, el fundamento para la existencia de dicha obligación está en el derecho a la información según se expone enseguida.

Derecho a la información en ciberincidentes

El derecho a la información es un derecho humano que comprende el derecho a recibir informaciones e ideas de toda índole por cualquier medio, estando reconocido en la Constitución, la Convención Americana de los Derechos Humanos (artículo 13) y el Pacto Internacional de los Derechos Civiles y Políticos (artículo 19).

El derecho a la información «es el derecho de todo habitante a ser informado; y

20. Secretaría de Relaciones Exteriores (2021). Respuesta de la Consejería Jurídica (CJA) a la solicitud de información con número de folio 0000500214121, 20 de septiembre de 2021, Plataforma Nacional de Transparencia.

precisamente informado por el Estado, fuente de esas noticias que tienen derecho a conocer las personas» (Castro, 1977, citado en Villanueva, 2008: 110-111), siendo la información un bien público, base para la democracia (Carbonell, 2019) y para el ejercicio de los derechos fundamentales de las personas (Filipini, 2021).

El derecho a la información hace posible también que se pueda exigir una debida rendición de cuentas de las autoridades con la posibilidad de contar con elementos para denunciar infracciones al marco jurídico (Brizio, 2008; Filipini, 2021), es decir, el derecho a la información se erige además como un instrumento para la rendición de cuentas. De ahí que la Corte Interamericana de Derechos Humanos (2006: párrafo 86) en el caso *Claude Reyes y otros con Chile* resolviera que:

> el actuar del Estado debe encontrarse regido por los principios de publicidad y transparencia en la gestión pública, lo que hace posible que las personas que se encuentran bajo su jurisdicción ejerzan el control democrático de las gestiones estatales, de forma tal que puedan cuestionar, indagar y considerar si se está dando un adecuado cumplimiento de las funciones públicas.[21]

Así, el derecho a la información comprende:

> a) el derecho a atraerse de información,
> b) el derecho a informar, y
> c) el derecho a ser informado
> […] 1. El derecho a ser informado incluye las facultades de i) recibir información objetiva y oportuna, ii) la cual debe ser completa, es decir, el derecho a enterarse de todas las noticias y, iii) con carácter universal, o sea, que la información es para todas las personas sin exclusión de alguna (Villanueva, 2008: 112)

La Constitución Mexicana establece en su artículo sexto:

> El derecho a la información será garantizado por el Estado.
> Toda persona tiene derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión.
> El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios.[22]

Con base en dicho precepto y en lo que interesa a esta investigación, el Estado

21. Corte Interamericana de Derechos Humanos, sentencia del caso *Claude Reyes y otros con Chile* (Fondo, Reparaciones y Costas), 19 de septiembre de 2006, disponible en https://bit.ly/3YIOdZu.

22. Para más información sobre este derecho y lo que comprende, véase Álvarez (2018): 59-61.

mexicano está obligado a garantizar el derecho a la información,[23] a que las personas tengan acceso de manera oportuna a información plural y a que accedan a las tecnologías de la información y comunicaciones y al internet.

Debe decirse que, en el caso mexicano respecto al derecho de acceso a la información pública y a las obligaciones de transparencia de los entes públicos, existe una ley general, una ley federal y leyes en cada una de las 32 entidades federativas. Dichas leyes regulan los procedimientos para que las personas puedan obtener documentos e información en archivos e información del quehacer de los entes públicos.[24]

Tanto en la ley general como en la ley federal se establece una obligación expresa de los sujetos obligados (por ejemplo, entidades públicas) de difundir proactivamente información de interés público,[25] es decir, sin que medie una solicitud de los gobernados.

Adicionalmente, la Suprema Corte de Justicia de la Nación, SCJN, ha desarrollado más la obligación del Estado de infomar de cuestiones que inciden en la vida o en el ejercicio de los derechos de los gobernados, sin necesidad de que exista una solicitud de un particular (Suprema Corte de Justicia de la Nación, 2016b; Suprema Corte de Justicia de la Nación, 2016c). La dimensión colectiva del derecho a la información «constituye el pilar esencial sobre el cual se erige todo Estado democrático, así como la condición fundamental para el progreso social e individual» (Suprema Corte de Justicia de la Nación, 2016a), para el ejercicio y control democrático del poder (Suprema Corte de Justicia de la Nación, 2020) lo cual «privilegia la transparencia, la buena gestión pública y el ejercicio de los derechos constitucionales en un sistema participativo, sin las cuales no podrían funcionar las sociedades modernas y democráticas»(Suprema Corte de Justicia de la Nación, 2016a). La información que está obligado el Estado a dar es aquella de interés o relevancia pública que se refiere a temas de trascendencia social o en el sistema económico, por las personas de impacto público o social involucradas, así como otras relevantes para la sociedad y el desarrollo democrático (Suprema Corte de Justicia de la Nación, 2018).

---

23. Villanueva (2008) afirma que el derecho a la información es el género, el derecho de acceso a la información pública es una especie y la transparencia es la garantía para el derecho de acceso a la información pública.

24. «Como resultado de la reforma constitucional de 2014 [sobre derecho a la información], se promulgó la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP, 2015), que estandarizó los principios, causales de clasificación, procedimientos, plazos, instancias y medios de impugnación a nivel nacional, además de sentar las bases para la construcción de un Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales. Un año más tarde, se publicó la nueva Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP, 2016) que abrogó al ordenamiento federal de 2002» (San Martín, 2020: 29).

25. Artículo 24 fracción II en relación con artículo 3 fracción XII de la Ley General de Transparencia y Acceso a la Información Pública, disponible en https://bit.ly/3WpUiZo; y artículo 11 fracción XII de la Ley Federal de Transparencia y Acceso a la Información Pública, disponible en https://bit.ly/3YLNIOl.

En cuanto al derecho de acceso a la información pública, para solicitarla en México, se encuentra la Plataforma Nacional de Transparencia, PNT, la cual permite que cualquier persona por internet pueda solicitar y obtener documentos e información pública de autoridades federales y de las 32 entidades federativas que conforman la República Mexicana, así como presentar recursos contra negativas de acceso a dichos documentos e información, y obtener la resolución definitiva de los órganos garantes (por ejemplo, a nivel federal del Instituto Nacional de Transparencia, Acceso a la Información y Datos Personales, INAI).[26]

No obstante, la disponibilidad de la PNT para acceder a información pública, en el caso de ciberincidentes de interés público, lo que procede es que las instituciones públicas directamente y sin que medie solicitud alguna, informen del mismo de manera oportuna, completa y comprensible con fundamento en el derecho a la información como derecho a saber.[27] De lo contrario puede desnaturalizar el derecho a saber en especial porque si la ciudadanía no sabe del ciberincidente, ¿cómo podrá ejercer su derecho de acceso a la información? Si posterior a conocerse el ciberataque, una persona desea ejercer su derecho de acceso a la información, está bien, pero un prerrequisito para ejercer dicho derecho es que tenga conocimiento oportuno de que ocurrió el incidente. Debe recordarse que esto es independiente del derecho que tiene el titular de datos personales de ser informado en caso de que estos hubieren sido comprometidos.

El derecho a saber busca dar a conocer información que permita ejercer otros derechos, como lo sostiene San Martín (2020) en relación al derecho a un medio ambiente sano, ya que se requiere tener información en la materia para conocer las acciones u omisiones que ha realizado el Estado para garantizarlo. Lo mismo es aplicable para casos de ciberseguridad donde, conforme al derecho a la información en su vertiente de derecho a saber, existe un deber de la institución pública afectada de proveer información a la sociedad.

En específico en cuanto a ciberseguridad, la Relatoría Especial para la Libertad de Expresión ha enfatizado el deber de las autoridades de informar de los lineamientos generales de políticas de ciberseguridad, de las autoridades a cargo y sus responsabilidades (Comisión Interamericana de Derechos Humanos, 2013: 126-127). Asimismo, puntualizó que las autoridades deben rendir cuentas también de las medidas de ciberseguridad y de los ataques y riesgos, sin tener que revelar información que

26. Disponible en https://bit.ly/2SrtqHX.

27. Esto tendría sustento jurídico en los artículos sexto, párrafos primero, segundo y tercero de la Constitución, 19 del Pacto Internacional de los Derechos Civiles y Políticos, 13 de la Convención Americana de Derechos Humanos, 24 fracción II en relación con el 3 fracción XII de la Ley General de Transparencia y Acceso a la Información Pública y 11 fracción XII de la Ley Federal de Transparencia y Acceso a la Información Pública.

arriesgue los programas de ciberseguridad (Comisión Interamericana de Derechos Humanos, 2013: 126-127).

Todas las instituciones por más precavidas y diligentes que sean son objeto de ciberataques y también de sufrir ciberincidentes, sin embargo, lo importante en una democracia es que la sociedad cuente con la información suficiente para saber si hubo o no alguna acción u omisión de la autoridad que propiciara ese ciberataque o ciberincidente. Para una debida rendición de cuentas es importante que la ciudadanía conozca del ciberincidente con la finalidad de estar en posibilidad de vigilar el cumplimiento a las normas y estándares, para, en su caso, fincar responsabilidades a servidores públicos que hayan incumplido sus deberes. Jara y Jorquera (2021) proponen que el estándar aplicable a las medidas de ciberseguridad de instituciones públicas debe ser aquel de la industria informática que puede variar según la actividad de la institución, su relevancia estratégica, información almacenada, tratada y el volumen de la misma.

Por tanto, en un ciberincidente relevante será importante saber si lo ocasionó un error humano involuntario, si existió negligencia o si se padeció independientemente de las medidas de seguridad razonables que se tenían; si se contaba con un programa de ciberseguridad y protocolos para la atención en casos de vulneraciones a la seguridad de la información o de los sistemas; si las señales del sistema de alerta se atendieron con la debida diligencia; si el ciberincidente pudo evitarse con la actualización del software o con otro medio; si el presupuesto asignado para ciberseguridad ha sido suficiente o no; etcétera.

Estándar para activar la obligación de comunicar sobre ciberincidentes relevantes

Mientras la labor fundamental de los profesionales en ciberseguridad es prevenir ese tipo de [ciber]ataques, ningún sistema es totalmente seguro, así que es importante que si una vulneración ocurre, las organizaciones puedan responder adecuadamente. […] Las maneras de afrontar la comunicación después de un incidente de ciberseguridad se han, por tanto, convertido en un área importante de investigación y práctica» (Knight y Nurse, 2020: 1-2).[28]

La comunicación es una de las categorías previstas dentro de las funciones de Responder y Recuperar del Marco para la mejora de la seguridad cibernética en infraestructuras críticas del Instituto Nacional de Estándares y Tecnología de EUA, NIST

28. «Whilst it is a key task of cyber security professionals to prevent such attacks, no system is totally secure, so it is important that if a breach occurs organisations respond appropriately. […] The approaches for communication following a cyber security incident have, therefore, become an important area of research and practice» (Knight y Nurse, 2020: 1-2, traducción de la autora de este artículo).

(en adelante referido como el Marco de Ciberseguridad NIST) (National Institute of Standards and Technology, 2018).[29] Si bien dicho marco es una guía y no una lista de comprobación, lo cierto es que refleja actividades y acciones a realizar para un mejor manejo de los riesgos de ciberseguridad los cuales deben personalizarse a la institución o empresa de que se trate (National Institute of Standards and Technology, 2018).

En la función de Responder a un ciberincidente, junto con la implementación del plan de respuesta, la realización de actividades para mitigar los daños y para mejoras en ciberseguridad, debe realizarse la comunicación relevante con el personal y otras partes interesadas (por ejemplo, autoridades, empleados, consejo de administración). En la función de Recuperación, la comunicación tiene un lugar importante que debe llevarse a cabo en paralelo con los planes de recuperación y la incorporación de mejoras con base en las lecciones aprendidas tras el incidente (National Institute of Standards and Technology, 2018).

Cuando un ciberincidente afecta a instituciones o bienes públicos, en este artículo se sustenta que con base tanto en el derecho a la información expuesto anteriormente como en lo sugerido por el Marco de Ciberseguridad del NIST, las instituciones públicas deben informar en los siguientes supuestos y de la siguiente manera.

Supuestos

Las instituciones están siendo ciberatacadas de manera permanente y en especial los gobiernos son los más ciberatacados (Castillo y otros, 2020; Jara y Jorquera, 2021).[30] Además, existen múltiples causas de ciberincidentes que las afectan, por lo que sería impráctico e indeseable inundar a la sociedad con información de todos y cada uno de los ciberincidentes a instituciones públicas. Adicionalmente, pueden existir consideraciones de seguridad nacional y orden público que justifiquen la no divulgación de ciberincidentes como se verá más adelante.

El nivel de criticidad de un ciberincidente puede establecerse con base en diferentes criterios. En el caso de México, se ha establecido el Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos[31] dentro del cual se contempla una tabla que determina el nivel de criticidad (crítico, muy alto, alto, medio y bajo) con base en

29. Las funciones del Marco de Ciberseguridad del NIST son: Identificar, Prevenir, Detectar, Responder y Recuperar. Cada una de estas funciones, tiene categorías y subcategorías (National Institute of Standards and Technology, 2018).

30. Refieren Jara y Jorquera (2021) que «por el valor e importancia estratégica de esta información [datos personales en tratamiento por organismos del Estado], es posible especular que el riesgo de ocurrencia de ciberataques es más alto, en tanto dicha información puede ser de gran interés para terceros que deseen acceder a los datos personales tratados por los diferentes organismos públicos».

31. El Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos establece la obligación de informar al CERT-MX sobre ciberincidentes, mas no de informar a la sociedad de los mismos.

el tipo de ataque (por ejemplo, ataque multivector, código dañino, intrusión) o afectación (por ejemplo, compromiso de la información, disponibilidad de esta) y el tipo de incidente (por ejemplo, amenazas persistentes avanzadas o APT, distribución de malware, denegación de servicio) (Secretaría de Seguridad y Protección Ciudadana, 2021, Anexo 8).

Adicional al nivel de criticidad del ciberincidente, es relevante establecer cuál es el nivel de gravedad e impacto que tiene. Dentro del propio Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos (Secretaría de Seguridad y Protección Ciudadana, 2021, Anexo 9) se describen los impactos que puede tener un ciberincidente. Se listan a continuación algunos ejemplos de los niveles e impactos descritos en el Anexo 9 del Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos (2021):

- Nivel crítico: afecta seguridad nacional; afecta la seguridad ciudadana con potencial peligro para la vida; afecta infraestructura crítica; afecta a más del 90% de los sistemas de la organización; interrupción en la prestación del servicio superior a 24 horas y superior al 50% de los usuarios; extensión geográfica nacional; daños reputacionales muy elevados y cobertura en medios internacionales.
- Nivel muy alto: afecta apreciablemente actividades oficiales en el extranjero; afecta un servicio esencial; afecta más del 75% de los sistemas de una organización; interrupción en la prestación del servicio superior a 8 horas y superior al 35% de los usuarios; extensión geográfica superior a 4 inmuebles o 4 estados de la República Mexicana; daños reputacionales muy elevados y cobertura en medios nacionales.
- Nivel alto: afecta a más del 20% de los sistemas de la organización; interrupción del servicio superior a una hora y superior al 10% de usuarios; extensión geográfica superior a 3 inmuebles o 3 estados de la República Mexicana; daños reputacionales de difícil reparación.
- Nivel medio: interrupción de servicios superior a 5% de usuarios; extensión geográfica superior a 2 inmuebles o 2 estados de la República Mexicana; resolución del ciberincidente entre 1 y 5 días hábiles.
- Nivel bajo: interrupción de la prestación de un servicio; extensión geográfica de 1 inmueble; resolución del ciberincidente en menos de 1 día hábil.

Las tablas de criticidad y de nivel de impacto pueden ser criterios orientadores para determinar cuándo la sociedad tiene derecho a conocer de un ciberincidente. No obstante lo anterior, debe precisarse que un ciberincidente puede ser de criticidad alta y de nivel de impacto muy alto, pero por consideraciones de seguridad nacional

se debe reservar la información como se explica más adelante en Excepciones. Por el contrario, un ciberincidente de criticidad alta (por ejemplo, denegación de servicio) con un nivel de impacto medio (por ejemplo, interrupción de servicios a la ciudadanía por 5 días hábiles), amerita que sea informado a la ciudadanía.

Si bien la activación de la obligación de instituciones públicas de informar deberá evaluarse caso por caso, los supuestos para activar la obligación de las instituciones públicas de informar sobre un ciberincidente serán cuando este:

- afecte de manera importante a una institución pública que sea considerada una de infraestructura de información esencial o infraestructura crítica,[32] que preste servicios públicos, que sea necesaria para el ejercicio de derechos o el cumplimiento de obligaciones;
- pueda llevar a obstaculizar labores de seguridad nacional, seguridad pública, procuración de justicia, combate al crimen y a la corrupción, y otras actividades gubernamentales de trascendencia;
- sea respecto de información que pueda manipularse para desinformar a la sociedad, minar la confianza en las instituciones o socavar la democracia;
- se haya dado a conocer ampliamente en medios de comunicación o redes sociodigitales; o
- se hayan vulnerado o afectado datos personales.

A estos supuestos de ciberincidentes se les denominará «Ciberincidentes Relevantes».

Información oportuna y actualización

En caso de un ciberincidente relevante debe la institución pública víctima proveer información de manera oportuna e ir actualizando la información según vaya siendo disponible, sin necesidad de que medie una solicitud de información. Esto debe ser independiente de las obligaciones específicas de informar a otras autoridades (por ejemplo, autoridades financieras, fiscalías encargadas de la investigación de crímenes, autoridades de protección de datos) y a terceros (por ejemplo, titulares de datos

32. La Secretaría de la Defensa Nacional define como infraestructura de información esencial a aquella formada por «redes, servicios, equipos e instalaciones asociados o vinculados con activos de TIC y de Tecnologías de Operación (TO), cuya afectación, interrupción o destrucción, tendrían un impacto en el individuo u organismos públicos o privados», mientras que la infraestructura crítica de información es aquella infraestructura de información esencial relacionada con bienes y servicios esenciales que puedan comprometer la seguridad pública o nacional (Secretaría de Marina y Secretaría de la Defensa Nacional, 2021).

personales cuando estos hayan sido comprometidos, proveedores, clientes, consejo de administración).

La comunicación de un ciberincidente relevante no debe basarse en especulación ni en valoraciones subjetivas, sino que debe realizarse con información veraz (Suprema Corte de Justicia de la Nación, 2016d), es decir, con información que sea una certera aproximación a la realidad en el momento en que se difunde, aun cuando por el transcurso del tiempo sea desmentida o no pueda ser demostrada debido a la importancia y trascendencia que representa en ese momento (Suprema Corte de Justicia de la Nación, 2016d).

Es posible y probable que al detectarse el ciberincidente la información sea escasa, lo cual no debe ser impedimento para difundir la información con que se cuente en ese momento. Asimismo, debe actualizarse con nueva información y acciones que se estén realizando, por ejemplo.

Esto es importante pues un ciberataque es posible que se detecte tiempo después de que inició o que sea un ataque del día cero[33] (López, 2020); puede ser que al detectarse no se sepa con exactitud qué tipo de ataque es, qué sistemas y qué datos estén comprometidos; ni saber cuál es el alcance del ciberataque; qué acciones se tienen que emprender para detenerlo, para restaurar los sistemas/información y recuperar lo que haya sido destruido/robado. Así, proveer información a la sociedad de un ciberincidente relevante obliga a actualizarla, porque probablemente un comunicado inicial tras conocer el ciberincidente sea insuficiente para colmar el derecho a la información de la sociedad sobre la magnitud del ciberincidente y sus repercusiones.

Información completa y comprensible

La información debe ser completa y comprensible[34] sobre lo que está pasando que incluye el tipo, tamaño y escala del ciberincidente relevante, cómo está afectando o puede afectar tanto a la institución como a la sociedad en general o a cierto grupo en particular.

Cada ciberincidente es diferente en su tipo (por ejemplo, *ransomware*, denegación de servicio), tamaño (por ejemplo, focalizado en una aplicación de un servicio de una institución, afectando todos los sistemas de una institución, impidiendo el acceso al sitio web) y escala (por ejemplo, local, nacional, regional, mundial). Puede afectar únicamente a la institución en su operación o por el contrario puede estar perturbando una cadena de suministro de bienes o servicios esenciales (por ejemplo, el caso Colonial Pipeline).

33. Disponible en https://bit.ly/3HYKEs3.

34. Artículo 2 fracción VII de la Ley General de Transparencia y Acceso a la Información Pública. Disponible en https://bit.ly/3WpUiZo.

Un ciberincidente puede o no comprometer datos personales. Si hubiera datos personales vulnerados o en riesgo, independientemente de la comunicación del ciberincidente relevante, deberá notificarse a los titulares de datos personales de la vulneración.

Por tanto la comunicación de un ciberincidente relevante sufrido por una institución pública debe ser completa y comprensible (lenguaje sencillo) en formatos accesibles para personas con discapacidad, de tal manera que habilite a las personas para la adopción de las medidas necesarias para protegerse o responder a los riesgos creados y que les afecten.

Grupos de interés

A cada grupo de interés debe comunicársele la información que necesite, de manera accesible y comprensible.

Un mismo ciberincidente relevante puede acarrear distintas consecuencias a distintos grupos (por ejemplo, empleados, ciudadanos, proveedores), pudiendo tener cada uno de estos diferentes necesidades (por ejemplo, saber cómo continuarán trabajando, qué hacer para ejercer sus derechos o reducir riesgos ulteriores por la captura de datos personales por delincuentes) y con diferentes grados de sofisticación (por ejemplo, la información a la sociedad en general diferirá de aquella proporcionada a los CERT).

Excepciones

En casos que pueda comprometerse la seguridad nacional y en algunos de orden público, informar de un ciberincidente relevante puede no ser obligatorio. Recuérdese que una excepción al derecho de acceder a información pública esta relacionado con asuntos de seguridad nacional o que pudieren afectar significativamente el interés público.[35]

En casos de seguridad nacional las autoridades deben hacer una ponderación de las consecuencias tanto de informar como de no informar. En ciertos casos, proveer información a la ciudadanía sobre un ciberincidente relevante de seguridad nacional puede ocasionar pánico en la sociedad y sin la posibilidad que esta actúe para miti-

35. Artículos 4 párrafo segundo, 104 y 113 fracción I de la Ley General de Transparencia y Acceso a la Información Pública. Incluso cuando el órgano garante (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, INAI) ordena a una autoridad federal dar acceso a información que fue clasificada como reservada por razones de seguridad nacional, la ley prevé un recurso extraordinario para una evaluación inmediata por parte de la Suprema Corte de Justicia de la Nación (v**éase** artículos 189 y siguientes de la Ley General de Transparencia y Acceso a la Información Pública). Disponible en https://bit.ly/3WpUiZo.

garlo; en otros casos no informar puede dar lugar a un vacío de información que sería llenado con especulaciones, informaciones inexactas o con propósitos de desestabilización, por ejemplo.[36]

Ciberataque EMA e información difundida

Para ilustrar la obligación de informar de un ciberincidente, se tomará el caso del ciberataque a la European Medicines Agency, EMA, de la Unión Europea de 2020.

EMA es la autoridad encargada de revisar y autorizar medicinas y vacunas, por lo que sobra decir de su importancia en plena pandemia del Covid-19. Las comunicaciones de EMA se sintetizan a continuación:

- 9 de diciembre de 2020: EMA al tener conocimiento del ciberataque, informó que había sufrido un ciberataque y que había iniciado la investigación con las autoridades.[37]
- 11 de diciembre de 2020: EMA informó que se había accedido ilegalmente a un número limitado de documentos de terceros a los cuales ya se les había informado[38] y que EMA seguía funcionando, sin que la evaluación de vacunas del Covid-19 estuviere afectada.[39]
- 18 de diciembre de 2020: EMA informó sobre la contratación a un proveedor especializado para realizar la investigación en conjunto con las autoridades y dar medidas de seguridad adicional.[40]
- 22 de diciembre de 2020: EMA informó que el ataque se limitó a una aplicación de la tecnología de la información y el foco del ataque fue información sobre medicinas y vacunas de Covid-19.[41]

36. Válgase el siguiente ejemplo por analogía. Al desatarse la pandemia de SARS-COV-2 en 2020, las autoridades fueron difundiendo información que en algunos casos generó alerta y pánico en la sociedad. Sin embargo, era indispensable que la sociedad supiera lo que estaba sucediendo para que también tomara cada persona las medidas necesarias para proteger la salud propia y de los demás. Caso distinto sería un ciberincidente relevante en materia de seguridad nacional en el cual difundir la información pudiera generar pánico, sin que los individuos pudieran realizar algo para contenerlo o remediarlo. En estos casos no debe haber obligación para informar del ciberincidente relevante al momento de ser detectado, ni al estar en el proceso de Responder y Recuperar con base en el Marco de Ciberseguridad NIST. Posteriormente, al desaparecer la razón que llevó a no informar, debe comunicarse lo sucedido a la ciudadanía en cumplimiento al derecho a la información de esta.

37. Disponible en https://bit.ly/3YLuMiQ.

38. Ejemplo de ello es BioNTech y Pfizer que fueron informadas dado que su vacuna estaba en un procedimiento regulatorio ante la EMA. Disponible en https://bit.ly/3Vnxacu.

39. Disponible en https://bit.ly/3WEkeQz.

40. Disponible en https://bit.ly/3I3Pgop.

41. Disponible en https://bit.ly/3hQbg42.

- 12 de enero de 2021: EMA informó que algunos de los documentos sujetos del ataque fueron filtrados en el internet y estaba apoyando la investigación criminal.[42]
- 15 de enero de 2021: EMA informó que la información filtrada incluyó correos electrónicos internos/confidenciales relacionados con el proceso de las vacunas contra Covid-19, así como que alguna de esa información fue manipulada de tal manera que puede afectar la credibilidad en vacunas.[43]

Las anteriores comunicaciones destinadas al público en general muestra cómo se mantuvo a la sociedad informada de manera oportuna, con lenguaje comprensible y actualizándose la información, según iba existiendo. Al inicio solo se avisó del ataque, después se fue precisando en qué consistió y a qué afectó, además de informar sobre la continuidad en la operación de EMA y lo relacionado a las vacunas contra el Covid-19. Los comunicados referidos fueron independientes de aquellas comunicaciones de la EMA con otras autoridades y terceros (por ejemplo, Pfizer-BioNTech), que tendrían sus particularidades según a quienes fueran dirigidas.

Atribución pública, no sustituye el deber de informar

Ahora bien, antes de pasar al análisis de los casos de autoridades mexicanas en la sección siguiente, vale la pena referir a la atribución pública de un ciberataque que ha sido materia de diversos artículos científicos (por ejemplo, Egloff y Menger, 2019; Egloff y Smeets, 2021; Finnemore and Hollis, 2020) y mostrar por qué la atribución pública no puede sustituir a la comunicación de que una institución ha sido víctima de un ciberataque que, como se argumenta en este artículo, es una obligación de las autoridades públicas.

«Definimos la atribución pública como el acto de revelar información sobre la ciberactividad maliciosa [atribuyéndola] a una máquina, perpetrador específico y/o adversario que es en última instancia el responsable» (Egloff y Smeets, 2021: 3). La atribución pública se estima como una medida para favorecer un ciberespacio más estable, la cual es considerada para Holanda como un aspecto medular en su estrategia de ciberdefensa (Egloff y Smeets, 2021). Si la imputación de un ciberataque puede realizarse respecto de un Estado nación, entonces se regirá por el Derecho Internacional (Cocchini, 2021).

¿Puede la atribución pública tomarse como una manera de cumplir con el derecho a saber de la ciudadanía respecto a un ciberataque? No, porque la atribución tiene finalidades diversas como desincentivar los ciberataques mediante la exhibición

42. Disponible en https://bit.ly/3YS1lvx.
43. Disponible en https://bit.ly/3jsmjAT.

pública de quién los realiza o para legitimar y generar confianza de quién realiza la atribución, entre otros (Egloff y Smeets, 2021). La atribución pública puede tomar tiempo para que se pueda realizar, dada la dificultad para identificar con precisión a quienes están detrás de un ciberataque y porque los ciberataques pueden realizarse desde distintos países (Cocchini, 2021). Asimismo, es común que quienes sufren un ciberataque provean información días después de que sucede, con la intención de dar aviso una vez que la situación está bajo control y para evitar afectaciones a su reputación (Mañas-Viniegra y otros, 2019; Cano y Almanza, 2020). Por lo anterior considero que el derecho a saber no se vería colmado con la atribución pública por razón de la oportunidad con que debe realizarse el informe de un ciberataque y por poder diferir en sus finalidades.

Ciberincidentes relevantes en México y el deber de informar: Análisis de casos

El gobierno de México recibe decenas de millones de ciberataques por año (Rodríguez y Molina, 2021), de los cuales muy pocos han salido a la luz pública. Para el análisis de casos de Ciberincidentes Relevantes a instituciones públicas mexicanas, se seleccionaron tres casos emblemáticos dada la cobertura mediática que recibieron y por ser instituciones con objetos importantes muy diferentes entre sí.

La primera institución es Petróleos Mexicanos, Pemex, que es una empresa del Estado mexicano dedicada a hidrocarburos de relevancia histórica y económica, la cual se considera la empresa más grande de México.[44] La segunda institución es la Secretaría de la Función Pública (SFP) con funciones de contraloría, supervisando a los servidores públicos federales e imponiéndoles sanciones cuando incumplen el marco jurídico, así como a cargo de las políticas de compras públicas. La SFP tiene a su cargo el registro de las declaraciones patrimoniales y de interés de los servidores públicos federales.[45] La tercera institución es la Lotería Nacional (Lotenal) que tiene sus orígenes cuando lo que hoy es México era la colonia española de la Nueva España y que, hasta la fecha, realiza sorteos para recaudar fondos para fines de beneficencia, siendo una institución reconocida por todos los estratos socioeconómicos.[46]

Enseguida se presentan las respuestas que tuvo cada institución en relación a los Ciberincidentes Relevantes en cuanto a informar a la ciudadanía, a partir de la información difundida por las propias instituciones, por los medios de comunicación y la información solicitada a las autoridades a través de la PNT. Después de cada tabla se expone el análisis para evaluar el nivel de cumplimiento del estándar relativo al

44. Disponible en https://bit.ly/3QohY3T.

45. Artículo 37 de la Ley Orgánica de la Administración Pública Federal. Disponible en https://bit.ly/3YLCUzR.

46. Disponible en https://bit.ly/3vm91IO.

derecho a saber del ciberincidente relevante con base en si la información fue dada a conocer de manera oportuna, si se actualizó, si fue completa y comprensible, y si se enfocó a cada grupo de interés o no.

Como se ve en la **tabla 1**, Pemex en sus comunicados evitó reconocer que fue sujeta a un ciberataque. Tampoco informó de que se trató de un *ransomware*, a pesar de que eso había trascendido ampliamente, se había señalado incluso el monto del rescate solicitado.[47] Además, la Secretaria de Energía había confirmado que Pemex había sufrido un ciberataque y que no se pagaría el rescate para recuperar la información.[48]

Cuando había sido ciberatacado, Pemex informó a sus empleados de la suspensión de servicios diciendo que era por una actualización a la plataforma de seguridad informática, mas sin reconocer el ciberataque ni informar las medidas que debían tomar en cuenta los empleados para la seguridad y la continuidad laboral. Las comunicaciones posteriores con empleados de Pemex tampoco refieren al ciberataque sino que versan sobre cultura de seguridad de la información.[49]

Con base en lo anterior se concluye que Pemex aunque informó de manera oportuna (al día siguiente de tener conocimiento del ciberataque) y con un lenguaje comprensible, no lo hizo de manera completa (nunca manifestó que fue un ciberataque) y tampoco actualizó la información conforme la iba recabando. Aun cuando sí informó a sus empleados como un grupo de interés, omitió información sobre lo que realmente estaba sucediendo e información que pudo haber sido importante como la manera en que los empleados podrían protegerse y proteger su información, por ejemplo.

En la **tabla 2** se muestra que la SFP no comunicó oportunamente, ni actualizó la información. Lejos de ser una comunicación completa y comprensible, la información resultó contradictoria por lo siguiente: si, como dijo la SFP, se trató de un acceso alternativo a información pública, ¿por qué tuvo que bloquear dicho acceso? Cuando es información pública, la sociedad se beneficia con la mayor disponibilidad de información y a través de más maneras de acceder. Otra pregunta que surge es, ¿cuál es el ilícito que dijo la SFP que investigaría para deslindar responsabilidades si solo era un acceso alternativo a información pública? Con base en el Código Penal Federal el acceder a información pública a través de un buscador no es un delito, tampoco sería una falta administrativa.

La comunicación que realizó al público en general no fue del todo comprensible al señalar que no se habían «vulnerado los datos» de las declaraciones patrimoniales y de intereses, pues eso admite varias interpretaciones como el que los datos de las declaraciones eran los mismos que antes del ciberataque, que no habían sido alterados,

47. En *El Economista*, disponible en https://bit.ly/3YLyvge.
48. En *El Economista*, disponible en https://bit.ly/3vcoRmb.
49. Disponible en https://bit.ly/3I2rYI7.

Tabla 1. Ciberincidente de Petróleos Mexicanos (noviembre de 2019)

Petróleos Mexicanos (Pemex)	
Importancia de la institución pública	Pemex es una empresa del Estado mexicano encargada de la cadena productiva de hidrocarburos desde la exploración, producción, transformación industrial y logística, hasta la comercialización.
Fecha del ciberataque	10 de noviembre de 2019.
Tipo de ciberataque	Ransomware.
Relevancia del ciberincidente	Pemex es una empresa del Estado que forma parte de la infreastrucruta crítica de la República Mexicana. Además, el ciberataque trascendió ampliamente en medios de comunicación.
Cuándo tuvo la institución conocimiento del ciberataque	10 de noviembre de 2019.
Fecha en qué informó al público y por qué medios	• 11 de noviembre de 2019, a través de un comunicado en su sitio web, por Facebook y Twitter. • 15 de noviembre de 2019, a través de un comunicado en su sitio web, por Facebook y Twitter.
Divulgación por parte de medios de comunicación	Sí, el mismo día que Pemex emitió el primer comunicado. Además, difundieron que se pedía un rescate por 565 bitcoins equivalentes en ese momento a aproximadamente 4.9 millones de dólares, lo cual no fue mencionado por Pemex.
¿Informó a otros grupos de interés?	Sí, a sus empleados vía correo electrónico. El 10 de noviembre de 2019 informó que por una actualización urgente estarían suspendidos el correo electrónico y algunas aplicaciones, mientras que los correos enviados el 16 de enero de 2020 y 28 de enero de 2020 fueron de seguridad, de la información en general.
Contenido del comunicado	Comunicado 11 de noviembre de 2019: • «Ante la ola de rumores y comunicados apócrifos, notas y comentarios en redes sociales sobre un ataque a los sistemas informáticos internos de Petróleos Mexicanos, se informa lo siguiente:» • Pemex opera con normalidad • Afectó el funcionamiento de menos del 5% de equipos personales • La producción y el abasto de combustibles están garantizados • Comunicado 15 de noviembre de 2019: • Exhorta a no hacer caso a noticias falsas sobre afectaciones al pago de los trabajadores • Garantiza que el pago a trabajadores fue con normalidad • Pemex opera con normalidad

Fuente: Elaboración propia con base en: Pemex, 2019a; Pemex, 2019b; Pemex, 2019c; Pemex, 2019d; Pemex, 2019e; Pemex, 2019f; Pemex, 2021a; Pemex, 2021b; Pemex, 2021c; Riquelme, 2019; Tourliere, 2020.

que no se accedió a ellos ilegalmente o que no fueron sustraídos dichos datos. ¿A qué supuesto se refería? Mientras que la comunicación a los titulares de los datos la SFP la realizó a través de un banner en el sitio web donde se capturan las declaraciones patrimoniales. Esto dista mucho de ser una notificación real al grupo que mayor interés tenía en saber la situación de sus datos personales, pues únicamente aquellos que accedieran al sitio web sabrían del ciberincidente. La SFP pudo, por ejemplo, enviar un correo electrónico a los servidores públicos además del banner.

En referencia a la **tabla 3**, se lee la falta de difusión en medios con respecto al ciberincidente relevante a Lotenal,[50] el día antes de que esta institución pública difundiera

50. En *Proceso*, disponible en https://bit.ly/3hIKDhv.

Tabla 2. Ciberincidente de la Secretaría de la Función Pública (mayo-junio de 2020)

Secretaría de la Función Pública (SFP)	
Importancia de la institución pública	La SFP es la dependencia del Ejecutivo Federal mexicano con funciones de contraloría, supervisión de servidores públicos federales, a cargo de las políticas de compras públicas y además responsable del registro de las declaraciones patrimoniales y de interés de los servidores públicos federales.
Fecha del ciberataque	Del 6 de mayo al 30 de junio de 2020
Tipo de ciberataque	Incidente de seguridad que permitía el acceso a los datos personales de 830,000 empleados que se encontraban en sus declaraciones patrimoniales (por ejemplo, domicilio, teléfono, inversiones, deudas).33
Relevancia del ciberataque	La SFP es responsable del sistema en el cual los servidores públicos a nivel federal introducen información con datos personales y datos sensibles, a través de sus declaraciones patrimoniales y de intereses. Asimismo, trascendió ampliamente en los medios de comunicación el ciberincidente.
Cuándo tuvo la institución conocimiento del ciberataque	30 de junio de 2020 cuando una persona informó a la SFP de la vulneración.
Fecha en qué informó al público y por qué medios	4 de julio de 2020 a través de un comunicado, en su sitio web, por Facebook y Twitter.
Divulgación por parte de medios de comunicación	4 de julio de 2020.
¿Informó a otros grupos de interés?	Sí, a los servidores públicos a través de un banner en el sitio web donde se presentan las declaraciones patrimoniales y de intereses de los servidores públicos. También informó al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
Contenido del comunicado	• No se han vulnerado los datos en las declaraciones patrimoniales y de intereses de los servidores públicos de la Administración Pública Federal • Existió «una forma alternativa de acceso a datos, por medio del buscador Shodan, de las versiones de las declaraciones patrimoniales y de intereses» • La vía alternativa «fue inmediatamente bloqueada y las medidas de seguridad fueron reforzadas» • La información clasificada está protegida • Están en curso investigaciones para establecer responsabilidades e informar a las autoridades competentes

* Posteriormente, algunas personas que accedieron a la base de datos pidieron rescate más no se trató de un ransomware (Soto, 2020).
Fuente: Elaboración propia con base en: SFP, 2020a; SFP, 2020b; SFP, 2021; Soto, 2020.

su primer comunicado. En este ni siquiera reconoció un ciberincidente sino que dijo que estaban en un plan de actualización de sistemas el cual provocaba intermitencia en las áreas. En el segundo comunicado, Lotenal aceptó que fue sujeta a un ciberataque desde hacía 2 semanas.[51] Lo señalado evidencia que incumplió con el derecho a saber en cuanto a oportunidad y veracidad.

La información parece incompleta, pues aun cuando reconoce la sustracción de información jamás precisa si esta incluyó o no datos personales. Si la información

51. En *Forbes México*, disponible en https://bit.ly/3WA202C.

Tabla 3. Ciberincidente de la Lotería Nacional (mayo de 2021)

Lotería Nacional (Lotenal)	
Importancia de la institución pública	Realiza sorteos para recaudar fondos para fines de beneficencia, siendo una institución reconocida por todos los estratos socioeconómicos.
Fecha del ciberataque	14-17 de mayo de 2021.
Tipo de ciberataque	Ransomware.
Relevancia del ciberataque	El ciberincidente fue difundido ampliamente en medios de comunicación. La compra de boletos y participación en sorteos de Lotenal es una costumbre en todos los estratos socioeconómicos.
Cuándo tuvo la institución conocimiento del ciberataque	14-17 de mayo de 2021.
Fecha en qué informó al público y por qué medios	El 28 de mayo de 2021 informó sobre un «plan de actualización de los sistemas». El 31 de mayo de 2021 informó del ciberataque que se había originado 2 semanas antes.
Divulgación por parte de medios de comunicación	27 de mayo de 2021 grupo Avaddon informó de un ransomware a Lotenal y se difundió en Twitter ese día, así como en otros medios a partir del 28 de mayo de 2021.
¿Informó a otros grupos de interés?	Sí, a adquirentes de boletos de sorteos y loterías. Asimismo, informó a la Policía Cibernética y a la Coordinación de la Estrategia Digital Nacional.
Contenido del comunicado	28 de mayo de 2021: • Se está implementando un plan de actualización de los sistemas lo que ha generado intermitencia en áreas administrativas y operativas. • El soporte para la realización de sorteos y concursos opera con normalidad . 31 de mayo de 2021: • «hace 2 semanas se detectó una sustracción de información en el área administrativa … por parte de delincuentes que operan a nivel internacional». • Inició gestión de modernización de los sistemas. • Se cuenta respaldo de la información de todas las áreas. • Los concursos, sorteos y pago de premios operan con normalidad.

Fuente: Elaboración propia con base en: Flores, 2021; Lotenal, 2021a; Lotenal, 2021b; Lotenal, 2021c; Proceso, 2021; Seekurity, 2021.

sustraída fue del área administrativa, es probable que incluyera datos personales porque ahí es dónde están documentos relativos a contratistas, empleados, entre otros.

Sin contar a las personas titulares de datos personales que pudieran estar en posesión de Lotenal, el grupo de interés que adquiere boletos de lotería fue informado a través de los comunicados proveyéndoles de información relevante como el que los concursos y sorteos operaban con normalidad, así como que estaban garantizados los pagos de los premios.[52] En este sentido, sí habrían cumplido con entregarles información relevante, comprensible y completa a este grupo de interés. No obstante lo anterior, es importante mencionar que muchas personas no tienen acceso a internet, ni redes sociales, por lo que debe cuestionarse la eficacia de comunicaciones de instituciones públicas cuando únicamente se realiza a través de medios digitales.

La **tabla 4** sintetiza la evaluación del cumplimiento con el derecho a la información de los Ciberincidentes Relevantes mencionados.

52. Disponible en https://bit.ly/3vcJvG1.

Tabla 4. Estándar de Evaluación de Cumplimiento

Información fue:	Pemex	SFP	Lotenal
¿Oportuna?	Sí	No	Sí
¿Actualizada?	No	No	No
¿Completa?	No	No	No
¿Comprensible?	Sí	No	Sí
¿Dirigida también a grupos de interés?	A empleados.	A servidores públicos.	A participantes de sorteos y lotería.

Fuente: Elaboración propia.

Los casos analizados de Pemex, SFP y Lotenal a la luz del derecho a la información de la sociedad mexicana, muestran que tras un ciberincidente relevante las instituciones públicas evitaron reconocerlo y tampoco comunicaron de manera oportuna información de interés público. Los comunicados de dichas autoridades no fueron completos al omitir dar a conocer que se trataron de ciberataques o de ciberincidente y al no referir a la manera en que podrían proteger su información y sistemas, por ejemplo. No existieron actualizaciones de la información por parte de las instituciones. Es de destacarse que la información de los Ciberincidentes Relevantes en los medios de comunicación fue más amplia que las de las instituciones, siendo que las autoridades debieran ser quienes proveen la información de primera mano y en observancia del derecho a la información de la sociedad.

¿Por qué las instituciones públicas evaden reconocer tener afectaciones por un ciberincidente relevante? Las respuestas pueden ser variadas, sin que a lo largo de esta investigación se hayan encontrado artículos, documentos o investigaciones que a esta fecha las estudien. Así que se abren nuevas líneas para futuras investigaciones que indaguen las razones por las cuales las instituciones públicas evitan reconocer los Ciberincidentes Relevantes en sus comunicados. ¿Será por temor a posibles auditorías[53] que revelen omisiones, negligencia o culpa de servidores públicos? ¿Será porque consideran que son aspectos técnicos que a la ciudadanía no les interesa? ¿Será porque hay tantos ciberincidentes en la operación cotidiana de sistemas que es complejo decidir cuál sería un ciberincidente relevante y cuál no? ¿Será para evitar afectar la imagen de las instituciones públicas? ¿Será porque se han dado otros ciberincidentes

53. Una auditoría puede revelar que el ciberincidente relevante pudo evitarse, por ejemplo, con la actualización de software, con tener procedimientos y protocolos de ciberseguridad establecidos y que funcionen ante una eventualidad. También es posible que sea insuficiente el presupuesto que se está invirtiendo en ciberseguridad, en servidoras públicas expertas en ciberseguridad y en capacitación del personal de las instituciones.

similares en la propia institución sin que se hayan implementado medidas para evitarlos? ¿Alguna razón distinta a las anteriores?

Conclusiones

La creciente dependencia a los sistemas informáticos, a las redes de telecomunicaciones, a las comunicaciones en el ciberespacio y al internet de las cosas (IoT, por sus siglas en inglés), exigen que la ciberseguridad sea un asunto de la mayor relevancia. México cuenta con un marco normativo que aborda la ciberseguridad, en algunos casos de manera expresa y en otros implícita. También existen leyes de protección de datos personales que obligan a notificar vulneraciones de estos a sus titulares.

El deber de informar a la sociedad sobre ciberincidentes que afectan a instituciones públicas encuentra su fundamento en el derecho a la información, así como también es un aspecto sugerido por el Marco de Ciberseguridad NIST. A partir de ello, se propone establecer un estándar para decidir si un ciberincidente debe comunicarse por ser un ciberincidente relevante o no, y los elementos que debe reunir la comunicación.

Las tablas de criticidad y nivel de impacto de ciberincidentes pueden ser criterios orientadores para determinar cuándo la sociedad tiene derecho a saber de un ciberincidente. Si bien cada ciberincidente debe analizarse en su contexto y caso por caso, los supuestos para que sea un ciberincidente relevante son:

- que afecte de manera importante a una institución pública que sea considerada una de infraestructura de información esencial o infraestructura crítica, que preste servicios públicos, que sea necesaria para el ejercicio de derechos o el cumplimiento de obligaciones;
- pueda llevar a obstaculizar labores de seguridad nacional, seguridad pública, procuración de justicia, combate al crimen y a la corrupción, y otras actividades de trascendencia;
- que sea respecto de información que pueda manipularse para desinformar a la sociedad, minar la confianza en las instituciones o socavar la democracia;
- que se haya dado a conocer ampliamente en medios de comunicación o redes sociodigitales; o
- que se hayan vulnerado o afectado datos personales.

Salvo en los casos debidamente justificados de seguridad nacional y orden público en que las consecuencias de informar sean contraproducentes, de suceder el ciberincidente relevante se detona el deber de infomar por parte de la institución pública y su correlativo derecho de la sociedad a ser informada. Este derecho es de trascendencia para la rendición de cuentas. Además, no puede equipararse la atribución pública

que un país realice de un ciberataque, con el deber de informar a su ciudadanía de un ciberincidente relevante porque aquel generalmente lleva tiempo para determinar la persona o el Estado nación detrás de un ciberataque y porque existen ciberincidentes relevantes que no derivan de un ciberataque, sino que pueden deberse a otras situaciones padecidas.

Las comunicaciones a la sociedad por parte de la institución pública deben ser oportunas, actualizarse conforme se vaya teniendo nueva información de importancia, ser completas y veraces, comprensibles y en formatos accesibles. Asimismo, si existen grupos de interés específicos (por ejemplo, empleados, jubilados, proveedores), deberán ser informados de manera directa proporcionando la información que requieren saber. Estas comunicaciones son independientes de la obligación de informar a titulares de datos personales en el supuesto de que estos haya sido vulnerados.

Los casos analizados de las instituciones públicas mexicanas (Pemex, SFP y Lotenal) muestran que aun la que emitió una comunicación de manera oportuna, ninguna reconoció el ciberincidente, ni actualizó la información según fue siendo disponible. La información difundida fue comprensible, salvo en un caso (SFP). Las tres autoridades informaron también a grupos de interés (Pemex a empleados, SFP a servidores públicos y Lotenal a participantes en sorteos y lotería), aun cuando la información proporcionada no fue completa. En suma, los casos analizados revelan que las instituciones públicas no cumplieron cabalmente con el derecho a informar a la ciudadanía cuando tuvieron un ciberincidente relevante.

Se recomienda que la Estrategia Nacional de Ciberseguridad prevea la elaboración de guías para colmar el derecho a la información de la sociedad tras un ciberataque o un ciberincidente relevante. Sabiendo que cada uno de estos puede ser diferente en tipo, tamaño, escala y causas, las guías pueden servir para generar conciencia de la importancia de informar a la sociedad en general y a los grupos de interés en particular cumpliendo con los requisitos mínimos. Estos son que: se informe de manera oportuna, se vaya actualizando la información según se obtenga, la información sea completa, comprensible y en formatos accesibles, y que se atienda a los diferentes grupos de interés con la información que cada uno requiera.

Finalmente, es claro que debe propiciarse más investigación en ciberseguridad desde la perspectiva del Derecho y la política pública que sea en español. Asimismo, se abren nuevas líneas de investigaciones en ciberseguridad sobre el objeto de este artículo en torno a encontrar las razones por las que las instituciones públicas evitan reconocer tener afectaciones por un ciberincidente relevante en las comunicaciones públicas.

Referencias

Álvarez, Clara Luz (2018). *Telecomunicaciones y Radiodifusión en México*. México: Posgrado en Derecho UNAM. Disponible en https://bit.ly/2KvYWEa.

Banco Interamericano de Desarrollo y Organización de los Estados Americanos (2020). *Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe. Reporte Ciberseguridad 2020.* OEA, pp. 1-204. DOI: 10.18235/0002513.

Becerril, Anahiby (2019). «La ciberseguridad en los Tratados de Libre Comercio». *Revista Chilena de Derecho y Tecnología,* 8 (2): 111-137. DOI: 10.5354/0719-2584.2019.53447.

Brizio, Guillermo (2008). «La auditoría, la transparencia y la rendición de cuentas». *Revista de Administración Pública*, 43 (especial): 211-2020.

Cano M., Jeimy y Andrés Almanza (2020). «Estudio de la evolución de la Seguridad de la Información en Colombia: 2000-2018». *Revista Ibérica de Sistemas e Tecnologías de Informacão*, E27: 470-483.

Carbonell, Miguel (2019). «Deber de publicidad del Estado». *Diccionario Enciclopédico de Derecho de la Información*. Tomo 1 (pp. 330-336). México: Ius Literatus y Posgrado en Derecho UNAM.

Castillo, Anderson, Mariuxi Bruzza y Manuel Tupia (2020). «Estado del arte sobre la identificación amenazas no intencionales de ciberseguridad de parte de personal interno en instituciones públicas». *Revista Ibérica de Sistemas e Tecnologías de Informacão,* 41: 70-82.

Cocchini, Andrea (2021). «Los ciberataques de los actores no estatales y la "ciberdiligencia debida" de los Estados». *Revista UNISCI,* 55: 69-98. DOI: 10.31439/UNISCI-106.

Comisión Interamericana de Derechos Humanos (2013). *Libertad de expresión e Internet.* Disponible en https://bit.ly/3VeH7ZH.

Egloff, Florian y Andreas Wenger (2019). «Public Attribution of Cyber Incidents». *CSS Analyses in Security Policy,* 244: 1-4. DOI:10.3929/ethz-b-000340841.

Egloff, Florian y Max Smeets (2021). «Publicly attributing cyber attacks: a framework». *Journal of Strategic Studies,* 1-32. DOI: 10.1080/01402390.2021.1895117.

Filipini, Jorge Alejandro e Inés Selvood (2021). «Las obligaciones de transparencia en las políticas públicas: los casos difíciles». *Estudios en Derecho a la Información,* 12: 61-88. Disponible en https://bit.ly/3BXVrPr.

Finnemore, Martha y Duncan B. Hollis (2020). «Beyond Naming and Shaming: Accusations and International Law in Cybersecurity». *European Journal of International Law*, 31 (3): 969-1003. DOI: 10.1093/ejil/chaa056.

Jara, Natalia y Antonia Jorquera (2021). «La responsabilidad de la Administración del Estado por incidentes de ciberseguridad». *Revista Chilena de Derecho y Tecnología,* 10 (1): 201-230. DOI: 10.5354/0719-2584.2021.58776.

Knight, Richard y Jason R. C. Nurse (2020). «A framework for effective corporate communication after cyber security incidents». *Computers & Security,* 99: 1-18. DOI: 10.1016/j.cose.2020.102036.

López, Jonathan (2020). *Ciberespacio & Ciberseguridad: Elementos esenciales.* México: Tirant lo Blanch.

Mañas-Viniegra, Luis, José Niño y Luz Martínez (2019). «La transparencia como variable reputación de la comunicación de crisis en el contexto mediático del ciberataque wannacry». *Revista de Comunicación de la SEECI,* 48: 149-171. DOI: 10.15198/seeci.2019.48.149-171.

National Institute of Standards and Technology (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. Disponible en https://bit.ly/2K116rA.

Oficina de la Presidencia de la República (2021a). «Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal». *Diario Oficial de la Federación*. Disponible en https://bit.ly/3YMowVo.

—. (2021b). «Acuerdo por el que se expide la Estrategia Digital Nacional 2021-2024». *Diario Oficial de la Federación*. Disponible en https://bit.ly/3HYuZsP.

Papakonstantinou, Vagelis (2022). «Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity». *Computer Law & Security Review*, 44: 1-15. DOI: doi.org/10.1016/j.clsr.2022.105653.

Parlamento Europeo y del Consejo de la Unión Europea (2019). *Reglamento 2019/881 sobre la Ciberseguridad de la UE*. Diario Oficial de la Unión Europea de 7 de junio de 2019. Disponible en https://bit.ly/3FOe4Xk.

Rodríguez-Márquez, Mariel (2021). «Ciberseguridad en la justicia digital: recomendaciones para el caso colombiano». *Revista UIS Ingenierías*, 20 (3): 19-46. DOI: 10.18273/revuin.v20n3-2021002.

San Martín, Marina (2020). «El derecho a saber información ambiental en México». *Estudios en Derecho a la Información,* 12: 25-47. DOI: 10.22201/iij.25940082e.2020.9.14277.

Secretaría de seguridad y protección ciudadana (2021). *Protocolo Nacional Homologado de* Gestión *de* Incidentes *Cibernéticos*. Gobierno de México. Disponible en https://bit.ly/3HXbTn3.

Suprema Corte de Justicia de la Nación (2016a). Tesis: 2a. LXXXIV/2016 (10a.). «Derecho a la información. Dimensión individual y dimensión colectiva». *Gaceta del Semanario Judicial de la Federación*, segunda sala, 9 de septiembre de 2016. Disponible en https://bit.ly/3YRfXLJ.

—. (2016b). Tesis: 2a. LXXXV/2016 (10a.). «Derecho a la información. Garantías del.». *Gaceta del Semanario Judicial de la Federación*, segunda sala, 9 de septiembre de 2016. Disponible en https://bit.ly/3C6ITFN.

—. (2016c). Tesis: 2a. LXXXVI/2016 (10a.). «Derecho a ser informado. Sus alcances y límites». *Gaceta del Semanario Judicial de la Federación*, segunda sala, 9 de septiembre de 2016. Disponible en https://bit.ly/3I83woz.

—. (2016d). Tesis: 2a. LXXXVII/2016 (10a.). «Derecho a ser informado y derecho al honor. Estándar para determinar su prevalencia». *Gaceta del Semanario Judicial de la Federación*, segunda sala, 9 de septiembre de 2016. Disponible en https://bit.ly/3YXFnHB.

—. (2018). Tesis: 2a. XXXIV/2018 (10a.). «Información pública emitida por el Estado. Requisitos para su difusión». *Gaceta del Semanario Judicial de la Federación*, segunda sala, 18 mayo de 2018. Disponible en https://bit.ly/3Gq9vUC.

—. (2020). Tesis: P. I/2019 (10a.). «Derecho a la información. No puede alegarse el carácter de "reservado" de las averiguaciones previas cuando la investigación verse sobre violaciones graves de derechos fundamentales o delitos de lesa humanidad». *Gaceta del Semanario Judicial de la Federación*, Pleno, 17 de enero de 2020. Disponible en https://bit.ly/3WQo8Tz

Villanueva, Ernesto (2008). *Derecho de la Información*. Quito: CIESPAL.

Agradecimientos

Mi gratitud por los comentarios y retroalimentación recibida de Abel Jonathan, Anahiby Becerril, Jorge Alvarado, Marina San Martín y Vanessa Díaz, así como mi agradecimiento por el apoyo en la investigación a Alberto Toledo, Lizeth Arely Estrada, Noé Aarón Ávalos y Ximena Barrera.

Sobre la autora

Clara-Luz Álvarez es doctora en Derecho y maestra en Ciencias Jurídicas por la Universidad Panamericana, maestra en Derecho Comparado por New York University y licenciada en Derecho por la Universidad de las Américas Puebla. Profesora de la Universidad Panamericana (campus México) e investigadora del Sistema Nacional de Investigadores de la República Mexicana. Su correo electrónico es calvarezg@up.edu.mx y su sitio web claraluzalvarez.org. https://orcid.org/0000-0002-5906-4450.

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

La *Revista de Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

DIRECTOR

Daniel Álvarez Valenzuela

(dalvarez@derecho.uchile.cl)

SITIO WEB

rchdt.uchile.cl

CORREO ELECTRÓNICO

rchdt@derecho.uchile.cl

La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipográfica
(www.tipografica.io).