Fotografía: Mati Mango para Pexels.com

De lo virtual a lo real: en diez meses el SIPOT ha sufrido 77 mil 927 ataques cibernéticos

María Del Rosario Navarro Zamora

Coordinadora de Procesos Normativos en el ITEI

Resumen

El Sistema de Portales de Obligaciones de Transparencia (SIPOT) de la Plataforma Nacional de Transparencia (PNT), fue creado derivado de una política pública transversal de Transparencia, Acceso a la Información y Protección de Datos, ante la falta de homologación en la publicación y actualización de la información fundamental general y específica de los sujetos obligados del país.

Lo anterior, debido a que cada sujeto obligado publicitaba en sus portales de Internet, sin ningún tipo de aprobación o estandarización con los demás países; acarreando un problema para la ciudadanía en la consulta de la información fundamental.

Es por ello, que se crea el SIPOT con los Lineamientos Técnicos Generales de Publicación, Homologación y Estandarización de la Información, para que todos los sujetos obligados del país publiquen la información fundamental de una misma manera; y con ello la ciudadanía pueda consultarla sin complicaciones.

Ahora bien, al ser una Plataforma a través de la cual su acceso es utilizando Internet, sabemos que los límites de éste no existen y es complicada la regulación debido a que en el *ciberespacio interactúan los sistemas informáticos, redes e infraestructura, utilizando medios físicos y el espectro electromagnético para interconectarse.*[1]

En razón de lo antes referido, el SIPOT se ha tornado vulnerable a ataques cibernéticos, dado que cualquier persona con tan solo utilizar un equipo de cómputo, móvil o tableta conectada a Internet puede acceder al Sistema y si éste no cuenta con las debidas medidas de seguridad puede ser vulnerado.

PALABRAS CLAVES:
Plataforma Nacional de Transparencia, Sistema de Portales de Obligaciones de Transparencia, Ciberespacio, Ciberseguridad, Pentesting

[1] Centro de Estudios Estratégicos CEEAG. (2018). La Ciberguerra: Sus impactos y desafíos. Chile: Comité Editorial del CEEAG, página 18.

No obstante que el INAI (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales) cuenta con seguridad informática dentro del Instituto necesaria para proteger el SIPOT, así mismo hace uso de herramientas de propósito específico tanto en el perímetro de comunicaciones del Instituto como en los puntos finales, para la protección de la tecnología que contiene éste.[2]

Sin embargo, el SIPOT de la PNT en tan solo diez meses ha sufrido 77 mil 927 ataques cibernéticos; los cuales si bien es cierto el INAI manifestó que fueron contenidos por las capas de seguridad, como consecuencia no se convirtieron en incidentes de seguridad que hayan provocado algún riesgo para el Instituto.

La situación es que lo virtual superó la realidad y a pesar de todas las medidas de seguridad el SIPOT sufrió ataques cibernéticos. Ciertamente *el INAI, es el administrador de la Plataforma, pero también los órganos garantes son responsables de verificar de manera periódica y constantes los sistemas de la PNT.*[3]

Introducción

El presente artículo antes de aterrizar en los ataques cibernéticos que ha sufrido el SIPOT de la PNT, hace un recorrido desde la creación de la Ley General de Transparencia y Acceso a la Información Pública, lo que establece ésta en relación a la PNT y al SIPOT; derivado de lo anterior la necesidad de crear unos lineamientos para implementar y operar la PNT. Se explica brevemente lo relacionado con el ciberespacio y todo lo que éste implica; se hace referencia al *Pentesting* para finalmente explicar el tema central del artículo en comento.

En relación a lo anterior, se establece que el 16 dieciséis de abril del año 2015 dos mil quince, el Congreso General de los Estados Unidos Mexicanos, aprobó el Proyecto de Decreto por el cual se expide la Ley General de Transparencia y Acceso a la Información Pública (Ley General), mismo que fue publicado en el Diario Oficial de la Federación, el 04 de mayo del año 2015 dos mil quince, entrando en vigor al día siguiente de su aprobación.

Ahora bien, en el artículo Quinto Transitorio de la Ley General, se establece que el Congreso de la Unión, las legislaturas de los Estados y la Asamblea Legislativa del Distrito Federal, tendrán un plazo de hasta un año, contado a partir de la entrada en vigor del Decreto aludido en el párrafo que antecede, para armonizar la leyes relativas, conforme a los principios, bases general y procedimientos para garantizar el derecho de acceso a la información en posesión de cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad de la Federación, las Entidades Federativas y los municipios.

Por otra parte, el artículo 49, de la Ley General, establece que los organismos garantes desarrollarán, administrarán, implementarán y pondrán en funcionamiento la plataforma electrónica que permita cumplir con los procedimientos, obligaciones y disposiciones

[2] Respuesta entregada el 04 de junio de 2019, a la solicitud de información presentada ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, a la cual le correspondió el número de folio 0673800104519.

[3] Lineamiento décimo tercero y décimo cuarto del Acuerdo del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales por el que se aprueban los Lineamientos para la implementación y operación de la Plataforma Nacional de Transparencia

señaladas en la Ley General para los sujetos obligados y organismos garantes, de conformidad con la normatividad que establezca el Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, atendiendo a las necesidades de accesibilidad de los usuarios.

Asimismo, el artículo 50, de la Ley General, refiere que la PNT se conformará por al menos, cuatro sistemas; esto es: Sistema de solicitudes de acceso a la información (SISAI); Sistema de gestión de medios de impugnación (SIGEMI); Sistema de portales de obligaciones de transparencia (SIPOT), y Sistema de comunicación entre organismos garantes y sujetos obligados (SICOM).

En otro orden de ideas, el 04 cuatro de mayo del año 2016 dos mil dieciséis, se publicó en el Diario Oficial de la Federación el Acuerdo del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales por el que se aprueban los Lineamientos para la implementación y operación de la Plataforma Nacional de Transparencia (Lineamientos de la PNT).

El lineamiento primero de los Lineamientos de la PNT, refiere que éstos tienen por objeto establecer las reglas de operación, garantizando su estabilidad y seguridad, promoviendo la homologación de procesos y la simplicidad del uso de los sistemas que conforman la citada PNT para los usuarios, garantizando en todo momento los derechos de acceso a la información y protección de datos personales en posesión de los sujetos obligados.

De igual forma, en el lineamiento quinto señala que la PNT es el instrumento informático a través del cual se ejercerán los derechos de acceso a la información y de protección de datos personales en posesión de los sujetos obligados, así como su tutela, en medios electrónicos, de manera que garantice su uniformidad respecto de cualquier sujeto obligado, y sea el repositorio de información obligatoria de transparencia nacional.

En ese sentido, el lineamiento décimo de los Lineamientos de la PNT, refiere que el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI) será el responsable de brindar la capacitación en la operación de la PNT a los organismos garantes y, éstos a su vez, tendrán la responsabilidad de capacitar a sus sujetos obligados.

Asimismo, el lineamiento décimo tercero de los Lineamientos de la PNT, establece que en caso de que ésta presente una falla técnica, el INAI, como administrador, deberá hacer del conocimiento de los organismos garantes y sujetos obligados la magnitud de la falla y el tiempo de recuperación, para que éstos estén en posibilidad de implementar las medidas necesarias para el cumplimiento de sus respectivas responsabilidades.

En relación con lo anterior, el lineamiento décimo tercero de los Lineamientos de la PNT, refiere que el impedimento temporal, por caso fortuito o fuerza mayor, suspenderá los términos establecidos para cualquier trámite realizado a través de la PNT, hasta en tanto dure dicho impedimento; caso en el cual, el INAI comunicará a los organismos garantes que correspondan el periodo de suspensión para que éstos a su vez lo informen a sus sujetos obligados.

Además, el lineamiento décimo cuarto de los Lineamientos de la PNT, señala que será responsabilidad de los organismos garantes verificar de manera periódica y constante los sistemas de la PNT, con la finalidad de dar pronta atención a los mismos.

Por otro lado, los lineamientos vigésimo y vigésimo primero, de los Lineamientos de la PNT, describe que en el caso del SIPOT, el INAI será el responsable de:

a) Realizar la configuración base de los formatos que atiendan lo establecido en la Ley General, y

b) Efectuar las configuraciones a: temas; subtemas; sectores; normatividad general, y formatos generales.

En ese mismo sentido, los lineamientos del vigésimo octavo, al trigésimo primero, de los Lineamientos de la PNT, establecen que el INAI, en relación a la PNT será responsable de:

a) Mantenerla disponible en todo momento, para tal efecto implementará los mecanismos necesarios para que la operabilidad sea garantizada en la medida de lo posible en caso de contingencias o casos fortuitos;

b) Vigilar el correcto funcionamiento;

c) Implementar el mecanismo de recuperación de desastres y contingencias, e

d) Implementar el plan de respaldos de ésta (el cual hará de conocimiento a los organismos garantes).

Por otra parte, los lineamientos vigésimos, vigésimo segundo, vigésimo sexto, vigésimo séptimo, centésimo décimo segundo y centésimo décimo tercero de los Lineamientos de la PNT, establecen que con el apoyo técnico del INAI, los organismos garantes serán responsables de:

a) Realizar la configuración de las particularidades según la normatividad local aplicable en cada entidad federativa;

b) Realizar las configuraciones a: normatividad local; formatos locales; criterios; metodología de evaluación; periodos de evaluación formal; clasificación de sujetos obligados, y asignación de normatividad, formatos y sujetos obligados;

c) Mantener actualizada la información relacionada con el listado, directorio y unidades administrativas de sus sujetos obligados;

d) Configurar los criterios y obligaciones de transparencia adicionales contemplados en la normatividad local correspondiente, y

e) Dar de alta a los sujetos obligados de su competencia.

De la misma manera, el uso de la PNT será obligatorio para todos los sujetos obligados a nivel federal, estatal y municipal, de conformidad con lo establecido en los Transitorios Octavo y Décimo de la Ley General.

Ahora bien, los lineamientos trigésimo tercero al trigésimo quinto de los Lineamientos de la PNT, describen que el uso de ésta no tendrá costo para los usuarios; asimismo algunas secciones requerirán que las personas dispongan de un usuario y contraseña; así como solicitará el uso de equipo de cómputo o dispositivos móviles que cuenten con acceso a Internet.

En relación con lo anterior, los lineamientos trigésimo sexto y trigésimo séptimo de los Lineamientos de la PNT, detallan que como consecuencia, la PNT permitirá la interoperabilidad de la información contenida en cada sistema y entre los diversos sistemas, mediante servicios web a través de un bus de servicios empresariales; y contará con servicios que permitirán exportar información contenida en ésta por cualquier particular, sujeto obligado u organismo garante que así lo requiera.

Para el caso que nos ocupa, es indispensable conocer la definición del SIPOT. Es por ello que el lineamiento centésimo décimo de los Lineamientos de la PNT, señala que es la herramienta electrónica a través de la cual los sujetos obligados de los tres niveles de gobierno, ponen a disposición de los particulares la información referente a las obligaciones de transparencia contenidas en la Ley General, Ley Federal o Ley Local.

Por lo antes vertido, el lineamiento centésimo décimo cuarto, de los Lineamientos de la PNT, refiere que el SIPOT permite tres métodos de carga de la información a través de:

a) Un formulario web;

b) Un archivo xml cuya estructura estará determinada por el INAI; y

c) De un servicio web.

Desde otro ángulo, en una Auditoría Financiera y de Cumplimiento, se estableció que el INAI, señaló que la PNT entraría en operaciones el 5 de mayo de 2016. Para ello el INAI planteó dos etapas para el desarrollo e implementación de la PNT, la primera de septiembre a diciembre de 2015 y su alcance consistía en llevar a cabo mejoras SISAI, SIPOT, y desarrollar el SIGEMI y el SICOM; y la segunda de febrero a diciembre de 2016, para realizar adecuaciones derivadas por la normatividad emitida por el SNT y la armonización con las Leyes Locales de los Estados de la República en la materia y desarrollos adicionales, y mejoras a la PNT.[4]

En relación con lo antes mencionado derivado de una presentación de power point hecha por el INAI, la cual tituló "Pruebas de PNT rediseñada", se refiere que el 12 doce de diciembre del año 2017 dos mil diecisiete, la Comisión de Tecnologías de la Información y Plataforma Nacional de Transparencia, realizaron mejoras a la consulta pública del SIPOT y trabajaron en un rediseño de la totalidad de la Plataforma.

De la misma forma, las citadas láminas establecieron que el 21 veintiuno de septiembre del año 2018 dos mil dieciocho, fueron presentados los avances a las mejoras y el rediseño de la PNT, acordando la retroalimentación de dichos avances y la realización de las pruebas con todos los organismos garantes del país.

Posteriormente, en la aludida presentación se describió que el 15 quince de noviembre del año 2018 dos mil dieciocho, se presentó a los organismos garantes el rediseño y se proporcionó una liga para realizar una revisión y pruebas.

Subsiguientemente, la exposición señaló que el 13 trece de diciembre del año 2018 dos mil dieciocho, el Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, mencionó que antes de la puesta en producción de la PNT rediseñada se realizarían pruebas de funcionamiento de los componentes que la integran.

De esta manera, el INAI a través de su presentación plasmó que las pruebas se llevaron a cabo a nivel nacional el 09 nueve y 16 dieciséis de febrero; así como el 09 nueve de marzo del año 2019 dos mil diecinueve.

Finalmente las "Pruebas de la PNT rediseñada" trajeron como consecuencia una reingeniería de los procesos, simplificación del lenguaje y mejora de rutas de navegación, que entró en funcionamiento el 08 ocho de abril del año 2019 dos mil diecinueve.

Por otro lado, el Centro de Estudios Estratégicos (CEEAG) a través de su libro titulado La Ciberguerra: Sus impactos y desafíos (2018.p.31), establece que el Internet carece de fronteras y el contenido ilícito circula de un país a otro en milésimas de segundos, además existe una escasa o nula regulación de los cibercafés, locutorios, salas de informática públicas, bibliotecas, centros educativos, máquinas populares de acceso a Internet y otras donde de forma anónima las personas pueden conectarse y realizar actividades ilícitas.

A lo anterior, el CEEAG (2018.p.45), refirió que se suma el desarrollo de los computadores y software, junto con los aparatos móviles de comunicaciones de grandes capacidades, siendo estos últimos en la actualidad los principales medios por los que se accede a Internet. Este desarrollo tecnológico ha traído consigo acceso a grandes cantidades de data, transmisión de archivos, correos electrónicos, mensajería instantánea, etc., incluyendo el acceso a información general, privada, incluso de tipo personal, lo que facilita y simplifica la vida tanto en los ámbitos personal como profesional.

Para facilitar o gestionar lo anterior, se han creado sistemas de redes, almacenamiento y distribución de megadatos, comunicaciones y otra variedad de infraestructuras que dan sustento al "negocio" de cada una de estas organizaciones en pos de sus fines. Pero así como se facilita y se hace más expedito todo

[4] Respuesta entregada el 17 de mayo de 2019, a la solicitud de información presentada ante la Auditoría Superior de la Federación, a la cual le correspondió el número de folio 0110000043319.

nuestro quehacer, también se hace más vulnerable, surgiendo riesgos que pueden llegar a convertirse en serias amenazas, afectando particularmente los servicios, organizaciones y estructuras que tienen un rol vital en el desarrollo de las actividades esenciales del ser humano del mundo moderno, las que en particular se denominan infraestructuras críticas (IC), cuyo daño o afección puede tener graves efectos en los intereses esenciales y la seguridad de cualquier país. Estos riesgos provienen de múltiples fuentes y se manifiestan mediante actividades de espionaje, sabotaje, fraudes o ciberataques realizados por otros países, por grupos organizados o por particulares, entre otros, surgiendo las denominadas ciberamenazas. (Centro de Estudios Estratégicos, 2018, p. 46)

Por otra parte, el Centro de Estudios Estratégicos, a través de su libro titulado La Ciberguerra: Sus impactos y desafíos, (2018. p. 17), estableció que la complejidad del tema informático aumentó con la conectividad de computadores y bases de datos, generando la aparición de un espacio virtual o "ciberespacio", como medio de transmisión de datos. Ya no bastaba contar con un computador aislado, sino que su integración a la transferencia de información vino a catalizar notoriamente su importancia como medio informático.

El referido Centro de Estudios Estratégicos, estableció que el ciberespacio consiste en una red interdependiente de infraestructuras de tecnologías de la información, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos, procesadores embebidos y controladores. Se puede complementar esta definición con lo que conceptualiza la Comisión Europea como *"el espacio virtual por donde circulan los datos electrónicos de los ordenadores del mundo"* y por último la UIT (Unión Internacional de las Telecomunicaciones) como el lugar creado para la interconexión de sistemas de ordenador mediante Internet.

En la consecuencia del análisis de las múltiples definiciones de ciberespacio tenidas a la vista, hay elementos comunes que se encuentran en cada una de ellas, resaltando la importancia estructural que dichos conceptos revisten, entre los que destacan "espacio virtual", "datos", "interdependencia e interconexión", "información" e "infraestructura de redes", términos todos que confluyen para un mejor entendimiento de lo que la quinta dimensión viene a significar. Por ello, el ciberespacio va a estar caracterizado por una red de información que lo conforma, donde confluyen redes de tecnología de comunicaciones interconectadas que harán que esa información esté globalmente disponible, usando para ello conexiones físicas e inalámbricas, a altas velocidades. (Centro de Estudios Estratégicos, 2018, p. 20).

Algunas de las características del ciberespacio establecidas en el Manual *Cybrespace and Electronic Warfare Operations*, FM 3-12, son: Opera en Red, catalizador social, tecnología, interdependiente e interrelacionada y vulnerable.

En otro orden de ideas, la ciberseguridad[5] puede ser entendida como el conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan. Entonces, asegura el uso de las redes propia y niega su empleo a terceros.

La Unión Internacional de Telecomunicaciones, referida en Gómez Abutridy Alejandro, Ciberseguridad y Ciberdefensa, Dos elementos de la Ciberguerra, Memorial del Ejército de Chile No. 492, agosto 2014. Define a la ciberseguridad como *"El conjunto de herramientas, políticas, conceptos de seguridad, directrices, métodos de gestión, acciones, formación, prácticas idóneas, seguros y tecnologías que vvpueden utilizarse para proteger los activos de una organización y a los usuarios en el ciberentorno"*.

La UIT dice que la ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos, cuales son amenazas de seguridad correspondientes en el ciberentorno. Luego, entendiendo que la problemática de la ciberseguridad

[5] Jeimy Cano J. Ciberseguridad y Ciberdefensa: Dos tendencias emergentes en un contexto global, Sistemas (Asociación Colombiana de Ingenieros de Sistemas). Vol. 000, No. 0119 (Abr-Jun. 2011) pp.4-7.

requiere un esfuerzo colectivo y coordinado entre los diferentes países, establece cinco elementos fundamentales para desarrollar una estrategia de ciberseguridad, acorde con la realidad de cada una de las naciones: desarrollo de un marco legal para la acción, desarrollo y aplicación de medidas técnicas y procedimentales, diseño y aplicación de estructuras organizacionales requeridas, desarrollo y aplicación de una cultura de ciberseguridad y la cooperación internacional.

La ciberseguridad consta de tres elementos fundamentales que forman parte de los objetivos que intentan afectar los potenciales atacantes. Estos son la confidencialidad, la integridad y la disponibilidad de los recursos, CIA *(Confidentiality-Integrity-Availability)*. (Centro de Estudios Estratégicos, 2018, p. 69).

Ahora bien, refiere Marcos Robledo Hoecker, Subsecretario de Defensa Secretario Ejecutivo, Comité Interministerial sobre ciberseguridad, PNCS 2017, p. 9, que *hace bastante tiempo que el ciberespacio dejó de ser parte de la ciencia ficción para convertirse en uno de los principales espacios de interacción social.*

En relación con lo antes vertido, es pertinente conocer el concepto de resiliencia el cual es definido por Arturo M. Calvente, *Resiliencia: un concepto clave para la sustentabilidad*, Universidad Abierta Interamericana, Centro de Altos Estudios Globales como "las condiciones de un sistema complejo alejado del equilibrio, donde las inestabilidades pueden transformar al mismo para que presente otro régimen de comportamiento, así la resiliencia es medida por la magnitud de perturbaciones que pueden ser absorbidas por el sistema antes de que sea reorganizado con diferentes variables y procesos".

Por lo antes mencionado, el concepto de la resiliencia está directamente asociado con la sustentabilidad de todo sistema complejo; ésta no es una propiedad absoluta y fija sino que, por el contrario, es variable en el tiempo y el espacio y depende, en gran medida, de las acciones y relaciones del sistema y la volatilidad ambiental del contexto en el que se encuentre. (Centro de Estudios Estratégicos, 2018, páginas 147 y 148).

En otro orden de ideas, el Instituto Nacional de Ciberseguridad (INCIBE), a través de un artículo publicado en julio del presente año, ha definido al *"pentesting como el conjunto de ataques simulados dirigidos a un sistema informático con una única finalidad: detectar posibles debilidades o vulnerabilidades para que sean corregidas y no puedan ser explotadas"*.

En ese mismo sentido refiere el artículo publicitado que *las auditorías comienzan con la información almacenada en fuentes de acceso abierto, de información sobre la empresa, los empleados, usuarios, sistemas y equipamientos*.

El INCIBE, establece que *las citadas auditorías examinan las vulnerabilidades que se intentarán explotar, incluso con técnicas de ingeniería social, atacando a los sistemas hasta conseguir sus objetivos*.

De igual forma, el citado artículo reseña que las auditorías emiten un informe a través del cual muestra si los ataques tendrían éxito, y en caso afirmativo por qué y qué información o acceso obtendrían, es decir, se simulan ataques tal y como los llevaría a cabo un ciberdelincuente que quisiera hacerse del control del sistema o de la información en él contenida.

Asimismo, el artículo publicitado relata que las auditorías establecen: *Si el sistema informático es vulnerable o no; evalúan si las defensas con las que cuenta, son suficientes y eficaces, y valoran la repercusión de los fallos de seguridad que se detecten*.

Ahora bien, manifiesta el INCIBE, que en el desarrollo del *pentesting se realiza un plan con un conjunto de ataques dirigidos, según la tecnología que se utilice en la empresa y sus necesidades de seguridad.*

Para ello, los auditores deben de contar con metodologías; elegir qué pruebas se requiere realicen y sobre qué aplicaciones o servicios.

En relación con lo anterior el referido INCIBE menciona que existen diferentes tipos de pruebas de penetración según la información inicial con la que cuenta el auditor, así, pueden ser:

a) **De caja blanca:** si disponen de toda la información sobre los sistemas, aplicaciones e infraestructura, pudiendo simular que el ataque se realiza por alguien que conoce la empresa y sus sistemas;

b) **De caja gris:** si dispone de algo de información pero no de toda;

c) **De caja negra:** si no dispone de información sobre nuestros sistemas; en este caso, se simula lo que haría un ciberdelincuente ajeno.

El Instituto Nacional de Ciberseguridad, concluye que *al realizar el servicio, el auditor o empresa va a intentar traspasar las medidas de seguridad de los equipos informáticos o de aplicaciones, poniendo en riesgo el funcionamiento de los sistemas, así como la información que contengan*.

Una vez expuesto lo anterior y debido a que el presente artículo está relacionado con la ciberseguridad en el SIPOT de la PNT, es pertinente mencionar que el 04 cuatro de junio del presente año, el INAI, dio respuesta a la solicitud 0673800104519, de la cual se desprende que éste no tiene implementado en su totalidad un Sistema de Gestión de Seguridad (SGSI). Sin embargo, actualmente lo está gestionando el área de Seguridad de la Información perteneciente a la Dirección General de Tecnologías de la Información (DGTI) del INAI.

De esta forma, manifiesta el INAI en su respuesta que cuenta con seguridad informática dentro del Instituto necesaria para proteger al SIPOT, misma que comprende desde políticas y controles de seguridad, apegadas al MAAGTICSI, haciendo uso de las mejores prácticas en materia de seguridad informática, alineadas a la norma ISO-27000. De igual forma, refiere que los controles cubren las siguientes áreas en materia de seguridad: Segregación de tareas; Acceso a redes y a los servicios de red; Registro y desregistro de usuarios; Provisión de acceso de usuario; Sistema de gestión de contraseñas; Controles físicos de entrada; Copia de seguridad de la información; Controles de red; Seguridad de servicios de red; Respuesta a incidentes de seguridad de la información; y Aplicación de la continuidad de la seguridad de la información.

De igual forma en la respuesta a la solicitud el INAI, asevera que hace uso de herramientas de propósito específico tanto en el perímetro de comunicaciones del Instituto, en los puntos finales como son *Firewall*, IPS, Antivirus, WAF, para protección de la tecnología que contiene el SIPOT, las cuales son utilizadas para la protección específica, esto es: Control de acceso; Analizador de tráfico; Filtrado *Web*; Prevención y detección de Intrusos; Protección de aplicaciones *Web*; Detección y protección de amenazas avanzadas; y Protección *Antimalware*.

Además, en la respuesta a la solicitud el INAI manifiesta que a través de la programación con la que está construida el SIPOT permite descartar que los sujetos obligados por desconocimiento, malicia y/o negligencia suban archivos que pudieran contener programas dañinos (virus, troyanos, *malware*, etc), toda vez que el SIPOT permite descartar archivos que no cumplen con ciertas características válidas que debe tener un archivo para ser cargado en el SIPOT lo cual disminuye riesgos de cargar programas dañinos. Adicional a esto, la infraestructura del sistema, cuenta con capas de seguridad robustas, desde el perímetro hasta los equipos (*endpoints*).

En su respuesta el INAI manifiesta que las intrusiones no autorizadas al SIPOT que pudieran extraer información, alterarla, borrarla, encriptarla, etc, tales como el *hackeo*, se previene mediante mecanismos de detección y prevención de amenazas avanzadas, así como la protección de seguridad perimetral y seguridad a nivel equipo (*endpoint*).

De igual manera, el INAI refirió en su respuesta que las medidas de resiliencia implementadas en el SIPOT son una alta disponibilidad en los servicios tanto de comunicación como de infraestructura utilizados en los sistemas mencionados.

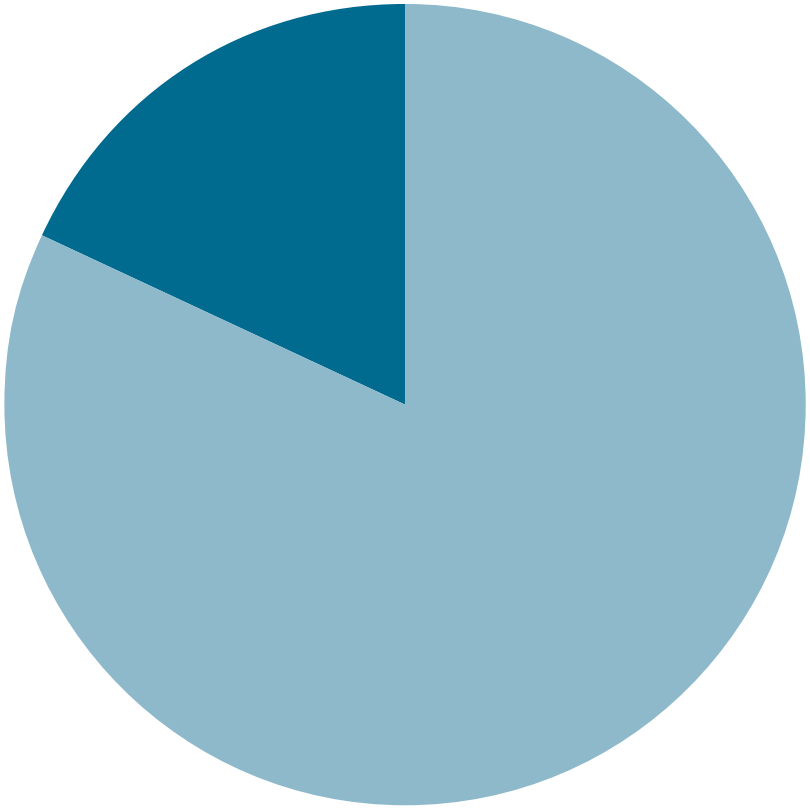
Por otra parte, en relación a ¿cuántos ataques cibernéticos detectados ha sufrido el SIPOT y/o PNT desde su creación y en qué fechas?, el INAI respondió que el SIPOT se encuentra protegido por varias capas de seguridad, las cuales al ser muy robustas generan grandes números de registros mismos que se van sobrescribiendo para la reutilización de recursos de memoria y almacenamiento en los mismos, es por esto que los datos que se proporcionaron son a partir del mes de agosto del año 2018; resaltó el INAI que dichos ataques fueron contenidos por las capas de seguridad, como consecuencia no se convirtieron en incidentes de seguridad que hayan provocado algún riesgo para el citado Instituto. El número de ataques, se ven reflejados en la siguiente tabla:

Periodo	Ago 2018	Sep 2018	Oct 2018	Nov 2018	Dic 2018	Ene 2019	Feb 2019	Mar 2019	Abr 2019	May 2019
No. de ataques	2,564	3,207	891	137	7,064	11,814	12,435	10,620	16,879	12,316

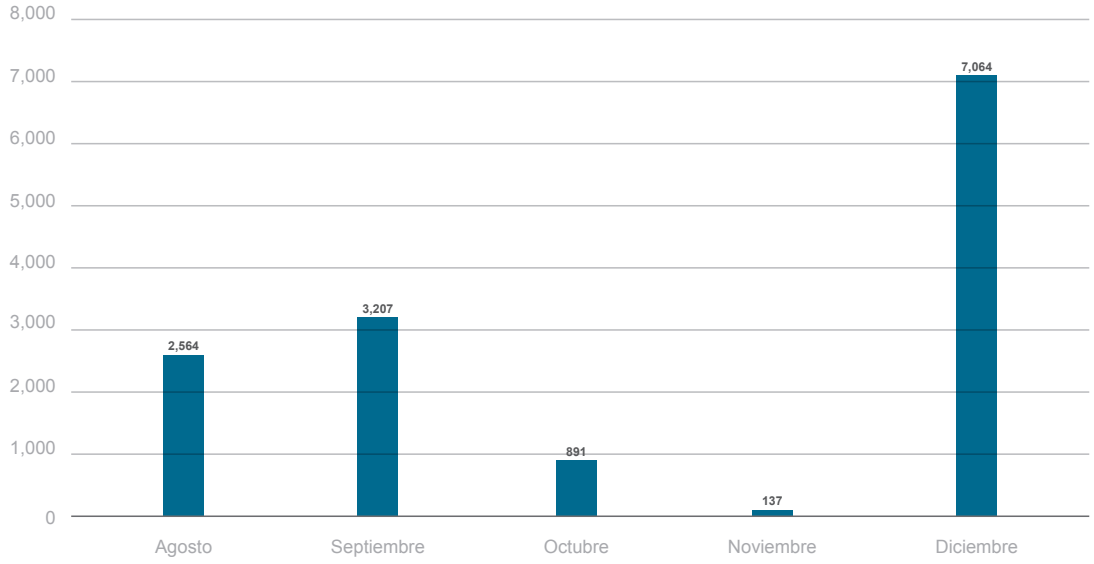
En virtud de lo antes referido la información proporcionada por el INAI, es a partir de agosto del año 2018 (y no desde la implementación del SIPOT, esto es 05 de mayo del año 2016) hasta mayo del año 2019 (derivado que la respuesta a la solicitud de información fue otorgada el 4 de junio del presente año).

De lo anterior se desprende que entre agosto de 2018 a mayo de 2019; ósea en tan solo diez meses el SIPOT recibió **77 mil 927** ataques cibernéticos; lo que se traduce que de **agosto a diciembre del año 2018 fueron 13 mil 863;** y de **enero a mayo del año en curso 64 mil 064** ciberataques, lo cual se ilustra de la siguiente manera:

Número de ataques en 10 meses



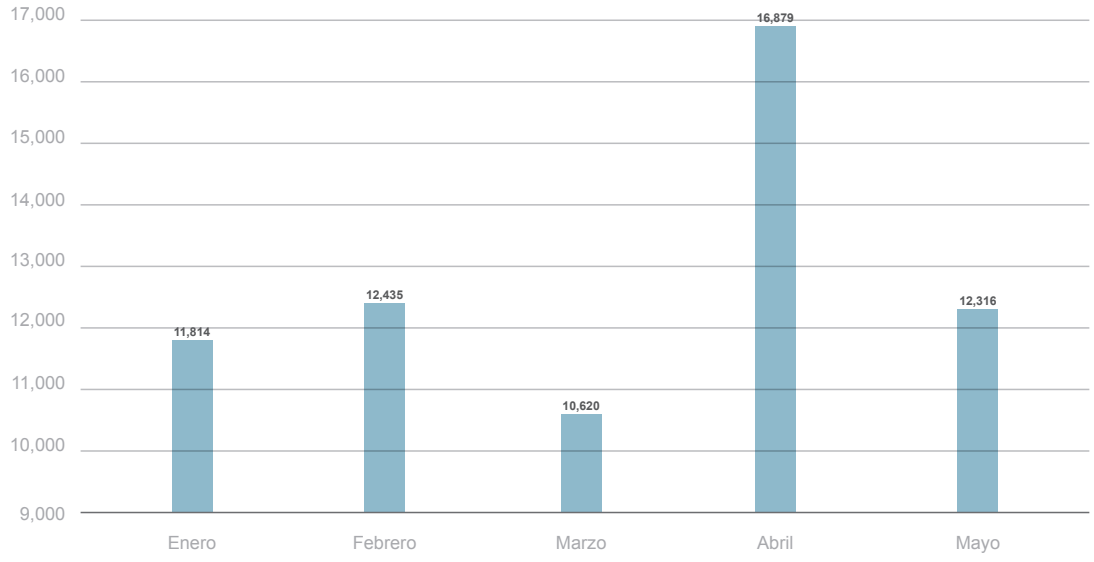
La siguiente gráfica muestra la cantidad de ataques cibernéticos que tuvo en cinco meses el SIPOT, en el año 2018:



2018

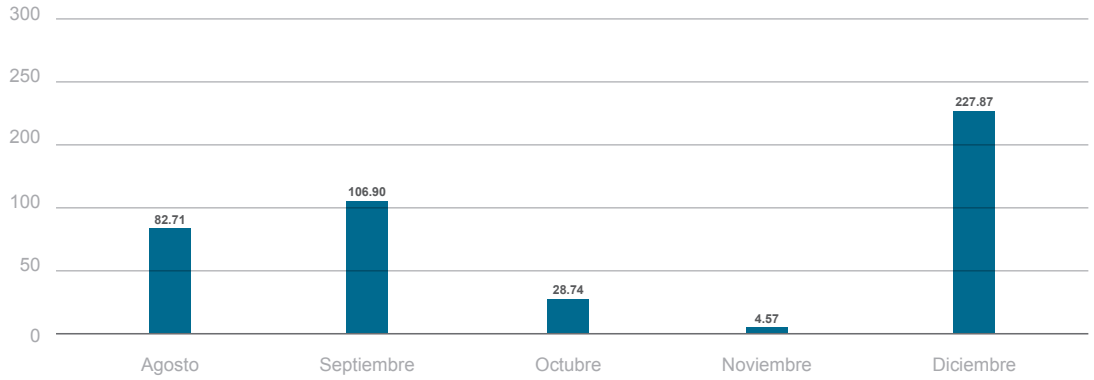
Gráfica de autoría propia

De igual forma, a continuación se visualiza la cantidad de ciberataques que sufrió el SIPOT en cinco meses del año 2019:



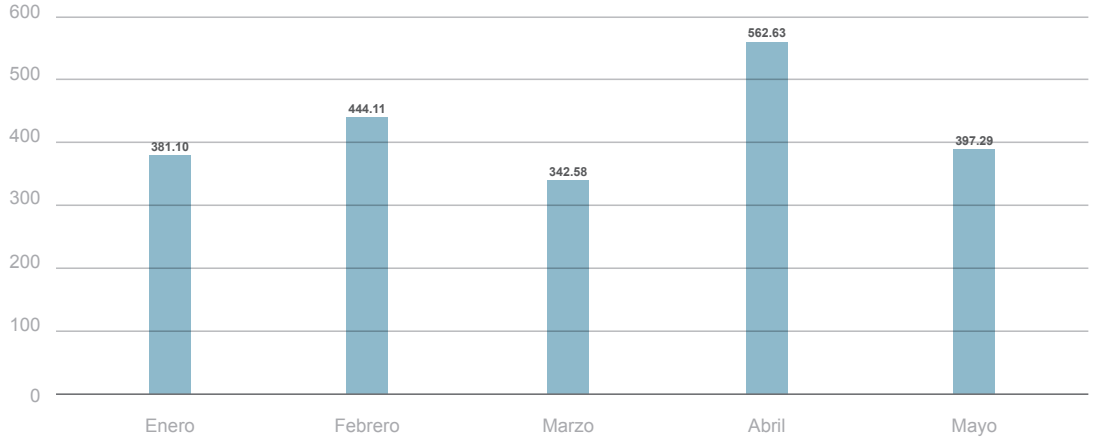
2019

Asimismo, se puede ilustrar la cantidad diaria de ataques cibernéticos recibidos en el SIPOT, por mes durante el año 2018:



2018

En ese mismo sentido, se muestra la cantidad de ciberataques diarios por mes recibidos en el SIPOT, durante el año 2019:



2019

De lo ilustrado en líneas que anteceden, se desprende que en los cinco meses del año 2018, el mes que tuvo menor cantidad de ataques cibernéticos fue noviembre con 137, no obstante el que tuvo más fue diciembre con 7,064.

En ese mismo sentido, en relación al año 2019, el mes que tuvo menor cantidad de ataques cibernéticos fue marzo con 10 mil 620, sin embargo el que tuvo más fue abril con 16 mil 879.

De la información descrita, se puede traducir en que diariamente durante los cinco meses del año 2018, mínimo se recibieron 4.57 ataques ciberataques y máximo 227.87.

Asimismo, se desglosa que diariamente durante los cinco meses del año 2019, mínimo se recibieron 342.58 ataques cibernéticos y máximo 562.63.

Todo lo antes mencionado, se ve reflejado en un acrecentamiento ya sea de una manera anual, mensual o diaria el incrementó de ataques cibernéticos que sufrió el SIPOT entre los cinco meses del año 2018 y de enero a mayo del presente año, es desorbitante.

Es decir, los 13 mil 863 ataques cibernéticos de cinco meses del año 2018 contra los 64 mil 064 ciberataques de enero a mayo del presente año, recibidos por el SIPOT se ve reflejado en un incremento de 362.12% entre 2018 y 2019.

No obstante todas las medidas de seguridad y protección específica con la que cuenta el SIPOT, en 10 meses ha sufrido una cantidad muy considerable de ataques cibernéticos (77 mil 927) y aunque resalta el INAI que dichos ataques fueron contenidos por las capas de seguridad y como consecuencia no se convirtieron en incidentes de seguridad que hayan provocado algún riesgo para ese Instituto; el incremento entre un año y otro es desmedido. Y no estamos hablando de años completos sino de una muestra de cinco meses por cada año; pero el incremento del 362.12% entre un año y otro es preocupante.

Conclusiones

En la política pública transversal de Transparencia, Acceso a la Información y Protección de Datos, sin tomar en cuenta el rediseño de la PNT (08 de abril del año 2019) ha costado alrededor de $40,008.70; esto es en el año 2015 el INAI ejerció 9,663.2 miles de pesos para el desarrollo de la PNT (Primera Etapa). Asimismo, en el año 2016, para continuar la segunda etapa se ejerció un presupuesto de 9,992.6 miles de pesos. En ese mismo, sentido también se invirtió 20,352.9 miles de pesos en la Tercerización de servicios profesionales de informática para los sistemas institucionales.[6]

Por otra parte, como se mencionó al inicio del presente artículo de conformidad con los lineamientos vigésimo, vigésimo primero, del vigésimo octavo al trigésimo primero de los Lineamientos de la PNT, el INAI tiene diversas responsabilidades, entre las que destacan: mantener disponible en todo momento la PNT, para implementar los mecanismos necesarios para que la operabilidad sea garantizada en la medida de lo posible en caso de contingencias o casos fortuitos; vigilar el correcto funcionamiento de la PNT; implementar el mecanismo de recuperación de desastres y contingencias, y el plan de respaldos de la PNT.

No obstante que el INAI es el administrador de la Plataforma, con sus cuatro sistemas SISAI; SIGEMI; SIPOT, y SICOM, de conformidad con el lineamiento décimo cuarto de los Lineamientos de la PNT, será responsabilidad de los organismos garantes verificar de manera periódica y constante los sistemas de la PNT, con la finalidad de dar pronta atención a los mismos.

De igual forma, el Centro de Estudios Estratégicos CEEAG. (2018), a través del libro titulado La Ciberguerra: Sus impactos y desafíos, refiere que el ciberespacio existe en lo virtual, con efectos en lo real, conformando un escenario creado y sustentado, con

[6] Respuesta entregada el 17 de mayo de 2019, a la solicitud de información presentada ante la Auditoría Superior de la Federación, a la cual le correspondió el número de folio 0110000043319.

una intangibilidad en su concreción, pero con un claro impacto cuando es afectado. Los efectos generados en el ciberespacio pueden tener impactos dentro de la dimensión física que ello implica.

En relación con lo anterior, el ciberespacio fue declarado por *The Economist* y las principales potencias mundiales como el quinto dominio después de la tierra, el mar, el aire y el espacio, debido a que durante la primera década del siglo XXI aparecieron nuevos paradigmas de ataque por medio del ciberespacio, los que basados en diferentes motivaciones individuales o colectivas, intentaban afectar a las instituciones, gobiernos y diversas corporaciones empresariales. Lo expresado es ratificado por Clarke, R. y R. Knake (Guerra en la red. Los nuevos campos de batalla, Ariel, 2010) al señalar que: *"el ciberespacio es una zona de guerra donde muchas de las batallas del siglo XXI se van a dar"*, aportando una visualización del ciberespacio como el lugar virtual donde surgirán acciones de amplia variedad y en donde se luchará por ejercer la protección de las redes informáticas.

De igual forma, el CEEAG, en síntesis, establece que el ciberespacio es la expresión de un espacio virtual y vital para que exista la transmisión de la información, razón por lo que se desarrollarán sucesivas acciones de amplia variedad para ejercer el control y la protección de las redes informáticas, originando por consecuencia la necesidad de asegurar el funcionamiento de estos sistemas frente a diversas amenazas.

Es por lo anterior que, en Lineamientos de Política para ciberseguridad y ciberdefensa, Consejo Nacional de Política Económica y Social, elaborados por el Departamento Nacional de Planeación, República de Colombia, la ciberseguridad puede ser definida como la *capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética*.

Ahora bien, en razón a la respuesta entregada el 04 cuatro de junio del año 2019 dos mil diecinueve, a la solicitud de información presentada ante el INAI, a la cual le correspondió el número de folio 0673800104519, nos hemos dado cuenta de los controles que cubren las áreas en materia de seguridad; del uso de herramientas de propósito específico tanto en el perímetro de comunicaciones del INAI como en los puntos finales como son *Firewall*, IPS, Antivirus, WAF, para protección de la tecnología que contiene el SIPOT.

Asimismo, el SIPOT permite descartar archivos que no cumplen con ciertas características válidas que debe cumplir un archivo para ser cargado en el SIPOT lo cual disminuye riesgos de cargar programas dañinos. Adicional a esto, la infraestructura del sistema, cuenta con capas de seguridad robustas, desde el perímetro hasta los equipos (*endpoints*).

De igual forma, las intrusiones no autorizadas al SIPOT que pudieran extraer información, alterarla, borrarla, encriptarla, etc, tales como el *hackeo*, se previene mediante mecanismos de detección y prevención de amenazas avanzadas, así como la protección de seguridad perimetral y seguridad a nivel equipo (*endpoint*).

Aunado a lo anterior, las medidas de resiliencia implementadas en el SIPOT son una alta disponibilidad en los servicios tanto de comunicación como de infraestructura utilizados en los sistemas.

Sin embargo, a pesar de todas las medidas y prevenciones tomadas por el INAI el SIPOT ha sufrido en tan solo diez meses 77,927 ataques cibernéticos, desglosado de agosto a diciembre de 2018 y de enero a mayo de 2019, con 13,863 y 64064 ciberataques respectivamente. Viéndose entre cinco meses de un año y cinco meses de otro un incremento de 362.12%; pero la interrogante sería ¿seguiremos esperando que la cantidad de ataques aumente?, simularemos que no es nuestra responsabilidad, o cambiaremos la mentalidad en buscar una solución a lo antes vertido.

Cabe hacer mención que la responsabilidad no solo le corresponde al INAI por ser el administrador de la PNT junto con sus sistemas entre ellos el SIPOT; sino también a los organismos garantes del país.

El presente artículo es un tema poco explorado, el cual puede utilizarse en futuras investigaciones y servir de base para mejorar la seguridad que contiene la PNT en específico el SIPOT y poder obtener ciertos patrones de ataques.

Propuesta para modificar el estado de las cosas

Por lo antes expuesto, considero que no debemos de ser indiferentes ante el problema planteado, sino buscar soluciones. Es por ello que se propone que no solo el INAI, sino todos los organismos garantes del país y ciertos sujetos obligados de las diversas entidades federativas, que cuenten con los recursos idóneos, realicen la contratación de un servicio de *pentesting*, y éste sea específico y defina la manera idónea de tal suerte que no exista ninguna duda del servicio contratado, entre los temas que se pueden contemplar en la elaboración del contrato, las autorizaciones; la información que estará disponible; la técnica que se utilizara para la intrusión; el tratamiento de la información que se pueda obtener.

María del Rosario Navarro Zamora

Es licenciada en Derecho por la Universidad Michoacana de San Nicolás de Hidalgo, Maestra en Derecho Constitucional y Amparo por el Institutito de Formación e Investigaciones Jurídicas de Michoacán y Especialista en Gestión, Publicación y Protección de Información, por el Centro de Estudios Superiores de la Información Pública y Protección de Datos Personales; cuenta con diversos diplomados en transparencia, protección de datos personales, sistemas anticorrupción, gobierno abierto, gestión documental y seguridad de la información. Actualmente, labora en la Coordinación General de Evaluación y Gestión Documental del ITEI.

Referencias y/o fuentes de consulta

Ley General de Transparencia y Acceso a la Información Pública, Diario Oficial de la Federación, 04 de mayo de 2015.

Acuerdo del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, por el que se aprueban loa Lineamientos para la implementación y operación de la Plataforma Nacional de Transparencia, Diario Oficial de la Federación, 04 de mayo de 2016.

Respuesta entregada el 04 de junio de 2019, a la solicitud de información presentada ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, a la cual le correspondió el número de folio 0673800104519.

Respuesta entregada el 17 de mayo de 2019, a la solicitud de información presentada ante la Auditoría Superior de la Federación, a la cual le correspondió el número de folio 0110000043319.

INCIBE. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. 29/07/2019, de Instituto Nacional de Ciberseguridad Sitio web: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

Centro de Estudios Estratégicos CEEAG. (2018). *La Ciberguerra: Sus impactos y desafíos.* Chile: Comité Editorial del CEEAG.

Calvente Arturo M. *Resiliencia: un concepto clave para la sustentabilidad*, Universidad Abierta Interamericana, Centro de Altos Estudios Globales.

Cano, Jeimy J. *Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global*, Sistemas (Asociación Colombiana de Ingenieros de Sistemas), vol. 000, Nº 0119 (abr-jun. 2011).

Hoecker Marcos Robledo. Subsecretario de Defensa Secretario Ejecutivo, Comité Interministerial sobre Ciberseguridad, PNCS 2017.

Unión Internacional de Telecomunicaciones, referida en Alejandro Gómez Abutridy, “Ciberseguridad y Ciberdefensa, Dos elementos de la Ciberguerra”, *Memorial del Ejército de Chile*, Nº 492, agosto 2014.