UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

La seguridad cibernética en México

TESIS

Que para obtener el título de

Ingeniero en Telecomunicaciones

P R E S E N T A

Everardo Escamilla Diego

DIRECTOR DE TESIS

Ing. Carlos Gabriel Girón García

Ciudad Universitaria, Cd. Mx., 2018

Contenido

Introducción

El presente documento tiene por objetivo proponer las bases de una estrategia de seguridad cibernética aplicable a México. Para lograrlo, el trabajo presenta en su primer capítulo, un análisis de las principales recomendaciones y normas de los más reconocidos organismos internacionales en el sector, en segundo lugar se expone un análisis de los casos internacionales más relevantes en el sector, y en tercer lugar se muestra la situación actual que atraviesa México en cuanto a seguridad cibernética se refiere, logrando así reunir un conjunto suficiente de insumos para generar, mediante un criterio justo, un conjunto de propuestas para una estrategia de seguridad cibernética en México.

En abril de 1967 el Ingeniero Willis H. Ware, un hombre adelantado a su era, publicaba un artículo llamado *Security and Privacy in Computer Systems* (Seguridad y privacidad en sistemas informáticos). Motivado por la creación del ARPAnet en 1960, sistema precursor del Internet, Ware señala en su artículo que

> Mientras los equipos se encontraban en cámaras aisladas, la seguridad no era un problema. Pero una vez que varios usuarios puedan acceder a los datos desde lugares no protegidos, cualquier persona con ciertas habilidades podría introducirse en la red y, una vez dentro, vagar a su voluntad, incluyendo el robo de archivos clasificados y secretos. (Ware, Willis H., 1967).

De esta forma, tenemos que hace más de 50 años fueron planteadas por primera vez las implicaciones en materia de seguridad y privacidad que acompañan al uso del espacio cibernético. Desde entonces las telecomunicaciones y sistemas informáticos han evolucionado de forma exponencial, lo que implica que también lo han hecho las amenazas. La pregunta que motiva y fundamenta este trabajo es si esa evolución también se ha visto reflejada en los sistemas de defensa cibernética de México, y en caso de que no lo haya hecho, cuáles medidas son las más urgentes de emprender.

En lo concerniente al capítulo primero, el análisis se centró en el estudio de las recomendaciones y normas emitidas por cinco organizaciones influyentes en el sector, la Unión Internacional de Telecomunicaciones, la Organización Internacional de Normalización, el Instituto de Ingenieros Eléctricos y Electrónicos, el Instituto Europeo de Normas de Telecomunicaciones y la Fuerza de Tareas de Ingeniería de Internet, presentando un conjunto de fichas técnicas que buscan sintetizar el contenido de la norma o recomendación en cuestión. Al respecto, cabe señalar que dichas organizaciones promueven recomendaciones y normas en un gran número de campos relacionados con las telecomunicaciones, la informática y las ingenierías, por lo que se debe advertir al lector que las normas presentadas en dicho capítulo no reflejan en su totalidad los campos de estudio de las instituciones analizadas. A su vez, en el primer capítulo se incluye una sección que busca comparar las normas analizadas, categorizándolas según su campo de aplicación.

Con respecto al segundo capítulo, este se enfoca en el estudio de los actos emprendidos por diversos países, dividiéndose en dos grupos. En el primer grupo se encuentran algunos de los que han sido señalados por diversos organismos internacionales como los países con las mejores prácticas en materia de seguridad cibernética, encontrando en este bloque a los Estados Unidos de América, la República de

Estonia, Israel y la República de Corea. En un segundo bloque se estudian los casos de países cuyas experiencias particulares puedan aportar a la madurez de México en el objeto que nos ocupa. Se trata de Colombia, Reino Unido y la Unión Europea. En ambos bloques, el estudio buscó presentar los actos emprendidos en el campo gubernamental, jurídico, académico, industrial y, de ser posible, militar.

Habiendo recolectado una amplia variedad de elementos relacionados con la seguridad cibernética en el contexto internacional, se procedió al estudio de la situación que guarda México en relación a la misma. Este tema, abordado en el tercer capítulo, siguió una metodología similar al capítulo segundo en cuanto al estudio sectorial del problema en cuestión, buscando poner sobre la mesa los elementos con los que cuenta actualmente México para hacer frente a las amenazas del entorno cibernético, mostrando así las principales áreas de oportunidad que se presentan a México en este ámbito.

Por último, el capítulo final busca condensar todos los resultados obtenidos en los capítulos anteriores, para lograr cumplir con el objetivo principal de este documento, y proponer así las bases de una estrategia de seguridad cibernética aplicable a México. Buscando ser consistentes con los capítulos anteriores, las recomendaciones ofrecidas se presentan por sector, señalando lo que se considera el ideal inmediato que se debe buscar en el mismo.

Problemática a resolver

México es un país que paulatinamente se ha integrado a la era digital, cada vez a pasos más grandes. Sin embargo, la evolución de la seguridad cibernética de México no ha obedecido a ese ritmo, sino a uno más lento, no obstante, lo que sí ha evolucionado a un ritmo aún mayor que la integración digital son las amenazas del entorno cibernético. Lo anterior se resume en un escenario en el que México avanza poco a poco a una integración digital y lo que le espera es un entorno que es cada vez más amenazador. El no tener la capacidad de hacer frente a esas amenazas se traduce en pérdidas millonarias en robo de información, espionaje, tráfico de datos personales, extorción, y un sinfín de actividades que frenan y condicionan la evolución digital de un país.

La experiencia internacional nos ha mostrado que el método más efectivo para hacer frente a las amenazas del entorno cibernético es un modelo de cooperación y acción que sume los esfuerzos de todos los sectores involucrados en dicho entorno.

En México los esfuerzos para asegurar el entorno cibernético han sido aislados e independientes entre sí, por lo que urge la planificación de una estrategia que marque las directrices e involucre a todos los sectores interesados para construir la seguridad cibernética en México

Objetivo

El presente documento tiene por objetivo proponer las bases de una estrategia de seguridad cibernética aplicable a México. Lo anterior derivado de un análisis de la experiencia internacional, abordada desde la perspectiva de la regulación y normatividad, hasta la aplicación de políticas y estrategias de diferentes países, así como de un análisis del estatus mexicano en seguridad cibernética.

Marco conceptual

Cibernética

La palabra cibernética proviene del vocablo griego *kybernêtikos,* el que gobierna, el que controla. Este término ha sido utilizado en diferentes campos de aplicación, por lo que goza de enfoques distantes entre sí. El enfoque aquí abordado tiene su primer antecedente en 1948, cuando Norbert Wiener (1894-1964), matemático estadounidense, publicó su libro *Cybernetics: or control and communication in the animal and the machine* (Cibernética: o el control y la comunicación en el animal y la máquina). En él, Wiener intenta establecer sus fundamentos como ciencia que se ocupa de cualquier sistema, anima o artificial, en el que se produzcan funciones de regulación y control, así como las leyes generales que gobiernan estos fenómenos (p. 41).[1] Diversos personajes han abonado a la construcción del concepto, hasta definirse como la ciencia que estudia los sistemas de comunicación y de regulación automática de los seres vivos y los aplica a sistemas electrónicos y mecánicos que se parecen a ellos (p.37).[2]

Informática

Fix Fierro (1996) menciona que el término informática surge de la combinación de las palabras "información" y "automática", por lo que se puede entender como la ciencia del tratamiento automático de información, primordialmente entre computadoras. En ese tenor de ideas, se entenderá por sistema informático como un conjunto de elementos que al interactuar entre sí permite el procesamiento automático de datos.

Seguridad

Entendiendo la seguridad como la ausencia de peligro o riesgo, este concepto matizará un poco según cambie el campo de aplicación de la misma. En consecuencia, resulta conveniente conceptualizar la seguridad en función de su campo de aplicación.

Seguridad cibernética

Cuando se habla de seguridad cibernética se puede llegar a pensar que es un término tan abstracto que dice, por sí mismo, muy poco. Para la Unión Internacional de Telecomunicaciones, la definición seguridad cibernética o ciberseguridad, si se traduce directamente del idioma inglés, se encuentra contenida en la recomendación UIT-T X.1205-Aspectos generales de la ciberseguridad-, que a la letra dice:

> el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno.

(UIT, 2008).[3]

Por lo tanto, la seguridad cibernética es el conjunto de recursos, medios y métodos destinados a proteger la información, los dispositivos informáticos, los servicios y aplicaciones, los sistemas de comunicaciones, lo usuarios y demás elementos que interactúen entre sí para generar un entorno cibernético.

Seguridad informática

Del párrafo anterior se desprende que el sistema informático es solo una parte del entorno cibernético, por lo que la seguridad informática será una parte de la seguridad cibernética. Al respecto, Costas (2014) menciona que la seguridad informática consiste en asegurar que todos los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se dedicó y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentran acreditadas y dentro de los límites de su autorización (p. 19). [4]

Seguridad técnica de las redes

Asimismo, la seguridad técnica de las redes se refiere a las arquitecturas de red y protocolos de comunicación, así como protocolos de acceso a la red, que tienen por objeto garantizar el acceso, disponibilidad, integridad y confidencialidad de la red de telecomunicaciones. [5]

Seguridad para las comunicaciones

En función del párrafo anterior, podemos definir la seguridad para las comunicaciones como los mecanismos, protocolos, programas informáticos o acciones tecnológicas que puedan emplearse para garantizar la integridad, confidencialidad y confiabilidad de las comunicaciones.

Seguridad para la infraestructura

También llamada seguridad física, Costas (2014) define a la seguridad para la infraestructura como los mecanismos de seguridad dentro y alrededor de la ubicación física de los recursos físicos que son parte del sistema, eso incluye la aplicación de barreras físicas y procedimientos de control, así como los medios de acceso remoto al y desde las instalaciones (p. 50). [6]

Seguridad para los usuarios

Siguiendo el orden de ideas de los párrafos, podemos entender como seguridad para los usuarios como el conjunto de políticas, medidas de acceso, buenas prácticas, y demás medidas que garanticen que la trayectoria del usuario por el entorno cibernético no se vea afectado por las amenazas que en él existen.

Datos personales

Este concepto se refiere a toda aquella información asociada a una persona o individuo que lo hace identificable del resto de las personas y/o como parte de un grupo determinado de individuos, por ejemplo: nombre, domicilio, teléfono, fotografía, huellas dactilares, sexo, nacionalidad, edad, lugar de nacimiento, raza, filiación, preferencias políticas, fecha de nacimiento, imagen del iris del ojo, patrón de la voz, etc. La idea central de este concepto es común en las legislaciones de protección de datos que distintos países han redactado. [7]

Referencias del Marco Conceptual

[1] Fix Fierro, Héctor (1996). *Informática y documentación jurídica.* 2da ed. México: UNAM, Instituto de Investigaciones Jurídicas.

[2] Ríos Estavillo, Juan José (2016). *Derecho e informática en México: informática jurídica y derecho de la informática*. México: UNAM.

[3] Unión Internacional de Telecomunicaciones (2008). *UIT-T Rec. X.1205 (04/2008) Aspectos generales de la ciberseguridad.* Ginebra: UIT.

[4] Costas Santos, Jesús (2014). *Seguridad Informática.* Madrid: Ra-Ma.

[5] Unión Internacional de Telecomunicaciones (2006). *La seguridad de las telecomunicaciones y las tecnologías de la información*. Ginebra: UIT.

[6] Costas Santos, Jesús (2014). *Seguridad Informática.* Madrid: Ra-Ma.

[7] Sánchez Pérez, Gabriel & Rojas González, Isaí (2012, junio). Leyes de protección de datos personales en el mundo y la protección de datos biométricos – parte I. *Revista .Seguridad, núm. 13*, Recuperado el 9 de febrero de 2018 de https://revista.seguridad.unam.mx/numeros/numero-13

Capítulo I: Recomendaciones y Normas Internacionales

Se estima que la población mundial supera los 7,000 millones de habitantes y, aunque la tasa de natalidad ha ido disminuyendo en la última década, se espera que para el 2050 haya alrededor de 9,600 millones de habitantes [1]. Los datos duros hablan por sí mismos, el progreso no espera a nadie. Las cifras de la UIT muestran que el 95% de la población mundial habita en áreas con cobertura de redes celulares y el 52.3% de los hogares del mundo cuenta con acceso a internet. Aunque es cierto que la penetración del internet es contrastante entre las ciudades más desarrolladas (87%) contra la penetración del mismo en las ciudades menos desarrolladas (17%), los datos sirven para hacer evidente una cuestión central, el uso de las telecomunicaciones avanza más rápido que la población mundial. Si es que llegara a quedar duda de esto, sólo hay que observar el incremento del ancho de banda utilizado mundialmente, simplemente en inicios del 2016 fue de un aproximado de 185,000 Gbit/s comparado con los 30 000 Gbit/s de 2008[2].

Producir tecnología sin regulación tendería directamente al caos, por lo que son necesarios organismos que se aseguren que exista interconexión entre tecnologías viejas y nuevas y que permitan compatibilidad entre los equipos que interactúan en la sociedad, por mencionar algunas tareas imprescindibles.

En los datos presentados se puede notar que la presencia de las telecomunicaciones es claramente mundial, es por ello que el desarrollo de las mismas debe ser de la misma dimensión. Las regulaciones importantes en materia de telecomunicaciones no pueden obedecer fronteras. Para vencer este impedimento existen organizaciones de carácter normativo que emiten recomendaciones, normas y estándares para regular aspectos esenciales de las telecomunicaciones como los son las posiciones orbitales, los puntos de interconexión, los estándares para la implementación de tecnologías, etcétera. Para ejemplificar lo mencionado anteriormente se puede decir que “Seguramente en internet […] la mayor parte de las regulaciones que se consideren imprescindibles tendrán que hacerse a escala universal”. (Muñoz, 2000)

Perspectiva histórica

Los avances que hoy se presentan en materia de seguridad cibernética han ido evolucionado a lo largo de las últimas décadas. Desde inicios de la década de los sesenta hasta finales de la década de los ochenta, las redes de datos y su administración eran una actividad correspondiente a computadoras locales sin las capacidades técnicas de una administración remota. Las bases de la discusión sobre la gestión de la seguridad en las redes de datos comenzaron a finales de la década de los ochenta. Pues, para el año de 1989, ya existían cuatro productos comerciales que se dirigían a la gestión de las redes de datos, los cueles eran:

- *Netview* de la compañía IBM (por sus siglas en inglés de *International Business Machine’s*)

- Arquitectura de gestión empresarial (EMA, por sus siglas en ingles de *Enterprise Management Architecture*) de la compañía DEC (por sus siglas en inglés de *Digital Equipment Corporation's*)
- Arquitectura de gestión de red unificada (UMNA, por sus siglas en inglés de Unified Network Management Architecture) de los Laboratorios Bell de la compañía AT&T (por sus siglas en inglés de *American Telephone & Telegraph*), y
- *OpenView* de la compañía HP.

El reconocimiento que estas y otras empresas de telecomunicaciones dieron a la importancia de actividades de gestión de las redes de datos derivó en estructurar dichas actividades en áreas de gestión.

En la década de los ochenta, la Unión Internacional de Telecomunicaciones (en adelante UIT) en conjunto con la Organización Internacional de Normalización (en adelante ISO) y la Comisión Electrotécnica Internacional (en adelante IEC) desarrollaron la norma internacional ISO/IEC 7498-1 (UIT-T X.200) que presenta un modelo de referencia para la interconexión para sistemas abiertos. A pesar de dedicar únicamente 2 de 60 páginas totales a la gestión de los activos de la red, esta norma marca el origen de las normas en materia de seguridad cibernética al incluir en el modelo de interconexión controles de seguridad en la gestión de los procesos de la capa de aplicación del modelo OSI. El tema de la seguridad en la gestión de los activos de la red continuó creciendo, y fue analizado con mucha más seriedad en las normas internacionales ISO/IEC 7498-4 (UIT-T X.700) e ISO/IEC 7498-2 (UIT-T X.800).

La norma internacional ISO/IEC 7498-4 (UIT-T X.700): Marco de gestión para la interconexión de sistemas abiertos para aplicaciones del Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones (UIT-T) categoriza la gestión de los activos en la red en cinco áreas principales, las cuales son la gestión de fallas, la gestión de configuración, la gestión de contabilidad, la gestión de rendimiento y la gestión de seguridad. De esta última, declara que son de su interés las siguientes funciones:

- la creación, supresión y control de servicios y mecanismos de seguridad;
- la distribución de información relativa a la seguridad, y
- la señalización de sucesos relacionados con la seguridad.

A pesar de dedicar únicamente un pequeño párrafo a la gestión de seguridad, esta recomendación presenta una serie de definiciones y conceptos que fueron de relevancia para las primeras normas exclusivas en materia de seguridad en las redes de telecomunicaciones. Muchos de estos conceptos fueron utilizados en la norma internacional ISO/IEC 7498-2 (UIT-T X.800).

La norma internacional ISO/IEC 7498-2 (UIT-T X.800): Arquitectura de seguridad de la interconexión de sistemas abiertos fue publicada a principios de la década de los noventa. Esta norma, enfocada completamente a la seguridad de los activos en la red, contiene las bases y conceptos que son empleados en recomendaciones y normas vigentes. El estudio de dichas normas y recomendaciones se aborda posteriormente en este Capítulo. Sin embargo, resulta conveniente describir los aspectos englobados por la norma internacional ISO/IEC 7498-2 (UIT-T X.800) para poder establecer un contexto básico y comprender mejor las normas y recomendaciones subsecuentes.

La recomendación UIT-T X.800 se define a sí misma como un marco de referencia, es decir, no presenta aspectos técnicos en materia de seguridad, lo cual queda claramente señalado en su alcance:

> Se han identificado servicios y mecanismos básicos de seguridad y su ubicación apropiada para todas las capas del modelo de referencia básico. Además, se han establecido las relaciones arquitecturales entre los servicios y mecanismos de seguridad y el modelo de referencia. Pueden necesitarse otras medidas de seguridad en los sistemas extremos (o sistemas de extremo), instalaciones y organizaciones.

Jacobs (2014) menciona que el valor central de esta recomendación radica en la introducción y definición de los siguienres conceptos:

- cinco servicios primarios de seguridad en la red;
- un conjunto de mecanismos de seguridad específicos en la red, y
- la gestión de los mecanismos de seguridad.

Debido a la importancia que cobraron los conceptos presentados en esta recomendación en normas y recomendaciones posteriores, es conveniente realizar una descripción detallada de los mismos.

Los servicios de seguridad primarios definidos en esta recomendación son usados en la práctica al aplicarse en las capas del modelo OSI correspondientes combinándose con diferentes protocolos para satisfacer las políticas de seguridad de la organización, los requisitos y/o reglas de la misma. En esta recomendación se definen cinco servicios básicos de seguridad con sus respectivos servicios específicos (véase Tabla 1.1.1):

- autenticación: estos servicios proporcionan la autenticación de una entidad par comunicante y de la fuente de datos;
- control de acceso: este servicio proporciona protección contra el uso no autorizado de recursos accesibles mediante la interconexión se sistemas abiertos;
- confidencialidad de los datos: estos servicios proporcionan la protección de los datos contra la revelación no autorizada;
- integridad de los datos: estos servicios contrarrestan las amenazas activas mientras dura la conexión, y
- no repudio: estos servicios proporcionan datos de prueba de entrega y origen entre el destinatario y el origen de la conexión.

Tabla 1.1.1: Servicios específicos de seguridad y su relación con las capas del modelo OSI de la Recomendación UIT-T X.800. Fuente: Creación propia [3]

Servicio de seguridad	**Servicio específico**	**Capas donde se suministra el servicio**						
		1	**2**	**3**	**4**	**5**	**6**	**7**

Autenticación	Autenticación de entidad par	-	X*	X	X	-	-	X
	Autenticación del origen de los datos	-	X*	X	X	-	-	X
Control de acceso	Control de acceso	-	X*	X	X	-	-	X
Confidencialidad de los datos	Confidencialidad de los datos en modo con conexión	X	X	X	X	-	X	X
	Confidencialidad de los datos en modo sin conexión	-	X	X	X	-	X	X
	Confidencialidad de campos seleccionados	-	-	-	-	-	X	X
	Confidencialidad del flujo de tráfico	X	-	X	-	-	-	X
Integridad de los datos	Integridad en modo con conexión con recuperación	-	-	-	X	-	-	X
	Integridad en modo con conexión sin recuperación	-	X*	X	X	-	-	X
	Integridad de campos seleccionados en modo con conexión	-	-	-	-	-	-	X
	Integridad en modo sin conexión	-	X*	X	X			X
	Integridad de campos seleccionados en modo sin conexión	-	-	-	-	-	-	X
No repudio	No repudio con prueba del origen	-	-	-	-	-	-	X
	No repudio con prueba de la entrega	-	-	-	-	-	-	X

X El servicio debe incorporarse en las normas de la capa.

\- No se suministra el servicio.

* La incorporación de estos servicios a las normas de las capas no forman parte original de la Recomendación UIT-T X.800, sino que fueron agregados en la Enmienda 1 de dicha recomendación.

Con el fin de garantizar algunos de los cinco servicios principales de seguridad, la Recomendación UIT-T X.800 sugiere que se utilicen mecanismos de seguridad específicos en la capa correspondiente, según sea el caso. La Tabla 1.1.2 muestra la relación de cada mecanismo de seguridad específico con el servicio

principal de seguridad en el que puede utilizarse. Esos mecanismos de seguridad específicos se describen a continuación junto con las actividades propias de su gestión.

- Cifrado: proporciona la confidencialidad de la información de datos o del flujo de tráfico y puede desempeñar una función en varios otros mecanismos de seguridad o complementarlos. La gestión del cifrado comprende:
    - la interacción con la gestión de claves;
    - el establecimiento de parámetros criptográficos, y
    - la sincronización criptográfica.
- Mecanismos de firma digital: se componen de dos procedimientos: la firma de una unidad de datos y la verificación de una unidad de datos firmada. La gestión de los mecanismos de firma digital puede comprender:
    - la interacción con la gestión de claves;
    - el establecimiento de parámetros y de algoritmos criptográficos, y
    - la utilización de un protocolo entre las entidades comunicantes y, eventualmente, un tercero.
- Mecanismos de control de acceso: pueden utilizar la identidad autenticada, la información o las capacidades de un elemento de la red, para determinar y aplicar los derechos de acceso de dicho elemento. La gestión de los mecanismos de control de acceso puede comprender la distribución de los atributos de seguridad (incluidas las contraseñas) o las actualizaciones de listas de control de acceso o de listas de capacidades.
- Mecanismos de integridad de datos: la integridad de los datos tiene dos aspectos: la integridad de una sola unidad de datos o de un solo campo, y la integridad de un tren de unidades de datos o de campos de unidad de datos. La gestión de integridad de los datos puede comprender:
    - la interacción con la gestión de claves;
    - el establecimiento de parámetros y de algoritmos criptográficos, y
    - la utilización de un protocolo entre las entidades comunicantes.
- Mecanismo de intercambio de autenticación: consiste en el uso de información de autenticación, como contraseñas, suministradas por una entidad expedidora y verificadas, por la entidad receptora, técnicas criptográficas y uso de características y/o propiedades de la entidad. La gestión de autenticación puede comprender la distribución de información descriptiva, de contraseñas o de claves entre las entidades que deben efectuar una autenticación.
- Mecanismo de relleno de tráfico: son utilizados para proporcionar diversos niveles de protección contra análisis del tráfico. Este mecanismo puede ser eficaz solamente si el relleno de tráfico está protegido por un servicio de confidencialidad. La gestión de relleno de tráfico puede comprender:
    - velocidades de datos especificadas previamente;
    - especificación de velocidades binarias aleatorias;
    - especificación de características de mensajes, como la longitud, y
    - variación deliberada de la especificación, eventualmente en función de la hora y/o del calendario.
- Mecanismo de control de encaminamiento: mediante este mecanismo, las rutas pueden elegirse dinámicamente o por acuerdo previo con el fin de utilizar sólo subredes, relevadores o enlaces físicamente seguros. La gestión de control encaminamiento puede comprender la definición de los

enlaces o las subredes que se consideran seguros, o de confianza, con respecto a determinados criterios.

- Mecanismo de notarización: mediante la provisión de este mecanismo de seguridad, pueden garantizarse las propiedades sobre los datos comunicados entre dos o más entidades, tales como su integridad, origen, fecha y destino. La gestión de notarización puede comprender:
    - la distribución de información relativa a los notarios;
    - la utilización de un protocolo entre un notario y las entidades comunicantes; y
    - la interacción con notarios.

Tabla 1.1.2: Relación entre servicios de seguridad y mecanismos de seguridad de la Recomendación UIT-T X.800. Fuente: Creación propia [4]

	Cifrado	Firma Digital	Control de acceso	Integridad de datos	Intercambio de automatización	Relleno de trafico	Control de encaminamiento	Notarización
Autenticación de entidad par	X	X	-	-	X	-	-	-
Autenticación del origen de los datos	X	X	-	-	-	-	-	-
Control de acceso	-	-	X	-	-	-	-	-
Confidencialidad de los datos en modo con conexión	X	-	-	-	-	-	X	-
Confidencialidad de los datos en modo sin conexión	X	-	-	-	-	-	X	-
Confidencialidad de campos seleccionados	X	-	-	-	-	-	-	-
Confidencialidad del flujo de tráfico	X	-	-	-	-	X	X	-

Integridad en modo con conexión con recuperación	X	-	-	X	-	-	-	-
Integridad en modo con conexión sin recuperación	X	-	-	X	-	-	-	-
Integridad de campos seleccionados en modo con conexión	X	-	-	X	-	-	-	-
Integridad en modo sin conexión	X	X	-	X	-	-	-	-
Integridad de campos seleccionados en modo sin conexión	X	X	-	X	-	-	-	-
No repudio con prueba del origen	-	X	-	X	-	-	-	X
No repudio con prueba de la entrega	-	X	-	X	-	-	-	X

X Se considera que el mecanismo es apropiado.

- Se considera que el mecanismo no es apropiado.

En el año de 1996 fue publicada la Recomendación UIT-T X.800 – Enmienda 1, pues se consideró que era necesario ampliar los servicios de seguridad de la capa de enlace de datos para tomar en cuenta la seguridad de las redes de área local, LAN (por sus siglas en inglés de *Local Area Network*). Este documento establece lo observado en la Tabla 1.1.2, donde se muestran los servicios de seguridad que la capa de enlace de datos puede proporcionar.

Unión Internacional de Telecomunicaciones.

La Unión Internacional de Telecomunicaciones, en adelante UIT, es el organismo especializado de la Organización de las Naciones Unidas, ONU, para las Tecnologías de la Información y la Comunicación, TIC. La UIT a través del Reglamento de Radiocomunicaciones es la encargada de atribuir el espectro radioeléctrico y adjudicar las posiciones orbitales de satélites con sus bandas de frecuencias asociadas a escala mundial, también elabora normas técnicas para garantizar la interconexión de las redes y tecnologías y promueve el acceso a las TIC en poblaciones cuyo desarrollo en el sector ha sido insuficiente. Con sede en Ginebra, Suiza, la UIT es una asociación público-privada con 193 países miembros y más de 700 entidades del sector privado e instituciones académicas. [5].

El interés de la UIT en materia de seguridad en las redes no se ha quedado atrás en cuestión de la emisión de recomendaciones con el fin de armonizar las políticas y estándares de seguridad a nivel internacional.

El sector de normalización de las telecomunicaciones de la UIT, (UIT-T), ha emitido diversas recomendaciones en materia de seguridad en las telecomunicaciones, principalmente en la Serie X: redes de datos, comunicaciones de sistemas abiertos y seguridad, y en la Serie Y: infraestructura mundial de la información, aspectos del protocolo internet y redes de la próxima generación. Sin embargo, también es posible encontrar recomendaciones con contenido referente a seguridad en las telecomunicaciones en otras series.

Dentro del sector de UIT-T existe un grupo de trabajo que se dedica específicamente al ámbito de la seguridad, el grupo de estudio 17. El SG 17 (por sus siglas en inglés de *Study Group 17*) tiene su origen en el año 2001 tras la fusión del grupo de estudio 10 y el grupo de estudio 7, cuyos orígenes datan desde 1972 y 1968, respectivamente. El grupo de estudio 17 tiene dentro de sus responsabilidades profundizar en temas de seguridad, gestión de identidad y leguajes y técnicas de descripción. Las normas resultantes del ejercicio de sus responsabilidades se encentran en su mayoría en la Serie X. Sin embargo, también han participado, aunque con menor frecuencia, en las Serie E: Funcionamiento general de la red, servicio telefónico, operación del servicio y factores humanos, Serie F: Servicios no telefónicos de telecomunicaciones, y la Serie Z: Lenguajes y aspectos generales de software para sistemas de telecomunicaciones. El Anexo A muestra un compendio de todas las recomendaciones UIT-T que están bajo la responsabilidad del grupo de estudio 17.

La arquitectura de seguridad definida en la recomendación UIT-T X.800 sirvió de base para desarrollar una serie de normas y recomendaciones específicas de este sector. Antes de que el UIT-T procediera a emitir recomendaciones acerca de protocolos específicos que debieran implementarse, emitió una serie de recomendaciones a modo de marcos de referencia de seguridad (UIT-T X.810-X.816) que tratan de la aplicación de servicios de seguridad en un entorno de sistemas abiertos, donde el término sistemas abiertos se considera que comprende sectores tales como bases de datos, aplicaciones distribuidas, procesamiento distribuido abierto e interconexión de sistemas abiertos. La finalidad de los marcos de

seguridad es definir los medios para proporcionar protección a los sistemas y a los objetos dentro de los sistemas y así como a las interacciones entre sistemas y, por ende, cimientan las bases para regulaciones posteriores a su publicación.

En la recomendación UIT-T X.810 Tecnología de la Información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: visión general (11/1995) se introducen los demás marcos de seguridad y se describen conceptos comunes, incluyendo los dominios de seguridad, las autoridades de seguridad y las políticas de seguridad que son utilizadas en los marcos presentados.

La recomendación UIT-T X.811 Tecnología de la Información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: marco de autenticación (04/1995) define los conceptos básicos de autenticación, presenta una posible clasificación de mecanismos de autenticación, define los servicios de estos mecanismos y expone la interacción de los servicios de autenticación con otros servicios y/o mecanismos de seguridad.

En la recomendación UIT-T X.812 Tecnología de la Información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: marco de control de acceso (11/1995) se describe un modelo que incluye todos los aspectos de control de acceso en sistemas abiertos, así como la interacción que se presenta con los otros sistemas de seguridad y la gestión necesaria en el servicio de control de acceso.

La recomendación UIT-T X.813 Tecnología de la Información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: marco de no rechazo (10/1996) extiende los conceptos de los servicios de seguridad de no repudio definidos en la recomendación UIT-T X.800 y provee un marco para el desarrollo de estos servicios y los mecanismos que le conciernen.

La recomendación UIT-T X.814 Tecnología de la Información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: marco de confidencialidad (11/1995) tiene como objetivo el establecer los parámetros básicos para proteger la información ante ataques de divulgación no autorizados. El marco aborda la confidencialidad de la información en la recuperación, transferencia y gestión al definir conceptos de confidencialidad, mecanismos de este servicio y abordando si interacción con otros servicios de seguridad.

En la recomendación UIT-T X.815 Tecnología de la Información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: marco de integridad (11/1995) se aborda la integridad de los datos en el proceso recepción y transmisión de la información. Al igual que los marcos descritos con anterioridad, define lo conceptos básicos de integridad, identifica posibles mecanismos de este servicio de seguridad y aborda su interacción con otros mecanismos de seguridad.

La recomendación UIT-T X.816 Tecnología de la Información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: marco de auditoría y alarmas de seguridad (11/1995) define los conceptos básicos y provee un modelo general de las auditorías y alarmas de seguridad, identifica los criterios para este servicio y enlista los mecanismos que podrían emplearse. Por último, provee los requerimientos generales para la gestión de este servicio.

En octubre de 2003, el UIT-T publicó la recomendación UIT-T X.805: Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo, recomendación con la que se podría dar por concluido el proceso de cimentación de las bases necesarias para emitir normas en el ámbito. Como se podrá observar más adelante, muchas normas que manejan conceptos de servicios de seguridad hacen referencia a esta recomendación y no a la recomendación UIT-T X.800 ni a la serie de recomendaciones UIT-T X.810-X.816. Esto es porque esta recomendación ofrece una arquitectura más completa que sus predecesoras.

Los cinco servicios prioritarios de seguridad de la recomendación UIT-TX.800 (autenticación, control de acceso, integridad de los datos, no repudio y confidencialidad de los datos) son retomados por la recomendación UIT-T X.805 presentados como dimensiones de seguridad, sin embargo, esta recomendación agrega tres dimensiones de seguridad, que son la disponibilidad, la privacidad y la seguridad de la comunicación, y que define de la siguiente manera:

- Dimensión de seguridad de la comunicación: garantiza que la información sólo circula entre los puntos extremos autorizados (no hay desviación ni interceptación de la información que circula entre estos puntos extremos).
- Dimensión de disponibilidad: garantiza que las circunstancias de la red no impiden el acceso autorizado a los elementos de red, la información almacenada, los flujos de información, los servicios y las aplicaciones.
- Dimensión de privacidad: protege la información que sería posible conocer observando las actividades de la red. Por ejemplo: los sitios web visitados por un usuario, la posición geográfica del usuario y las direcciones IP y los nombres de dominio (DNS) de los dispositivos en la red de un proveedor de servicio.

Otra diferencia significativa con otras recomendaciones es que esta recomendación no hace uso del modelo OSI para ubicar en dónde es necesario aplicar las dimensiones de seguridad. Para ello esta recomendación define tres capas de seguridad:

- capa de seguridad de infraestructura;
- capa de seguridad de servicios, y
- capa de seguridad de aplicaciones.

Este modelo resulta más funcional puesto que cada capa de seguridad cumple un papel de potenciación a la capa siguiente, de tal forma que se permita realizar soluciones de red seguras, es decir, al presentar una perspectiva secuencial de la seguridad de la red, determina en dónde hay que intervenir para garantizar la seguridad de los activos de la red. La arquitectura de seguridad tiene en cuenta que las vulnerabilidades de seguridad de cada capa son diferentes, y ofrece la flexibilidad necesaria para reaccionar a las posibles amenazas de la forma más apropiada para una determinada capa de seguridad. El empleo de esta metodología representa una considerable ventaja cuando se observa que estas capas de seguridad constituyen una categoría aparte, y las tres capas de seguridad se pueden aplicar a cada capa del modelo de referencia OSI.

La recomendación UIT-T X.805 también define tres planos de seguridad para representar los tres tipos de actividades protegidas realizadas en la red. Estas son, (i) el plano de gestión, (ii) el plano de control

y (iii) el plano de usuario de extremo. Estos planos de seguridad corresponden a necesidades de seguridad particulares relativas a las actividades de gestión de red, control de red o señalización, así como las actividades de usuario de extremo correspondientes. El plano de seguridad gestión tiene que ver con la protección de las funciones OAMP (operaciones, administración, mantenimiento y configuración, del inglés *operations, administration, maintenance and provisioning*) de elementos de red, dispositivos de transmisión, sistemas administrativos y centros de datos. El plano de seguridad control tiene que ver con la protección de las actividades que permiten una distribución eficiente de información, servicios y aplicaciones en la red. Por último, el plano de seguridad usuario de extremo tiene que ver con la seguridad cuando los clientes acceden y utilizan la red del proveedor de servicio.

Estructurando de esta forma la arquitectura de seguridad, esta puede aplicarse a todos los aspectos y las estas de un programa de seguridad. Se puede decir que un programa se seguridad está compuesto, en general, de políticas, procedimientos y tecnología, y se desarrolla en tres etapas significativas:

1. etapa de definición y planificación;
2. etapa de implementación, y
3. etapa de mantenimiento.

La Ilustración 1.2.1 muestra a la perfección la aplicación de la arquitectura de seguridad a los programas de seguridad y muestra la organización de las dimensiones de seguridad, las capas de seguridad y los planos de seguridad definidas a lo largo de la recomendación.

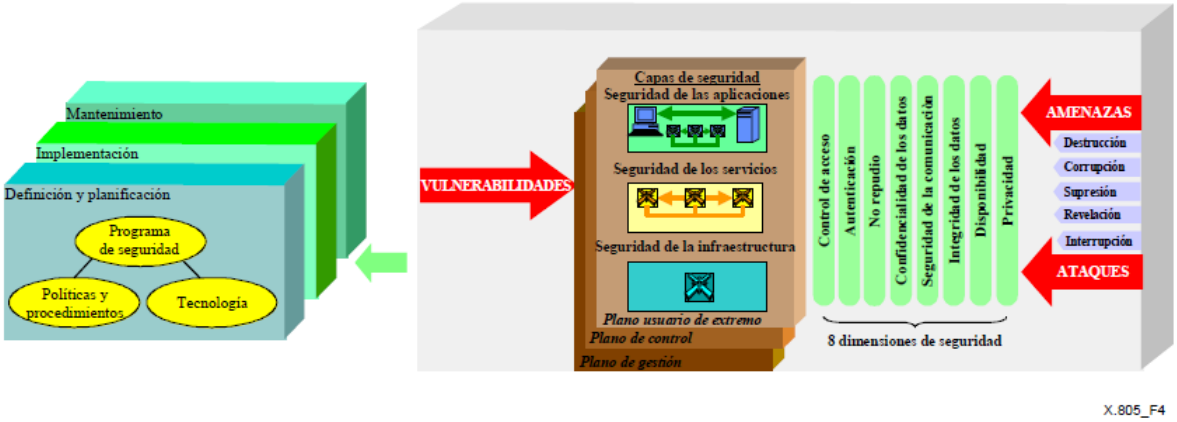


Ilustración 1.2.1: Arquitectura de seguridad UIT-T X.805 [6]

Como es de esperarse, los esfuerzos del UIT-T fueron mucho más allá de las recomendaciones presentadas hasta ahora. Las Tablas 1.2.1 - 1.2.13[1] ofrecen una breve descripción de las principales recomendaciones emitidas por este órgano en materia de seguridad cibernética. Asimismo, las tablas mencionadas destacan los principales aspectos técnicos

[1] Las Tablas 1.2.1 - 1.2.13 son de creación propia.

Tabla 1.2.1: Aspectos generales de la ciberseguridad.

Aspectos generales de la ciberseguridad	**UIT-T X.1205**	**(04/2008)**
Descripción: Esta recomendación ofrece una definición de ciberseguridad. En ella se expone la clasificación de las amenazas de seguridad desde el punto de vista de una organización. Se presentan las amenazas a la ciberseguridad, así como sus puntos débiles, incluidas las herramientas más utilizadas por los piratas informáticos. Se tratan las amenazas en las distintas capas de red.		
Aspectos técnicos relevantes: categoriza los tipos de empresa en empresa cerrada, empresa extendida y empresa abierta según los aspectos técnicos de sus propias redes. Considera que los ataques se pueden categorizar en tres tipos, que se nombran, (i) ataques de interrupción del servicio, (ii) activos en peligro y (iii) piratería de componentes. Con respecto a las estrategias de protección de red, recomienda que los administradores de TI (tecnologías de la información) cuenten con herramientas de ataque para realizar evaluaciones de las vulnerabilidades de su red. Propone una gestión de acceso uniforme que cuente con un servidor de autenticación centralizado basado en RADIUS (servicio de usuario de marcación de autentificación a distancia, del inglés *remote authentication dial-in user service*), bases de datos de autenticación de diferentes niveles, y elementos de frontera de red que puedan proporcionar servicios de IP (protocolo de internet, del inglés *internet protocol*). Enlista tecnologías de encriptado para redes de datos, voz y las redes móviles, en las cueles figuran las siguientes tecnologías: • técnicas VPN (red privada virtual, siglas del inglés *virtual private network*) con IPSec (seguridad del protocolo de internet, del inglés *internet protocol security*), con encabezamiento de autentificación, AH (siglas del inglés *authentication header*) y encapsulación de cabida útil de seguridad (ESP, siglas del inglés *encapsulating security payload*) o tunelización gracias al protocolo de tunelización de capa 2 (L2TP, del inglés *layer 2 tunneling protocol*); • la gestión de claves puede basarse en el intercambio de claves Internet (IKE, del inglés *Internet key exchange*); • la gestión de certificados se basa en la infraestructura de clave pública (PKIX, del inglpes *public key infrastructure*); • el protocolo de gestión de certificados (CMP, del inglés *certificate management protocol*) y el protocolo de estado de certificado en línea (OCSP, del inglés *online certificate status protocol*), y • en la capa de aplicación, mediante la utilización de TLS (seguridad de capa de transporte, del inglés *transport layer security*) con claves fuertes.		

Aunado a lo anterior, la recomendación insta al uso de algoritmos de encriptado normalizados y funciones de aleatorización como el DES (norma de encriptado de datos, del inglés *data encryption standard*), 3DES (norma de encriptado de datos triple , del inglés *triple data encryption standard*), AES (norma de encriptado avanzada, del inglés *advanced encryption standard*), RSA (algoritmo de clave pública Rivest Shamir Adleman, del inglés *Rivest Shamir Adleman public key algorithm*), MD5 (algoritmo 5 de resumen de mensaje, del inglés *message digest algorithm 5*), SHA-1 (algoritmo de aleatorización segura1, del inglés *secure hash algorithm 1*)y Diffie-Hellman. También alerta de las vulnerabilidades en las redes de área local cuando se use la privacidad equivalente a las redes inalámbricas, WEP (del inglés *wired equivalent privacy*), para contrarrestar esta vulnerabilidad, insta al uso del acceso protegido a Wi-Fi, WPA (del inglés *Wi-Fi protected access*). Menciona que en las redes de área local se puede obtener una profundidad de seguridad variable mediante el uso de un grupo de dispositivos de red, tales servidores y otros recursos, configurado para funcionar como si estuvieran conectados a un mismo segmento de red a modo de una red virtual de área local (VLAN, del inglés *virtual local area network*) y fortificando esta VLAN con VPN de capa 3 (capa de red: enrutamiento y direccionamiento). Con respecto a la gestión de la seguridad, considera que es necesario contar con un centro de operaciones de red, NOC (por sus siglas en inglés de N*etwork Operations Center*) que sirva como canal o plano de gestión seguro y funcione como base de todos los demás elementos de gestión de la red, y se asegure de mantener una calidad de funcionamiento óptima y su supervivencia. Por la naturaleza de las funciones del NOC, recalca la necesidad de encriptar el tráfico de gestión de la red utilizando, por lo menos, algunas de las tecnologías mencionadas anteriormente.

Tabla 1.2.2: Marco general de tecnologías de seguridad para las comunicaciones móviles de datos de extremo a extremo.

Marco general de tecnologías de seguridad para las comunicaciones móviles de datos de extremo a extremo	**UIT-T X.1121**	**(04/2004)**
Descripción: Esta recomendación describe las amenazas contra la seguridad en las comunicaciones móviles de datos de extremo a extremo y los requisitos de seguridad con relación al usuario móvil y al proveedor de servicio de aplicación (ASP, de sus siglas en inglés *Application Service Provider*). Asimismo, esta Recomendación indica cuándo aplicar tecnologías de seguridad que realizan funciones de seguridad en los modelos de comunicaciones móviles de datos de extremo a extremo		
Aspectos técnicos relevantes: Al presentar una metodología de marco general no presenta profundos aspectos técnicos, más bien retoma conceptos y defunciones presentadas en la recomendación UIT-T X. 800.		

Presenta los requisitos de seguridad para las comunicaciones móviles de extremo a extremo, las cuales las secciona en:

- Desde el punto de vista de usuario móvil, que menciona son:
    - gestión de la identidad;
    - confidencialidad de los datos;
    - integridad de los datos;
    - autenticación;
    - control de acceso;
    - no repudio;
    - anonimato;
    - privacidad;
    - aptitud para el uso, y
    - disponibilidad.
- Desde el punto de vista del ASP:
    - confidencialidad de los datos;
    - integridad de los datos;
    - autenticación;
    - control de acceso;
    - no repudio, y
    - disponibilidad.

Por otra parte, menciona que las funciones de seguridad para satisfacer los requisitos de seguridad de los sistemas móviles pueden ser los definidos en la recomendación UIT-T X.800, es decir:

cifrado;

- intercambio de claves;
- firma digital;
- control de acceso;
- integridad de los datos;
- intercambio de autenticación, y
- notarización.

Tabla 1.2.3: El directorio: Marcos para certificados de claves públicas y atributos.

El directorio: Marcos para certificados de claves públicas y atributos	**UIT-T X.509**	**(12/2016)**
Descripción: Fue desarrollada con el fin de proveer mecanismos de autenticación electrónica sobre redes públicas, a través del uso de certificados de llaves públicas y el diseño de aplicaciones relacionadas con infraestructura de llave pública. En diciembre de 2016 fue publicada la octava		

edición, sin embargo, por acuerdo entre el UIT-T, ISO e IEC, esta recomendación sólo es accesible mediante el pago por la misma.

Tabla 1.2.4: Arquitectura de interrelaciones externas para un sistema de seguridad de la red de telecomunicaciones IP.

Arquitectura de interrelaciones externas para un sistema de seguridad de la red de telecomunicaciones IP	**UIT-T X.1032**	**(12/2010)**
Descripción: Esta recomendación propone cuatro modelos para poder examinar las interrelaciones entre el sistema de seguridad de la red de telecomunicaciones IP (TNSS, por sus siglas en inglés de *Telecomunications Network Security System*) y elementos externos. Los cuatro tipos de interrelaciones sobre los que propone modelos son: - interrelaciones del TNSS con los sistemas de seguridad superpuestos a sistemas de información de infraestructura y las estructuras de información; - interrelaciones del TNSS con los objetos del sistema de telecomunicaciones; - interrelaciones del TNSS con otros objetos; es decir, organizaciones externas, e - interrelaciones del TNSS con las amenazas de seguridad, que pueden ser los objetos antes nombrados o nuevos objetos.		
Aspectos técnicos relevantes: La instalaciones de operadores de telecomunicaciones que aplican para el término "red de telecomunicaciones" son las instalaciones de suministradores de infraestructura (es decir, nodos de red, sus circuitos de conexión y redes de acceso, etc.), las instalaciones de proveedores de servicio (es decir, servidores de servicio y otros), instalaciones de los proveedores de aplicaciones (es decir, servidores de aplicaciones y otros), instalaciones de conexión del usuario con el proveedor de telecomunicaciones e información transferida y almacenada en las instalaciones mencionadas.		

*Tabla 1.2.5: Directrices para los proveedores de servicios de telecomunicaciones acerca del riesgo de programas espías y de software potencialmente no deseado***.**

Directrices para los proveedores de servicios de telecomunicaciones acerca del riesgo de programas espías y de software potencialmente no deseado.	**UIT-T X.1207**	**(04/2008)**
Descripción: Esta recomendación está dirigida principalmente a los proveedores de servicios de telecomunicaciones y ofrece directrices para abordar el riesgo que suponen programas espías y		

software no deseado. Con ello se desarrollan, proponen y promueven prácticas óptimas basadas en principio de claridad de información y el consentimiento por parte del usuario.
Aspectos técnicos relevantes: Presenta las definiciones de software engañoso, software potencialmente no deseado y software espía.

Tabla 1.2.6: Un indicador de riesgo de ciberseguridad para mejorar la confianza y la seguridad en la utilización de las tecnologías de la información y la comunicación

Un indicador de riesgo de ciberseguridad para mejorar la confianza y la seguridad en la utilización de las tecnologías de la información y la comunicación	**UIT-T X.1208**	**(01/2014)**
Descripción: Esta recomendación está dirigida principalmente a organizaciones que explotan una parte de la infraestructura mundial de las tecnologías de la información y la comunicación. Describe una metodología para la utilización de indicadores de ciberseguridad en el cálculo de la medida de riesgo, de tal manera que sirva de criterio para saber si deberían invertir recursos para mejorar sus capacidades en esta materia.		
Aspectos técnicos relevantes: Presenta un total de 30 indicadores que podrían ser utilizados por organizaciones como parte de su metodología. Presentando de ellos su nombre, objetivo, formula de obtención, datos necesarios, frecuencia de medición, tipo de indicador, nivel de exigencia, a quiénes es aplicable y la referencia técnica de CYBEX (intercambio de información de Ciberseguridad, del inglés *cybersecurity information exchange*).		

Tabla 1.2.7: Técnicas para prevenir ataques en la web.

Técnicas para prevenir ataques en la web.	**UIT-T X.1211**	**(09/2014)**
Descripción: En esta recomendación se describen técnicas que pueden atenuar ataques en la red que ocurren cuando se explotan vulnerabilidades en los servidores de sitios web y se introducen códigos malignos en la computadora de algún usuario.		
Aspectos técnicos relevantes: Presenta una descripción detallada del malware y los tipos de programas que incluye esa categoría. Presenta técnicas para hacer frente a ataques típicos en la web como la inyección SQL y la falsificación de petición en sitios cruzados		

Tabla 1.2.8: Enumeración y clasificación de pautas de ataques comunes.

Enumeración y clasificación de pautas de ataques comunes	**UIT-T X.1544**	**(04/2013)**
Descripción: Esta recomendación facilita el intercambio estructurado de los patrones de ataques comunes disponibles públicamente a través de la enumeración y clasificación de patrones de ataques comunes (CAPEC, por sus siglas en inglés de *common attack pattern enumeration and classification*)		
Aspectos técnicos relevantes: Esta recomendación aplica para los patrones de ataques comunes que están basados en el lenguaje XML/XSD (del inglés *Extensible Markup Language y XML Schema Definition*, respectivamente) para su identificación, descripción y enumeración. Presenta anexos donde enlista los requisitos específicos de los tipos de capacidades, de las herramientas, de los servicios de seguridad, de las capacidades en línea, de los documentos electrónicos y de la interfaz gráfica del usuario para el uso de CAPEC.		

Tabla 1.2.9: Protocolos de transporte para el intercambio de información de ciberseguridad.

Protocolos de transporte para el intercambio de información de ciberseguridad	**UIT-T X.1582**	**(01/2014)**
Descripción: Esta recomendación está dirigida principalmente a los diseñadores e implementadores que tienen como objetivo habilitar la transferencia e intercambio de información de ciberseguridad, CYBEX. En ella se presentan los protocolos de transferencia e intercambio que se han normalizado y adaptado para su utilización con las recomendaciones de la serie UIT-T 1500 (Intercambio de información de ciberseguridad).		
Aspectos técnicos relevantes: Se describen los protocolos pregunta – respuesta y los bidireccionales que podrían ser utilizados por las entidades de ciberseguridad como protocolos de transporte. Se presentan también las extensiones de HTTP (siglas del inglés *Hipertext Transfer Protocol)* que pueden servir para mejorar la seguridad. Por último se describen consideraciones para la capa de transporte y sesión de tal forma que se proteja contra la denegación de servicios por diversos medios y los ataques reflejo, por lo que se alienta a utilizar TCP (Protocolo de control de transmisión, del inglés T*ransmission Control Protocol*) o SCTP (Protocolo de transmisión de control de trenes, del inglés *Stream Control Transmission Protocol*) en lugar de UDP (Protocolo de datagrama de usuario, del inglés U*ser Datagram Protocol*).		

Tabla 1.2.10: Marco de seguridad para la computación en la nube

Marco de seguridad para la computación en la nube (Edición 2.0)	UIT-T X.1601	(10/2015)
Descripción: En esta recomendación se analizan las amenazas y problemas que comúnmente se presentan en el contexto de la computación en la nube y se describen las capacidades de seguridad que podrían mitigar estas amenazas. Esta recomendación defina a la computación en la nube como un paradigma que permite ofrecer acceso en red práctico y por demanda a un conjunto compartido de recursos configurables (como, por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios Explica que los servicios de computación en la nube se suelen suministrar en ciertas categorías de servicio, por ejemplo, infraestructura como servicio (IaaS), plataforma como servicio (PaaS), software como servicio (SaaS), red como servicio (NaaS), etc. Especifica que la adopción de computación en la nube conlleva amenazas y problemas de seguridad, pues los requisitos de seguridad varían sobremanera en función de los modelos y las categorías de servicio de computación en la nube.		
Aspectos técnicos relevantes: Al utilizar una metodología de marco esta recomendación no ahonda en los aspectos técnicos de las amenazas y problemas de la computación en la nube o en las capacidades de seguridad para mitigarlas.		

En el 2004 fue presentado por la UIT el concepto de redes de la próxima generación. La recomendación UIT-T Y.2001 presenta una descripción general y las define como redes basadas en la conmutación de paquetes capaces de proveer servicios de telecomunicaciones utilizando múltiples tecnologías de transporte de banda ancha en donde las funciones relacionadas con los servicios son independientes de las tecnologías relacionadas con el transporte. En dicha recomendación se enlistan los aspectos fundamentales de las redes de la próxima generación, que cuales son:

- Transferencia basada en paquetes;
- Separación de las funciones de control y el servicio;
- Desacoplamiento del servicio de transporte y las interfaces abiertas;
- Capacidades de banda ancha con transparencia y calidad de servicio de extremo a extremo;
- Interconexión con redes heredadas a través de interfaces abiertas;
- Movilidad garantizada;
- Acceso ilimitado a proveedores de servicios;
- Una variedad de opciones de identificación asignadas a direcciones IP con el propósito de direccionarlas a redes IP;
- Unificación de servicios de telecomunicaciones;
- Independencia entre las funciones relacionadas a los servicios y las tecnologías de transporte subyacente;

- Soporte de las múltiples tecnologías de última milla; y
- Cumplir con las regulaciones en materia de energía, comunicaciones seguridad y privacidad, entre otras.

El UIT-T ha emitido ciertas recomendaciones en materia de seguridad para las redes de la próxima generación. A continuación, se presenta la descripción de algunas recomendaciones sobresalientes (Tablas 1.2.11-1.2.13[2]).

Tabla 1.2.11: Requisitos de seguridad para las redes de la próxima generación.

Requisitos de seguridad para las redes de la próxima generación, versión 1	**UIT-T Y.2701**	**(04/2007)**
Descripción: Esta recomendación dispone requisitos de seguridad para las redes de la próxima generación y sus interfaces. Para lograrlo se aplica la recomendación UIT-T X.805, *Arquitectura de seguridad para sistemas de comunicaciones de extremo a extremo**, a la REC. UIT-T Y.2201, *Requisitos de la versión 1 de las redes de la próxima generación*, y a la REC. UIT-T Y.2012, *Requisitos y arquitectura funcional de las redes de la próxima generación, versión 1*.		
Aspectos técnicos relevantes: Los requisitos presentados en esta recomendación pretenden proteger a los siguientes elementos en un entorno multired: • la infraestructura de la red y el proveedor de servicios y sus activos, sus recursos, sus comunicaciones y sus servicios; • servicios y capacidades de las NGN (del inglés *Next Generation Networks*) (por ejemplo, servicios de voz, vídeo y datos), y • comunicaciones de información de usuario extremo (por ejemplo, información privada).		

Tabla 1.2.12: Mecanismos y procedimientos de seguridad para las NGN.

Mecanismos y procedimientos de seguridad para las NGN	**UIT-T Y.2704**	**(01/2010)**
Descripción: Esta recomendación presenta una serie de mecanismos de identificación, autentificación y autorización. Aunado a esto examina la seguridad de transporte para la señalización y OAMP, así como la seguridad de medios de comunicación. Por último, se exponen los mecanismos de registro de auditoría y el aprovisionamiento a zonas no fiables. Los mecanismos de seguridad descritos en esta Recomendación se basan en el modelo de confianza definido en la Recomendación UIT-T Y.2701.		

[2] Las Tablas 1.2.11-1.2.13 son de creación propia.

Aspectos técnicos relevantes: Los aspectos técnicos de esta regulación se pueden presentar en cuatro bloques • Con respecto a los mecanismos de identificación, autentificación y autorización, en particular se describen aquellos que interesan a los servicios basados en el SIP (protocolo de iniciación de sesión, del inglés S*ession Initiation Protocol*). • Con respecto a la seguridad de transporte para la señalización y OAMP se especifican los perfiles de TLS e IPsec que deben emplear los elementos de la red para ofrecer garantías de confiabilidad e integridad de datos. • Con respecto a la seguridad de medios, esta recomendación indica que encriptar los medios no es necesario en la infraestructura NGN, pero puede utilizarse si hay clientes que así lo deseen. En caso de que se solicite encriptación, esta tendía lugar en los elementos de red de frontera y se lograría aplicando en él algoritmos de encriptado y autentificación (como el SRTP [protocolo seguro en tiempo real, del inglés S*ecure Real Time Protocol*], AES [estándar de cifrado avanzado, del inglés *Advanced Encryption Standard*] o HMAC-SHAI [código de autentificación de mensajes mediante troceo con clave, del inglés *Hash Message Authentication Code*]). • Con respecto a la auditoria, se enlistan mecanismos para realizar un registro de auditoria de los intentos de acceso y eventos significativos a OAMP. Para lograr esto se recomienda la implementación en los elementos de la red de protocolos que envíen la información de registro al servidor distante encargado. Por ejemplo, el protocolo Syslog, SNTP (protocolo simple de tiempo de red, del inglés *Simple Network Time Protocol*), SNMP (protocolo de gestión de red simple, del inglés S*imple Network Management Protocol*). Estas medidas incluyen tanto a los elementos terminales de la red como a los elementos de frontera de la red.

Tabla 1.2.13: Requisitos de seguridad para las transacciones financieras móviles a distancia en las redes de la próxima generación.

Requisitos de seguridad para las transacciones financieras móviles a distancia en las redes de la próxima generación	**UIT-T Y.2740**	**(01/2011)**
Descripción: En esta recomendación se describen riesgos de seguridad asociados a las transacciones financieras móviles a distancia soportadas por los servicios de aplicación de las redes de la próxima generación y las medidas de supresión y mitigación del riesgo con cuatro niveles de seguridad. Se especifican asimismo los requisitos mínimos para la protección de la privacidad de los datos personales en el marco de las transacciones financieras móviles a distancia.		
Aspectos técnicos relevantes: Los cuatro niveles de seguridad se logran al aplicar principios de la recomendación UIT-T X.805, *Arquitectura de seguridad para sistemas de comunicaciones de extremo a extremo* en diferentes dimensiones de seguridad. El control de acceso, no repudio,		

seguridad de la comunicación y la disponibilidad son dimensiones implantadas en pie de igualdad a todos los niveles de seguridad, mientras que la autenticación, la confidencialidad de los datos, la integridad de los datos y la privacidad son dimensiones de seguridad que tienen una implantación diferente en cada uno de los niveles de seguridad.

Con base en las tablas anteriores es imposible negar el invaluable esfuerzo que realiza la Unión Internacional de Telecomunicaciones para hacer de las redes de datos y el espacio cibernético un ambiente más seguro. Considerando que las recomendaciones analizadas abarcan temas como marcos de referencia para seguridad en comunicaciones de extremos a extremo, aspectos generales de la ciberseguridad, algoritmos de cifrado, computación en la nube, entre otras, se puede decir que el UIT-T se ha encargado de brindar las herramientas necesarias para que se tomen medidas necesarias para fortalecer la seguridad cibernética en general, desde la implementación de sistemas de gestión de riesgos en organizaciones de cualquier tipo, hasta el hecho de que los órganos normalizadores y/o reguladores de los diferentes países del mundo puedan fortalecer los requerimientos técnicos en sus respectivas estrategias nacionales de seguridad cibernética empleando de base las recomendaciones del UIT-T.

Por otra parte, es conveniente resaltar que el UIT-T mantiene una postura abierta ante las normas que emitan otros organismos internacionales, e incluso establece un trabajo conjunto en algunos casos. Evidencia de esto es el reconocimiento habitual que brinda el UIT-T a diferentes organismos internacionales en las introducciones de sus respectivas recomendaciones y particularmente en sus listas de referencias, evidenciando así que el proceso normalizador dentro del UIT-T mantiene un perfil abierto ante los aportes de otros organismos. Este tema se aborda con mayor profundidad en la quinta sección de este capítulo.

Organización Internacional de Normalización

Con sede central en Ginebra, Suiza, la Organización Internacional de Normalización (ISO, nombre derivado del acrónimo reordenado del inglés de *International Organization of Standarization*) es una organización internacional, independiente y no gubernamental que se conforma de los cuerpos nacionales de normalización de los 164 países miembros [7].

A través del trabajo conjunto de los cuerpos nacionales de normalización de sus países miembros, ISO busca desarrollar normas internacionales de consenso mutuo y carácter voluntario que resulten de relevancia en los mercados mundiales, presentando así soluciones innovadoras a los cambios del mundo moderno. México es miembro de ISO y es la Dirección General de Normas de la Secretaría de Economía quien asume el papel de cuerpo nacional de normalización mexicano

En sus más de 70 años de trayectoria, ISO ha publicado más de 21 mil normas internacionales enfocadas a prácticamente todas las áreas de tecnología y manufactura. Ya se ha hablado del aporte inicial

de ISO a la seguridad cibernética con las normas ISO/IEC 7498-1, 7498-2 y 7498-4, sin embargo, el aporte que ISO ha tenido en el sector consta de un total de 176 normas publicadas en materia de técnicas de seguridad en las tecnologías de la información. Los temas desarrollados en esas normas abarcan desde técnicas de encriptado, gestión de llaves públicas y firmas digitales, la implementación de plataformas de confianza, técnicas de no repudio y autenticación, protección de información biométrica, y sistemas de gestión de seguridad de la información, entre otros.

Uno de los problemas que los organismos se enfrentaban al momento de emitir recomendaciones en seguridad en las redes, era el hecho de estos tópicos mantenían una diversificación de criterios que complicaban el desarrollo de normas y recomendaciones. Es por eso que en el año 2000 se unificaron los criterios dando lugar a un estándar conocido con el nombre de Criterios Comunes (ISO/IEC 15408).

El catálogo de normas ISO con tiene una sección enfocada a Tecnologías de la Información, la 35. Dentro de ella se puede acceder a las familias de normas en materia de seguridad en las Tecnologías de la Información (con el código 35.030) y en materia de la codificación de la información (con el código 35.040).

La naturaleza de adquisición por pago de las normas ISO dificulta su análisis a profundidad, sin embargo, los estándares ISO/IEC 27000, 27001, 27002, 27003, 27004, 27005, 27006 y 15408 (todas ellas pertenecientes a la familia 35.030 Seguridad en las Tecnologías de la Información) son estándares de relevancia para la literatura de seguridad cibernética, lo que permite ahondar en sus contenidos. Las Tablas 1.3.1 y 1.3.2[3] presentan una descripción de los contenidos y los aspectos técnicos relevantes de las normas a las que, por convenio con diversos organismos, se tienen un libre acceso.

Tabla 1.3.1: Criterios de evaluación para la seguridad informática.

Criterios de evaluación para la seguridad informática	**ISO/IEC 15408**	**(12/2009)**
Descripción: Esta norma fue presentada en tres partes: (i) introducción y modelo general, (ii) componentes generales de seguridad y (iii) componentes de garantía de seguridad. En su primera parte, se definen los conceptos generales y los principios de evaluación de la seguridad informática. Se definen también conceptos clave como objetivo de evaluación, TOE (del inglés *target of evaluation*), perfiles de protección y paquetes de requerimientos de seguridad. En la segunda parte de esta norma se definen los componentes funcionales de seguridad que son la base de los requerimientos de seguridad funcionales destinados a contrarrestar amenazas en el ambiente operativo de los objetivos de evaluación o en sus políticas de seguridad.		

[3] Las Tablas 1.3.1 y 1.3.2 son de creación propia.

En la tercera parte se catalogan el conjunto de componentes de garantía de seguridad. También define criterios de evaluación para perfiles de protección e introduce los niveles de garantía de evaluación (EALs, pos sus siglas en inglés de *Evaluation Assurance Levels*)
Aspectos técnicos relevantes: La primera parte de la norma no presenta grandes aspectos técnicos, pues simplemente específica los aspectos generales del modelo. La segunda parte presenta los siguientes aspectos: - En la cláusula 5 describe el paradigma usado en los requerimientos funciones de seguridad - La cláusula 6 presenta un catálogo de los componentes funcionales de seguridad. - De la cláusula 7 a la 17 se describe las clases funcionales de seguridad. La tercera parte presenta los siguientes aspectos: - La cláusula 5 describe el paradigma usado en los requerimientos de garantía de seguridad - La cláusula 6 describe la estructura de las garantías y las caracteriza según su clase - La cláusula 7 provee detalladas definiciones de los EALs - La cláusula 8 provee detalladas definiciones de los paquetes de garantías. - Las clausulas 9-16 describen as clases de garantías de seguridad.

Tabla 1.3.2: Tecnologías de la información- Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Descripción y vocabulario

Tecnologías de la información- Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Descripción y vocabulario	**ISO/IEC 27000**	**(02/2016)**
Descripción: Este estándar provee el panorama general de los sistemas de gestión de seguridad de la información, ISMS (por sus siglas en inglés de I*nformation Security Management Systems*) y los términos y definiciones comúnmente empleados en la familia de normas ISMS. Por otra parte, cataloga a las normas ISMS en los siguientes grupos: - Normas de vocabulario: 27000 - Normas de requerimientos: 27001, 27006 y 27009 - Normas guía: 27002, 27003, 27004, 27005, 27007, TR 27008, 27013, 27014 y TR 27016 - Normas guía específicas de sector: 27010, 27011, 27015, 27017,27018 y 27019		
Aspectos técnicos relevantes: Al presentar una metodología descriptiva y de vocabulario, no se presentan aspectos técnicos.		

La norma ISO/IEC 27001, Requerimientos de los ISMS, tiene su versión más actual en el año 2013, sin embargo, al ser una norma cerrada, surge la necesidad de recurrir a la literatura existente para dar una descripción de la misma. Calder y Watkins (2008) analizan la versión de 2005 y la importancia de que los gobiernos implementen sistemas de gestión de seguridad de la información y busquen una certificación en la norma internacional ISO/IEC 27001 y 270002. Su punto de vista será abordado con más fuerza en el capítulo siguiente. Al igual que Calder y Watkins, Jacobs (2014) analiza la versión de 2005 y menciona que presenta un conjunto de requisitos funcionales específicos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un programa de gestión de seguridad de la información, ISMP (por sus siglas en inglés de I*nformation Security Management Program*), con el cual una organización puede ser certificada conforme a la misma norma.

Los requerimientos para la implementación de los controles de seguridad presentados en la norma ISO/IEC 27001 fueron desarrollados para los siguientes usos:

- Establecer los objetivos y requerimientos de seguridad;
- Garantizar que los riesgos de seguridad se administren de manera rentable;
- Garantizar conformidad con las leyes y regulaciones;
- Especificar una metodología para la implementación y administración de controles que aseguren el cumplimento de los objetivos de seguridad establecidos,
- Definir nuevos procesos de gestión de la seguridad de la información.

Asimismo, en la norma ISO/IEC 27001 se definen los conceptos de PDCA (planear, hacer, checar, y actuar, del inglés: *plan*, *do*, *check* y *act*), los cuales derivan de los términos empleados en la familia de normas de control de calidad ISO 9000. La adaptación de estos conceptos al contenido de la norma se muestra a continuación:

- *Plan*: establece la política, objetivos, procesos y procedimientos del ISMS;
- *Do*: implementa y opera la política, objetivos, proceso y procedimientos del ISMS;
- *Check*: evalúa, mide el rendimiento del proceso contra la política, objetivos y la experiencia, y reporta los resultados de la gestión para revisión; y
- *Act*: toma acciones de corrección y prevención basándose en los resultados del ISMS para continuar mejorando el propio ISMS.

En el Proceso de Evaluación de la Conformidad (PEC) de la norma ISO/IEC 27001 se espera que las organizaciones mantengan una política de seguridad de la información. La norma internacional ISO/IEC 27002 presenta las directrices necesarias para que una organización prepare una política de seguridad de la información adecuada, esta política implica que se cumplen con los requisitos de la norma ISO/IEC 27001, así estas normas están íntimamente relacionadas.

La norma internacional ISO/IEC 27002 provee las directrices para la gestión de un programa de seguridad de la información. A pesar de que estos lineamientos pueden ser interpretados desde diferentes perspectivas, se espera que las organizaciones cumplan estos lineamientos enfocándose en cumplir la norma ISO/IEC 27001. Esta norma abarca los siguientes temas centrales:

- Política de seguridad;
- Organización de la seguridad de la información;
- Gestión de activos;
- Seguridad de los recursos humanos;
- Seguridad física y ambiental: gestión de comunicaciones y operaciones;
- Control de acceso;
- Adquisición, desarrollo y manejo de los sistemas de información;
- Gestión de los incidentes en la seguridad de la información;
- Gestión de la continuidad de los negocios; y
- Conformidad leyes y regulaciones.

La naturaleza de adquisición de sus normas, que es su mayoría es mediante el pago por la misma, hace complicada la investigación sobre las mismas. Por otra parte, es importante resaltar que la misión de ISO no es brindar de normas técnicas exclusivas en telecomunicaciones, sino en un amplio campo de sectores industriales que van desde la industria médica hasta a la metalúrgica, pasando por un buen número de giros industriales.

De lo presentado en esta sección se puede concluir que uno de los principales aportes de norma mundial ISO a la seguridad cibernética está en los sistemas de gestión de la seguridad, pues han seguido una línea directa en estas familias de normas y ese aporte ha sido constantemente recogido por la literatura circundante en materia de seguridad cibernética. Sin embargo, los aportes de ISO han llegado más allá de los sistemas de gestión de la seguridad en las redes, sino que ahondan en otros temas relevantes, como la codificación y encriptado de la información, la autenticación de entidades en la red y técnicas de mitigación de los ataques en la red, entre otras. El Anexo B se presenta un desglose de las familias de normas ISO 35.030 y 35.040.

Instituto de Ingenieros Eléctricos y Electrónicos.

El Instituto de Ingenieros Eléctricos y Electrónicos, IEEE (*Institute of Electrical and Electronics Engineers*) es una asociación mundial sin fines de lucro dedicada a la elaboración de normas técnicas, y demás recursos con la intención de generar invocación tecnológica en beneficio de la humanidad. Actualmente cuenta con más de 420 mil miembros en alrededor de 160 países [8].

El grupo de seguridad de conexiones industriales, ICSG (por sus siglas en inglés de I*ndustry Connections Security Group*) es un grupo perteneciente a la asociación de normas del IEEE que se conforma de entidades de seguridad informáticas y que se encarga de dar respuestas eficientes a la creciente tendencia en amenazas a la seguridad cibernética. El ICSG se divide en tres subgrupos que abordan temas más específicos respecto a la seguridad, los cuales son:

- Grupo de trabajo sobre el *malware*;
- Grupo de trabajo de inspección de tráfico encriptado; y
- Grupo de trabajo sobre el formato de intercambio de metadatos de *malware*.

Una de las contribuciones más significativas del IEEE a las telecomunicaciones mundiales, la familia de normas IEEE 802 LAN's. Estas normas han permitido implementar puntos de acceso de redes de área local al alcance de una significativa porción de la población mundial. Con respecto a la seguridad en las normas IEEE 802, el IEEE ha desarrollado diferentes normas para fortalecer la misma, las Tablas 1.4.1 -1.4.5[4] describen algunas de relevancia.

Tabla 1.4.1: Control de acceso a la red basado en puertos

Control de acceso a la red basado en puertos[5]	**IEEE 802.1 X**	**(04/2010)**
Descripción: Con ediciones anteriores en 2001 y 2004, esta norma tiene como objetivo regular los accesos a las redes para resguardarla de recepción y transmisión de datos por parte elementos no autorizados que derivan en interrupciones en la red, robo del servicio o pérdida de datos. En otras palabras, tiene como objetivo proveer mecanismos de autenticación compatible, autorización y claves criptográficas para brindar comunicaciones seguras entre dispositivos conectados por una red de área local. Esto lo hace con estos tres campos generales: - Especifica un método general para la provisión del control de acceso a la red basado en puertos. - Especifica protocolos que establecen asociaciones seguras para la norma IEEE 802.1 AE seguridad MAC (Control de acceso a los medios del inglés M*edia Access Control*) - Facilita el uso de normas industriales de protocolos de autenticación y autorización.		
Aspectos técnicos relevantes: Esta norma especifica una arquitectura común que abarca de elementos funcionales que cumplen con: - Usar el servicio de MAC en un común punto de acceso de una red de área local; - Soportar autenticación manual entre una entidad de acceso por puerto (PAE, por sus siglas en inglés de P*ort Access Entity*) asociada a un puerto controlado y otro de la misma clase. - Asegurar las comunicaciones entre un puerto controlado y su par de autenticación excluyendo a los demás dispositivos presentes en la red LAN - Proporcione al puerto controlado los atributos que especifiquen los controles de acceso apropiados a la autorización concedida a la estación par o a su usuario. La indicación de usar el protocolo EAP para la autenticación, presenta en las versiones anteriores, es actualizada en esta versión, señalando una separación del protocolo de control de acceso a puertos (PACP, del inglés P*ort Access Control Protocol*) y lo métodos del protocolo EAP. En esta		

[4] La Tablas 1.4.1-1.4.5 son de creación propia.

[5] Esta norma fue preparada por el comité de normas del IEEE y adoptada posteriormente por la ISO con el nombre de ISO/IEC/IEEE 8802-1X.

edición de la norma se agregan EAPOL PDU (unidades de datos de protocolo de los protocolos de autenticación extensible sobre redes de área local, del inglés *EAP over LANs Protocol Data Unit*) para soportar el protocolo MKA (del inglés *MAC sec Key Agreement Protocol*).

En ésta norma se establecen lo principios de operación del protocolo de control de acceso basado en puertos, exponiendo los componentes del mismo y de su implementación y se ilustran los protocolos y componentes que suelen resaltar en un caso típico de control de acceso a la red. Así mismo se presentan los lineamientos para el uso del protocolo EAP en las entidades del acceso por puerto para soportar la autenticación y autorización usando autenticación centralmente administrada o servidores AAA (Autenticación, Autorización y Contabilidad, del inglés A*uthentication, Authorization, and Accounting*).

En la parte final se describe el uso del protocolo MKA, que es usado por las entidades de acceso por puerto para describir asociaciones y acuerdos clave utilizados por una entidad con seguridad MAC y se establece que un protocolo de aviso EAPOL permite a una entidad de acceso por puerto indicar la disponibilidad de los servicios de la red, ayudando a otras entidades elegir credenciales y parámetros adecuados para su autenticación.

Tabla 1.4.2: Seguridad de control de acceso a los medios

Seguridad de control de acceso a los medios [6]	**IEEE 802.1 AE**	**(12/2013)**
Descripción: En esta norma se indican los lineamientos de la seguridad de control de acceso a los medios, MACsec, los cuales permiten que los sistemas autorizados interconectar redes de área local en una red para mantener la confidencialidad de los datos transmitidos y tomar medidas contra las tramas transmitidas o modificadas por dispositivos no autorizados. De la forma que MACsec provee: - El mantenimiento de los servicios y conexiones en la red; - Aislamiento de ataques de denegación del servicio; - Comunicaciones seguras entre organizaciones, usando transmisiones mediante una LAN; - Localización de cualquier fuente de comunicación de red la LAN de origen; y - Protección a los componentes más vulnerables de la red. Es importante recalcar que, para obtener estos beneficios, MACsec debe ser utilizado con políticas adecuadas para operación de protocolos de alto nivel.		

[6] Esta norma fue preparada por el comité de normas del IEEE y adoptada posteriormente por la ISO con el nombre de ISO/IEC/IEEE 8802-1AE.

Aspectos técnicos relevantes: Esta norma: - Especifica los requerimientos que debe satisfacer un equipo buscando estar en conformidad con esta norma; - Especifica los requerimientos para MACsec en términos del servicio MAC; - Describe las amenazas que pudieran aparecer; - Especifica servicios de seguridad para hacer frente a las amenazas descritas; - Examina el impacto que podrían tener estas amenazas en la calidad del servicio del MACsec; - Modela el porte el servicio MACsec seguro en términos de métodos independientes en entidades de seguridad MAC; - Especifica el formato de unidades de datos de protocolo del MACsec; - Define las funciones de cada entidad de seguridad MAC; - Especifica la interfaz y el intercambio entre entidades de seguridad MAC y sus entidades MKA asociadas, con lo que se provee la actualización de las claves encriptadas; - Especifica los requisitos de rendimiento y recomienda valores predeterminados y rangos aplicables para parámetros operativos de una entidad de seguridad MAC; - Especifica cómo se incorporan las entidades de seguridad MAC dentro de la arquitectura estructurada dentro de estaciones finales y puentes; - Especifica el módulo base de gestión de la información (MIB, por sus siglas en inglés de *Management Information Base*) para gestionar la operación del MACsec en redes TCP/IP; y - Establece requerimientos, criterios y decisiones de *Cipher Suites* (un conjunto de uno o más algoritmos, diseñados para proporcionar cualquiera de los siguientes servicios: confidencialidad de los datos, autenticidad de los datos, integridad de los datos) para el uso de esta norma.

Tabla 1.4.3: Identidad del dispositivo seguro

Identidad del dispositivo seguro [7]	**IEEE 802.1 AR**	**(02/2015)**
Descripción: Esta norma describe los lineamientos para establecer identificadores de dispositivos seguros, DevIDs (del inglés *Secure Device Identifiers*), conectados a una red de área local. Su origen se remonta al problema que representan los dispositivos que se conectan automáticamente a la red como enrutadores y puentes, y/o no soportan mecanismos de autenticación. Una normalización de la identidad de los dispositivos que se conectan a las redes de área local facilita la autenticación de dispositivos seguros interoperables, y con ello, facilita la emisión de		

[7] Esta norma fue preparada por el comité de normas del IEEE y adoptada posteriormente por la ISO con el nombre de ISO/IEC/IEEE 8802-1AR.

normas de desarrollo y gestión de dispositivos seguros, y es por eso que esta norma beneficia a los fabricantes de equipos de redes. Los identificadores de dispositivos seguros están diseñados para ser utilizados como credenciales de autenticación de dispositivos seguros interoperables con el protocolo EAP y alguna otra norma industrial de autenticación.
Aspectos técnicos relevantes: Esta norma específica un identificador único por cada dispositivo y su respectiva gestión y encriptado, la relación entre la identidad instalada inicialmente y próximas identidades significativas, e interfaces y métodos para el uso de identificadores de dispositivos seguros con los existentes y nuevos protocolos de autenticación.

Un problema al que el IEEE ha estado haciendo frente de manera reciente, es el alto costo de la instalación de las redes *fieldbus*[8] en su implementación a escala. El problema surge porque la mayoría de los sistemas que se instalan para redes de protocolos TCP/IP son desarrollados, implementados y operados de manera independiente. Tradicionalmente se han empleado *gateways* para lograr dar accesibilidad los elementos de la red *fieldbus* mediante internet, sin embargo, las recientes aplicaciones de las redes a gran escala, hacen que sea necesario algo más que un simple acceso a estos dispositivos. En la mayoría de las implementaciones prácticas son necesarias memorias de almacenamiento de datos y lecturas de los sensores, interfaces para operación manual, sistemas de reporte y analizadores de datos.

En 2014 fue publicada por el IEEE la Norma para el protocolo de control comunitario, ecológico y ubicuo de la red 1888 (*IEEE Standard for Ubiquitous Green Community Control Network Protocol*) y en abril del 2015 fue adoptada por la ISO. Esta norma define un protocolo de intercambio de datos que generaliza e interconecta los componentes presentes en una red *fieldbus* (*gateways*, unidades de almacenamiento, y dispositivos de aplicaciones específicas) sobre redes diseñadas con protocolos IPV4/IPV6. Esto permite la integración capacidades como el almacenamiento de datos, servicios de gestión centralizada, el ahorro de energía y sistemas de monitoreo y alerta.

La seguridad del protocolo definido en la norma IEEE 1888 fue presentada en la norma IEEE 1888.3 (2013), adoptada internacionalmente en abril de 2016 con el nombre ISO/IEC/IEEE 18883. La Tabla 1.4.4 ofrece un análisis sobre la misma.

Tabla 1.4.4: Control comunitario, ecológico y ubicuo de la red: seguridad

Control comunitario, ecológico y ubicuo de la red: seguridad	**IEEE 1888.3**	**(04/2016)**

[8] En la cima de la cadena de control de un sistema de control distribuido, se encuentra el bus de campo (*fieldbus*) que enlaza los controladores lógicos programables con los elementos operantes, por ejemplo, sensores, motores eléctricos, consolas de luces, interruptores, etc.

Descripción: Esta norma mejora la gestión de la seguridad para el protocolo presentado en la norma IEEE 1888. En ella, se especifican los requerimientos de seguridad, se establece una arquitectura segura, se ofrece una descripción normalizada de autenticación y autorización, y se enlistan protocolos y procedimientos seguros. El contenido de esta norma ayuda a evitar la revelación accidental de datos al público y el acceso no autorizado a los recursos de la red. Aunado a lo anterior, provee integridad y confidencialidad a los datos del protocolo de control comunitario, ecológico y ubicuo de la red.
Aspectos técnicos relevantes: Esta norma especifica un marco de seguridad para proteger el intercambio de mensajes entre el plano de datos y el plano de control de los sistemas que operan en una red IEEE 1888 estableciendo autenticación manual, control de acceso, integridad del mensaje y confidencialidad de los datos. Se establece que para lograr cumplir las expectativas de seguridad se debe implementar el protocolo HTTP sobre la seguridad de la capa de transporte, HTTPS (del inglés *HTTP over TLS*), el cual es capaz de satisfacer los requerimientos de seguridad con un bajo costo de implementación.

En criptografía es común el uso de cifrado por bloques como algoritmo para el encriptado de datos almacenados. Los cifrados por bloques son algoritmos que operan sobre una cadena de grupos de bits que emplean una transformación invariable descrita por una llave simétrica. Liskov, Rivest y Wagner (2010) introducen el *tweakable block cipher*, un cifrado que entrega tres salidas, el mensaje, la llave criptográfica y el *tweak* (retoque), a diferencia de los cifrados por bloques comunes que solo entregan el mensaje y la llave criptográfica. Los beneficios de esta tercera salida permiten un diseño más sencillo tanto en el cifrado como en las aplicaciones de seguridad que se instauren sobre el mismo.

La norma IEEE 1619 (2007) retoma los *tweakable block cipher* y especifica los elementos de una arquitectura para la protección criptográfica de datos en dispositivos de almacenamiento, describiendo los métodos, algoritmos y modos de protección que deben ser empleados. La Tabla 1.4.5 muestra una descripción más profunda.

Tabla 1.4.5: Protección de datos en dispositivos de almacenamiento orientados a cifrado por bloques.

Protección de datos en dispositivos de almacenamiento orientados a cifrado por bloques.	**IEEE 1619**	**(04/2007)**
Descripción: Esta noma describe un método de encriptado para datos almacenados en dispositivos sectoriales donde las posibles amenazas incluyan el acceso no autorizado a los datos almacenados. Asimismo, esta norma específica la transformación de encriptado y un método		

para exportar e importar las llaves de encriptado para la compatibilidad entre diferentes implementaciones. Es importante mencionar que el encriptado de datos en tránsito no está cubierto por esta norma.
Aspectos técnicos relevantes: En esta norma se define el *XTS-AES tweakable block cipher*. Este cifrado es utilizado para el cifrado de datos en dispositivos de almacenamiento sectoriales. Dicho cifrado actúa en unidades de 128 o más bits. Utiliza el cifrado por bloques de la norma de encriptado avanzada, AES, como una subrutina. La singularidad del cifrado por bloques XTS-AES consiste en una clave de cifrado de datos y una clave *tweak* que es usada para incorporar la posición lógica del bloque de datos en el cifrado. El XTS-AES aborda amenazas como el ataque de copiar y pegar, al tiempo que permite la paralelización y el entubado en implementaciones de cifrado.

Uno de los problemas de seguridad cibernética más recientes es la seguridad en el internet de las cosas, IoT (del inglés *internet of things*). Esta tecnología que permite un sinfín de aplicaciones de la tecnología en la vida cotidiana, sin embargo, también representa una seria amenaza por las vulnerabilidades que presenta. Basta recordar el masivo ataque de denegación de servicio distribuido que sufrió Estados Unidos el pasado 21 de octubre de 2016 y causo una interrupción generalizada de duración variable en el servicio de internet. Dicho ataque fue dirigido a los servidores de la empresa Dyn, uno de los proveedores más importantes del sistema de nombres de dominio, DNS (por sus siglas en inglés de *Domain Name System*), lo que derivó en la suspensión de diferentes servicios de un gran número de usuarios al día, por ejemplo: Twitter, Pinterest, Reddit, GitHub, Etsy, Tumblr, Spotify, PayPal, Verizon, Comcast y la red de Playstation. El ataque fue posible gracias a todos los dispositivos digitales conectados a internet que forman parte del IoT, es decir, cámaras de vigilancia, sensores e incluso *routers* domésticos. Únicamente fue necesario infectar estos elementos del IoT con malicioso para formar una *botnet*[9], pues las medidas de seguridad en los dispositivos del IoT son usualmente escasas, y en algunos casos, nulas.

La norma IEEE 802.15.4 (abril de 2016) para redes inalámbricas de baja velocidad de transmisión establece los requerimientos de la capa física y el control de acceso a los medios enfocándose en los dispositivos que requieren baja potencia de transmisión y baja velocidad de transmisión en sus comunicaciones. Posicionándola como una norma que sirve para establecer un conveniente punto de partida para el desarrollo de normas de las capas superiores del IoT.

Reziok, Laurent y Demay (2016) analizan las medidas de seguridad empleadas por la norma IEEE 802.15.4 y enlistan las vulnerabilidades conocidas en materia de seguridad de la misma, entre las que destacan:

[9] *Botnet*: término que hace referencia a un conjunto de robots informáticos que se ejecutan de manera autónoma y automática.

- Denegación del servicio (DoS): ya sea enviando tramas no solicitadas para aumentar el consumo de energía y reducir la vida útil del dispositivo, o reenviando paquetes capturados para incrementar el contador de las tramas de tal forma que, en el futuro, las tramas legítimas sean rechazadas por una desincronización del contador.
- Conflicto de identificación en la red de área personal (*PANid*): sucede cuando hay dos coordinadores de la red de área personal con la misma identificación. Esto produce una recepción cruzada de alertas que deshabilita las comunicaciones mientras es resuelto el problema de identidad. Alguien mal intencionado podría mandar falsas alertas de conflicto de identificación forzando a interrumpir las comunicaciones por un problema falso.
- Acuse de recibido falsificado (*Spoofed ACK*): en IoT es sencillo falsificar las tramas, pues el encriptado de las mismas es sencillo o nulo. Una persona maliciosa podría enviar falsos acuses de recibido al dispositivo transmisor para evitar que los paquetes perdidos no sean reenviados. Haciendo esto de manera reiterativa se interrumpirían las comunicaciones entre los dispositivos y el coordinador de la red.
- Ataques GTS (Slot de tiempo garantizado, del inglés *Guaranteed Time Slot*): en algunas configuraciones de redes IoT, el coordinador de la red destina porciones de las súper tramas para evitar colisiones en la red, es decir, los periodos GTS. El inicio y la longitud de esos periodos no presenta encriptado, y es información que se envía en las alertas entre dispositivos. Algún individuo con intenciones negativas podría interceptar esta información y deshabilitar las comunicaciones en el tiempo preciso según cada dispositivo.
- Ataques de misma clave temporal (*Same-nonce attacks*): ese ataque es posible siempre y cuando dos tramas sean encriptadas con la misma llave y la misma clave temporal. Si una clave temporal es usada constantemente, las cadenas de laves permanecen idénticas y si dos tramas de este tipo son interceptadas, es posible descifrarlas al efectuar una operación XOR.
- Ataques de repetición (*Replay attacks*): como se mencionó anteriormente, el contador de la trama entrante es comparado contra el contador local. Si el contador entrante es menor o igual al local, la trama debe ser rechazada. Por otra parte, si se logran concretar ataques de la misma clave temporal, el contador local puede ser reiniciado en algún punto, lo cual implica que los ataques pueden repetirse una y otra vez.
- Ataques de maleabilidad (*Malleability attacks*): resulta de la combinación de dos ataques descritos anteriormente: si un texto sin formato fuera interceptado usando un ataque de misma clave temporal, una operación XOR revelaría su cadena de claves. A partir de ahí, si el contador de una trama utilizada previamente es aceptado en la recepción, se pueden falsificar tramas a partir de la cadena de claves y el contador interceptado.

El contenido presentado referente al IEEE muestra que las normas que ha presentado en materia de seguridad cibernética han atacado elementos muy específicos de la misma. A diferencia del UIT-T o ISO, donde se han publicado normas referentes a sistemas de gestión de la seguridad o a arquitecturas generales de los mismos, IEEE ha emitido normas en cuestiones más puntuales como la seguridad en las redes LAN.

Es muy importante recalcar que la mayoría de las publicaciones del IEEE son publicaciones de conferencia y artículos de divulgación. Es decir, sus principales publicaciones son sobre cuestiones muy específicas que fueron trabajadas por grupos de investigadores e hicieron públicos sus resultados.

Instituto Europeo de Normas de Telecomunicaciones

El instituto Europeo de Normas de Telecomunicaciones, ETSI (por sus siglas en inglés de *European Telecommunications Standards Institute*), es una organización independiente, sin fines de lucro y ampliamente respetada por su neutralidad e integridad que se encarga de producir normas globales aplicables para las TIC, incluyendo tecnologías fijas, móviles, de radio, convergentes, de radiodifusión y de internet. Existe para todos aquellos que necesitan ser involucrados en la normalización de las telecomunicaciones y es una organización abierta, es decir, crea normas mediante consensos a través de la participación directa de sus miembros.

El ETSI es el organismo regional reconocido para emitir normas en Europa (conocido como un ESO, por sus normas en inglés, *European Standards Organization*), abarcando a las telecomunicaciones, la radiodifusión, así como a otras redes de comunicaciones electrónicas y diversos servicios.

Este organismo juega un papel muy importante en Europa, incluyendo el soporte a la regulación y legislación europea a través de la creación de normas armónicas. Únicamente las normas desarrolladas por las tres ESO: CEN (por sus siglas en inglés de *European Committee for Standardization*), CENELEC (por sus siglas en inglés de *European Committee for Electrotechnical Standardization*) y el ETSI; son reconocidas como Normas Europeas (también conocidas en inglés como *European Standards,* EN).

El ETSI actualmente tiene su sede en el parque científico de Sophia Antípolis, Francia, en el cual está desde Julio de 1989. Cuenta con 857 miembros procedentes de diversos países y provincias dentro y fuera de Europa de los que conforman parte 66 países de cinco continentes, e incluyen a fabricantes, operadores de redes, administraciones, proveedores de servicios, organismos de investigación, universidades, compañías de consultoría y organizaciones de usuarios.

El ETSI, ha encarado la problemática de la seguridad en las redes principalmente con la creación de grupos de trabajo que desarrollen estándares en la materia. Los grupos de trabajo en estos temas que han destacado son los siguientes:

- El Grupo de Expertos en Algoritmos de Seguridad (SAGE, por sus siglas en inglés *de Security Algorithms Group of Experts*): cuya función es desarrollar algoritmos de seguridad y encriptación para usos de las tecnologías estandarizadas por la ETSI. Dentro de las últimas 20 publicaciones de este grupo se encuentran 17 especificaciones técnicas referentes a encriptados en telefonía móvil, un reporte técnico acerca de la generación de claves en telefonía móvil, una guía ETSI para escoger un algoritmo de forma adecuada, y un reporte de grupo acerca del encriptado cuántico;
- El comité técnico de firmas electrónicas e infraestructuras: es el encargado de lidiar con las formas digitales, sus formatos y sus certificados, proveedores de servicios de confianza y servicios auxiliares. Dentro de las últimas 20 publicaciones de este comité se encuentran 16 especificaciones técnicas sobre lo diferentes formatos de cifrado (principalmente XAdES, CAdES, ASiC y XML), 3 reportes técnicos sobre los formatos de cifrado y un reporte especial sobre las normas para el formato de firma digital AdES en ambientes móviles y distribuidos;

- El grupo de especificaciones de la industria sobre indicadores de seguridad de la información (ISG ISI, por sus siglas en inglés de *Industry Specification Group on Information Security Indicators*): produce especificaciones que en conjunto generan un amplio modelo de referencia para el manejo de las amenazas a la seguridad de la información. Al día de hoy este grupo ha emitido un total de 10 especificaciones de grupo ETSI, algunas de las cuales han sido adoptadas por algunas agencias gubernamentales europeas de seguridad de la información.

- El comité técnico de seguridad cibernética (TC CYBER, del inglés *Cybersecurity Technical Committee*): creado en 2014, trabaja estrechamente con las partes interesadas para desarrollar normas para aumentar la privacidad y la seguridad de las organizaciones y ciudadanos en toda Europa. En sus últimas 20 publicaciones se encuentran 12 reportes técnicos de temas de defensa cibernética o similar, 3 especificaciones técnicas y una guía ESTI sobre el impacto que tendrán las computadoras cuánticas en la seguridad cibernética.

- El grupo de especificaciones de la industria sobre Criptografía cuántica segura (ISG QSC, por sus siglas en ingles de *Industry Specification Group on Quantum-safe cryptography*): está tomando una iniciativa proactiva para definir normas que sean capaces de garantizar la seguridad de la información conforme la tecnología avanza. Aunque a principios de 2017 este grupo de trabajo fue cerrado y pasó a ser un grupo de trabajo más pequeño dentro del comité técnico de seguridad cibernética, vale la pena reconocer el esfuerzo vanguardista del ETSI y mencionar los 4 reportes de grupo que fueron emitidos, donde se bosqueja el marco para normas de algoritmos seguros en ambientes cuánticos, los tamaños que deberían tener las claves criptográficas, y los escenarios de desarrollo y los de amenazas que acompañarán a la época de la computación cuántica.

A pesar de que los grupos de trabajo del ETSI no han emitido hasta ahora una norma de seguridad cibernética, hay que reconocer la labor que hacen en los diferentes frentes de la misma, pues el ETSI mantiene grupos y comités trabajando en temas de encriptado, indicadores de seguridad, firmas electrónicas y el impacto de la computación cuántica en la seguridad. Este último grupo es un notable esfuerzo del ETSI en mantenerse a la vanguardia en las tecnologías que hoy nos rodean.

La Fuerza de Tareas de Ingeniería de Internet

La Fuerza de Tareas de Ingeniería de Internet, IETF (por sus siglas en inglés de *Internet Engineering Task Force*) es una amplia comunidad internacional formada por diseñadores de red, operadores, vendedores e investigadores preocupados por la evolución de la arquitectura de internet y el correcto funcionamiento del mismo.

El trabajo técnico de la IETF se logra a través de sus grupos de trabajo, que se enfocan en diferentes áreas como enrutamiento, seguridad, transporte, etc.

El área de seguridad de la IETF está conformada por los 16 grupos de trabajo siguientes:

- Autenticación u autorización en ambientes forzados;
- Ambiente de gestión de certificados autorizados;
- Depreciación y curvas de cifrado;
- Señalización de francas amenazas DDoS;
- Funciones de la interface de la red de seguridad;
- Mantenimiento y ampliación de la seguridad en el protocolo de internet;
- Tecnología de autenticación común de la próxima generación;
- Mecanismos adicionales limitados para certificados PKIX y SMIME;
- Intercambio ligero de incidentes gestionados;
- Protocolo de autorización web;
- Especificaciones abiertas para muy buena privacidad;
- Automatización de la seguridad y monitoreo continuo;
- Eventos de seguridad;
- Seguridad de la capa de transporte;
- Enlace simbólico; y
- Transparencia del notario público.

El área de seguridad de la IETF, además de trabajar en estos grupos de trabajo, participa en grupos de trabajo de otras áreas de la IETF, como el autenticación y manejo de laves para protocolos de enrutamiento, extensiones DNS y seguridad web, entre otros.

Las publicaciones por este organismo son de una relevancia internacional. A cada publicación emitida se le asigna un número de solicitud de comentarios (RFC, del inglés *Request for Comments*). Esta metodología ha resultado altamente eficaz para la elaboración de normas por parte de otros organismos internacionales. Por ejemplo, las publicaciones de la IETF son empleadas frecuentemente como referencia para normas internacionales por organismos internacionales como el UIT-T y el IEEE. La Tabla 1.6.1 muestra las referencias en las normas internacionales del UIT-T analizadas hasta ahora correspondientes a publicaciones de la IETF.

Tabla 1.6.1: Participación de la IETF en la UIT[10]

Norma	Referencias
UITTT X.1205, Aspectos generales de la ciberseguridad	IETF RFC 1918 (1996), *Address Allocation for Private Internets* IETF RFC 2396 (1998), *Uniform Resource Identifiers (URI): Generic Syntax*
UIT-T X.1582, Intercambio de	IETF RFC 2616 (1999), *Hypertext Transfer Protocol* – HTTP/1.1. IETF RFC 3080 (2001), *The Blocks Extensible Exchange Protocol Core*.

[10] La Tabla 1.6.1 es de creación propia.

información de ciberseguridad	IETF RFC 3436 (2002), *Transport Layer Security over Stream Control Transmission Protocol*. IETF RFC 4895 (2007), *Authenticated Chunks for the Stream Control Transmission Protocol*. [b-IETF RFC 4960] IETF RFC 4960 (2007), *Stream Control Transmission Protocol*. IETF RFC 4987 (2007), *TCP SYN Flooding Attacks and Common Mitigations*. IETF RFC 5062 (2007), *Security Attacks Found Against the Stream Control Transmission Protocol (SCTP) and Current Countermeasures*. IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*. IETF RFC 5925 (2010), *The TCP Authentication Option*. IETF RFC 6265 (2011), *HTTP State Management Mechanism*. RFC 6455 (2011), *The WebSocket Protocol*. IETF RFC 6797 (2012), *HTTP Strict Transport Security*.
UIT-T Y.2704, Mecanismos y procedimientos de seguridad para las redes de próxima generación	IETF RFC 4302 (2005), *IP Authentication Header* IETF RFC 4303 (2005*), IP Encapsulating Security Payload (ESP).* IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.
UIT-T Y.2701 Requisitos de seguridad para las redes de próxima generación. Versión 1	IETF RFC 2085 (1997), *HMAC-MD5 IP Authentication with Replay* *Prevention*. IETF RFC 2403 (1998), *The Use of HMAC-MD5-96 within ESP and AH*. [IETF RFC 2404 (1998), *The Use of HMAC-SHA-1-96 within ESP and* *AH*. IETF RFC 2405 (1998), *The ESP DES-CBC Cipher Algorithm With* *Explicit IV*. IETF RFC 2410 (1998), *The NULL Encryption Algorithm and Its Use*

	With IPsec. IETF RFC 2411 (1998), *IP Security Document Roadmap*. IETF RFC 2451 (1998), *ESP CBC-Mode Cipher Algorithms*. IETF RFC 2709 (1999), *Security Model with Tunnel-mode IPsec for NAT Domains*. IETF RFC 2857 (2000), *The Use of HMAC-RIPEMD-160-96 within ESP and AH*. IETF RFC 3526 (2003), *More Modular Exponential (MODP) Diffie-* *Hellman groups for Internet Key Exchange (IKE)*. IETF RFC 3602 (2003), *The AES-CBC Cipher Algorithm and Its Usewith IPsec*. IETF RFC 3664 (2004), *The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)*. IETF RFC 4109 (2005), *Algorithms for Internet Key Exchange version 1 (IKEv1)*. IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol*. IETF RFC 4302 (2005), *IP Authentication Header*. IETF RFC 4303 (2005), *IP Encapsulating Security Payload (ESP)*. IETF RFC 4304 (2005), *Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)*. *Cryptographic Algorithm Implementation* *Requirements for Encapsulating Security Payload (ESP) and* *Authentication Header (AH)*. IETF RFC 4306 (2005), *Internet Key Exchange (IKEv2) Protocol*. IETF RFC 4307 (2005), *Cryptographic Algorithms for Use in the* *Internet Key Exchange Version 2 (IKEv2)*. IETF RFC 4308 (2005), *Cryptographic Suites for IPsec*. IETF RFC 4309 (2005), *Using Advanced Encryption Standard (AES)*

	CCM Mode with IPsec Encapsulating Security Payload (ESP). IETF RFC 4312 (2005), *The Camellia Cipher Algorithm and Its Use* *With IPsec*.

Como se puede observar, la IETF ha aportado una vasta cantidad de normas en cuanto a la seguridad en las redes, de las cuales la UIT-T ha empleado varias para generar sus propias recomendaciones, principalmente en materia de ciberseguridad y en los mecanismos, procedimientos y requerimientos de seguridad para las redes de próxima generación.

Por otra parte, la IETF también ha sido de ayuda para el desarrollo de las normas del IEEE. La Tabla 1.6.2 muestra una relación de las referencias con las que ha contribuido y las normas IEEE analizadas anteriormente que las presentan.

Tabla 1.6.2: Participación de la IETF en el IEEE[11]

Norma	Referencias
IEEE 802.1X, Control de acceso a la red basado en puertos	IETF RFC 787, *Connectionless data transmission survey/tutorial*, 1981. IETF RFC 2246, *The TLS Protocol Version 1.*0, 1999. IETF RFC 2865, *Remote Authentication Dial In User Service (RADIUS),* 2000. IETF RFC 2866, RADIUS *accounting,* 2000. IETF RFC 3268, *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Securit*y, 2002. IETF RFC 3414, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*, 2002. IETF RFC 3575, *IANA Considerations for RADIUS*, 2003. IETF RFC 3588, *Diameter Base Protocol*, 2003. IETF RFC 3748, *Extensible Authentication Protocol* (EAP), 2004. IETF RFC 4072, *Diameter Extensible Authentication Protocol (EAP) Application*, 2005.

[11] La Tabla 1.6.2 es de creación propia.

	IETF RFC 5176, *Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS*), 2008. IETF *Internet Draft, RADIUS Attributes for IEEE 802 Networks*, 2008.
IEEE 802.1AE, Seguridad MAC	IETF RFC 2279, *UTF-8, a Transformation format of ISO 10646*, 1998. IETF RFC 2406*, IP Encapsulating Security Payload (ESP),* 1998. IETF RFC 2737, *Entity MIB (Version 2),* 1999. IETF RFC 3232, *Assigned Numbers: RFC 1700 is Replaced by an On-line Database*, 2002. IETF RFC 3410, *Introduction and Applicability Statements for Internet-Standard Management Framework*, 2002. IETF RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Manage-ment Frameworks*, 2002.
IEEE 802.1AR, Identidad del dispositivo seguro.	IETF RFC 787, *Connectionless data transmission survey/tutoria*l, 1981. IETF RFC 2104, *HMAC: Keyed-Hashing for Message Authentication,* 1997. IETF RFC 2279, *UTF-8, A transformation format of ISO 10646*, 1998. IETF RFC 2865, *Remote Authentication Dial In User Service (RADIUS*), 2000. IETF RFC 3232, *Assigned Numbers: RFC 1700 is Replaced by an On-line,* 2002. IETF RFC 3279, *Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,* 2002. IETF RFC 3411, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*, 2002. IETF RFC 3412*, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*, 2002. IETF RFC 3413, *Simple Network Management Protocol (SNMP) Applications,* 2002. IETF RFC 3415, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*, 2002.

	IETF RFC 3416, *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP*), 2002. IETF RFC 3417, *Transport Mappings for the Simple Network Management Protocol (SNMP),* 2002. IETF RFC 3575*, IANA Considerations for RADIUS*, 2003. IETF RFC 3576, *Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS*), 2003. IETF RFC 3579, *RADIUS Support for Extensible Authentication Protocol (EAP*), 2003. IETF RFC 3580, *IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*, 2003. IETF RFC 3748, *Extensible Authentication Protocol (EAP*), 2004. IETF RFC 4108, *Using Cryptographic Message Syntax (CMS) to Protect Firmware Package*s, 2005. IETF RFC 4133, *Entity MIB (Version 3*), 2005. IETF RFC 4346, *The Transport Layer Security (TLS) Protocol, Version 1.1*, 2006. IETF RFC 5216, *The EAP-TLS Authentication protocol*, 2008.
IEEE 1888.3, Control comunitario, ecológico y ubicuo de la red: seguridad.	IETF RFC 791*, Internet Protocol,* 1981. IETF RFC 1035, *Domain Names—Implementation and Specification,* 1987. IETF RFC 2459*, Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, 1999. IETF RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*, 1998. IETF RFC 5246, *The Transport Layer Security (TLS) Protocol, Version 1.2*, 2008. ETF RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, 2008. IETF RFC 5322, Internet *Message Format*, 2008. IETF RFC 6066, *Transport Layer Security (TLS) Extensions: Extension Definitions*, 2011.

	IETF RFC 6277, "*Online Certificate Status Protocol Algorithm Agility*," 2011.

Las Tablas 1.6.1 y 1.6.2 tienen la intención de mostrar la gran importancia de las publicaciones de la IETF en los procesos de normalización de las telecomunicaciones, particularmente en la seguridad de las redes, en los organismos más importantes.

Se puede decir que la IETF ha sido esencial en el proceso regulatorio de internet, y que dicha esencia trasciende en las normas en materia de seguridad cibernética. Este organismo opera en un nivel técnico con mayor profundidad y constancia que los demás organismos presentados. Esta premisa no es tan atrevida si se considera que, de todos los organismos analizados, la IETF es la única con un enfoque específico hacia el internet, lo cual permite que el grueso de las investigaciones y publicaciones de la IETF sean en función de la red y sus especificaciones.

Es conveniente ahondar en el posicionamiento que ha logrado tener la IETF a nivel global, pues el hecho de que sus publicaciones sirvan de materia prima para emitir normas y recomendaciones internacionales hace evidente el nivel de compromiso y eficiencia que impera en esta organización.

Aspectos Técnicos

Uno de los problemas a los que se enfrentan los reguladores y normalizadores con frecuencia es el empleo de términos ambiguos o poco utilizados por otros organismos. Tal es el caso del concepto "ciberseguridad". De acuerdo con la UIT, la ciberseguridad es:

> El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes:
>
> - Disponibilidad;
> - Integridad, que puede incluir la autenticidad y el no repudio;
> - Confidencialidad.
>
> (Unión Internacional de Telecomunicaciones, 2008) [9]

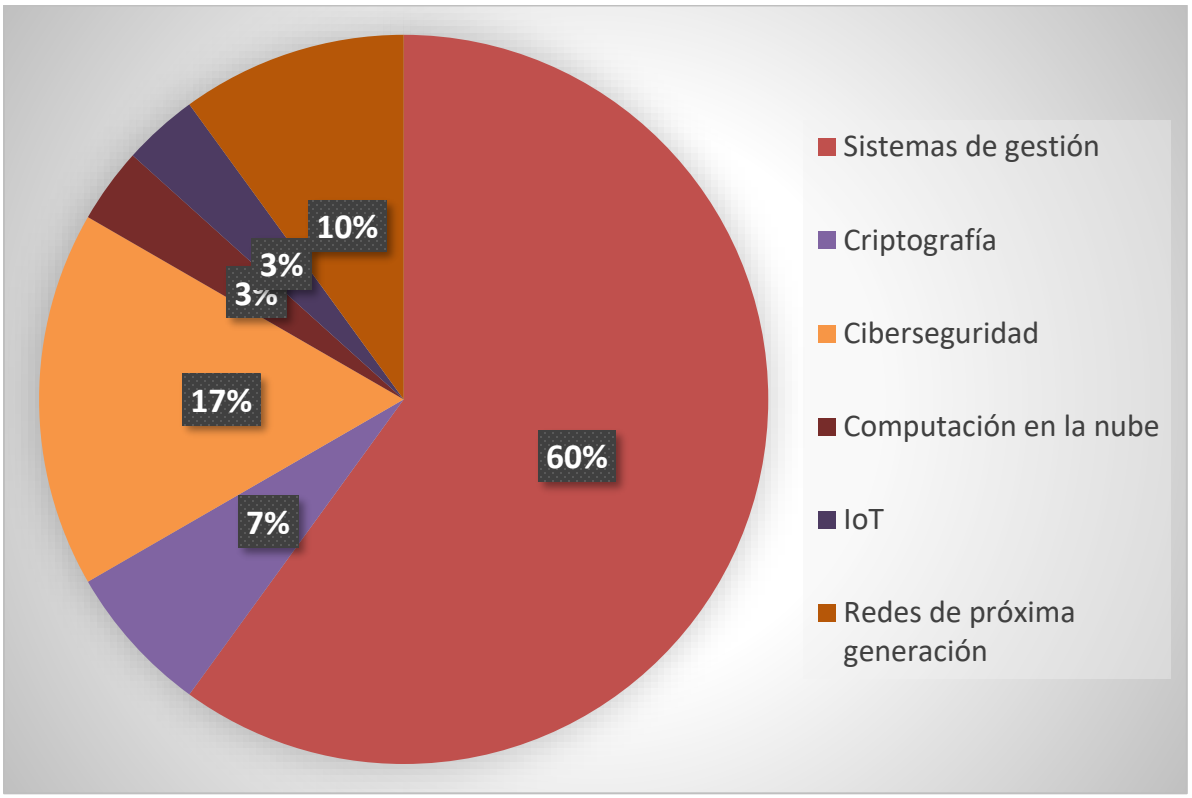
Claramente se observa que la seguridad de la información, depende de un entorno o un ciberentorno para garantizar las propiedades, mismo que incluye a los usuarios, a las redes dispositivos, software, procesos, información almacenada, información que circula a través de las redes, aplicaciones y servicios que se encuentren conectados directa o indirectamente a las redes. Esto implica que las normas analizadas en el Capítulo I son, de una forma u otra, partícipes de la ciberseguridad. Sin embargo, el término no ha terminado de cobrar la fuerza necesaria para unificar a las normas de los sistemas de gestión de seguridad en las redes, computación en la nube, criptografía, internet de las cosas o seguridad en las redes de la próxima generación en un solo término.

Es por lo anterior que para sintetizar lo expuesto a lo largo del capítulo es conveniente realizar una categorización de las normas analizadas en los campos de:

- Sistemas de gestión de la seguridad: en este campo se encuentran las normas que proponen explícitos sistemas de gestión de la seguridad, arquitecturas de red para comunicaciones específicas, marcos de referencia en requerimientos de los sistemas de gestión o las arquitecturas de red, y los criterios de evaluación de los sistemas de gestión y/o arquitecturas de red. De tal forma que, del conjunto de normas analizadas, las normas que entran en esta categoría son:
    - ISO/IEC 7498-2 (UIT-T X.800): Arquitectura de seguridad de interconexión de sistemas abiertos, 1991;
    - UIT-T X.810-X.816: Marcos de seguridad para sistemas abiertos, 1995-1996;
    - UIT-T X.805: Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo, 2003;
    - UIT-T X.1121: Marco general de tecnologías de seguridad para las comunicaciones móviles de datos de extremo a extremo, 2004;
    - ISO/IEC 15408: Criterios de evaluación para la seguridad informática, 2009;
    - UIT-T X.1032: Arquitectura de interrelaciones externas para un sistema de seguridad de la red de telecomunicaciones IP, 2010;
    - IEEE 802.1 X: Control de acceso a la red basado en puertos, 2010;
    - IEEE 802.1 AE: Seguridad del control de acceso a los medios, 2013;
    - IEEE 802.1 AR: identidad del dispositivo seguro, 2015; e
    - IEEE 1888.3: Control comunitario, ecológico y ubicuo de la red: seguridad.
- Criptografía: fueron ubicadas en este campo aquellas normas que explícitamente definen algoritmos de cifrado, certificados de claves públicas, etc. Las normas que entran a esta categoría son las siguientes:
    - IEEE 1619: Protección de datos en dispositivos de almacenamiento orientados a cifrado por bloques, 2007; y
    - UIT-T X.509: El directorio: Marcos para certificados de claves públicas y atributos, 2016.
- Seguridad en las redes de la próxima generación: retomando la definición de las redes de la próxima generación presentada con anterioridad, las normas que pertenecen a este sector son:
    - UIT-T Y.2701: Requisitos de seguridad para las redes de la ´próxima generación, versión 1, 2007;
    - UIT-T Y.2704: Mecanismos y procedimientos de seguridad para las redes de a próxima generación, 2010; y

    - UIT-T Y.2740: Requisitos de seguridad para las transacciones financieras móviles a distancia en las redes de la próxima generación, 2011.
- Computación en la nube: la norma que presenta lineamientos en este sector son:
    - UIT-T X.1601: Marco de seguridad para la computación en la nube, versión 2,2015.
- Internet de las cosas: al igual que la computación en la nube, este sector aún no cuenta con muchas publicaciones, valiéndose únicamente de la norma:
    - IEEE 802.15.4: Norma IEEE para redes inalámbricas de baja velocidad de transmisión, 2016.
- Ciberseguridad: ELUIT-T ha publicado normas haciendo uso de este término que, como se expresó con anterioridad, abarca en gran medida los temas que cubren otras normas. De las normas analizadas, aquellas que hacen alusión directa a la ciberseguridad son:
    - UIT-T X. 1205: Aspectos generales de la ciberseguridad, 2008;
    - UIT-T X. 1207: Directrices para los proveedores de servicios de telecomunicaciones acerca del riesgo de programas espías y de software potencialmente no deseado, 2008;
    - UIT-T X.1544: Enumeración y clasificación de pautas de ataques comunes, 2013;
    - UIT-T X. 1208: Un indicador de riesgo de ciberseguridad para mejorar la confianza y la seguridad en la utilización de las tecnologías de la información y la comunicación, 2014;
    - UIT-T X.1211: Técnicas para prevenir ataques en la web, 2014; y
    - UIT-T X. 1582: Protocolos de transporte para el intercambio de información de ciberseguridad, 2014.

Es cierto que el universo de normas en materia de seguridad cibernética es mucho más amplio que las presentadas en este capítulo. No obstante, las organizaciones analizadas ofrecen la oportunidad de ingresar a sus compendios de sus normas y ordenarlas por relevancia, de tal forma que las normas presentadas representan un conjunto suficientemente representativo del total de las mismas. La Gráfica 1.7.1 muestra el porcentaje que representa cada categoría descrita anteriormente.



Gráfica 1.7.1: Categorización de las normas presentadas en el Capítulo I[12]

De la Gráfica 1.7.1 se puede notar que el grueso de las normas en materia de seguridad cibernética abarca temas de sistemas de gestión de la seguridad, cuyos puntos más repetidos son:

- El establecimiento de los objetivos del sistema de gestión;
- El uso de indicadores como criterios de evaluación de dichos objetivos;
- La implementación de dimensiones de seguridad (control de acceso, autentificación, no repudio, integridad de los datos, confidencialidad de los datos, disponibilidad, privacidad, seguridad de las comunicaciones, entre otros);
- El uso del protocolo MKA y MAC
- Establecer planos de control, de gestión y de usuarios externos, esto implica percibir os requerimientos de seguridad desde el punto de vista del usuario de la red y desde el punto de vista del proveedor del servicio; y
- Establecer conexiones seguras en los elementos del borde de la red.

Con respecto a los algoritmos de cifrado y los aspectos criptográficos tomados en cuenta en las normas analizadas los puntos más contundentes son:

- La implementación de un servidor RADIUS en la gestión de acceso;
- El empleo de técnicas VPN e IPsec, AH, ESP, LSTP, entre otras;

[12] La Gráfica 1.7.1 es de creación propia.

- La gestión de llaves públicas y certificados con técnicas como PKIX, CMP, OSCP, entre otras;
- Implementar seguridad en la capa de transporte;
- Hacer uso de algoritmos de encriptado como el DES, 3DES, AES, MD5, SHA-1, entre otros;
- Hacer uso de la tecnología de acceso protegido a WiFi, WPA y WPA2; y
- Contar con un centro de operaciones de red.

Las normas de seguridad para las redes de la próxima generación presentan aspectos técnicos contundentes muy similares a los que se exhiben en las normas de sistemas de gestión de la seguridad. Los más destacables se enlistan a continuación:

- Mecanismos de dimensiones de seguridad como autenticación, identificación y autorización, entre otros;
- El empleo de técnicas como IPsec y TLS;
- El uso de técnicas de encriptado como SRTP, AES, HMAC-SHAI; y
- Mecanismos de auditoria a la red a través de protocolos SNMP, SNTP o Syslog.

La norma IEEE 802.15.4 sirve de referencia para publicaciones posteriores que busquen normalizar el internet de las cosas. Los aspectos más contundentes de la misma, en cuanto a seguridad se refiere, son:

- Encriptar utilizando AES con contador o AES con contador combinado con CBC-MAC (cifrado por bloques encadenados en el código de autenticación de mensajes, del inglés *ipher Block Chaining Message Authentication Code)* de 32, 64 o 128 bits; y
- Agregar un encabezado auxiliar de seguridad a la trama transmitida;

Al presentar los puntos presentes con contundencia en las normas categorizadas en el tema de ciberseguridad se comprende por qué es deseable tener un término que abarque todos estos aspectos, pues estas retoman muchos puntos que destacan en los otros tópicos. Los puntos más contundentes en estas normas son:

- Establecer dimensiones de seguridad control de acceso, autentificación, no repudio, integridad de los datos, confidencialidad de los datos, disponibilidad, privacidad, seguridad de las comunicaciones, entre otros);
- El uso de prácticamente todas las medidas de encriptado expuestas anteriormente;
- El uso de indicadores para mejorar los servicios de seguridad;
- El empleo de técnicas para proteger la capa de transporte, como TLS, HTTP, SCTP y UDP; y
- El manejo de catálogos de ataques comunes.

La norma UIT-T X. 1601, no presenta elementos técnicos contundentes. Sin embargo, es valioso recalcar que la computación en la nube es inherentemente más vulnerable a amenazas externas e internas que otros campos del ciberespacio, debido a su naturaleza distribuida y múltiple, al predominio del acceso a distancia a sus servicios y al número de entidades que intervienen en cada proceso. Es por eso que la gestión de la seguridad de los servicios de computación en la nube, así como de los recursos afines, es un aspecto fundamental.

Referencias del Capítulo I

[1] Organización de las Naciones Unidas (2014*). La situación demográfica del mundo, 2014. Informe conciso.* Recuperado de http://www.un.org/en/development/desa/population/publications/pdf/trends/Concise%20Report%20on%20the%20World%20Population%20Situation%202014/es.pdf

[2] Unión Internacional de Telecomunicaciones (2016). *ICT Facts and figures 2016*. Recuperado de http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

[3] Creación propia, basada en el Cuadro 2/X.800 de la Recomendación UIT-T X.800: Arquitectura de Seguridad de la Interconexión de Sistemas Abiertos, UIT, 1991.

[4] Ibid

[5] Datos promocionados por la UIT en su página de internet, recuperados el 8 de marzo de 2017. Disponibles en http://www.itu.int/es/about/Pages/default.aspx

[6] Unión Internacional de Telecomunicaciones (2003). *UIT-T Rec. X.805 (10/2003) Arquitectura de seguridad para sistemas de comunicaciones de extremo a extremo*. Ginebra: UIT

[7] Datos promocionados por la ISO en su página de internet, recuperados el 30 de marzo de 2017. Disponibles en https://www.iso.org/about-us.html

[8] Datos promocionados por la IEEE en su página de internet, recuperados el 5 de abril de 2017. Disponibles en https://www.ieee.org/about/about_index.html

[9] Unión Internacional de Telecomunicaciones (2008). *UIT-T Rec. X.1205 (04/2008) Aspectos generales de la ciberseguridad*. Ginebra: UIT

Capítulo II: Casos Internacionales.

La seguridad cibernética es un tema de gran importancia para los organismos reguladores. Comenzando con la afronta que representa a los cuidadanos de cualquier nacionalidad el robo de información personal a insituciones públicas o privadas. Para ahondar en este aspecto es conveniente mostrar las cifras presentadas por Symantec en su Reporte de Amenazas a la Seguridad de Internet 2016, en el cual se expone que 429 millones de identidades estuvieron expuestas en intenret en el año 2015, lo cual representa un aumento del 23% con respecto al año anterior[1].

Otro aspecto que es importante entender es la cantidad de ataques que hay entre naciones. Estos pueden ser orquestados por organizaciones o individuos, ajenos al gobierno o no, que dirigen sus ataques hacia objetivos fuera de las fronteras políticas de sus páises. Los motivos de estos ataques son variados, entre ellos puede haber desde ataques activistas que sirvan de protesra, hasta atques encaminados a afectar los controles de armas nucleares y bases militares.

Un ejemplo de lo anteior es el programa W32.Stuxnet, considerado como el primer ataque cibernético que ataca específicamente a sistemas de control industrial. Se piensa que este sofisticado programa fue diseñado por un equipo especializado con la intención de inhabilitar las armas nucleares de Iran en 2010. En principio, se señala como responsable a los gobiernos de Israel y Estados Unidos por la cantidad de recursos necesarios para el desarrollo de este sotware malicioso y por los intereses que mantenian dichos gobiernos ante el programa de armas nucleares de Iran.

Como es de esperarse, los ataques entre naciones han aumentado significativamente en los últimos años, ya sea por competencia desleal entre empresas, vandalismo, activismo, guerra cibernética entre naciones, represiones o cualquier otro motivo, el entorno cibernético está continuamente en lucha. En la Perspectiva Global de la organización Norse presentada en diciembre de 2015 se muestran datos específicos acerca de los ataques cibernéticos que son recibidos y emitidos por ciertas naciones, entre los que destacan que:

- China fue la mayor fuente de ataques por volumen;
- Islandia fue la mayor fuente de ataques si se considera la población;
- Estados Unidos fue el objetivo de los ataques más común; y
- Arabia Saudita fue situada en la cabecera de la lista tanto de ataques como objetivo de los ataques por volumen y también cuando se consideró la población.

Aunado a lo anterior, Norse emplea ocho millones de sensores en una red de monitoreo de ataques cibernéticos, la cual ofrece la posibilidad de observar en tiempo real los ataques que se están dando a lo largo del mundo. La Ilustración 2.1 muestra un ejemplo de la red de monitoreo de Norse. Son estas cuestiones las que permiten a firmas que el entorno cibernético es un nuevo frente en los conflictos entre naciones.

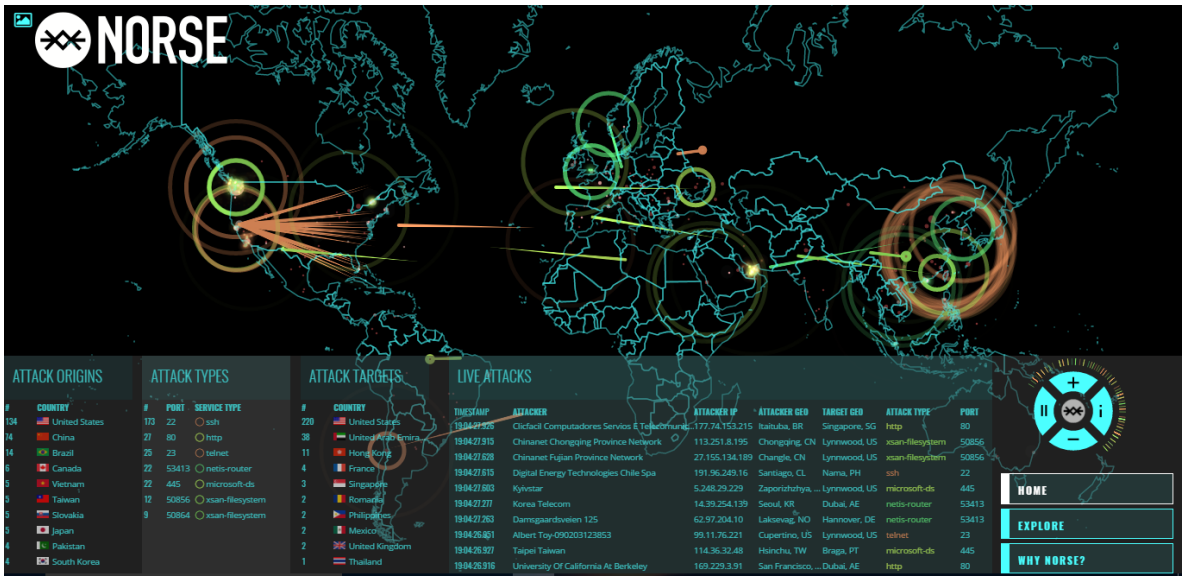


Ilustración 2.1: Mapa de ataques cibernéticos en tiempo real [2]

Otro aspecto por el cual es importante hablar de las regulaciones que siguen los países es por el hecho de que son los gobiernos los únicos con la capacidad de castigar a los delincuentes criminales. Se podría llegar a pensar que para generar entornos cibernéticos seguros sólo bastaría con que los proveedores de tecnología y servicios cibernéticos reforzaran las medidas de seguridad y que los usuarios conozcan estas medidas. Esta idea es ilusa. No se puede negar la responsabilidad de los gobiernos ante las amenazas del entorno cibernético. Esta responsabilidad debe verse reflejada en los diferentes aparatos legislativos y penales de los gobiernos.

Es por esta razón que en 2001 los Estados Miembros del Consejo de Europa y otros Estados del resto del mundo establecieron el Convenio sobre la Ciberdelincuencia, mejor conocido como el Convenio de Budapest. Dicho convenio tiene como objetivo principal la adopción de una legislación que facilite la prevención de las conductas delictivas y contribuya con herramientas eficientes en materia penal que permitan detectar, investigar y sancionar las conductas antijurídicas.

El Convenio de Budapest establece las medidas que los Estados adheridos deberán adoptar a nivel nacional. Entre estas medidas destacan el considerar como un delito el acceso no autorizado a los sistemas informáticos, los ataques a la integridad de los datos y lo sistemas, la falsificación informática, el fraude informático, las acciones relacionadas con la pornografía infantil y las afecciones a la propiedad intelectual. Así mismo establece las acciones referentes a la cooperación internacional que deberán seguir las acciones adheridas a este convenio.

Mejores Prácticas

En esta sección se presenta un análisis de las medidas emprendida por Estados Unidos, la República de Estonia, Israel y la República de Corea en cuestiones de ciberseguridad. Es importante entender que si estos países han sido elegidos es porque son un buen ejemplo para poner en evidencia el hecho de que la seguridad cibernética debe ser atacada por un frente amplio, es decir, no es una cuestión de intereses exclusivos de un sector de la población. Por lo tanto, en este análisis se encontrarán aspectos estratégicos, políticos, jurídicos, académicos, culturales e, incluso, militares.

Estados Unidos de América

Estados Unidos ha brindado una especial atención a la seguridad en las redes, pues la seguridad económica y nacional de este país depende directamente del funcionamiento óptimo de sus telecomunicaciones. El gobierno estadounidense se ha permitido blindar la seguridad en las redes de telecomunicaciones desde diversos frentes, los cuales involucran agencias especializadas, un gran trabajo de su órgano regulador y creación de grupos especializados de trabajo, por mencionar algunos.

Se puede afirmar que varias organizaciones estadounidenses son un objetivo recurrente de los ataques cibernéticos, ya sea que estos ataques vengan del interior de su territorio o de cualquier otro país. Son múltiples los factores políticos y económicos que hacen de este país el destino de un gran número de ataques cibernéticos, se puede mencionar una lista no exhaustiva de estos, entre los que destacan su poder económico, sus intervenciones militares en los conflictos de oriente medio, su proceso electoral reciente, etcétera. Describir a fondo estos factores no obedece a los objetivos de este escrito, sin embargo, es importante destacar los retos, derivados de dichos factores, que enfrenta aquella nación en materia de seguridad cibernética. Los retos que enfrentan los Estados Unidos en materia de seguridad cibernética son descritos de forma muy clara en el informe sobre el crecimiento y aseguramiento de la economía digital de la Comisión de Mejora de la Ciberseguridad Nacional (en adelante CENC, por sus siglas en inglés de *Commission on Enhancing National Cybersecurity).*

La CENC se creó en febrero de 2016 bajo la orden ejecutiva 13718. Dicha comisión fue la encargada de emitir una serie de recomendaciones que, a corto y a largo plazo, fortalecieran la seguridad cibernética del país en el sector público y privado. Resulta útil destacar que la CENC fue encabezada por doce individuos pertenecientes al sector académico, industrial, militar y gubernamental. En diciembre de 2016 dicha comisión logró su objetivo al publicar el informe sobre el crecimiento y aseguramiento de la economía digital, en el que se enlistan seis urgencias prioritarias en cuanto a seguridad cibernética nacional se refiere. Dichas urgencias se describen en los párrafos subsecuentes.

La primera urgencia nace de la vulnerabilidad que representa la protección exclusiva de las infraestructuras críticas. En la década inicial de este milenio se optó por ubicar a *aquellas redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor*

en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas [3], etiquetarlas como Infraestructuras Críticas (CI, por sus siglas en inglés de *Critical Infrastructure*) y buscar asegurarlas con especial atención. La CENC expone que las interconexiones se han vuelto tan grandes y complejas que hoy en día, por asociación o interconexión, todas las infraestructuras deben ser consideradas como críticas. Es por eso que la CENC enuncia la primera urgencia como proteger, defender y asegurar la infraestructura de información y las redes digitales actuales. Explica que dicha urgencia que debe ser lograda con la cooperación mutua entre gobierno e industria, pero reconociendo que es el gobierno la única organización responsable ante la actividad maliciosa o perjudicial a gran escala en el entorno cibernético. Aunado a lo anterior, enlista cinco recomendaciones para atacar esta urgencia y varias acciones específicas para atender dichas recomendaciones. La idea general de las recomendaciones es instar a una cooperación comprometida entre el sector privado, incluyendo a las pequeñas y medianas empresas, y el gobierno para generar planes y marcos de referencia actualizados que brinden mejor seguridad, privacidad y mejores sistemas de identificación a las redes digitales nacionales y a sus infraestructuras, sean críticas o no.

La segunda urgencia presentada por la CENC consiente en innovar y acelerar la inversión para la seguridad y el crecimiento de las redes digitales y la economía digital. Esta urgencia nace de la rapidez con la que se ha introducido el IoT en los diversos sectores de la sociedad, desde la salud hasta el entretenimiento, y de los descuidos en los que han caído fabricantes y usuarios de IoT en cuestión de seguridad. Dichos descuidos y vulnerabilidades hacen de los usuarios responsables de la seguridad cibernética mucho más de lo que ya lo eran. La gravedad de los daños causados por ataques a gran escala que involucren IoT hace de este hito una urgencia que debe ser atacada desde diversos ángulos. Por ejemplo, el CENC recomienda la pronta unión de fuerzas entre gobierno y sector privado para mejorar la seguridad del internet de las cosas a través de la prioritaria introducción del tema a las agendas de investigación y desarrollo.

La innovación acelerada en el sector de las tecnologías de la información crea la necesidad de generar buenos hábitos cibernéticos en los usuarios de las mismas. De esta idea parta la tercera urgencia presentada por la CENC, que es preparar a los consumidores para prosperar en una era digital. El gran ecosistema digital en el que se vive, y en el que cada vez se sumerge más la humanidad requieren de esfuerzos significativos para emplear correctamente los productos y servicios que lo conforman. Ante esto la CENC recomienda que los líderes laborales de las TIC trabajen íntimamente con la sociedad civil y la Comisión Federal de Comercio con el fin de mantener informados los consumidores sobre las medidas necesarias para el buen uso de sus productos y servicios. Por otra parte, señala el deber del gobierno de establecer, fortalecer y ampliar las inversiones investigaciones para mejorar la seguridad cibernética en los productos y servicios consumidos con regularidad.

La siguiente urgencia es acerca de desarrollar fuerza de trabajo eficiente que se encargue de la seguridad cibernética, pues se estima que de 2015 a 2020 se necesitarán aproximadamente 1.5 millones de profesionales en seguridad cibernética nuevos. Ante este reto se recomienda que el gobierno trabaje en conjunto con la industria para abordar proactivamente las deficiencias de la mano de obra y promueva la

superación en este sector, mientras se invierte en soluciones innovadoras como el aprendizaje a temprana edad, la automatización e incluso la inteligencia artificial, soluciones que redistribuirán la fuerza laboral requerida.

La quinta urgencia que señala la CENC sugiere que, dado que el gobierno mismo es un gran consumidor de los servicios de internet y que; a través de sus diversas instituciones, tiene en su poder considerables datos personales, información confidencial, y demás activos valiosos, es necesario que el gobierno mismo tome medidas para ser líder en seguridad cibernética y tener la capacidad de asegurar un entorno cibernético fiable. Es por lo anterior que la urgencia se resume en un mejor equipo de gobierno que funcione de manera efectiva y segura en la era digital. Las recomendaciones pertinentes para entender dicha urgencia incluyen la consolidación de las operaciones básicas gubernamentales en la red, la promoción y la pronta actualización del uso de las tecnologías de la información en las agencias federales, la transición de requerimientos de seguridad cibernética a sistemas empresariales de gestión de riesgos en las agencias federales, enlazar las responsabilidades de seguridad cibernética a la oficina ejecutiva del presiente, y mantener una evaluación constante en todos los niveles de gobierno sobre las capacidades para defenderse, responder y recuperarse ante cualquier incidente cibernético.

La última urgencia presentada por la CENC parte de la penetración global que tiene la economía estadounidense. A pesar de que cada nación es responsable de las regulaciones que emprende, es esta condición de economía global la que desemboca en la urgencia de asegurar una economía digital global abierta, justa, competitiva y segura. Para hacer frente a dicha urgencia se recomienda que la administración entrante anime y proponga cooperación entre la comunidad internacional proponiendo políticas, prácticas internacionales y acuerdos sobre la seguridad cibernética.

En el año 2013 se emitió la Orden Ejecutiva 13636 [4], la cual presenta lineamientos para prevenir y disipar los ciberataques y perturbaciones en las redes que soportan las funciones consideradas críticas e incluye estrategias para el mejoramiento en la prevención, detección y respuesta a los incidentes cibernéticos de tal forma que la información sobre los ataques pueda aprovecharse para la defensa ante los mismos. Dicha Orden Ejecutiva fue la pauta para desarrollar el marco de referencia de seguridad cibernética del Instituto Nacional de Normas y Tecnología, NIST (por sus siglas en inglés de *National Institute of Standards and Technology*). El marco de referencia desarrollado por el NIST es de carácter voluntario y tiene la intención de que las organizaciones que lo adopten puedan proteger sus infraestructuras críticas.

Por su parte la Comisión Federal de Comunicaciones (en adelante FCC, por sus siglas en inglés, *Federal Communications Commission*), ha reforzado sus esfuerzos a través del Consejo de la seguridad, fiabilidad e interoperabilidad de las telecomunicaciones (en adelante CSRIC), cuya misión es proporcionar recomendaciones a la FCC para asegurar, entre otras cuestiones, la seguridad y la fiabilidad de los sistemas de comunicaciones, incluidas las telecomunicaciones, los medios de transmisión y la seguridad pública.

En 2004, la sexta edición del Consejo de la fiabilidad e interoperabilidad de las redes (NRIC VI, por sus siglas en inglés), predecesor del CSRIC, presentó un conjunto de reportes donde, por primera vez en este consejo, se atacaban directamente temas como la seguridad nacional, seguridad física,

recomendaciones en seguridad cibernética y seguridad pública, entre otros. En el año de 2009 se organizó formalmente el CSRIC, que dedica dos años a realizar un conjunto de reportes finales [5] donde se definen las mejores prácticas aplicables en el tema asignado a cada grupo de trabajo. Desde entonces se ha dedicado por lo menos un grupo de trabajo en cada edición del CSRIC para reportar las mejores prácticas en la seguridad en las redes, seguridad cibernética, o temas afines. La cuarta y quinta edición, correspondientes a los periodos marzo 2013 a marzo 2015 y marzo 2015 a marzo 2017, respectivamente, han mantenido grupos de trabajo de significativa relevancia para el tema que aquí se aborda. La Tablas 2.1.1.1, 2.1.1.2, 2.1.1.3 y 2.1.1.4[13] presentan una descripción de las recomendaciones que se exponen en lo reportes finales de algunos de los grupos de trabajo de estas ediciones.

Tabla 2.1.1.1: Reporte final del grupo de trabajo #4: Gestión de riesgos de seguridad cibernética y mejores prácticas.

Reporte final del grupo de trabajo #4: Gestión de riesgos de seguridad cibernética y mejores prácticas.	**CSRIC IV**	**03/2015**
Descripción: La FCC dio a este grupo de trabajo la misión de generar mecanismos voluntarios que sean adoptados por los proveedores de servicios de telecomunicaciones y que sirvan de garantía ante FCC de que se están tomando las medidas necesarias para gestionar los riesgos de seguridad cibernética a lo largo de la industria. Por lo tanto, este informa también sirve de guía para aquellos proveedores de telecomunicaciones que quieran adoptar el marco de referencia voluntario del NIST. Para lograr recomendaciones integrales, el cuarto grupo de trabajo se enfocó en áreas específicas de los proveedores de telecomunicaciones, incluyendo a los servicios de radiodifusión, cable, satélite, inalámbricos y de línea fija		
Recomendaciones: En primer lugar, desglosa los mecanismos voluntarios que pueden ser adoptados como medio para lograr los fines ya explicados. En dichos mecanismos resaltan tres por ser su primera aparición, que son: - Reuniones confidenciales con agendas específicas entre la FCC y las diferentes empresas; - La adición de un nuevo punto en los informes anuales del sector de las comunicaciones donde se destaquen los riesgos de seguridad cibernética hacia las infraestructuras críticas básicas; y - La participación activa en el programa C^3 (conversando, conectando y coordinando) del Departamento de Seguridad Nacional Con respecto a la guía para que las empresas adapten de manera individual el marco de referencia de seguridad cibernética del NIST el reporte final se enfatiza en la idea de que la seguridad cibernética no puede ser tratada como una simple categoría de la administración de la red, sino		

[13] La Tablas 2.1.1.1, 2.1.1.2, 2.1.1.3 y 2.1.1.4 son de creación propia.

que es necesario entender a la seguridad cibernética como parte de la gestión de la empresa. De tal forma que se sugiere un proceso de gobernanza de los riesgos que incluya:

- Identificar los riesgos potenciales y una variedad de soluciones a dichos riesgos;
- Conceder independencia y autonomía a las actividades de gestión de riesgos;
- Garantizar la transparencia en la toma de decisiones y la implementación de procesos de gestión de riesgos; y
- Adaptar y evaluar continuamente metas y objetivos en la gestión de riesgos.

Por último, hace un llamo a recordar que los avances en el entorno cibernético implican la necesidad de avanzar en la gestión de los riesgos en la red, por lo que el atender estas medidas debe de venir acompañado de un esfuerzo continuo de adaptarse a las nuevas amenazas.

Tabla 2.1.1.2: Reporte final del grupo de trabajo #5: Compartición de información de seguridad cibernética

Reporte final del grupo de trabajo #5: Compartición de información de seguridad cibernética	**CSRIC V**	**03/2017**
Descripción: El objetivo que la FCC le dio al grupo de estudio en la quinta edición del CSRIC fue el de emitir recomendaciones con el fin de ampliar y fortalecer la compartición de información de seguridad cibernética entre compañías en el sector de las telecomunicaciones.		
Recomendaciones: Las recomendaciones que se presentan en el reporte final se enlistan a continuación: - La FCC debe reconocer los potenciales riesgos cibernéticos implicados en la compartición de información de seguridad cibernética entre la industria y el gobierno, así como reconocer que es el Departamento de Seguridad Nacional (en adelante DHS por sus siglas en inglés de *Department of Homeland Security*) quien lidera esta cuestión y debe permanecer así. Por lo que se recomienda a la FCC a adaptarse a las medidas emitidas por el DHS y no caer en una sobre regulación; - La industria debe mantener sus esfuerzos para implementar, ampliar y determinar si son apropiados los protocolos de intercambio de información cibernética STIX / TAXII (expresión de información de amenazas estructuradas e intercambio automatizado y confiable de información de indicadores, del *inglés Structured Threat Information Expression* y *Trusted Automated eXchange of Indicator Information*, respectivamente). También insta a la industria a usar el protocolo de compartición automatizada de indicadores, AIS (del inglés *Automated Indicator Sharing*) del DHS; - La industria debe desarrollar un sitio web privado en el que las entidades gubernamentales, los socios de la industria y los representantes de las pequeñas y medianas empresas puedan acceder a recursos de seguridad cibernética;		

- Se deberá continuar con la cooperación entre gobierno e industria por educar en estos tópicos, sin descuidar las necesidades de las pequeñas y medianas empresas, y - Continuar alentando a la compartición de información de seguridad cibernética tomando las precauciones necesarias.

Tabla 2.1.1.3: Reporte final del grupo de trabajo #7: Desarrollo de fuerza de trabajo en seguridad cibernética. Recomendaciones de las mejores practicas

Reporte final del grupo de trabajo #7: Desarrollo de fuerza de trabajo en seguridad cibernética. Recomendaciones de las mejores practicas	**CSRIC V**	**03/2017**
Descripción: El gran incremento en cantidad, sofisticación y profundidad de los ataques cibernéticos de nuestra generan la necesidad imperiosa de desarrollar profesionales de la seguridad cibernética. El grupo de trabajo del quinto CSRIC fue encargado con la misión de recomendar a la FCC las acciones que se deben emprender para mejorar la seguridad de las comunicaciones de las infraestructuras críticas, a través del reclutamiento, entrenamiento, retención y movilidad laboral de profesionales de la seguridad cibernética. Para lograr su objetivo este grupo de trabajo aprovechó el trabajo existente en esta área, en especial del Marco Nacional de Fuerza Laboral de Seguridad Cibernética, NCWF (por sus siglas en inglés de *National Cybersecurity Workforce Framework*) y la Iniciativa Nacional para la Educación en Seguridad Cibernética, NICE (por sus siglas en inglés de *National Initiative for Cybersecurity Education*).		
Recomendaciones: El reporte final incluye un total de nueve recomendaciones concisas, las cuales se destacan a continuación. - La FCC debe alentar procesos para que la industria de las comunicaciones apoye en la actualización del NCWF; - Convencer de los beneficios que traería a la industria de las comunicaciones integrar programas educativos para estudiar y concientizar sobre aspectos de ciberseguridad en la educación primaria y secundaria; - La FCC debe alentar en la industria de las comunicaciones el desarrollo de programas que involucren acuerdos del sector académico y laboral; - La FCC debe procurar que la industria desarrolle o amplifique becas y programas de servicio en la industria; - La FCC debe comprometerse con los profesionales en seguridad cibernética de la industria de las comunicaciones a ayudar a formar a la próxima generación de profesionales; - La FCC debe de procurar que la industria de las comunicaciones participe en la elaboración del plan de estudios de la educación en seguridad cibernética;		

- La FCC deberá colaborar con la industria de las comunicaciones, las entidades de seguridad pública y el programa federal *GenCyber* para desarrollar un programa de educación en seguridad cibernética a distancia para las entidades de seguridad pública de comunicados rurales; - La industria de las comunicaciones debe de apoyar programas de desarrollo de habilidades de seguridad cibernética para personas con discapacidades, y - Los expertos en seguridad cibernética de la industria de las comunicaciones deben de unirse a los grupos de trabajo de la Iniciativa Nacional para la Educación en Seguridad Cibernética

Tabla 2.1.1.4: Reporte final del grupo de trabajo #9: Mejores práctica en seguridad de WiFi

Reporte final del grupo de trabajo #9: Mejores práctica en seguridad de WiFi	**CSRIC V**	**02/2017**
Descripción: El noveno grupo de trabajo del CSRIC V fue encomendado con la misión de publicar las mejores prácticas en cuestión de seguridad de WiFi. Ante esto se emitieron recomendaciones basadas en el análisis de las amenazas a la seguridad de WiFi y que son complementarias a las recomendaciones emitidas por el grupo de trabajo 2a del CSRIC y las emitidas por la empresa Cisco.		
Recomendaciones: El reporte final complementa las mejores prácticas con tres recomendaciones principales, las cuales son: - Que la FCC resuelva las cuestiones políticas y legales respecto a la capacidad de los clientes de empresas u operadores de red de usar la *des autenticación*[14] para proteger a los usuarios de WiFi de ataques cibernéticos legítimos; - Que los proveedores de redes inalámbricas y/o redes empresariales implementen redes con autenticación utilizando la recomendación UIT-T X.509 o tarjetas SIM que incluya también un método más robusto método de registro para clientes a corto plazo, y - Por último, recomienda que se desarrollen los métodos y las tecnologías necesarias que permitan a los clientes, durante su registro para usar una red inalámbrica, ser capaces de obtener llaves de autenticación específicas en sus dispositivos. Esto con la intención de proteger a los clientes de problemas de confianza entre terceros.		

De las recomendaciones presentadas en las tablas anteriores se ha mencionado el papel fundamental que juega el DHS en la seguridad cibernética de los Estados Unidos, dichas sospechas no son un error. El DHS comparte la responsabilidad de la seguridad cibernética con otras organizaciones gubernamentales como

[14] El protocolo de WiFi IEEE 802.11 contiene el uso de una trama de des autenticación. Esta se envía con la intención de terminar la conexión entre estaciones cuando sea necesario.

la Oficina Federal de Investigación (FBI, por sus siglas en inglés de *Federal Bureau of Investigations*) y el Departamento de Justicia, entre otros. Sin embargo, es el DHS quien tiene la responsabilidad mayor en este ámbito. A través de sus diferentes direcciones, el DHS opera los Equipos de Respuesta ante Emergencias Cibernéticas (en adelante CERT, por sus siglas en inglés de *Computer Emergency Response Team*) de los Estados Unidos (US-CERT) y en los Sistemas de Control Industrial (ISC-CERT). Como su nombre o indica, los CERT responden ante amenazas a la seguridad cibernética del país. Cabe mencionar que, dada la interconexión e interoperabilidad global del internet, para cumplir esa labor es necesario el intercambio de información constante con los CERT de otros países.

Otro esfuerzo que el gobierno estadounidense hace para enfrentar los retos de seguridad cibernética es la Asociación Nacional de Seguridad Nacional, NIAP (por sus siglas en inglés de *National Information Assurance Partnership)*. La NIAP es operada por la Agencia de Seguridad nacional, y es la asociación responsable de la implementación y evaluación de los Criterios Comunes (ISO/IEC 15408) en los Estados Unidos. Esta responsabilidad es ejercida a través del órgano de validación del Sistema de Evaluación y Validación de los Criterios Comunes, CCEVS (por sus siglas en inglés de *Common Criteria Evaluation and Validation Scheme*). También es importante destacar que, junto con el NIST, la NIAP es responsable de la acreditación de los laboratorios de prueba de los criterios comunes.

Se pueden encontrar políticas públicas que hagan frente a las amenazas del entorno cibernético, por ejemplo, la Orden Ejecutiva 13010 “Protección de la Infraestructura Crítica” (julio de 1996). Desde entonces las administraciones correspondientes se han preocupado por la emisión de estrategias y planes nacionales, órdenes ejecutivas, formación de comisiones y marcos de referencia. Comprender que el manejo constante de la seguridad cibernética en las políticas públicas del país ha permitido a los Estados Unidos posicionarse en el entorno cibernético como una nación con resistencia a las amenazas del mismo será útil en capítulos.

Con respecto al ámbito legal los esfuerzos del congreso estadounidense por fortalecer la seguridad cibernética se remontan al año de 1984 con la publicación de la ley pública 98-473, “Ley de dispositivos de acceso falsificado y abuso y fraude computacional, 1984” en la que se decreta ilegal el acceso a redes de computadoras de manera no autorizada. Estos esfuerzos han continuado hasta nuestros días. La Tabla 2.1.1.5 muestra un compendio de las leyes en materia de seguridad cibernética promulgadas desde 2010 a la fecha y presenta un pequeño párrafo descriptivo de las mismas.

Tabla 2.1.1.5: Marco legal aplicable a la seguridad cibernética en E.E.U.U[15]

Fecha	Ley	Descripción
18 de diciembre de 2014	Ley Pública 113-246 "Ley de evaluación de la fuerza de trabajo de seguridad cibernética."	Esta ley exige evaluaciones regulares a la fuerza de trabajo de seguridad cibernética del Departamento de Seguridad Nacional
18 de diciembre de 2014	Ley Pública 113-274 "Ley de mejora de la seguridad cibernética."	Alienta a los sectores público y privado a trabajar juntos para mejorar la seguridad cibernética en términos de investigación y desarrollo, preparación de la fuerza de trabajo y conciencia pública.
18 de diciembre de 2014	Ley Pública 113-282 "Ley de protección de la seguridad cibernética nacional."	Esta ley sirvió para organizar las funciones del centro nacional de seguridad cibernética e integración de las comunicaciones, NCCIC (siglas del inglés *National Cybersecurity and Communications Integration Center*).
18 de diciembre de 2014	Ley Pública 113-283 "Ley de modernización de la información federal de seguridad."	Esta ley modifica a su homónima predecesora del año 2002 para instar a la revisión de incidentes de seguridad cibernética exponiendo los requerimientos para las agencias federales de tal forma que se agilicen los informes de seguridad cibernética.
19 de diciembre de 2015	Ley Pública 113-291 "Ley de autorización de la defensa nacional para el año fiscal 2015."	El subtítulo D del título octavo de esta ley señala cambios en las prácticas federales en cuestión de las tecnologías de la información. Dichos cambios tiene implicaciones en la seguridad cibernética, específicamente en la consolidación de centros de datos federales.
18 de diciembre de 2015	Ley Pública 114-113 "Ley de seguridad cibernética."	Esta le contiene, entre otros puntos, el decreto de compartición de información de seguridad cibernética, CISA (por sus siglas en inglés de *Cybersecurity Information Sharing Act*). CISA fortalece la compartición de información de amenazas a la seguridad cibernética entre organizaciones del sector público y privado.

[15] La Tabla 2.1.1.5 es de creación propia

Una práctica destacable de las instituciones norteamericanas es la promoción de una cultura cibernética en sociedad. En este ámbito se han promovido varios esfuerzos como la publicación de guías [6] por parte de la FCC, la disposición de potárteles de internet con todo tipo de plataformas interactivas y materiales audiovisuales que promuevan los buenos hábitos que deben manejar los usuarios de internet. Ejemplo de estos portales son el sitio *Staysafeonline.org*[16] y el blog de información del consumidor[17], administrados por la Alianza Nacional de Seguridad Cibernética y la Comisión Federal de Comercio, respectivamente.

La Alianza Nacional de Seguridad Cibernética ha aportado bastante a la concientización de la población en los hitos de la seguridad cibernética. El Mes de la Concienciación sobre la Seguridad Nacional es una campaña que organiza dicha alianza todo lo años desde 2004, y tiene por objetivo la promoción de una cultura de seguridad cibernética en el trabajo y el uso seguro de dispositivos conectados a internet, así como servir de inspiración a las próximas generaciones para que opten desarrollarse como profesionales de la ciberseguridad. Asimismo, puso en marcha en octubre de 2010 la campaña *Stop. Think. Connect* (Para. Piensa. Conéctate) que busca alentar a los usuarios de internet a ser más atentos acerca de las prácticas seguras del uso del internet. En el sitio web de la campaña se puede acceder a varias publicaciones sobre estos temas cuya presentación se encuentra en inglés, español, portugués (brasileño), japonés, ruso y francés (canadiense).

En síntesis, Estados Unidos es un referente en materia de seguridad cibernética por su estrecha colaboración entre el sector púbico y el privado, la cantidad de instituciones a las que el gobierno ha hecho partícipes de la seguridad cibernética, la inclusión que se le ha dado al tema en las agendas presidenciales de las administraciones recientes, los esfuerzos del congreso estadounidense por mantenerse a la vanguardia en el terreno legal , la importancia que se la ha brindado a la educación de los usuarios de internet en cuanto a los hábitos necesarios para mantenerse seguro en la red y la previsión de las necesidades futuras, como la fuerza de trabajo que será necesaria próximamente.

República de Estonia

La República de Estonia figura como uno de los referentes en materia de seguridad cibernética. Diversos factores de su historia nacional son los que han derivado en este hecho.

Es importante comprender que el avance en seguridad cibernética que presenta la República de Estonia se debe, en principio, a la gran penetración de internet y las telecomunicaciones que presenta. Para ejemplificar este hecho se pueden mencionar , por ejemplo, que apenas un año después de lograr su independencia se logra el registro del dominio nacional ".ee", que para 1996 ya existiera un proyecto nacional con el fin de que todas las escuelas de Estonia tuvieran computadoras y acceso a internet, o que durante la primera década del siglo XXI se implementaran servicios en línea como la declaración de impuestos, los servicios policiacos, las solicitudes de información a dependencias gubernamentales e,

[16] Sitio web: https://staysafeonline.org/blog/
[17] Sitio web: https://www.consumer.ftc.gov/blog

inclusive, el voto. Sin embargo, las defensas cibernéticas de esa nación no estaban a la altura de los demás servicios. Este país conocería el lado oscuro del entono cibernético en una oleada de ataques cibernéticos sin precedentes.

La amenaza a su sociedad digital llegó de diversas formas, sin duda la más destacable fue durante los ataques cibernéticos que enfrentaron en abril del 2007, también conocidos como los ataques del Solado de Broce. La estatua del soldado de bronce fue instalada por las autoridades Soviéticas en 1947 con el nombre original de "Monumento para los liberadores de Tallin". Sin embargo, en 2007 el gobierno de Estonia decidió mudar la estatua del centro de la capital a un cementerio a las afueras de la misma. Este acto provocó una serie de protestas y jornadas de ataques cibernéticos que dejaron paralizado al país. Principalmente los servicios bancarios, los medios de comunicación y las organizaciones gubernamentales colapsaron debido a un ataque masivo de denegación de servicio distribuido (*DDoS*), mensajes basura (*spam*) y peticiones de respuesta (*ping*). El 19 de mayo de 2007 los ataques cesaron, dejando a su paso una huella de una guerra cibernética propiciada por un agresor sin rostro. A pesar de las declaraciones del Ministro de Relaciones Exteriores Estonio culparon al *Kremlin* (parlamento ruso) por los ataques cometidos, no fue posible identificar a un claro responsable, pues la única evidencia es que las direcciones *IP* de los ataques eran rusas [7].

Los ataques del 2007 no son el único factor que han obligado a Estonia a blindar su seguridad cibernética. Ser un blanco constante de intentos robos y fraudes cibernéticos por su proximidad con centros de crímenes cibernéticos de Europa del este, los flujos de datos transfronterizos que corren por sus redes, y otros factores, han obligado a formar una sinergia entre el sector privado y el gobierno para generar medidas eficientes en este tema.

Estas amenazas y ataques han contribuido para que Estonia se vuelva un digno representante de las mejores iniciativas en seguridad cibernética. Estonia es reconocido por esto internacionalmente.

La Organización del Tratado del Atlántico Norte, mantiene la sede del Centro de Excelencia para la Ciberdefensa Cooperativa (CCD COE, por sus siglas en inglés de *Cooperative Cyber Defence Centre of Excellence*) en este país desde 2008. Tiene como objetivo la formación de profesionales de la seguridad cibernética para los países miembros.

Para construir las capacidades de seguridad cibernética que goza hoy la Republica de Estonia, fue necesario que se desarrollaran una serie de estrategias y programas que formaban parte de una política pública de seguridad cibernética. Como se puede suponer, la primera oleada de iniciativas vino después de los ataques del 2007. Estas iniciativas se vieron sintetizadas en la primera estrategia nacional de seguridad cibernética, publicada en 2008 por el Ministerio de Defensa.

En la estrategia nacional del 2008 se trazaron como metas generales el desarrollo e implementación de medidas de seguridad, el incremento de las capacidades de aseguramiento de información, el desarrollo de marcos legales de seguridad cibernética, la promoción de la cooperación internacional y producir una sensibilización sobre la seguridad cibernética en la población.

Las primeras medidas emprendidas fueron organizacionales, por ejemplo, la creación del Consejo de Seguridad Cibernética en 2009. A este consejo se le confió la tarea de supervisar el cumplimiento de la estrategia nacional y promover la cooperación entre los demás organismos participes de la estrategia. Por parte, a la Autoridad del Sistema de Información de Estonia (RIA, por sus siglas del estonio *Riigi Infosüsteemi Amet*) se le dotó de mayores recursos económicos y poderes legales con el fin de agilizar su participación en la protección de las redes públicas. Siguiendo con estos cambios, se puede mencionar la fusión de las unidades de delitos informáticos de la Dirección de la Policía y la Guardia de Fronteras en el 2012. La estrategia nacional también impulsó la labor de respuesta ante incidentes por parte de los CERT estonios, con el fin lograr una eficiente cooperación internacional, así como entre el sector público y privado.

Es muy importante resaltar que dentro de esta primera estrategia nacional ya se reconoce como imprescindible la cooperación entre todos los entes con intereses en la seguridad cibernética, esto incluye a las academias, la sociedad civil, la iniciativa privada y el gobierno. Esta cooperación resultó en programas como el que llevó a cabo el Departamento de Protección de Información de Infraestructuras Criticas, dependiente de la RIA, en el que se logó mapear la información de las infraestructuras criticas gracias a la cooperación de los sectores público y privado. Otros ejemplos de esta cooperación serán mencionados más adelante.

En 2014 fue presentada la estrategia nacional en seguridad cibernética 2014-2017 [8]. Esta estrategia complementa las metas planteadas en su primera estrategia nacional haciendo frente a las nuevas amenazas y necesidades que no fueron previstas en la estrategia 2008-2013. Además de mantener muchos objetivos de la primera estrategia, esta versión comprende las siguientes metas:

- Revitalizar un enfoque integral y de todo el gobierno sobre la ciberseguridad;
- Crear un nivel muy alto de competencia y concienciación sobre la ciberseguridad en los organismos, las empresas y el público;
- Fortalecer la regulación para asegurar los sistemas de información, y
- Apoyar los esfuerzos para poner en marcha la cooperación internacional en ciberseguridad.

Estonia se ha nutrido en el terreno legal con un conjunto de leyes y reglamentos que le han permitido fortalecer la seguridad cibernética en este sector. Se podría decir que este esfuerzo comienza en 1996 cuando fue publicada la Ley de Protección de Datos Personales. En la Tabla 2.1.2.1 se pueden observar algunas de las medidas jurídicas que se han emprendido hasta el momento.

Tabla 2.1.2.1: Marco legal aplicable a la seguridad cibernética en la República de Estonia[18]

Año	Ley	Descripción
1996	Ley de Protección de Datos Personales	Promueve y protege el ejercicio de los derechos civiles en línea. Fue actualizada en 2010 para cumplir con las normas establecidas por la Unión Europea.
2004	Ley de comunicaciones electrónicas	Con la reforma en 2011 se autoriza a la Autoridad de vigilancia Técnica de Estonia a que solicite a los proveedores de servicios de TIC la realización de evaluaciones de seguridad en sus sistemas.
2007	La Ley de Secretos de Estado y de Información Confidencial de Estados Extranjeros	Solicita una evaluación anual de la seguridad de almacenamiento digital de documentos gubernamentales considerados como "secretos" o "muy secretos"
2013	Reglamento de Medidas de Seguridad de los Sistemas de Información de Servicios Vitales y Activos de Información Vinculados	Establece cómo debe ser la aplicación de la infraestructura crítica en el sector de las TIC. Obliga a los proveedores de servicios vitales a notificar de los incidentes cibernéticos y presentar informes a la RIA una vez que se restaure la integridad del sistema.

De forma complementara a lo presentado en la Tabla 2.1.3.1 es importante mencionar que a raíz de los acontecimientos del 2007 Estonia ha promovido reformas a su código penal para castigar de forma más severa la alteración, eliminación, daño o bloqueo de datos ejecutados de manera ilegal; la interferencia u obstaculización del funcionamiento de los sistemas informáticos; la difusión de herramientas maliciosas; la preparación de delitos informáticos y al uso ilegal de los sistemas informáticos.

Aunado a lo anterior, Estonia ha desarrollado su propia norma de seguridad de TI, la norma ISKE. Esta norma fue basada en la norma de seguridad *IT Grundschutz* (Protección Básica en las TI) desarrollada por Alemania. Como se puede suponer, tiene por objetivo lograr el equilibrio entre la confidencialidad, integridad y disponibilidad de datos. La norma clasifica en tres niveles los requisitos de seguridad de una organización (alto, medio y bajo) y es obligatoria para el sector público desde 2008.

Un aspecto que no puede pasar desapercibido al hablar de la seguridad cibernética en Estonia es la promoción de una cultura cibernética. Con una tasa de penetración de internet superior al 80% de la

[18] La Tabla 2.1.2.1 es de creación propia.

población, la búsqueda de una sociedad digital responsable no puede ser un tema secundario. Esta búsqueda se ha emprendido a través de la implementación de una serie de programas y medidas logradas gracias a la participación conjunta de los sectores público y privado.

Un ejemplo de esta participación conjunta son los programas de la fundación *Look@theWorld* que busca apoyar a la educación, ciencia y cultura a través del buen uso del internet y las TIC. Uno de sus proyectos en marchas es el "Proyecto Estonio de seguridad de dispositivos inteligentes: *NutiKaitse* 2017" [9], el cual busca que para 2017 el 70% de los usuarios de dispositivos inteligentes conozcan y mantengan los hábitos apropiados para el buen uso de sus dispositivos en cuanto a seguridad se refiere. Aunado a lo anterior, la fundación *Look@theWorld* mantiene el programa "Laboratorios inteligentes: Clubes extraescolares de las TIC" [10], programa en el que se busca aumentar el número de jóvenes que decidan estudiar de manera profesional los aspectos de la seguridad cibernética.

Los esfuerzos por educar a las próximas generaciones en estos hitos van más allá de lo mencionado anteriormente. Por un lado, se puede nombrar a La Fundación de Tecnologías de la Información para la Educación (HITSA, por sus siglas en estonio) [11], la cual ha creado programas educativos para acercar a las próximas generaciones a la defensa cibernética desde el nivel preescolar hasta la formación universitaria. Por otra parte, a partir de junio de 2015 se imparte en la Facultad de Tecnologías de la Información de Estonia la carrera de Ingeniería en Seguridad Cibernética

De lo expuesto anteriormente los que nos permiten afirmas que Estonia es un país que presenta gran experiencia en el capo de la defensa cibernética. En este sentido, es destacable el papel que han desempeñado sus estrategias nacionales, pues es gracias a ellas que se pudieron dar los cambios estructurales y organizacionales necesarios para fortalecer su seguridad cibernética. Es necesario reconocer la labor de sus aparatos legislativos en lo mencionado anteriormente. Por último, es ampliamente destacable colaboración entre la industria, el gobierno y los entes académicos en la formación de profesionales competentes en seguridad cibernética.

Israel

Israel es una nación con una evolucionada experiencia en ciberseguridad por diferentes factores. Comenzado por la gran actividad militar, política e industrial que depende del ciberespacio de Israel, esto deriva en una necesidad constante de generar las condiciones de una defensa integral en este sector. A raíz de lo anterior, se han emprendido las medidas necesarias que derivan en una repetida clasificación de Israel como uno de los mejores estados del mundo en materia de seguridad cibernética. Al respecto, Einat Meisel, experta en políticas de seguridad cibernética israelíes, opina que

> El auge militar y comercial de la seguridad cibernética en Israel […] toma en cuenta el hecho de que la seguridad ha sido una prioridad social, cultural y política a lo largo de la historia del país. También diría que la creación del Estado de Israel fue en sí misma un esfuerzo emprendedor. Y desde su creación, Israel ha tenido que estar continuamente vigilante para manejar enemigos y amenazas a

lo largo de sus fronteras y más allá. Proteger a Israel de las amenazas a todos los niveles, tanto en línea como fuera de ella, es uno de los principales objetivos de la estrategia gubernamental israelí. Como resultado, los militares invierten fuertemente en tecnologías informáticas, particularmente en las ramas de inteligencia. (Einat Meisel, 2017). [12]

Israel es la segunda nación con inversión privada en seguridad cibernética, únicamente debajo de Estados Unidos. Por otra parte, Israel es una nación que cuenta con capacidades ofensivas cibernéticas serias, prueba de esto es el lanzamiento del ya mencionado malware Stuxnet, lanzado contra Irán en conjunto con Estados Unidos. [13]

Ya se ha analizado la experiencia de los Estados Unidos en materia de seguridad cibernética. En 2014 la revista Forbes publicó el artículo "Lo que puede aprender Estados Unidos de Israel en seguridad cibernética", en donde se destacó la creación de una nueva autoridad de defensa cibernética para defender las redes de datos civiles de Israel. En dicho artículo Sugarman menciona la interactividad del gobierno israelí con sector privado, la academia y la sociedad civil en cuestiones de seguridad cibernética [14].

La estrategia que Israel ha seguido para posicionarse en la cima de las capacidades de seguridad cibernética de los estados se compone de diversos factores. Comenzando con que Israel fue uno de los primeros países que emprendió acciones respecto a la seguridad cibernética. En 1997 comenzaron las funciones de *Tehila*, un proyecto gubernamental que busca proteger las conexiones a internet de las oficinas gubernamentales, ofrecer un alojamiento seguro a los sitios web del gobierno, mejorar la interacción en la red entre el gobierno y los ciudadanos, entre otras. Desde 2011 *Tehlia* es operado por la Autoridad gubernamental de las TIC y se han logrado concretar una gran gama de servicios electrónicos por parte del gobierno como el pago de impuestos, información de cuidado de salud, búsqueda de empleo, planes de inversión, etcétera. Esto ha posicionado a Israel como un referente de gobierno electrónico.

Las medidas de Israel por fortalecer su seguridad cibernética fueron más alá de *Tehlia*. Uno de los primeros esfuerzos de Israel por fortalecer su seguridad cibernética se sitúa en el año 2002 con la Resolución No. B/84 del Comité Ministerial de Seguridad Nacional. Cuyo objetivo es la protección a los servicios digitales esenciales de Israel, es decir, a sus infraestructuras críticas. Derivada de esta resolución se encuentra la creación de una nueva agencia, la Autoridad Nacional de Seguridad de la Información (NISA, por sus siglas en inglés de *National Information Security Agency*). Esta autoridad fue dotada de las herramientas legales para regular los aspectos de seguridad de la información de dependencias gubernamentales, la corte, las prisiones, el sistema bancario, específicos sectores de la industria como el energético, hospitales, proveedores de servicios de comunicaciones y los aeropuertos.

En 2010, el primer ministro emprendió la creación de la Iniciativa Cibernética Nacional, con lo que la seguridad cibernética se volvió un explícito objetivo nacional. Seis meses de arduo trabajo institucional dieron lugar a la Resolución 3611 publicada en agosto de 2011, que consiste de siete recomendaciones clave, que son [16]:

- Mejorar la educación.

- Desarrollar una infraestructura de conocimiento.
- Crear un “escudo protector” en todo el Estado, y hacer frente a los problemas de privacidad.
- Desarrollar una capacidad nacional operativa en el ciberespacio.
- Mejorar la defensa combinando medidas legislativas técnicas y no técnicas y participando en iniciativas internacionales, especialmente con el Convenio sobre la Ciberdelincuencia del Consejo de Europa, para promover la defensa cibernética.
- Implantar tecnologías únicas, desarrolladas a nivel nacional, y fomentar las adquisiciones locales.
- Crear un organismo nacional para la política cibernética integral de Israel.

En consecuencia, de la Iniciativa Cibernética Nacional de 2010 se han generado planes nacionales de educación, lo que deriva en la dinámica formación y contratación de expertos cibernéticos. Aunado a esto, el país cuenta con centros de investigación y desarrollo de muchas de las principales multinacionales de alta tecnología.

La iniciativa mencionada también ordena la creación de la Oficina Cibernética Nacional (INCB, por sus siglas del inglés *Israel National Cyber Bureau*). En 2015, la INCB establece una política regulatoria de la formación de profesionales en ciberseguridad para asegurarse que tanto el sector privado como el gobierno y las demás organizaciones interesadas sean capaces de garantizar la formación de calidad de profesionales de la seguridad cibernética [15]. Otros cambios importantes a la estrategia israelí de ciberseguridad suscitados en 2015 fueron las Resoluciones 2443 y 2444. Las principales consecuencias de estas resoluciones fueron la creación de un segundo órgano nacional se ciberseguridad, la Autoridad Nacional de Seguridad Cibernética (NCSA, por sus siglas en inglés de *National Cyber Security Authority*) y la Dirección Nacional Cibernética, que está conformada por la INCB y la NCSA

La NCSA tiene la misión de defender el ciberespacio realizando, operando e implementando todos los esfuerzos defensivos operativos en el ciberespacio a nivel nacional, desde una perspectiva integral, con el propósito de proporcionar una respuesta completa y continua a los ciberataques. Entre otras tareas, se encarga de mantener el CERT de Israel, de aumentar la preparación y resiliencia del país, de desarrollar un sistema de información y de la promulgación de una doctrina cibernética nacional y de una ley de seguridad cibernética que modificará la legislación existente y añadirá una nueva reglamentación, según sea necesario. [17]

El CERT de Israel es operado por la NCSA. Tiene la responsabilidad gestionar los incidentes nacionales de ciberseguridad, el intercambio de inteligencia con socios de confianza del sector privado de Israel y con sus aliados en el extranjero, el desarrollo de mejores prácticas de seguridad cibernética, la promoción de la conciencia de seguridad cibernética y proporcionar un el punto de contacto en Israel de las amenazas e incidentes de seguridad cibernética de las corporaciones internacionales , empresas de seguridad cibernética y otros CERT.

Las estrategias nacionales de seguridad cibernética deben de reconocer que cabe la posibilidad de que las amenazas cibernéticas vengan desde dentro del propio país. Esto implica la necesidad de tomar medidas para evitar y sancionar las amenazas internas. En este sentido, Israel ha desarrollado un cuerpo de élite dentro de su cuerpo policiaco, la división *Lahav* 433. Esta división fue creada en 2012 con la intención de combatir el crimen cibernético, y ser un centro de desarrollo de habilidades digitales forenses.

Además de las resoluciones mencionadas, Israel cuenta con un conjunto de leyes que atienen específicamente a cuestiones de seguridad cibernética. El marco jurídico israelí en materia de seguridad cibernética se ha desarrollado más lentamente que en la República de Estonia o Estados Unidos, sin embargo, los esfuerzos realizados no son menospreciables. En la Tabla 2.1.3.1 se describen algunas de las leyes y convenios relevantes en materia de seguridad cibernética.

Tabla 2.1.3.1: Marco legal aplicable a la seguridad cibernética en Israel[19]

Año	Ley	Descripción
1981	Ley de Protección de la privacidad.	Considera la privacidad como un derecho humano fundamental garantizado por su marco constitucional. Esta ley viene acompañada de las Regulaciones como la 5741 y a 5777 que establecen los lineamientos de la protección a los datos personales.
1984	La Reforma a la Ley de Investigación y Desarrollo Industrial.	Se establecen canales de comunicación más estrechos entre el sector privado y el gobierno en materia de investigación y desarrollo de capacidades cibernéticas.
1995	Ley Informática	Establece, entre otras cosas, que cualquier cambio, distorsión o daño provocado a los programas informáticos, cualquier violación de los permisos de acceso en el uso de una computadora o cualquier presentación de información de pantalla falsa constituye un delito punible de hasta cinco años de prisión. En 2005 se reformó esta ley para obligar al estado a adoptar las medidas establecidas en el convenio de Budapest.
2009	Ley de bases de datos biométricos.	Se establecen las disposiciones para la inclusión segura de datos biométricos en documentos de identificación oficiales, como tarjetas de identificación y pasaportes, y se estableció la Autoridad de gestión de bases de datos

[19] La Tabla 2.1.3.1 es de Creación propia.

		biométricas. El período de transición a la documentación biométrica comenzó en 2013 y la ley se modificó a principios de 2017 con respecto, entre otras cosas, a la finalización del período de transición.

Con respecto a la regulación de Israel, las acciones se han centrado en la cooperación del gobierno con el sector privado, y la adopción de normas tecnológicas, principalmente dos de ellas, ISO27001 e ISO27002. Estas normas ofrecen certificaciones voluntarias ISO/IEC para la industria. Aunado a lo anterior, se cuenta con la Norma de Buenas Prácticas para la Seguridad del Foro de Seguridad de la Información (ISF), que busca reducir riesgos para empresas asociadas a sistemas de la información.

Israel es un estado que fomenta la cohesión entre el sector privado, publico, académico y militar. El servicio militar obligatorio crea un flujo constante de personas con experiencia cibernética. La unidad 8200 de las Fuerzas de Defensa de Israel (IDF, por sus siglas en inglés de *Israeli Defense Forces*) se dedica, entre otras cosas, al desarrollo de la seguridad cibernética, y encuentra sus principales talentos visitando escuelas secundarias para identificar potenciales candidatos a una edad temprana. Otro avance destacable de las IDF es la Estrategia IDF publicada en 2015. Este documento marca las pautas de la defensa cibernética de Israel en tiempos de guerra o situaciones de emergencia y busca asegurar el buen funcionamiento de las instituciones en tiempos de tensión.

La cooperación entre las IDF, el Ministerio de Educación y diversas ONG, ha dado frutos en forma de programas para estudiantes destacados de nivel secundaria, como el *Magshimim* (Estudiantes destacados) y el *Gvahim* (Alturas), que centran sus esfuerzos en la formación y el desarrollo de habilidades de seguridad cibernética.

Israel es uno de los pioneros en plantear la seguridad cibernética como una situación que debe de ser enfrentada por todos aquellos con interés en ella o que tengan intereses que puedan ser afectados por las vulnerabilidades cibernéticas. Cabe mencionar que esta cooperación entre los diversos sectores interesados no es exclusiva de la seguridad cibernética en esa nación. Un ejemplo de esto es la Iniciativa de Innovación *CyberSpark*[20] en Beersheva, que desde 2014 busca crear un ecosistema cibernético con la participación del gobierno, la academia, la industria y la sociedad civil.

La Iniciativa Cibernética Nacional de 2010 trajo consigo un mayor financiamiento y priorización de estudios universitarios en ciberseguridad por parte de Ministerio de Ciencia, Tecnología y Espacio. En 2014 la INCB estableció acuerdos para instaurar centros de excelencia cibernética en varias universidades del país, comenzando con la creación Centro Interdisciplinario de Investigación Cibernética en la Universidad de Tel Aviv en 2014.

[20] Sitio web: http://cyberspark.org.il/

Israel es una nación con amplias capacidades cibernéticas, no sólo en cuestiones de seguridad, sino también en producción de tecnología, defensa cibernética e integración de proyectos. Es preciso destacar el lugar que le da el estado de Israel a la investigación y desarrollo, aspectos fundamentales para mantenerse a la vanguardia de una cuestión. La ambición vanguardista de Israel en cuestiones digitales se puede ver reflejada en el hecho de que Israel decidió participar como estado fundador en la iniciativa de Reino Unido *Digital 5.*

Por otra parte, es importante resaltar el papel de las estrategias nacionales para el fortalecimiento de las capacidades de seguridad cibernética. Israel ha acertado en entender que la seguridad cibernética es una cuestión de múltiples intereses. Los esfuerzos plasmados en las iniciativas y planes nacionales demuestran un acto de responsabilidad gubernamental al ser él mismo quien convoca a los interesados y promueve una cohesión entre ellos. Israel es un ejemplo más de que el combate a las amenazas cibernéticas requiere un frente amplio con espacios en los que participen todos los interesados.

Por último, es importante resaltar el papel de las instituciones gubernamentales con objetivos específicos en el sector, con capacidades legales para lograr los mismos y con ánimos de cooperación con los demás sectores de la población. Sin duda alguna son las autoridades, instituciones y organismos gubernamentales israelíes responsables de un gran porcentaje del éxito obtenido en materia de seguridad cibernética. El dinamismo con el que cambian las tecnologías contemporáneas exige una gran capacidad de adaptación de los gobiernos a ese entorno tecnológico. La creación de nuevas dependencias con funciones específicas demuestra que Israel busca hacerle frente a ese dinamismo. Los resultados hablan por sí mismos, lo logra.

República de Corea

La República de Corea, mejor conocida como Corea del Sur, es un país que ha destacado rápidamente en el avance del progreso en las últimas décadas. En la primera mitad del siglo XX el panorama no fue muy favorable para la península coreana. Azolada por las consecuencias de 35 años de ocupación japonesa, una de las ocupaciones militares más crueles de la historia moderna, y las de una guerra de tres años con sus vecinos del norte, la República de Corea conoció la relativa paz hasta el año de 1953. A partir de entonces Corea del Sur ha emprendido la misión de consolidarse como uno de los países más sofisticados del mundo, estatus que sin duda ha logrado.

En 1953, al terminar la Guerra de Corea, la República de Corea era un país más pobre que la mayoría de los países Latinoamericanos. Ejemplo del progreso mencionando es que para 2014 la tasa de penetración de internet en la población de esa nación era del 84%. Hoy en día se considera la nación más conectada del mundo. [18]

Como se ha mencionado con anterioridad, la integración de los servicios digitales al día a día de los ciudadanos de una nación implica riesgos en ese entorno. Quizá el mayor reto que enfrenta Corea del Sur

en materia de seguridad cibernética son las tensiones bélicas que imperan entre esta nación y Corea del Norte [19].

La delicada situación entre Corea del Norte y la República de Corea ha orillado a esta última a mejorar constantemente su seguridad cibernética, pues se espera que, en caso de desatarse un conflicto bélico entre esas naciones, Corea del Norte lanzaría ataques cibernéticos contra las infraestructuras críticas, las redes de comando y las redes de control de Corea del Sur.

El desarrollo que ha presentado la República de Corea ante la seguridad cibernética comenzó en 1996 con el establecimiento del KrCERT/CC. Este organismo es el responsable de la detección temprana de incidentes en los sistemas y las redes no gubernamentales de Corea del Sur, y es el representante de la República de Corea ante el CERT del pacífico asiático. Hoy en día el KrCERT/CC es operado por la Agencia Coreana de Internet y Seguridad (KISA por sus siglas en inglés de *Korean Internet and Security Agency*).

También bajo el control de la KISA se encuentra el KNCERT Este centro de respuesta ante incidentes informáticos fue establecido en el año de 2004 y se encarga de coordinar las respuestas a incidentes cibernéticos que tengan lugar en las redes de uso gubernamental o de sus agencias y dependencias.

En 2011 fue presentado por la Comisión de Comunicaciones de Corea el Plan Maestro de Seguridad Cibernética Nacional, también conocido como Plan 11. Este plan fue desarrollado en conjunto con 15 organismos gubernamentales con el objetivo de tener la capacidad de responder a los ataques cibernéticos. Parte importante de la estrategia presentada en el plan maestro es obligar a los organismos gubernamentales y a las empresas privadas a cifrar los datos importantes y a hacer copias de estos, y a utilizar software especializado que evite ataques cibernéticos. El plan maestro se basa en tres pilares principales: (i) la inversión en capacidades de seguridad, (ii) el desarrollo de un marco jurídico y (iii) la cooperación internacional. El Plan 11 también se enfoca en la defensa cibernética y le atribuye poderes adicionales a la Agencia Nacional de Inteligencia [20].

Los esfuerzos por mejorar la seguridad de la información y las redes de Corea de Sur han abarcado más acciones que las expresadas en el Plan 11. Otro ejemplo que es conveniente citar es el nombramiento en abril del 2015 de un nuevo consejero presidencial enfocado en ciberseguridad. Este acto refleja el nivel de compromiso gubernamental con las cuestiones de seguridad cibernética en el país del este asiático [21].

La colaboración entre el sector público y privad también ha tenido lugar en la República de Corea, aunque en menor medida que en los casos anteriores. A pesar de que Corea del Sur no tiene claramente definido un convenio entre el sector público y privado, hay varios esfuerzos que merecen ser mencionados. Por ejemplo, el KrCERT/CC maneja el programa *Cyber Emergency Shelter* que proporciona un alojamiento de información en un servidor seguro a pequeñas y medianas empresas que han presentado incidentes en su seguridad cibernética.

Es importante destacar que los esfuerzos de cooperación entre el sector público y privado no son orquestados exclusivamente por el gobierno. Por ejemplo, en marzo de 2016 Microsoft Corea inauguró su centro se ciberseguridad. Se espera que este centro impulse una mayor colaboración entre los sectores

público y privado para luchar contra los crímenes cibernéticos, refuerce la cooperación con las empresas locales, las organizaciones gubernamentales y académicas en materia de seguridad cibernética y aumente la contribución del sector privado a proteger a los usuarios informáticos e informáticos coreanos [22].

La República de Corea cuenta con una serie de leyes y reglamentos en materia de protección de la información, incluidas leyes sobre secretos militares, telecomunicaciones, delitos informáticos, gobierno electrónico y protección de las infraestructuras de la información. Como se ve reflejado en la Tabla 2.1.4.1 la República de Corea ha mantenido una legislación constante respecto a temas que tengan que ver con las TIC

Tabla 2.1.4.1: Marco legal aplicable a la seguridad cibernética en la República de Corea.[21]

Año	Ley	Descripción
1995	Ley Marco de Promoción de la Informatización	En ella se establece que la seguridad de la información es una obligación gubernamental. Por otra parte, describe las obligaciones de la KISA y establece los requisitos de información para los proveedores de servicios de información y comunicaciones.
2002	Ley de Protección de la Infraestructura de Información y Comunicación	Constituye la base legislativa para la aplicación de la legislación sobre delitos cibernéticos en la República de Corea. Por otra parte, presenta la definición de protección de la infraestructura crítica
2003	Ley de Promoción del Uso de la Información y las Redes de Comunicación y de la Protección de la Información	Complementa la Ley de Protección de la Infraestructura de Información y Comunicación esclareciendo las obligaciones del gobierno electrónico con sus ciudadanos.
2006	La Ley de Prevención de la Divulgación y de Protección de la Tecnología Industrial	Dispone la suspensión y prohibición total de la exportación de tecnologías cuando se considere que comprometa la seguridad nacional de la República de Corea. Esta ley sufrió una reforma en el 2013 agregando métodos alternativos de solución de controversias.
2007	La Ley de Gobierno Electrónico	Declara los procedimientos de autenticación y los certificados aceptados para garantizar la seguridad en la provisión digital de servicios gubernamentales.

[21] La Tabla 2.1.4.1 es de creación propia.

2009	La Ley de Promoción de la Industria de la Tecnología de la Información y de las Comunicaciones	Crea las condiciones para un entorno propicio pala el sector de las TI e incluye una sección acerca de la seguridad de la información.
2009	Ley de la Firma Digital	Regula la distribución de certificados públicos.
2015	Ley sobre el Desarrollo de la Computación en la Nube y la Protección de los Usuarios	Establece que los proveedores de servicios en la nube están obligados a informar a los usuarios afectados de cualquier fuga de datos que se produzca. Además, la ley prohíbe explícitamente compartir información personal con proveedores de servicios y obliga a destruir tales registros de información tras la interrupción del servicio. También hace responsables a los proveedores de servicios de los daños causados a los usuarios en caso de intrusiones en la red

En busca de generar una cultura cibernética ejemplar, el gobierno de la República de Corea comparte a sus ciudadanos las mejores prácticas y envía alertas de amenazas específicas. Esta búsqueda se genera desde varios sectores como el militar y el académico.

La KISA ha mantenido esfuerzos constantes para fortalecer los conocimientos de la población surcoreana con respecto a la seguridad cibernética. Un esfuerzo significativo de la KISA es dirigir el Programa de Vacunación Cibernética, el cual busca identificar y contactar a los usuarios cuyos equipos estén siendo secuestrados por una *botnet,* además de brindar herramientas gratuitas para combatir y detectar el malware y evitar que los usuarios caigan en prácticas como el *phishing*[22].

Otra iniciativa del gobierno surcoreano para educar a la población en responsabilidades del uso de internet tuvo lugar en octubre de 2013 cuando la Comisión de Comunicaciones de Corea lanzó una campaña denominada Mantenimiento de la Seguridad en Internet, donde se valieron de pancartas y anuncios en una gran cantidad de medios para aumentar la concienciación en la población.

El fomento de la educación y formación de expertos en seguridad cibernética ha sido propiciado dentro el ejército de la República de Corea y el sector empresarial. Por otra parte, al tener una normativa

[22] El *phishing* es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima.

que publique a las grandes empresas a contratar a jefes de seguridad de los servicios de información ha conllevado a un a aumento en la demanda de expertos en cuestiones cibernéticas.

Por parte del sector militar, Corea del Sur aprovecha el carácter obligatorio de su servicio militar para impulsar la participación de programas educativos y de capacitación para formar expertos en cuestiones cibernéticas.

La formación de profesionales en el entorno cibernético es un tema al que se le ha brindado seriedad en esta nación. En 2008 el Ministerio de Educación creo el Centro de Formación en Ciberseguridad, organismo en el que participan instituciones educativas de nivel superior y que intercambia información con el KrCERT/CC. Por otra parte, la Universidad de Corea creó en 2011 el Departamento de Defensa Cibernética, el cual tiene como objetivo la formación de expertos cibernéticos especializados.

Las estrategias de seguridad cibernética emprendidas por la República de Corea sirven para poner en claro el impacto que llega a tener en la sociedad la voluntad política de transformar una realidad. Si bien, al poner en contraste lo logrado por Corea del Sur y los otros paséis analizados, se puede decir que este país aún tiene pasos que dar para lograr la excelencia en la seguridad cibernética, no son menospreciables los logros que han tenido en este sector.

Siendo objetivos, los logros de Corea del Sur en ciberseguridad son derivados de la definición de un plan nacional, la creación de dependencias gubernamentales con objetivos específicos en materia de seguridad cibernética, el desarrollo de un marco jurídico aplicable al sector de las TIC, la interacción de los diferentes sectores de la población en la formación de capacidades individuales y colectivas de aspectos cibernéticos y la promoción de una cultura digital.

La República de Corea ha logrado, en poco más de medio siglo, pasar de ser un país de economía similar a las naciones latinoamericanas a ser el país con mayor conexión a internet en el mundo. Hay diferentes motivos para explicar este fenómeno, y abordarlos no corresponde a esta investigación. Sin embargo, es preciso entender que el triunfo tecnológico de un país está ligado a las políticas públicas que se implementan en él. La naturaleza de múltiples intereses e interesados en la ciberseguridad obliga, por lógica, a la integración de diversas disciplinas para lograr buenos resultados. Es ahí donde radica el éxito de Corea del Sur, y de los demás países analizados anteriormente, en la seguridad cibernética.

Comparativa de las Mejores Prácticas

Realizando una comparativa de los tres casos analizados se pueden extraer las medidas que rigieron como factor común es sus progresos de seguridad cibernética.

La gran mayoría de las acciones emprendidas por los países analizados surgieron a partir de una estrategia nacional bajo las cuales de definieron las acciones concretas que se iban a emprender, la Ilustración 2.1.5.1 que a continuación se presenta, muestra una generalización de la metodología con la que se emprendieron acciones en este sector.

Ilustración 2.1.5.1: Metodología emprendida en cuestiones de seguridad cibernética por los países analizados[23]

Los países analizados determinaron los objetivos y responsabilidades propias de cada órgano actor en materia de seguridad cibernética. En algunos casos se podría observar que hay redundancia entre las responsabilidades y objetivos de los órganos implicados. Sin embargo, todos los países crearon nuevas entidades especializadas que sirvieron como punto de encuentro entre todos los implicados y permita una coordinación entre ellos.

Aunque no se puede notar un factor común en torno a la regulación para el sector privado, lo que es común en todos es la cooperación entre los diversos sectores de la población. En la mayoría de los casos esa propuesta de cooperación fue orquestada desde el gobierno y escaló rápidamente por los intereses de los demás que están en juego ante las amenazas cibernéticas. Los que se ve aquí es la aplicación de un modelo *multi-stakeholder*, el cual es un modelo necesario al considerar que la seguridad del entorno cibernético está más allá de las capacidades de cualquier sector de la población que lo intente tacar de forma individual.

[23] Creación propia.

Otro aspecto divergente entre los países analizados es su marco jurídico, sin embargo, la metodología es similar. El marco jurídico en torno a la seguridad cibernética se fue ensamblando por leyes individuales a medida que fueron necesarias, en lugar de presentar una ley general.

Todos los países analizados mostraron un gran interés en generar profesionales de la seguridad cibernética. Todos los países encontraron algún método para trabajar con las universidades, por lo menos, y generar programas más adecuados a las exigencias de la seguridad cibernética. Dos de ellos, Israel y la República de Corea, usaron también su servicio militar obligatorio para fortalecer este ámbito.

Por último, todos los países han participado activamente en la cooperación internacional y el intercambio de buenas prácticas en materia de seguridad cibernética, ya sea a través de su CERT principal o su participación en programas de formación de profesionales de la seguridad cibernética.

La Ilustración 2.1.5.2 muestra medidas relevantes emprendidas por los países estudiados e identifica cuáles de ellos incurrieron en esa práctica. En orden de izquierda a derecha aparecen las banderas de la República de Corea, Israel, República de Estonia y Estados Unidos.

Ilustración 2.1.5.2: Medidas relevantes comunes entre los países analizados[24]

[24] Creación propia.

Otros casos relevantes

Los casos presentados en esta sección exponen un análisis más sencillo que los presentados en la primera sección de este capítulo, pues no ahondan en cuestiones de estrategias políticas para fortalecer las capacidades de ciberseguridad de sus países o uniones. En este caso se presentan algunas de las regulaciones presentes en estos países o uniones que servirán para generar contraste con la situación mexicana y, en su caso, justificar las medidas que se proponen para el caso de México.

Unión Europea

Una de las instituciones que ha aportado mucho al desarrollo de la seguridad cibernética en Europa es la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA, por sus siglas en inglés de *European Union Agency for Network and Information Security*). Desde su establecimiento en 2004, la ENISA ha promovido cambios en la Unión Europea que se reflejen en un significativo avance en la seguridad de la información y las redes.

Esta agencia trabaja en estrecha colaboración con los Estados Miembros y el sector privado para ofrecer asesoramiento y soluciones en ciberseguridad. Esto incluye los ejercicios de seguridad cibernética, el desarrollo de estrategias nacionales de seguridad cibernética, la cooperación CERT de las naciones y la creación de capacidad. Por otro lado, también genera estudios sobre el uso seguro del alojamiento de información en la nube, tratando cuestiones de protección de datos, privacidad y tecnología de privacidad, y la identificación del panorama de las amenazas cibernéticas, entre otros temas. La ENISA también apoya el desarrollo y la aplicación de la política y el derecho de la Unión Europea en asuntos relacionados con la seguridad de las redes y la información.

Dada la misión de ENISA, las recomendaciones emitidas por este instituto están imitante relacionadas con las Directivas de la Unión Europea que promulga el Parlamento Europea y el Consejo de la Unión Europea, y que deberán de ser acatadas de forma obligatoria por los estados miembros de la misma. Entonces, podría decirse que las recomendaciones de este instituto son, en más de una ocasión, las bases de las Directivas regulatorias de la Unión Europea en materia de seguridad de las redes y la información.

La Directiva 2016/1148, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea, fue publicada el 6 de julio de 2016 y tiene el objetivo de lograr un elevado nivel común de seguridad de las redes y sistemas de información dentro de la Unión a fin de mejorar el funcionamiento del mercado interior. Puntualmente, esta Directiva [23]:

- Establece obligaciones para todos los Estados miembros de adoptar una estrategia nacional de seguridad de las redes y sistemas de información;

- Crea un Grupo de cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y desarrollar la confianza y seguridad entre ellos;
- Integra a los CERT de cada nación en una red con el fin de contribuir al desarrollo de la confianza y seguridad entre los Estados miembros y promover una cooperación operativa rápida y eficaz;
- Establece requisitos en materia de seguridad y notificación para los operadores de servicios esenciales y para los proveedores de servicios digitales, y
- Establece obligaciones para que los Estados miembros designen autoridades nacionales competentes, puntos de contacto únicos y los CERT con funciones relacionadas con la seguridad de las redes y sistemas de información.

Una de las consecuencias que trajo la Directiva 2016/1148 [24] fue el hecho de considerar a los mercados en línea, los servicios de búsqueda en internet y los servicios de computación en la nube como proveedores de servicios digitales (DPS, por sus siglas en inglés de *Digital Service Providers*). Ante este hecho, la ENISA ha publicado en diciembre de 2016 las Directrices Técnicas para la Implementación de Mínimas Medidas de Seguridad para los DSP.

La publicación de estas Directrices Técnicas incluye un total de 27 objetivos de seguridad a los que los DPS deberían de aspirar. Aunado a lo anterior, describe las medidas necesarias para atender cada objetivo en tres niveles diferentes (básico, intermedio y avanzado). Por último, mapea cada objetivo presentado a algunas normas industriales, marcos regulatorios o esquemas de verificación que incluyen el objetivo de seguridad en cuestión.

La protección a los datos personales ha sido tema relevante en las medidas de seguridad cibernética dentro de la Unión Europea. La Directiva 95/46 del Parlamento Europeo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, sirvió como pilar para poner en marcha diferentes instrumentos legislativos, entre los que figuran la Directiva 2002/58/CE (modificada en 2009) sobre la privacidad y las comunicaciones electrónicas, la Directiva 2006/24/CE sobre la conservación de datos (declarada inválida por el Tribunal de Justicia de la Unión Europea el 8 de abril de 2014 al constituir una injerencia de especial gravedad en la vida privada y la protección de datos) y el Reglamento (CE) No. 45/2001 relativo al tratamiento de datos personales por las instituciones y los organismos comunitarios.

El 25 de enero de 2012, la Comisión publicó un amplio paquete legislativo destinado a reformar la legislación de la Unión en materia de protección de datos. La reforma persigue salvaguardar los datos personales en todo el territorio de la Unión mediante una visión más vanguardista, aumentando el control de los datos por parte de los usuarios y reduciendo los costes para las empresas.

Los avances tecnológicos y la globalización han cambiado profundamente los métodos de recogida, acceso y uso de los datos. Además, los 28 Estados miembros han aplicado de manera distinta las normas de 1995. Por lo que, en diciembre de 2015, el Parlamento y el Consejo Europeo generaron un acuerdo sobre

las nuevas normas en materia de protección de datos. Las nuevas normas se publicaron en abril de 2016 y se aplicarán a partir de mayo de 2018, estas son:

- El Reglamento (UE) 2016/679 del Parlamento y del Consejo Europeo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, y
- La Directiva (UE) 2016/680 del Parlamento y del Consejo Europeo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

A estas normas se les conoce como el nuevo marco europeo de protección de datos personales, cuyo análisis se encontrará en los párrafos siguientes, sin embargo, antes de sumergirse en el contenido de las normas ya se puede observar un cambio significativo respecto del viejo régimen legal. La Unión Europea alcanza el objetivo de sus tratados mediante distintos actos legislativos, cuyo impacto en los estados miembros estará en función de la forma jurídica que tengan dichos actos. Al respecto, el acto legislativo de mayor peso en el Unión Europea es el de Reglamento, cuyo carácter es vinculante y debe adoptarse íntegramente en todos los países miembros de la Unión Europea. Por otra parte, cabe señalar que el las Directivas son actos legislativos en los cuales se establecen objetivos que todos los países de la Unión Europea deben cumplir, sin embargo, corresponde a cada país elaborar sus propias leyes sobre cómo alcanzar esos objetivos, por lo que se sitúan jerárquicamente por debajo de los Reglamentos de la misma. En ese sentido, el hecho de que la Directiva 95/46/CE haya evolucionado en un Reglamento muestra la seriedad con la que se ha abordado la protección de datos personales al interior de la Unión Europea.

Del Reglamento (UE) 2016/679[25] se puede destacar no sólo la seriedad regulatoria mencionada en el párrafo anterior, sino también la actitud vanguardista con la que defiende a los usuarios de internet. A continuación, se listan los puntos más destacables y vanguardistas, y después de explicarlos no será difícil entender por qué los estados miembros de la Unión Europea tienen poco más de dos años para lograr la implementación del Reglamento en comento en sus administraciones.

- Derechos y libertades fundamentales respecto a los datos personales: si bien el reglamento retoma y mejora los derechos fundamentales contenidos en la Directiva 95/46/CE (acceso, rectificación, limitación y oposición), se integran dos nuevos derechos fundamentales (derecho de supresión, también conocido como derecho al olvido y a la portabilidad de datos), ambas categorías se describen a continuación:
    - Derecho al acceso: el artículo 15 de dicho Reglamento establece que cualquier interesado tendrá derecho de recibir confirmación del responsable del tratamiento si en efecto está tratando sus datos personales y, en tal caso, el interesado tendrá derecho a conocer la naturaleza del tratamiento, así como información en general de dicho proceso;
    - Derecho de rectificación: de acuerdo a lo establecido en su artículo 16, el interesado tendrá derecho a solicitar la rectificación de los datos personales que sean inexactos;

- Derecho al olvido: contenido en su artículo 17, el derecho al olvido confiere poder al individuo para que sus datos sean olvidados si él así lo desea, o bien, si el responsable del tratamiento ha incurrido en ciertas faltas;
- Derecho a la limitación del tratamiento: el artículo 19 del Reglamento en cuestión establece que el interesado podrá solicitar al responsable del tratamiento limitar dicho tratamiento;
- Derecho de portabilidad de datos: según lo establecido en su artículo 20, cualquier interesado tendrá derecho a recibir los datos personales en posesión del respectivo responsable del tratamiento en un formato estructurado, de uso común y de lectura mecánica, y
- Derecho de oposición: Por último, su artículo 21 establece que el interesado tendrá derecho a oponerse en cualquier momento, a que sus datos personales sean objeto de un tratamiento, esto incluye la elaboración de perfiles con fines de mercadotecnia directa o cualquier otro.

- Alcance del Reglamento: como se comentó en párrafos anteriores, el Reglamento en cuestión le será aplicable íntegramente a todos los países miembros. Sin embargo, la evolución del alcance de la protección de datos personales va más allá de eso. Uno de los avances más significativos es que el reglamento será aplicable tanto para los responsables del tratamiento de datos que se encuentren al interior de Europa tanto como a aquellas empresas situadas fuera de la Unión Europea cuyas actividades impliquen el tratamiento de datos personales y realicen actividades al interior de la Unión Europea, esto será aplicable aun cuando no tengan presencia física dentro de la Unión Europea. Esto constituye una regulación sin precedentes, pues una de las mayores limitantes de la regulación y gobernanza del internet consiste en que muchas veces las empresas que ofrecen los contenidos y servicios de internet tienen situada prácticamente toda su infraestructura, e incluso su constitución como persona moral en otros países, lo que genera un vacío legal que hasta ahora, con este Reglamento, se está atendiendo.
- Designación de un Delegado de Protección de Datos (DPO, por las siglas en inglés de *Data Protection Officer*): La Sección 4 del Reglamento en cuestión establece que los responsables del tratamiento de datos personales deberán designar a un DPO para garantizar el cumplimiento de la nueva normativa. Asimismo, el dicha Sección establece que la designación del DPO deberá tomar en cuenta cualidades profesionales y conocimientos normativos en la materia, por lo que este punto viene a reforzar directamente a lo señalado en el párrafo anterior.
- Violaciones de seguridad: Se establece que las empresas deberán notificar a la autoridad de protección de datos correspondiente cualquier violación en un máximo de 72 horas desde que hubieran tenido constancia de la misma, siempre que constituya un riesgo para los derechos y libertades de los ciudadanos y, en caso de que se concrete el riesgo, deberán comunicarla al afectado.
- Creación del Consejo Europeo de Protección de Datos: El Reglamento en cuestión comprende la creación de un Consejo Europeo de Protección de Datos, que estará formado por los representantes de cada una de las respectivas autoridades de los países miembros y tendrá la capacidad de adoptar decisiones jurídicamente vinculantes.
- Sanciones: El Reglamento establece la imposición de sanciones administrativas, que deberán imponer las autoridades de protección de datos nacionales, y cuyo importe puede llegar a alcanzar los 20.000.000 euros o el 4% del volumen de negocio total anual global del ejercicio financiero anterior. Asimismo, el Capítulo IX del mismo, incluye un régimen sancionador completo.

Como se podría suponer, la Directiva (UE) 2016/680[26] está muy relacionada con lo establecido en el Reglamento analizado en los párrafos anteriores, incluso se podría decir que esta Directiva es la contraparte del Reglamento antes analizado, pues la Directiva sienta las obligaciones a las que estarán sujetas las autoridades de los Estados Miembros en lo relativo al tratamiento de satos personales, así como los lineamientos que dichas autoridades deberán seguir cuando hay intercambio de datos personales entre ellos, y las bases de la cooperación entre administraciones. A continuación, se listan aquellos puntos que se consideran importantes:

- La Directiva Establece las disposiciones generales de la Directiva, en donde se establece que el objetivo de la misma será a "establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales por parte de las autoridades competentes, con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública". Asimismo, se define que esta Directiva será aplicable a las autoridades competentes de los Estados Miembros;
- Se enumeran los principios que rigen el tratamiento de datos personales, conforme a los cuales los datos en cuestión deben ser exactos, adecuados, pertinentes y no excesivos, siendo obligación de los Estados Miembros adoptar todos los mecanismos que permitan garantizar un adecuado nivel de seguridad y confidencialidad, además de fijar unos plazos "*apropiados para la supresión de los datos personales o para una revisión periódica de la necesidad de conservación*" de los mismos;
- Los artículos 12-18 garantizan el ejercicio de los derechos reconocidos a los interesados, previendo las limitaciones que puedan establecer los Estados Miembros en los supuestos previstos en la Directiva;
- El Capítulo IV establece las obligaciones y medidas de seguridad a las que se deben apegar los responsables del tratamiento, entre ellas destaca la designación de un Delegado de Protección de Datos, figura que también está integrada en el reglamento;
- EL Capítulo V establece las pautas para la transferencia de datos personales a diferentes países de la Unión Europea, así como a organizaciones internacionales;
- La Directiva dedica su Capítulo VI a las Autoridades de Control Independientes, que serán las responsables de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta a la protección de sus datos personales. Cabe mencionar que dichas autoridades gozarán de independencia en el desempeño de sus funciones;
- Los artículos 50 y 51 de la Directiva se enfocan en las pautas que deberán seguir las autoridades de control de los países miembros relativas a la cooperación entre sí. Este punto es destacable pues facilita el intercambio directo de información entre las autoridades competentes, y
- Por último, la Directiva ofrece una serie de recursos que podrían usarse en caso de que algún interesado considere que el tratamiento de sus datos personales no es acorde a lo establecido en la misma directiva.

Por los puntos antes expuestos, se podría decir que, a través de dicha Directiva, el legislador europeo pretende agilizar la cooperación judicial y policial, facilitando la libre circulación y el intercambio

de datos personales entre los Estados Miembros. Lo anterior obedeciendo al derecho fundamental de personas físicas a que se protejan sus datos personales.

A pesar de que los Estados Miembros tienen hasta el 25 de mayo de 2018 para adaptarse al Reglamento (UE) 2016/679 y la Directiva (UE) 2016/680, algunas administraciones se han adelantado a esta fecha y ya han modificado su regulación para satisfacer las exigencias de las mismas. De forma explicativa, mas no limitativa, se pueden mencionar los casos de Francia y Alemania, quienes desde 2016 y 2017 publicaron leyes que se anticipan a la entrada en vigor del Reglamento y la Directiva en cuestión.

La República Francesa cuenta con un marco jurídico que considera la protección de datos personales desde el 6 de junio de 1978, cuando se publicó la Ley No 78-17 *Informatique Et Libertes* (informática y libertad) que, entre otras cosas, establece una autoridad reguladora independiente en materia de protección de datos personales, la CNIL, por sus siglas en francés de *Commission nationale de l'informatique et des libertés,* que , a su vez, funge como autoridad francesa en materia de protección de datos personales. Desde entonces, diversas reformas han contribuido a robustecer el marco legal aplicable a la protección de datos personales, por mencionar algunas, la Ley No 2004-801, de agosto de 2004, con la que se implementan las medidas establecidas en la Directiva 95/46/CE y, particularmente, la Ley No 2016-1321 del 7 de octubre de 2016 *pour une République numérique* (por una Republica digital), con la que Francia se anticipa a la entrada en vigor del Reglamento (UE) 2016/679 y la Directiva (UE) 2016/680.

Algo destacable de la Ley No 2016-1321 es que, en algunos puntos, esta es más exigente y vanguardista que lo establecido en el nuevo marco jurídico de la Unión Europea en la materia, por ejemplo:

- El artículo L.111-7-1 del Código francés de consumidores, reformado mediante esta Ley, establece que aquellas plataformas de internet que superen un umbral de número de conexiones tendrán obligaciones adicionales en cuestiones de transparencia, y
- El artículo L. 224-42-1 del Código francés de consumidores establece que, en cualquier caso, los consumidores tienen derecho a recuperar todos sus datos. Al apuntar a "todos" los datos, la Ley en cuestión va más allá del Reglamento antes analizado, que se limita a los datos personales. Es decir, la ley por una República digital amplía su alcance a los datos no personales de los consumidores (por ejemplo, cualquier archivo cargado por el consumidor y datos de uso asociados, como una lista de reproducción de música). [27]

Por otra parte, la República Federal de Alemania, es un país que, al igual que su vecino del este aquí mencionado, incorporó la protección de datos personales a su marco jurídico en la década de los 70. En 1970 fue aprobada la primera ley de protección de datos (*Datenschutz*), y en 1977, el Parlamento Federal Alemán aprueba *Bundesdatenschutzgesetz* (ley federal de protección de datos). Desde entonces, estas leyes impiden la transmisión de cualquier dato personal sin la autorización de la persona interesada. Asimismo, el 27 de abril de 2017 se aprobó una nueva *Bundesdatenschutzgesetz* (en adelante BDSG) [28], a través de la cual Alemania se adapta a las nuevas obligaciones derivadas del vigente marco jurídico europeo en materia de protección de datos personales. La BDSG no solo da cumplimiento a las exigencias marcadas por el Reglamento y la Directiva antes mencionadas, sino que impone sanciones y derechos que van más allá de lo ahí establecido, por ejemplo:

- La Sección 7 establece el derecho a ser compensado si un responsable del tratamiento de datos personales cae en un incumplimiento de las obligaciones establecidas por la normativa sobre protección de datos personales y, derivado de dicho incumplimiento, el interesado resulta dañado.
- La Sección 43 establece un régimen sancionador para aquellas conductas en las que el responsable del tratamiento incumpla en obligaciones que no están definidas originalmente en el Reglamento antes analizado, para las cuales se podrán imponer sanciones de hasta un máximo de 50.000 euros.

Si bien los avances de estos y otros países representan un avance hacia la implementación del marco jurídico europeo en materia de protección de datos personales, lo cierto es que aún queda mucho camino por recorrer, y lo más probable es que llegada la fecha límite de adaptación y la entrada en vigor del mismo, muchos responsables del tratamiento de datos personales sean susceptibles a sanciones por no cumplir lo ahí establecido. De hecho, según el diario el país, José Luis Zimmermann, director de la Asociación Española de Economía Digital (Adigital); Borja Adsuara, exdirector de Red.es y abogado experto en derecho digital y José Alberto Rodríguez, director global de Protección de Datos de la empresa de software en nube Cornerstone OnDemand, concuerdan en que la sociedad europea no está preparada para la implementación del Reglamento.[29] Si a esto se le suma que diversos aspectos del reglamento les serán aplicables a empresas extranjeras que brinden servicios en territorio europeo, el reto se complica aún más.

Reino Unido

Las medidas que se han tomado en Reino Unido en favor de la seguridad cibernética han sido, en gran medida, dependientes de los acuerdos establecidos en la Unión Europea. Como es bien sabido, el Reino Unido ha declarado su salida de la Unión Europea y se encuentra en negociaciones sobre los términos bajo los cuales efectuará dicho acto. En febrero de 2017 la Oficina del Primer Ministro presentó al Parlamento de esa nación el informe titulado La Salida del Reino Unido y las Nuevas Asociaciones con la Unión Europea, en el que se expresa que la cooperación de Reino Unido con la Unión Europea, y sus aliados en general, no disminuirá. Además, se buscará mantener un trabajo estrecho con sus aliados internacionales para generar capacidades que hagan frente a las amenazas cibernéticas y se buscará garantizar el fomento de un ciberespacio libre, abierto, pacífico y seguro.

En 2009 fue presentada por la Oficina del Primer Ministro al Parlamento la Estrategia de Ciberseguridad del Reino Unido, la cual es la primera en su clase. La Estrategia destaca la necesidad de que el gobierno, las organizaciones de todos los sectores, los socios internacionales y los ciudadanos trabajen juntos para cumplir objetivos de reducir los riesgos del entorno cibernético y aprovechar las oportunidades del mismo mejorando el conocimiento, las capacidades y la toma de decisiones con el fin de asegurar un entorno favorable en el ciberespacio.

Para abordar los desafíos de seguridad cibernética del Reino Unido, la Estrategia nacional puntualiza que el Gobierno deberá:

- Establecer un programa intergubernamental para abordar las áreas prioritarias persiguiendo los objetivos estratégicos de seguridad cibernética del Reino Unido, entre ellos:
    - Proporcionar fondos adicionales para el desarrollo de un futuro innovador en tecnologías para proteger las redes del Reino Unido;
    - Desarrollar y promover el crecimiento de habilidades específicas;
- Trabajar estrechamente con el sector público, la industria, los grupos de la sociedad civil y con sus socios internacionales;
- Establecer una Oficina de Seguridad Cibernética para proporcionar liderazgo y coherencia por parte del Gobierno, y
- Crear un Centro de Operaciones de Seguridad Cibernética para:
    - Vigilar activamente la salud del ciberespacio y coordinar la respuesta a los incidentes;
    - Permitir una mejor comprensión de los ataques contra las redes y usuarios del Reino Unido, y
    - Proporcionar mejor asesoramiento e información sobre los riesgos para las empresas y los ciudadanos.

Por otra parte, el órgano regulador de las comunicaciones en Reino Unido, Ofcom, emitió un documento clave con el fin de fortalecer aspectos muy puntuales de la seguridad cibernética, específicamente hablando, la seguridad de las redes.

En diciembre de 2013 fue publicada la Guía de Ofcom sobre Seguridad en las Redes [30]. El objetivo de este documento es brindar a los proveedores de comunicación información de alto nivel de cómo se aplicarán los requerimientos establecidos por la Unión Europea. Este documento abarca las siguientes áreas:

- Procedimientos de gestión de riesgos y medidas básicas de seguridad: con respecto a esta sección se establecen que los proveedores de comunicaciones deberán contar con sistemas de gestión de riesgos y mantenerse en conformidad con la familia de normas ISO27000, asegurarse de que en su organización se encurten expertos capaces de cumplir sus responsabilidades de seguridad, gestionar los riesgos que pueda generar la creciente práctica de *outsourcing* (contratación externa) y, en el caso de rentar bases de datos, verificar que sus arrendadores cumplan las medidas de seguridad necesarias;

- Información transparente para los consumidores: esta sección establece que se deben de emprender las medidas necesarias para mejorar los niveles de seguridad en los servicios que ofrecen y que se debe buscar que el servicio brindado este habilitado bajo cualquier circunstancia razonable;

- Medidas para proteger la interconexión de las redes: exige que los proveedores de comunicaciones cumplan con la norma NICC ND1643 (Normas Mínimas de Seguridad para la Interconexión de Proveedores de Comunicaciones) del Centro Nacional de Coordinación de Infraestructuras (NICC, por sus siglas en ingles de *National Infrastructure Coordinating Center*) [31];

- Medidas para mantener la disponibilidad de los servicios: se establece que los proveedores e comunicaciones deberán mostrar evidencia de que mantienen un alto nivel de disponibilidad del

servicio, y que deberán asegurarse que los usuarios de sus redes puedan acceder a los servicios de emergencia bajo cualquier circunstancia, y

- Reportes de los incidentes ocurridos: establece el proceso para reportar incidentes importantes. Incluye una plantilla de informes que describe el tipo de información qua reportar para cada incidente. Esto incluye reportar el número de clientes afectados y la duración del incidente.

Esta guía también destaca la regulación que, a la fecha de su publicación, ya se ejercía sobre los proveedores de comunicaciones. Los actos regulatorios que se mencionan abarcan los reportes anuales de incidentes de seguridad, reportes de la infraestructura, la compartición de información de incidentes de seguridad entre los proveedores de comunicaciones y la imposición de medidas de seguridad en los puntos de interconexión de las redes de los proveedores de comunicaciones.

A pesar de que Ofcom no ha publicado más regulaciones de seguridad cibernética a la fecha, ha declarado en su Plan Anual 2016-2017 [32] el deber de asegurarse que los diseños y la operación de las redes se alienen con las mejores prácticas en materia de seguridad, ofreciendo un guía para lograr esa comitiva. Por otra parte, tiene el deber de reportar a la Comisión Europea un recopilado de informes acerca de las fallas en la red. Esto con el fin de entender las causas y deducir los pasos a seguir para responder con el fin de minimizar los riesgos futuros.

Colombia

Al encontrarse en una situación con relativa similitud que México, Colombia figura como un caso interesante para los propósitos de este trabajo. En esta sección se expondrán los factores que han llevado a Colombia a obtener el estatus que le corresponde en este ámbito, y las medas que ha emprendido para mejorar su condición.

En el 2005, el Ministerio de Relaciones Exteriores creó un grupo de trabajo entre agencias para analizar y profundizar en los temas concernientes al ciberespacio. Posteriormente, el Ministerio de las Tecnologías de la información y la Comunicación, por medio de una consultoría, identificó las brechas y los vacíos de Colombia en materia de seguridad informática.

En el campo legal, Colombia ha realizado algunas mejoras a su situación de seguridad cibernética al reformar el Código Penal en 2009 mediante la Ley 1273 (Protección de la información y de los Datos). Con la reforma mencionada, Colombia ahora puede abordar los delitos cibernéticos, y por ello, estar en mayor sintonía con los estándares internacionales, específicamente, con el Convenio de Budapest.

Colombia es uno de los pocos países latinoamericanos que ha mantenido una estrategia nacional para la seguridad cibernética y defensa cibernética operando durante varios años. El Consejo Nacional de Política Económica y Social emitió en julio de 2011 los Lineamientos de Política para Ciberseguridad y Ciberdefensa (CONPES 3701), el cual presenta un detallado plan de acción que presenta las acciones necesarias, así como las fechas en que se realizarán, para fortalecer tras aspectos de la seguridad cibernética, los cuales son:

- Implementar la institucionalidad adecuada;
- Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en ciberseguridad y ciberdefensa, y
- Fortalecer la legislación y la cooperación internacional en materia de ciberseguridad y ciberdefensa.

En abril de 2016 fue publicada la Política Nacional de Seguridad Digital (CONAPES 3854), el cual puede ser considerado una actualización al plan nacional presentado en el documento CONAPES 3701. Lo cierto es que se trata de una estrategia nacional mucho más ambiciosa que la presentada en 2011, pues explica que

> El enfoque de la política de ciberseguridad y ciberdefensa, hasta el momento, se ha concentrado en contrarrestar el incremento de las amenazas cibernéticas bajo los objetivos de (i) defensa del país; y (ii) lucha contra el cibercrímen. Si bien esta política ha posicionado a Colombia como una de los líderes en la materia a nivel regional, ha dejado de lado la gestión del riesgo en el entorno digital. Enfoque esencial en un contexto en el que el incremento en el uso de las TIC para realizar actividades económicas y sociales, ha traído consigo nuevas y más sofisticadas formas de afectar el desarrollo normal de estas en el entorno digital. Hecho que demanda una mayor planificación, prevención, y atención por parte de los países. (CONAPES 3854, 2016)

A raíz de esta reflexión, Colombia buscó incluir en sus planes nacionales acciones que involucren activamente a todos los interesados en la seguridad digital, de tal manera que logre, como objetivo general, el fortalecer las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital.

Para lograr cumplir el objetivo general, el Plan Nacional de Seguridad Cibernética enlista los siguientes objetivos específicos:

- Establecer un marco institucional para la seguridad digital consistente con un enfoque de gestión de riesgos, que a su vez se compone de las siguientes acciones:
    - Establecer un marco institucional articulado que involucre a las múltiples partes interesadas para la implementación de la política nacional de seguridad digital, y
    - Implementar en el Gobierno nacional un modelo de gestión de riesgos de seguridad digital.
- Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital, lo cual implica:
    - Establecer mecanismos de participación activa y permanente de las múltiples partes interesadas en la gestión del riesgo de seguridad digital;
    - Adecuar el marco legal y regulatorio en torno a la dinámica de la economía digital y sus incertidumbres inherentes;
    - Identificar y abordar los posibles impactos negativos que otras políticas pueden generar sobre las actividades de las múltiples partes interesadas en el entorno digital o sobre la prosperidad económica y social;
    - Generar confianza en las múltiples partes interesadas en el uso del entorno digital, y

    - Promover en los diferentes niveles de formación comportamientos responsables en el entorno digital.
- Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y transnacional, con un enfoque de gestión de riesgos, como resultado de las siguientes acciones:
    - Fortalecer las instancias y entidades responsables de ciberseguridad;
    - Adecuar el marco jurídico sobre los delitos cibernéticos, cibercrímenes y fenómenos en el entorno digital;
    - Socializar y concientizar las tipologías de cibercrímen y ciberdelincuencia a las múltiples partes interesadas, y
    - Fortalecer las capacidades de los responsables de seguridad nacional en el ciberespacio y de la judicialización de delitos cibernéticos y cibercrímenes.
- Fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos, que se logrará a partir de:
    - Fortalecer las instancias y entidades responsables de la defensa nacional en el entorno digital;
    - Adecuar el marco jurídico para abordar la protección y defensa del entorno digital nacional;
    - Generar una estrategia de protección y defensa de la infraestructura crítica cibernética nacional;
    - Fortalecer el esquema de identificación, prevención y gestión de incidentes digitales, con la participación activa de las múltiples partes interesadas, y
    - Fortalecer las capacidades de los responsables de garantizar la defensa nacional en el entorno digital.
- Generar mecanismos permanentes y estratégicos para impulsar la cooperación, colaboración y asistencia en seguridad digital, a nivel nacional e internacional, a través de:
    - Generar mecanismos para impulsar la cooperación, colaboración y asistencia a nivel internacional, en materia de seguridad digital, y
    - Fortalecer la cooperación, colaboración y asistencia a nivel nacional, entre las múltiples partes interesadas en temas de seguridad digital.

Con respecto a regulaciones específicas a la industria se pueden mencionar las Resoluciones 3066 y 3067 de la Comisión Reguladora de Comunicaciones (en adelante CRC), las cuales atienen cuestiones muy puntuales de seguridad, por ejemplo:

- La Resolución 3066 [33] de 2011 sostiene el Principio de Protección de Datos Personales, en el que se obliga a los proveedores de servicios de comunicaciones a apegarse a las disposiciones legales en materia, y
- La Resolución CRC 3067 [34] de 2011 establece que los prestadores de servicios en materia de telecomunicaciones y radiodifusión deben utilizar los recursos técnicos y logísticos tendientes a garantizar la seguridad en la red y la integridad del servicio, por lo cual debe informar en su página web las acciones adoptadas en relación con el servicio prestado al usuario final, tales como el uso de firewalls, filtros antivirus y la prevención del *spam*, *phishing*, *malware* entre otros, y adicionalmente los prestadores que ofrezcan acceso a internet deben implementar modelos de seguridad, de acuerdo con los marcos definidos por la UIT (Series X.800).

Aunque aún es prematuro declarar si las medidas presentadas en este Plan Nacional están funcionando o no, no lo es para reconocer la responsabilidad de Colombia ante las crecientes amenazas del dentro cibernético. Es de destacar la madurez inmersa en las medidas emprendidas al reconocer la variedad de interés e interesado que son participes de la seguridad cibernética de una nación. Sin duda Colombia aún tiene mucho por hacer para poder gozar de un entorno cibernético seguro al nivel de los países más desarrollados. Sin embargo, es de reconocer la iniciativa que han emprendido.

De este análisis se puede observar la clara tendencia a reconocer que la seguridad cibernética es una meta de múltiples grupos de interés e interesados, por lo que un modelo en el que el Estado es el único participante en las acciones de seguridad es obsoleto e inútil.

También es importante señalar que todas las naciones analizadas han entendido que la interconexión que permiten las diversas redes de telecomunicaciones es, y será cada vez más, global. Esto implica que el trabajo de los Estados al momento de ejercer regulación sobre el tema debe ser muy cuidadosa en no afectar la interconexión con otras redes. Este aspecto ha sido considerado hasta el momento y debe de seguir así, puesto que una de las metas de las telecomunicaciones es lograr que todos los usuarios estén conectados.

Por último, es importante destacar la tendencia que se ha marcado en cuanto a la intervención de los gobiernos en la seguridad cibernética. Como se ha observado en el caso de Colombia, gracias al Convenio de Budapest y a intervenciones de organismos como la OEA y la OCDE, se ha entendido que uno de los primeros pasos es generar una política nacional que pretenda enfrentar a las amenazas del entorno cibernético desde un enfoque integral, buscando el establecimiento de instituciones capaces de atender cuestiones específicas de este sector, reformas o resoluciones de las leyes correspondientes, integración de los demás sectores interesados, la cooperación internacional, la formación de profesionales, el fomento a la educación y la promoción de un cultura cibernética.

Referencias del Capítulo II

[1] Symantec (2016). *Internet Security Threat Report.* California: Symantec. Recuperado de https://www.symantec.com/security-center/threat-report

[2] Norse (2017). *Norse Attack Map*. Recuperado el 10 de abril de 2017de http://map.norsecorp.com/#/

[3] Consejo de la Unión Europea (2008). *Directiva europea: 2008/114/CE del 8 de diciembre de 2008.* Diario Oficial de la Unión Europea. Recuperado de https://www.ccn-cert.cni.es/publico/InfraestructurasCriticaspublico/DirectivaEuropea2008-114-CE.pdf

[4] Casa Blanca (2013). *Executive Order -- Improving Critical Infrastructure Cybersecurity*. Recuperado de https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[5] Disponibles en el sitio web de Cuarto Concilio para la seguridad, fiabilidad e interoperabilidad de las redes: https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-0

[6] Disponibles en: https://www.fcc.gov/general/privacy-and-security-guides#block-menu-block-4

[7] McGuinness, Damien (2017). Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país. BBC. Recuperado de www.bbc.com/mundo/noticias-39800133

[8] Ministerio de Economía y Comunicación (2014). *Estrategia de Seguridad Cibernética 2014-2017*. recuperado de https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf

[9] Disponible en: http://www.vaatamaailma.ee/en/projektid/ikt-huviringid-noortele

[10] Disponible en: http://www.vaatamaailma.ee/en/nutikaitse

[11] Disponible en: http://www.hitsa.ee/about-us/news/article-2

[12] Ron Cheng, A. (2017). *Israel: The Next Key Player in the Cybersecurity Industry*. Forbes. Recuperado de https://www.forbes.com/sites/roncheng/2017/02/27/israel-the-next-key-player-in-the-cybersecurity-industry/#16ceae5810c8

[13] Nakashima, Ellen & Booth, William, A. (2016). How Israel is turning part of the Negev Desert into a cyber-city, The Washington Post. Recuperado de https://www.washingtonpost.com/world/national-security/how-israel-is-turning-part-of-the-negev-desert-into-a-cyber-city/2016/05/14/f44ea8e4-0d58-11e6-bfa1-4efa856caf2a_story.html?token=33d5607298204ac0b0ee0961cae07bca&utm_term=.f9a95c117a8b

[14] Sugarman, Eli. A. (2014). What The United States Can Learn From Israel About Cybersecurity. Forbes. Recuperado de https://www.forbes.com/sites/elisugarman/2014/10/07/what-the-united-states-can-learn-from-israel-about-cybersecurity/

[15] INCB (2015). *'Policy on Regulation of Cybersecurity Professions'* (hebreo). Israel. Recuperado de http://www.pmo.gov.il/SiteCollectionDocuments/cyber/hagana.pdf

[16] Oficina del Primer ministro israelí (2011). *Resolución Gubernamental 3611*. Israel Recuperado el 7 agosto 2011 de http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Advancing%20National%20Cyberspace%20Capabilities.pdf

[17] Oficina del Primer ministro israelí. (2015). *Resolución Gubernamental 2444, ast.2 (a).* Israel. Recuperado el 7 agosto 2011 de

https://ccdcoe.org/sites/default/files/documents/Government%20Resolution%20No%202444%20-%20Advancing%20the%20National%20Preparedness%20for%20Cyber%20Security.pdf

[18] Redacción BBC (2015). ¿Cómo logró Corea del Sur su milagro económico? *BBC Mundo.* Recuperado de http://www.bbc.com/mundo/noticias/2015/01/150116_economia_corea_del_sur_razones_desarrollo_lf

[19] García, Daniel. (2016). La Corea superconectada frente a la Corea 'incomunicada' [Sic.]. *El País.* Recuperado de https://elpais.com/tecnologia/2016/06/23/actualidad/1466696570_269717.html?token=2e71167b408b47599178a245b4ac8ab0?token=2e71167b408b47599178a245b4ac8ab0

[20] Gobierno de Corea (2011). *National Cyber Security Masterplan*. República de Corea Recuperado de https://ccdcoe.org/sites/default/files/strategy/KOR_NCSS_2011.pdf

[21] Kang, Tae-jun (2015). South Korea Beefs Up Cyber Security With an Eye on North Korea. *The Diplomat.* Recuperado de https://thediplomat.com/2015/04/south-korea-beefs-up-cyber-security-with-an-eye-on-north-korea/

[22] Microsoft Asia News Center (2016). Microsoft launches Korea Cybersecurity Center advancing fight against cyberthreats. *Microsoft News*. Recuperado de https://news.microsoft.com/apac/2016/03/04/microsoft-launches-korea-cybersecurity-center-advancing-fight-against-cyberthreats/?token=2e71167b408b47599178a245b4ac8ab0#sm.0000apfi671bi4do4pxsjzd8swcyg

[23] Parlamento Europeo (2016). *DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión*, Recuperado de http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L1148&from=ES

[24] European Union Agency for Network and Information Security (2016). *Technical guidelines for the implementation of minimum security measures for DSPs*. Recuperado de https://www.enisa.europa.eu/publications/minimum-security-measures-for-digital-service-providers

[25] Parlamento Europeo (2016). *REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)*, Recuperado de http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=es

[26] Parlamento Europeo (2016). *DIRECTIVA (UE) 2016/680 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.* Recuperado de http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016L0680&from=ES

[27] Gateau, Christine & Faron, Pauline (2016). French law for a Digital Republic: what you should know, what you should expect. Global Media and Comunications Watch. Recuperado de https://www.hlmediacomms.com/2016/10/24/french-law-for-a-digital-republic-what-you-should-know-what-you-should-expect/#page=1

[28] Parlamento Alemán (2017). *Bundesdatenschutzgesetz.* Alemania. Recuperado de https://www.gesetze-im-internet.de/englisch_bdsg/

[29] Paniagua, Esther (2017). El destape de España en protección de datos. El País. Recuperado de https://retina.elpais.com/retina/2017/08/11/tendencias/1502446063_042539.html

[30] Ofcom (2013). *Updating Ofcom's guidance on network security*. Recuperado de https://www.ofcom.org.uk/__data/assets/pdf_file/0024/81456/security_and_resilience_guidance1.pdf

[31] NICC Standards Limited (2015). *Minimum Security Standards For Interconnecting Communications Providers*, Versión 4.1.1. Recuperado de http://www.niccstandards.org.uk/files/current/ND1643V4.1.1.pdf?type=pdf

[32] Ofcom (2016). *Annual Plan 2016/17; Making communications work for everyone*, recuperado de https://www.ofcom.org.uk/__data/assets/pdf_file/0036/59499/annual-plan-2016-17.pdf

[33] Comisión de Regulación de Comunicaciones (2011). *Resolución No. 3066 de 2011 "Por la cual se establece el Régimen Integral de Protección de los Derechos de los Usuarios de los Servicios de Comunicaciones"*, Recuperado de http://www.sic.gov.co/sites/default/files/normatividad/00003066.pdf

[34] Comisión de Regulación de Comunicaciones (2011). *Resolución No. 3067 de 2011 "Por la cual se definen los indicadores de calidad para los servicios de telecomunicaciones y se dictan otras disposiciones"*, Recuperado de https://www.crcom.gov.co/recursos_user/Normatividad/Normas_Actualizadas/Res_3067_Act_4807_15.pdf

Capítulo III: Situación en México

México tiene un serio problema de seguridad cibernética. Según el mapa de amenazas cibernéticas en tiempo real que ofrece el portal de la empresa de seguridad Kapersky, mostrado por la Ilustración 3.1, México fue el séptimo país más atacado en el mundo en el mes de junio del año 2017. Diversas empresas de seguridad cibernética expresan que México se mantiene en condiciones similares a las presentadas por Kapersky.

A pesar de que México cuenta con elementos que le permiten sobresalir en cuestiones cibernéticas, como "la impresionante base de datos criminal nacional de México y tal vez el mejor modelo de sistema de datos integrados que hay en funcionamiento hoy en día " (Schmidt & Cohen, 2012), México aún está en una etapa formativa de capacidades cibernéticas que le permitan hacer frente a las amenazas de su entorno cibernético de manera integral.

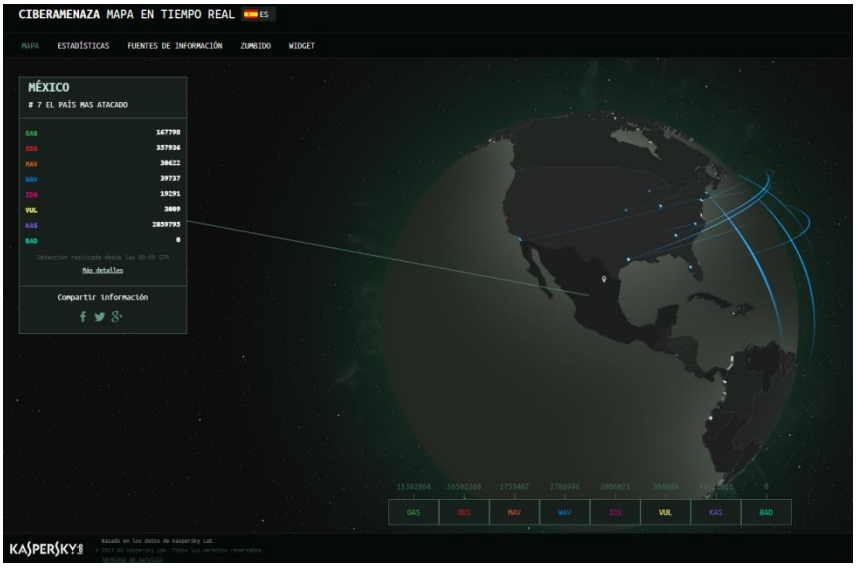


Ilustración 3.1: México, séptimo país más atacado en el espacio cibernético: Kapersky Lab. (junio de 2017) [1]

Las dos grandes tendencias mundiales de acceso a internet son a través de los servicios de banda ancha fija y banda ancha móvil, tendencia de la que México no es la excepción. Para el cuarto trimestre de 2016, el Banco de Indicadores de Telecomunicaciones del Instituto Federal de Telecomunicaciones (en adelante IFT) reportó que, en el servicio de Banda Ancha Fija, México contaba con 48 líneas de acceso por cada 100 hogares abarcando diferentes tecnologías de accesos. Es importante destacar que, de entre las velocidades anunciadas por la industria, las que han tenido un auge significativo son aquellas que se ofrecen en el rango de entre los 10 y los 100 Mbps, tal como lo señala el Gráfico 3.1.1. Lo anterior es evidencia y reflejo de una sociedad que cada día se sumerge más en la era digital, y, por ende, en el entorno cibernético.

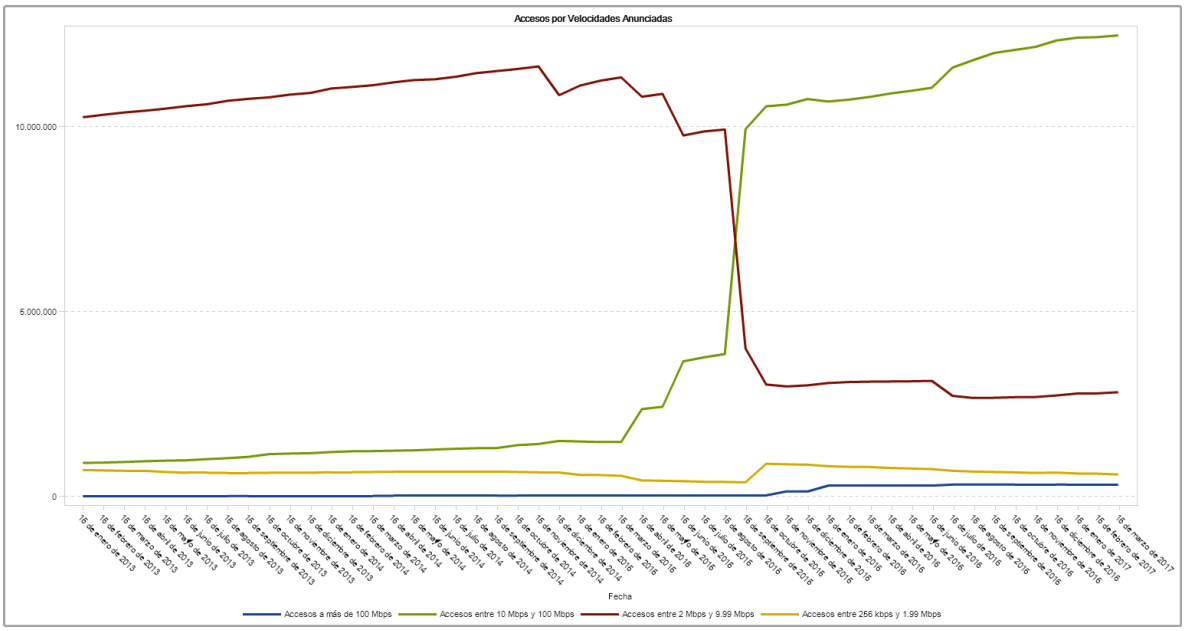


Gráfico 3.1.1: Velocidades de banda ancha ofrecidas por la industria en México (enero 2013-marzo 2017) [2]

En relación con lo anterior, se estima que, al primer trimestre de 2017, México contaba con una teledensidad de banda ancha móvil de 63 líneas por cada 100 habitantes, y al analizar los datos del IFT, se puede notar que México cuenta con un creciente consumo de datos móviles entre sus habitantes, tal y como lo muestra el Grafico 3.1.2. Las cifras anteriores indican, necesariamente, un incremento en el número de personas que interactúan en el entorno cibernético, así como un incremento en la información que están produciendo e intercambiando los usuarios de internet en México.

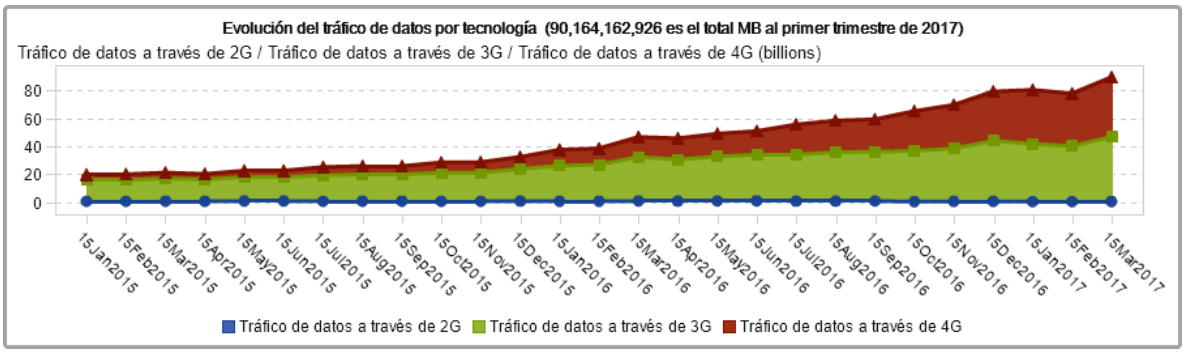


Gráfico 3.1.2: Evolución de datos por tecnología del servicio de banda ancha móvil en México (junio 2015- marzo 2017) [3]

Si, además de las cifras presentadas, se considera que la Red Compartida Mayorista, pretende ser el proyecto de telecomunicaciones más grande de la historia de México, tendrá una cobertura poblacional del 92% en el servicio de Banda Ancha Móvil y otros servicios de telecomunicaciones, resulta urgente que México aumente sus estándares de calidad en cuanto seguridad cibernética se refiere. De lo anterior se desprende que uno de los principales retos del gobierno mexicano es fomentar una sociedad digital que mantenga una conducta responsable en el entorno cibernético, y que pueda contar con el respaldo de un

conjunto de normas nacionales, instituciones sólidas y leyes ágiles que le permitan mantenerse seguro en entono cibernético.

Algunos estudios mencionados anteriormente sitúan a México, junto con otros países de Latinoamérica, en una situación media de madurez en cuanto a prácticas y políticas de seguridad cibernética se refiere. Diversos elementos se pueden poner sobre la mesa para entender esta situación. Por ejemplo, México es un país que se ha adherido al Convenio de Budapest, sin embargo, sólo lo ha hecho en calidad de observador. Incluso, personalidades como Alexander Seger, responsable de la división de ciberdelincuencia del Consejo de Europa y secretario del Comité del Convenio de Budapest, ha señalado que es un buen momento de que México pase de ser un país observador del Convenio a uno que ha completado su adhesión [4].

En junio de 2017 fue publicado por la UIT el reporte del Índice Global de Seguridad Cibernética 2017 [5]. En dicho informe se señala que México se encuentra en el grupo de países en etapa de "Maduración" de seguridad cibernética, es decir, se encuentra entre el percentil 50 y el percentil 89 del estudio mencionado. Esta categoría implica que México se encuentra desarrollando compromisos complejos en la materia, y participando y promoviendo iniciativas de seguridad cibernética. De hecho, dicho informe señala que México es el tercer país de América más comprometido con el desarrollo óptimo de la seguridad cibernética, sólo después de Estados Unidos y Canadá. De ello se desprende que México es, al día de hoy, un país ocupado en el fortalecimiento de su seguridad cibernética.

Es importante recalcar que, aunque México ocupa el tercer lugar de América en el estudio, es un país con mucha trayectoria que recorrer en cuestiones de seguridad cibernética. Esta cuestión se ilustra al notar que México suma 16 puntos menos que el segundo lugar de América, que es, Canadá. Ese hecho marca la división que existe en la región entre las naciones más desarrolladas en este ámbito y el resto de los países del continente.

Al realizar una observación más exhaustiva del informe, se puede notar que México tiene aspectos aceptables, promedio y endebles, los cuales se describen a continuación.

- Aspectos aceptables: El informe señala que México mantiene de forma aceptable la legislación en materia de criminalidad cibernética y seguridad cibernética; el establecimiento de CERTS (de sus siglas del inglés Computer Emergency Response Team) nacionales, gubernamentales y sectoriales; las normas para profesionales; la protección a la población infantil; la responsabilidad de las instituciones; las buenas prácticas en seguridad cibernética; las campañas de conciencia a la población; los cursos de formación profesional; los programas educativos; la participación internacional, y la colaboración interinstitucional con gobiernos extranjeros.
- Aspectos promedio: se señala que las normas para las organizaciones; las métricas de seguridad cibernética; los programas de investigación y desarrollo, y los mecanismos para incentivar la mejora continua en el sector, se encuentran en un estado promedio en comparación con el resto de los países.

- Aspectos endebles: se señala que los aspectos endebles son las cuestiones referentes a las estrategias de seguridad cibernética; los cuerpos de normalización; los acuerdos bilaterales; los acuerdos multilaterales, y la colaboración entre el sector público y privado.

En la conclusión de dicho informe, México se posiciona en el número 28 de los 165 evaluados con una calificación promedio de 0.660, en un a escala que va desde el 0.000 al 0.925.

De las acciones que México ha emprendido para ocupar dicho lugar, se puede destacar el Plan Nacional de Desarrollo 2013–2018 [6], el cual dispone el fortalecimiento de las capacidades institucionales en el ciberespacio y la seguridad cibernética. Esto en respuesta a que los delitos de suplantación de identidad, fraudes financieros, distribución de pornografía infantil, entre otros, han prosperado en el ciberespacio generando un alto costo económico y humano. En este sentido, el plan sugiere la necesidad de concentrar esfuerzos y recursos para combatir el ciberdelito e impulsar una legislación en la materia a nivel nacional. De igual modo, resulta prioritario fortalecer la cooperación internacional, en particular con América del Norte, con el fin de identificar, prevenir y contener los riesgos y amenazas a la Seguridad Nacional que provengan del ciberespacio.

En busca de cumplir con los objetivos en materia de seguridad nacional planteados en el Plan Nacional de Desarrollo, fue publicado el Programa para la Seguridad Nacional 2014–2018 [7], el cual dedica su apartado tercero del sexto capítulo "Riesgos y Amenazas" a la Ciberseguridad, donde plantea que el propósito central de la estrategia debe ser el fortalecimiento de la cuarta dimensión de las operaciones de seguridad: la ciberseguridad y la ciberdefensa. Las líneas de acción comprendidas en este programa para el logro de los objetivos en materia de seguridad cibernética, son los siguientes:

- Impulsar proyectos normativos que regulen esquemas de seguridad de la información homólogos en todos los sectores del país, para prevenir y enfrentar ataques cibernéticos;

- Designar a la unidad administrativa encargada de emitir, evaluar e impulsar el cumplimiento de la política de seguridad cibernética y ciberdefensa para el Ejecutivo Federal;

- Fortalecer los mecanismos de coordinación para la atención a incidentes de seguridad cibernética en el ámbito del Ejecutivo Federal;

- Impulsar el cumplimiento y el desarrollo de procedimientos para evaluar y fortalecer el funcionamiento de los equipos de respuesta a incidentes de seguridad cibernética en el ámbito del Ejecutivo Federal;

- Fortalecer las capacidades humanas, tecnológicas y la infraestructura para atender incidentes de seguridad cibernética; y

- Establecer esquemas de cooperación internacional en materia de seguridad cibernética y ciberdefensa para prevenir y enfrentar ataques a los sistemas informáticos del país.

Por otra parte, en mayo de 2014 fue publicado en el Diario Oficial de la Federación el Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como establecer el Manual Administrativo de Aplicación General en dichas materias [8], el cual se desarrolló con base en las normas internacionales ISO 27001, ITIL (por sus siglas en inglés de *Information Technology Infrastructure Library*) y COBIT (por sus siglas en inglés de *Control Objectives for Information and Related Technology*), entre otras. Que dicho Acuerdo quedó establecido que las medidas planteadas en él le son aplicables a todas las dependencias y entidades de la Administración Pública Federal a partir del 9 de mayo de 2014.

En cuanto a la capacidad de respuesta ante incidentes cibernéticos, México cuenta con un Equipo de Respuesta ante Emergencias Informáticas (CERT) que está localizado en la Coordinación de Seguridad de la Información (CSI) de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación, de la Universidad Nacional Autónoma de México, UNAM (UNAM-CERT). Dicho CERT está conformado por un equipo de profesionales en seguridad en cómputo que se encarga de proveer el servicio de respuesta a incidentes de seguridad en cómputo a sitios que han sido víctimas de algún "ataque", así como de publicar información respecto a vulnerabilidades de seguridad, alertas de la misma índole y realizar investigaciones de la amplia área del cómputo y así ayudar a mejorar la seguridad de los sitios.

El UNAM-CERT promueve la cultura de seguridad en las redes a los usuarios a través de diferentes herramientas, una de ellas es la plataforma Usuario Casero, la cual es un portal que cuenta con información detallada y clara sobre las principales amenazas que pueden dañar a los equipos personales de cómputo y de los mecanismos de defensa.

Otro elemento considerable en la construcción de una seguridad cibernética en México es el papel que desempeña la Comisión Nacional de Seguridad a través de la División Científica de la Policía Federal, se ha generado una metodología científica y tecnológica para la prevención e investigación del delito, con el desarrollo de herramientas técnico-científicas, la participación de personal experto en criminalística, investigación cibernética y seguridad de sistemas de información y servicios científico tecnológicos, contribuyendo a los objetivos de la Policía Federal. Una de las múltiples tareas de la División Científica de la Policía Federal es la operación del CERT-MX, el cual trabaja en coordinación con los CERT de otros países para gestionar los incidentes a nivel global, y mantener un estado de alerta ante los incidentes originados fuera del territorio mexicano.

En materia de la protección de datos personales, en Julio de 2010 se publicó en el Diario Oficial de la Federación la Ley Federal de Protección de Datos Personales en Posesión de los Particulares [9], con el objetivo de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

Esta ley pretende salvaguardar el respeto a la privacidad, dignidad e información de las personas, en ella se establecen cuatro derechos fundamentales que tienen los individuos sobre su información en posesión de cualquier persona física o empresa particular. Dichos derechos son: (i) Acceso; (ii) Rectificación; (iii) Corrección, y (iv) Oposición.

La ley también indica que los particulares deberán avisar, a cada persona de la que obtengan información personal, sobre el tratamiento que planean dar a sus datos. Lo anterior se debe hacer mediante un aviso de privacidad, el cual deberá ser respetado por el particular, y cada persona notificada tendrá la libertad de otorgar o no su consentimiento respecto al procesamiento de su información.

Derivado de lo anterior, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) ha redoblado esfuerzos en la emisión convenios, reglamentos y resoluciones en favor de cumplir con las garantías establecidas en dicha ley.

Aunado a lo anterior, el INAI también ha procurado un acercamiento con la sociedad a través de guías y recomendaciones que buscan preparar a la misma en diversas cuestiones relacionadas con la protección de datos personales, que van desde los conceptos básicos de la materia, hasta el cómo hacer valer sus derechos al amparo de la legislación correspondiente y el cómo evitar el robo de identidad, entre otros.

Asimismo, en enero de 2017, el Honorable Congreso de la Unión aprobó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados [10], misma que fue propuesta por el gobierno del Presiente Enrique Peña Nieto, tiene por objetivos:

1. Distribuir competencias entre los Organismos garantes de la Federación y las Entidades Federativas, en materia de protección de datos personales en posesión de sujetos obligados;
2. Establecer las bases mínimas y condiciones homogéneas que regirán el tratamiento de los datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, mediante procedimientos sencillos y expeditos;
3. Regular la organización y operación del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales a que se refieren esta Ley y la Ley General de Transparencia y Acceso a la Información Pública, en lo relativo a sus funciones para la protección de datos personales en posesión de sujetos obligados;
4. Garantizar la observancia de los principios de protección de datos personales previstos en la presente Ley y demás disposiciones que resulten aplicables en la materia;
5. Proteger los datos personales en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, de la Federación, las Entidades Federativas y los municipios, con la finalidad de regular su debido tratamiento;
6. Garantizar que toda persona pueda ejercer el derecho a la protección de los datos personales;
7. Promover, fomentar y difundir una cultura de protección de datos personales;
8. Establecer los mecanismos para garantizar el cumplimiento y la efectiva aplicación de las medidas de apremio que correspondan para aquellas conductas que contravengan las disposiciones previstas en esta Ley, y
9. Regular los medios de impugnación y procedimientos para la interposición de acciones de inconstitucionalidad y controversias constitucionales por parte de los Organismos garantes locales y de la Federación; de conformidad con sus facultades respectivas.

Al comparar los derechos individuales, obligaciones y pautas generales contenidos en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, así como en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, contra lo contenido en los otros marcos jurídicos analizados, como el de la Unión Europea, se hace evidente el rezago del marco jurídico en México, y, como se verá más adelante, resulta preocupante la lentitud con la que evoluciona el proceso legislativo en México.

Por lo que respecta al IFT, al día de hoy no se han emitido documentos regulatorios en materia de seguridad de las redes, situación de alarma si se considera el incremento del número de usuarios de los servicios de banda ancha fija y/o móvil.

A pesar de lo anterior, es justo señalar que el IFT ha procurado un acercamiento con los usuarios de los servicios de banda ancha fija y móvil a través de campañas multimedia en redes sociales, como la campaña "Conoce a los enemigos públicos de tu celular", mediante el portal "Soy usuario", e incluso a través de acercamientos presenciales como el ofrecido por la "Unidad Móvil IFT", la cual tiene como objetivo formar usuarios responsables y audiencias activas a través de la impartición de talleres gratuitos.

De lo anterior se desprende que es el IFT el órgano gubernamental que más ha promovido los buenos hábitos de cultura digital, sin embargo, los esfuerzos comprendidos hasta ahora quedan muy lejos de satisfacer las necesidades del país en este sector, pues los alcances de los programas emprendidos al momento no han sido lo suficientemente ambiciosos ni han logrado penetrar en un número considerable de usuarios, pues la difusión ha sido pobre, y el poder de convocatoria del IFT en ese sector es limitado.

Prueba de lo anterior es el lugar que ocupó México en la lista de los países más afectados por el *ransomwere Wannacry*, posicionándose en el quinto lugar mundial y el país más afectado de América Latina [11]. Para comprender esto, hay que recordar que dicho malware se propagó principalmente en las computadoras que funcionaban con un sistema operativo no actualizado. Actualizar el sistema operativo de las computadoras es un acto fundamentalmente gratuito y abierto al público en general, los que sugiere que la omisión del acto implica un descuido deliberado, mismo que es reflejo de malos hábitos digitales y de una falta de cultura cibernética.

El ataque de *WannaCry* no es el único incidente de seguridad cibernética en el que México se ha visto envuelto recientemente, sin embargo, el monitoreo de los ataques en México es escaso. Por ejemplo, los informes de incidentes de seguridad en México realizados por la División Científica de Policía Federal son inexistentes o inaccesibles y la difusión de incidentes se delega a boletines casuísticos en el portal de la Comisión Nacional de Seguridad, uno de ellos, justamente publicado para alertar sobre el *ransomware WannaCry*, menciona que del año 2012 al 15 de mayo de 2017 (fecha de su publicación) se habían atendido 170 mil 864 incidentes se seguridad cibernética en el país, de los cuales aproximadamente el 60% estuvieron relacionados con *malware*[12] . Esta situación ha generado que la principal difusión de informes en la materia venga por parte de instituciones académicas u organizaciones civiles, como los recuentos de los incidentes detectados dentro de la RedUNAM, publicados por la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC) de la UNAM.

Según lo reportado por la DGTIC [13], hasta septiembre de 2017 se habían detectado un total de 44013 incidentes de seguridad cibernética tan solo en la RedUNAM, siendo los ataques de fuerza bruta y de *Malware* los detectados con mayor frecuencia. Así mismo, la DGTIC publicó un total de seis boletines en 2017 para informar a la población de diversas amenazas cibernéticas. Dichos boletines alcanzaron las siguientes categorías:

- Amenaza crítica:
  - Publicado el 16 de octubre de 2017, el Boletín de Seguridad UNAM-CERT-2017-002 Ataque de reinstalación de llave en WPA2 informa sobre una vulnerabilidad en el protocolo WPA2 que permite al atacante la manipulación de los mensajes enviados y transmitidos, el descifrado de la comunicación y hasta la inyección arbitraria de paquetes. Así mismo, dicho boletín recomienda la instalación de actualizaciones en los productos afectados conforme estén disponibles.
- Amenaza alta:
  - Publicado el 12 de mayo de 2017, el Boletín de Seguridad UNAM-CERT-2017-001 Alerta por *ransomware WannaCry* informa sobre la afectación de dicho *ransmomware* al explotar una vulnerabilidad que afecta a sistemas Windows, por el que cifra los archivos en el equipo y los de las unidades de red a las que estén conectadas, además de propagarse por la red afectando a otros sistemas Windows. Dentro de las recomendaciones que enuncia dicho boletín, se encuentra el actualizar los equipos Windows que se posean, aislar los equipos infectados, realizar respaldos de información y no pagar a el rescate de información, y
  - Publicado el 28 de junio de 2017, la "Alerta por *ransomware* Petya" informa sobre el avance de dicho *Malware* en las redes europeas, específicamente en los equipos con sistema operativo Windows. Dentro de las recomendaciones que enuncia dicho boletín, se encuentra el actualizar los equipos Windows que se posean, aislar los equipos infectados, realizar respaldos de información y no pagar a el rescate de información.
- Amenaza media:
  - Publicado el 16 de octubre de 2017, el Boletín "Término de soporte de Windows 10 en su versión November Update (1511)" informa que Microsoft no continuará dando soporte a los equipos cuto sistema operativo sea Windows 10 en su versión 1511, por lo que se recomienda actualizar los equipos a una versión posterior de dicho sistema operativo, y
  - Publicado el 25 de octubre de 2017, el Boletín de Seguridad UNAM-CERT-2017-003 Alerta por *ransomware Bad Rabbit* informa un programa malicioso con características de *ransomware* propagándose principalmente en Rusia, Ucrania, Alemania y Turquía en los equipos con sistema operativo Windows. Asimismo, el boletín informa que el ataque utiliza técnicas de *phishing*¸ pues se hace pasar por una actualización del programa Adobe Flash, por lo que recomienda validar las peticiones de actualización de dicho programa, concientizar a los usuarios sobre las buenas prácticas de navegación en internet, realizar respaldos de información y no realizar los pagos solicitados por el atacante.

Al considerar el hecho de que los 44013 incidentes reportados por la DGTIC de la UNAM ocurrieron únicamente en RedUNAM, surge la sospecha de que el número total de ataques registrados en el país debe ser inmenso. Al respecto, la empresa de seguridad cibernética Arbor Networks ha seguido de cerca los incidentes registrados en México, particularmente, los ataques DDoS.

Arbor informa que en entre noviembre de 2017 y octubre de 2017, México sufrió un total de 14,237 ataques DDoS detectados, lo que se traduce en 39 ataques por día. Al respecto, dichos ataques variaron en intensidad y en origen, siendo el ataque de mayor tamaño de 44.4 Gbps. Respecto al origen, el 44.61% de estos ataques provinieron desde el mismo México, siguiéndole Estados Unidos, con 26.96%, Irlanda, con 16.18% y Alemania, con 12.26%.

La falta de divulgación de los incidentes de seguridad cibernética y la falta de colaboración entre el sector público y privado para el análisis de incidentes, mejora de respuestas e implementación de las mejores prácticas internacionales no sólo es un problema de México, sino de la región (América latina) en general. Belisario Contreras, gerente del Programa de Seguridad Cibernética de la OEA, ha hecho un llamado a los países miembros de la misma[14], para fomentar la colaboración entre sectores público y privado, y a perder el miedo a la difusión de incidentes, llamado que, en función de lo expresado por los párrafos anteriores, México debería atender si condiciones.

En relación con lo anterior, resulta alentador saber que la Policía Federal se ha dado cuenta de esta situación y ha comenzado a generar propuestas para avanzar en este sentido. Desde su perspectiva, uno de los problemas que enfrenta el organismo encargado de la seguridad en ambientes digitales, es decir, su División Científica, es la falta de criterios homologados dentro de las policías científicas estatales. Al respecto, en junio de 2017, Patricia Trujillo Mariel, titular de dicha división, dijo al diario El Economista que se ha puesto sobre la mesa la creación de un Consejo Nacional de Ciberseguridad[15], lo que permitiría que todas las policías cibernéticas del país operen bajo los mismos estándares y la misma visión respecto a las amenazas en el ciberespacio. Así mismo, la funcionaria destacó que uno de los mayores retos que enfrentan como cuerpo de seguridad en el ambiente digital, es la falta de denuncias por parte de la ciudadanía, lo que genera que los incidentes cibernéticos que se atienden son producto de un patrullaje cibernético. Esta naturaleza ciudadana de pasar por alto los delitos cibernéticos de los que han sido víctimas, refleja que México tiene mucho que trabajar en la integración de la sociedad civil en cuanto a seguridad cibernética se refiere.

Si bien es cierto que lo planteado en el párrafo anterior refleja una preocupación activa por robustecer la seguridad cibernética en México, se debe señalar que esta intención está viniendo de uno de los tres poderes que componen al Estado Mexicano, por lo que resulta justo cuestionar, y criticar, los avances del Poder Legislativo y el Poder Ejecutivo en la materia.

Anteriormente se mencionaron Acuerdos y Leyes Mexicanas enfocadas a fortalecer la seguridad cibernética en México, específicamente se habló de la protección de los sistemas informáticos operados al interior de la función pública, y de las leyes de protección de datos personales. Es claro que dicha legislación aporta al fortalecimiento de la nación en la materia, sin embargo, se debe recordar que las mejores prácticas

internacionales enfrentan las amenazas del entorno cibernético de una forma integral, por lo que resulta necesario estudiar más a fondo las acciones del Poder Legislativo en la materia.

El Poder Legislativo cuenta con diversos mecanismos para generar las propuestas legislativas que después de un debido proceso podrían convertirse en publicaciones oficiales. Algunos de los principales mecanismos son las respectivas comisiones de estudio de la Cámara de Diputados y la Cámara de Senadores. Estas comisiones legislativas son "Formas internas de organización que asumen las cámaras que integran el Congreso de la Unión, con el fin de atender los asuntos de la competencia constitucional y legal de éstas, para el mejor y más expedito desempeño de sus funciones"[16]

En la LXIII Legislatura del Congreso de la Unión, cuyas funciones se desempeñan desde el 1 de septiembre y hasta el 31 de agosto de 2018, se han planteado diversas propuestas en materia de seguridad cibernética por parte algunas comisiones de estudio de sus respectivas cámaras. Al interior de la Cámara de Diputados existen tres comisiones que se han involucrado en diferente medida en la seguridad cibernética del país. La Tablas 3.1, 3.2 y 3.3[25] muestran los proyectos legislativos que se han presentado en la Cámara de Diputados a lo largo de la LXIII Legislatura.

Tabla 3.1: Proyecto de decreto que reforma y adiciona diversas disposiciones del Código Penal Federal y de la Ley Federal de Telecomunicaciones y Radiodifusión.

Nombre de la iniciativa: Proyecto de decreto que reforma y adiciona diversas disposiciones del Código Penal Federal y de la Ley Federal de Telecomunicaciones y Radiodifusión.		**Proponente**: Diputada María Elena Orantes López (Movimiento Ciudadano)
Fecha de presentación:	**Situación:**	**Comisiones involucradas:**
16 de marzo de 2016	Pendiente	Justicia y Radio y Televisión
Sinopsis: Sancionar con trabajo a favor de la comunidad, al que ingrese a la cuenta de correo electrónico de terceros, excluyendo a los padres de menores de edad, tutores y cónyuge. Sancionar con prisión al empleado de una compañía concesionaria de telecomunicaciones o similar, que colabore en la intervención de comunicaciones privadas sin mandato de autoridad judicial. Establecer que los concesionarios que operen redes públicas de telecomunicaciones deberán desarrollar programas para la detección de intervenciones ilegales de comunicaciones.		

Tabla 3.2: Proyecto de decreto que reforma y adiciona diversas disposiciones del Código Penal Federal y de la Ley Federal de Telecomunicaciones y Radiodifusión.

[25] Las Tablas 3.1-3.3 son de elaboración propia con los datos presentados en el sitio web de la Cámara de Diputados (http://sitl.diputados.gob.mx/LXIII_leg/listado_de_comisioneslxiii.php?tct=1)

<table>
<tr><td colspan="2">Nombre de la iniciativa: Proyecto de decreto que reforma y adiciona 14 ordenamientos legales, en materia de prevención, investigación, procuración de justicia y sanción de delitos cometidos por usurpación, robo, fraude y suplantación de datos e identidad personales.</td><td>Proponente: Diputado José Máximo García López (Partido Acción Nacional)</td></tr>
<tr><td>Fecha de presentación:</td><td>Situación:</td><td>Comisiones involucradas:</td></tr>
<tr><td>9 de febrero de 2017</td><td>Pendiente</td><td>Justicia y Gobernación</td></tr>
<tr><td colspan="3">Sinopsis: Este proyecto se compone de propuestas específicas en diversos ordenamientos legales vigentes, las cuales se listan a continuación:
Código Penal Federal: Tipificar y sancionar a quien haga uso indebido de los datos personales e identidad de las personas.
Ley Federal contra la Delincuencia Organizada: Sancionar la utilización de datos personales de identidad robada y cometan un delito.
Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita: Desarrollar herramientas científicas, tecnológicas, cibernéticas y electrónicas, para prevención e identificación de operaciones con recursos de procedencia ilícita.
Ley de la Policía Federal: Evitar la afectación el derecho de las personas sobre sus datos de identidad personales.
Ley General de Transparencia y Acceso a la Información Pública: Observar los derechos personales e identidad de los titulares y considerar información reservada aquella cuya publicación pueda poner en riesgo la personalidad, patrimonio o identidad de una persona física;
Ley Federal de Protección de Datos Personales en Posesión de los Particulares: Exceptuar de los sujetos regulados por la ley a las personas a que tengan en su poder datos de identidad personal y responsabilizarlos por la difusión, distribución y entrega por si o terceros.
Ley de Protección y Defensa al Usuario de Servicios Financieros: Promover, asesorar, proteger y defender los datos de identidad personal
Código Fiscal de la Federación: Garantizar la identidad de las personas y sus datos personales
Ley del Servicio de Administración Tributaria: Atribuir al Servicio de Administración Tributaria vigilar y asegurar el debido cumplimiento de las disposiciones aplicables sobre la conservación, tratamiento y resguardo de datos de identidad personal.
Ley de Firma Electrónica Avanzada: Resguardar los datos de identidad personal.
Ley General en materia de Delitos Electorales: Sancionar al funcionario electoral que disponga, divulgue, publique, datos de identidad personal del electorado.
Ley General de Partidos Políticos: Salvaguardar la información de identidad personal de sus militantes, afiliados y simpatizantes.
Ley Orgánica de la Administración Pública Federal: Salvaguardar la identidad de las personas
Ley Federal de Protección al Consumidor: Preservar los derechos de las partes y prohibir la comercialización de datos personales e identidad de los consumidores.</td></tr>
</table>

Tabla 3.3: Proyecto de decreto que reforma y adiciona diversas disposiciones de la Ley de Seguridad Nacional.

Nombre de la iniciativa: Proyecto de decreto que reforma y adiciona diversas disposiciones de la Ley de Seguridad Nacional.		**Proponente**: Diputado Waldo Fernández González (Partido de la Revolución Democrática)
Fecha de presentación:	**Situación:**	**Comisiones involucradas:**
30 de octubre de 2017	Pendiente	Gobernación
Sinopsis: Considerar como amenazas a la seguridad nacional a los actos provenientes del ciberespacio tendientes a sustraer, alterar o dañar información o infraestructura de la administración pública.		

Sin menospreciar las propuestas antes mencionadas, se pueden resaltar algunos puntos específicos de ellas que pueden mejorarse. Si bien es cierto que en su conjunto estas propuestas podrían abonar al marco legal aplicable a la seguridad cibernética en México, al analizarlas de forma individual se puede notar el contenido de estas propuestas aborda de forma muy superficial la seguridad cibernética en México. Este problema es herencia de la estructura de las comisiones de estudio de la Cámara de Diputados, pues al no haber una comisión específica de seguridad cibernética, las propuestas que se presenten y analicen en las comisiones aledañas difícilmente tendrán la profundidad necesaria para abordad el problema, en especial si se considera que México enfrenta grandes retos en materia de justicia y gobernación, por lo que las prioridades de las comisiones de estudio en esas materias podrían ser muy diferentes sin que ello represente un incumplimiento de sus funciones.

Si bien no existe en la Cámara de Diputados una Comisión Ordinaria encargada de proponer y estudiar los proyectos exclusivamente en materia seguridad cibernética, sí existe una Comisión Especial que se acerca al tema más que las Comisiones antes mencionadas; la Comisión Especial Tecnologías de Información y Comunicación.

La Comisión Especial Tecnologías de Información y Comunicación de la Cámara de Diputados refiere en su Programa de Trabajo 2016-2017[17] que uno de sus objetivos específicos será:

> "Colaborar estrechamente con las comisiones ordinarias de la Cámara, para fundamentar y respaldar las propuestas legislativas en materia de justicia cotidiana y seguridad cibernética, en particular aquellas que tiendan a:
>
> - Modernizar, agilizar y hacer más eficientes los servicios públicos.
> - Brindar seguridad para oficinas y organismos públicos ubicados en sectores estratégicos para el país.
> - Combatir el robo de identidad, que tiene como soporte las diversas TIC y que conduce a la comisión de múltiples ilícitos.

- Proteger a los niños y adolescentes de las actividades de los acosadores que emplean internet y otras tecnologías de comunicación para consumar sus propósitos.
- Luchar contra la delincuencia organizada dedicada a la prostitución infantil, el tráfico de órganos y cualquier otra actividad que lesione la cohesión social y la paz de los mexicanos "

A pesar de que el objetivo planteado por dicha Comisión es una propuesta más completa y enfocada en la materia que los objetivos de otras comisiones, se debe comentar que, no abarca en de forma íntegra los aspectos de la seguridad cibernética, ni se involucra con otros sectores que puedan robustecer los proyectos legislativos al respecto. Por otra parte, hay que señalar la lenta evolución que ha tenido el cumplimiento de este objetivo, pues el micrositio de esa comisión refleja que, a enero de 2018, dicha comisión únicamente había opinado acerca de tres propuestas legislativas, dentro de las cuales se encuentra la opinión al proyecto abordado en la Tabla 3.1, así como la opinión respecto al entonces Proyecto de Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, hoy ya aprobada, la cual fue abordada en párrafos anteriores.

Por otra parte, al interior de la Cámara de Senadores las propuestas legislativas al respecto son más escasas. La única propuesta que abarca temas de seguridad cibernética es el "Proyecto de decreto que reforma y adiciona diversas disposiciones del Código Penal Federal, en materia de seguridad cibernética", turnada para su estudio a la Comisión de Justicia el 11 de enero de 2018, y de la que la Tabla 3.4 ofrece una descripción más detallada. Asimismo, cabe mencionar que en las Comisiones Especiales de la cámara alta no existe alguna comisión que aborde cuestiones legislativas respecto a la seguridad cibernética en México.

Tabla 3.4: Proyecto de decreto que reforma y adiciona diversas disposiciones del Código Penal Federal, en materia de seguridad cibernética.

Nombre de la iniciativa: Proyecto de decreto que reforma y adiciona diversas disposiciones del Código Penal Federal, en materia de seguridad cibernética.		**Proponente**: Senador Luis Humberto Fernández Fuentes (Partido del Trabajo)
Fecha de presentación:	**Situación:**	**Comisiones involucradas:**
11 de enero de 2018	Pendiente	Justicia
Sinopsis: Tipificar y sancionar a quien haga uso indebido de los datos personales e identidad de las personas, así como a quienes accedan de forma ilegítima a sistemas y equipos informáticos		

Por lo anterior expuesto se puede notar que el Congreso de la Unión no se está abordando la seguridad cibernética de forma integral. Si a eso se suma los largos tiempos de estudio de las propuestas, se puede concluir que el proceso legislativo se está quedando corto en cuanto a las exigencias cibernéticas de la actualidad. Consecuencia de lo anterior surge un cuestionamiento importante; si el Poder Judicial, a través de su brazo coercitivo, es decir, los cuerpos policiales, reconoce la necesidad de generar cuerpos especializados que atiendan cuestiones de ciberseguridad, qué esperan los demás poderes que conforman

el Estado Mexicano. En la situación en la que se encuentra el país, resulta evidente la necesidad de la creación de Comisiones Ordinarias en materia de seguridad cibernética en el Congreso de la Unión, e instituciones cuyo principal mandato sea ejecutar y garantizar el cumplimiento de las leyes que emanen al respecto.

Respecto a la formación de profesionales de seguridad cibernética, el país cuenta con muy pocas vías para lograr satisfacer la demanda que tiene de los mismos. Según lo publicado en el portal del Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM), para 2019 se necesitarán 148,052 puestos laborales en materia de seguridad cibernética [18]. Este dato es alarmante si se considera que, al revisar la oferta académica de las mejores cinco universidades del país, sólo cuatro de ellas ofrecen estudios de posgrado relacionados con la seguridad cibernética, y ni uno de estas ofrece educación profesional a nivel licenciatura relacionada con este campo.

Lo presentado en este capítulo es coherente con los informes internacionales mencionados en los que se señala que México es un país de madurez mediana en las cuestiones políticas, regulatorias, académicas y culturales relacionadas con la seguridad cibernética. Y aunque, sin duda hay sectores que han avanzado más en la materia, ninguno de nuestros sectores ha alcanzado un desarrollo óptimo en cuanto a seguridad cibernética se refiere. En ese tenor de ideas parece preciso recalcar lo señalado en el informe Índice Global de Seguridad Cibernética 2017 de la UIT mencionado en el cuerpo del capítulo, en donde se señala que si México cuenta con un estado de madurez media es, en cierta medida, porque el mundo en general se encuentra rezagado respecto a las mejores prácticas de seguridad cibernética. Esto implica una gran área de oportunidad para mejorar, pero sin duda implica también que México es un país altamente vulnerable a las amenazas del entorno cibernético.

Referencias del Capítulo III

[1] Kaspersky Lab (2017). *CIBERAMENAZA; Mapa en tiempo real*. Recuperado en junio de 2017 de https://cybermap.kaspersky.com/es/

[2] Cifras del Instituto Federal de Telecomunicaciones (2017). Banco de Información de Telecomunicaciones. Recuperado de https://bit.ift.org.mx/BitWebApp/

[3] Ibíd.

[4] Arreola, Javier & Murillo, Juan Carlos (2016*).* Ciberseguridad (casi) a prueba del enemigo 'invisible'. *Forbes México*. Recuperado de https://www.forbes.com.mx/ciberseguridad-casi-prueba-del-enemigo-invisible/

[5] Unión Internacional de Telecomunicaciones (2017). *Global Cybersecurity Index* 2017, Recuperado de https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

[6] Gobierno de la República de los Estados Unidos Mexicanos (2013). *Plan Nacional de Desarrollo 2013-2018*. Recuperado de http://www.dof.gob.mx/nota_detalle_popup.php?codigo=5299465

[7] Gobierno de la República de los Estados Unidos Mexicanos (2014). *Programa para la Seguridad Nacional 2014-2018; Una política multidimensional para México en el siglo XXI*. Recuperado de http://www.dof.gob.mx/nota_detalle.php?codigo=5342824&fecha=30/04/2014

[8] Secretaría de Gobernación & Secretaría de la Función Pública (2014). *Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como establecer el Manual Administrativo de Aplicación General en dichas materias*. Recuperado de http://www.dof.gob.mx/nota_detalle.php?codigo=5343881&fecha=08/05/2014

[9] Presidencia de la República de los Estados Unidos Mexicanos (2010). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. Recuperado de http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

[10] Presidencia de la República de los Estados Unidos Mexicanos (2017). *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*. Recuperado de http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017

[11] Sánchez, Julio (2017). México ya es el más afectado por el WannaCry en América Latina, *El Economista*, Recuperado de https://www.eleconomista.com.mx/tecnologia/Mexico-ya-es-el-mas-afectado-por-el-WannaCry-en-America-Latina-20170515-0056.html

[12] CNS (2017). Boletín: CNS, a través de la División Científica de la PF, instrumenta acciones ante ataque cibernético internacional. México. Recuperado de https://www.gob.mx/policiafederal/prensa/cns-a-traves-de-la-division-cientifica-de-la-pf-instrumenta-acciones-ante-ataque-cibernetico-internacional

[13] DGTIC (2017). *Informes trimestrales 2017.* México: UNAM. Recuperado de https://www.seguridad.unam.mx/boletines

[14] Sánchez Onfore, Julio (2017). La OEA llama a reportar incidentes de ciberseguridad. *El Economista*. Recuperado de https://www.eleconomista.com.mx/tecnologia/La-OEA-llama-a-reportar-incidentes-de-ciberseguridad-20170823-0078.html

[15] Sánchez Onfore, Julio (2017). Policía Federal quiere un Consejo Nacional de Ciberseguridad. *El Economista*. Recuperado de https://www.eleconomista.com.mx/tecnologia/Policia-Federal-quiere-un-Consejo-Nacional-de-Ciberseguridad-20170719-0101.html

[16] Instituto de Investigaciones Jurídicas (1991*). Diccionario Jurídico Mexicano*. México: Porrúa.

[17] Comisión Especial Tecnologías de Información y Comunicación (2016). *Programa de Trabajo de la Comisión Especial de Tecnologías de Información y Comunicación Segundo Año Legislativo*. México: Cámara de Diputados. Recuperado de http://www5.diputados.gob.mx/index.php/camara/Comision-Especial-Tecnologias-de-Informacion-y-Comunicacion/Programa-de-Trabajo

[18] Chávez, Gabriela (2016). *México no tiene expertos suficientes en ciberseguridad, Revista del Instituto Tecnológico y de Estudios Superiores de Monterrey*, Recuperado de http://tecreview.itesm.mx/mexico-no-tiene-expertos-suficientes-en-ciberseguridad/

Capítulo IV: Conclusiones

A lo largo de los capítulos anteriores se han puesto sobre la mesa los elementos necesarios para fortalecer la seguridad cibernética de México. Esto se ha logrado a través del análisis de regulaciones propuestas por instituciones internacionales, políticas regulatorias de países seleccionados estratégicamente, y un análisis de la situación actual de México en esta materia.

Tomando en cuenta todos estos elementos, es el objetivo de este capítulo es presentar una recomendación fundamentada en los análisis presentados.

Del segundo capítulo se desprende que el núcleo de toda mejora sustantiva en la seguridad cibernética de un país es consecuencia de una estrategia nacional de seguridad nacional. Esto hace sentido si se considera que el entorno digital y las amenazas adjuntas a él son relativamente nuevos comparándose con la institución de los aparatos gubernamentales como lo es el estado, las constituciones y las leyes que de ellas emanan.

Se necesita establecer una Estrategia Nacional contra las amenazas cibernéticas, para producir entornos digitales seguros, con la participación de todos los sectores interesados y que tengan intereses en los mismos.

En los párrafos subsecuentes se mencionan los puntos fundamentales que deberían formar parte de la estrategia nacional:

- Normativo.

La necesidad de este punto emerge al considerar que México mantiene un crecimiento constante en el consumo de ancho de banda. Las principales instituciones responsables de este fenómeno son la Secretaría de Comunicaciones y Transportes (“SCT”), manteniendo una política pública en favor de la conectividad en México, como el programa “México Conectado”, y el IFT, atendiendo la regulación técnica y económica del sector.

A pesar de las funciones que tienen atribuidas estos dos Organismos del Gobierno, no queda claro quién es el responsable de procurar la seguridad cibernética ni a qué grado. Esto principalmente porque la seguridad cibernética va más allá de las funciones atribuidas a estos Organismos, y dista mucho de ser una de sus preocupaciones principales. Por lo tanto, aunque se lleguen a emprender pequeñas acciones para fortalecer algún aspecto de la seguridad, como los programas antes mencionados, no se lograrán atender todas las necesidades correspondientes a la seguridad cibernética nacional con el marco institucional actual.

El ideal de este punto sería contar con un Órgano Autónomo facultado para emitir una normativa de esta materia, general vinculación institucional con las demás oficinas del gobierno, especialmente con aquellas responsables de la política pública en materia digital, y contar con un presupuesto suficiente para poder realizar campañas eficientes en materia de educación cibernética. De tal forma que se establezca un

marco institucional claro que garantice que las responsabilidades y las modalidades de implementación sean claras y que las instituciones tengan la autoridad y los recursos para actuar.

En este orden de ideas, la institución encargada de emitir la normativa en materia de seguridad cibernética debe de obligar a la industria a adoptar normas internacionales que les permitan hace frente a las necesidades del sector. Según las necesidades de cada giro industrial, se deben definir los niveles de exigencia, ya que es evidente que el grado de responsabilidad que tendrá cada agente de este sector, dependerá en gran medida del nivel de involucramiento en el ámbito digital que sus labores.

Un punto altamente aplicable a México que se puede aprender del análisis presentado en el Capítulo II, es la colaboración entre la industria y gobierno en este sector. Mantener un canal de comunicación fluido entre estos entes respecto a las amenazas cibernéticas que surjan en el día a día servirá para mantener un frente amplio ante las mismas. Incluso no se debe descartar aplicar un modelo similar al que opera en los países más desarrollados en este sector, donde algunos agentes de la industria son obligados a entregar un reporte anual con todos los incidentes de seguridad cibernética que fueron detectados en dicho periodo.

En ese sentido, la creación de una autoridad regulatoria en materia de seguridad cibernética obligadamente debe figurar dentro de una estrategia nacional. Pues desde ella se impulsaría estrechamente el trabajo conjunto entre el sector público y privado, así como el apego a los estándares, normas, convenios y buenas prácticas internacionales que al respecto se definan.

Adicionalmente, se debe tener muy en claro una visión prospectiva de la seguridad cibernética. En ese sentido, la institución mexicana que sea la encargada de abordar los aspectos normativos del campo, debe tener en cuenta la acelerada evolución que acompaña a las tecnologías cibernéticas, en el entendido que estas tecnologías pueden ser utilizadas tanto para proteger a las redes de la nación, como para amenazar a las mismas.

Por último, el ente gubernamental encargado de normar las cuestiones que se desprendan de la seguridad cibernética, debe procurar una participación activa en el entorno internacional.

- Marco Jurídico

México tiene un nivel aceptable en los aspectos legales del sector que nos ocupa, si se compara con el resto del mundo, pero atrasado, si se compara con las legislaciones más exigentes en la materia. Por lo tanto, aún se pueden señalar algunos aspectos esenciales para fortalecer este aspecto.

Se puede encontrar que los fundamentos legales de un Gobierno que busque fortalecer la seguridad cibernética de su nación, debe estar:

- Basada en riesgos: esto porque las amenazas cibernéticas vienen en diversas formas y magnitudes, teniendo un impacto particular en la sociedad cada una de ellas. Establecer una jerarquía de prioridades, basada en una evaluación objetiva del riesgo implicado, encabezada por los sectores

más críticos, podría ser un punto de partida efectivo para garantizar que las medidas de defensas cibernéticas se centran en aquellas amenazas cuyo potencial de daño es mayor;

- Neutralidad tecnológica: se trata de un enfoque vital para la seguridad cibernética. Este punto garantiza una posibilidad de acceso a los servicios más seguros y a las soluciones más eficientes del mercado. Establecer requisitos específicos o políticas que exigen el uso de tecnologías exclusivas sólo socavan la seguridad al restringir la evolución de los controles de seguridad y las mejoras tecnológicas, creando potenciales puntos de falla;

- Integrativa: es indispensable que, desde el marco legal aplicable a la seguridad cibernética, se busque que se involucre al mayor número de grupos de interesados y de personas activas en el sector. No dar claridad en este punto generaría barreras a la entrada a sectores de la población que podrían aportar a este campo. Aunado a lo anterior, una intervención normativa desproporcionadamente intrusiva podría resultar contraproducente, y derivaría en una falta de interés por parte de la industria en la colaboración con el gobierno;

- Flexible: se debe de entender que la gestión de los riesgos cibernéticos no puede ser abordada desde un enfoque único. Cada sector industrial, sistema y/o empresa se enfrenta a desafíos particulares, por ello, el marco legal debe considera cierta flexibilidad para atender sus necesidades únicas, sin permitir defensas laxas por parte de la industria, y

- Respeto de la privacidad y las libertades civiles: El marco legal aplicable debe de estar debidamente equilibrado entre la seguridad y las necesidades de protección de la privacidad y las libertades civiles. Garantizar que los requisitos y las obligaciones que se establezcan en una nueva legislación no representarán una intrusión en los derechos fundamentales más allá de lo estrictamente necesario, que seguirán los debidos procesos y que las acciones contenidas en dicha legislación contarán con el respaldo de una apropiada supervisión judicial, son consideraciones importantes a abordar en cualquier marco de seguridad cibernética.

Aunado a lo anterior, y al considerar que el tema es altamente complejo y evoluciona constantemente, la Estrategia Nacional debe impulsar la creación de Comisiones de Estudio ordinarias en las Cámara que componen el Congreso de la Unión que estudien y propongan legislación específicamente temas de seguridad cibernética.

- Política pública

Un aspecto fundamental de las estrategias exitosas de seguridad cibernética es la promoción de una cultura digital.

En el caso de México, se ha promovido una política pública para que cada vez más miembros de la población tengan acceso al mundo digital, y se ha realizado un buen trabajo por parte del Gobierno Federal, como lo muestra el Gráfico 4.1, los sitios y espacios públicos con acceso a internet han aumentado más de

10 veces en los últimos 6 años. Esto es un avance significativo en la inclusión de la población al mundo digital, aunque la capacidad de transmisión es muy limitada.

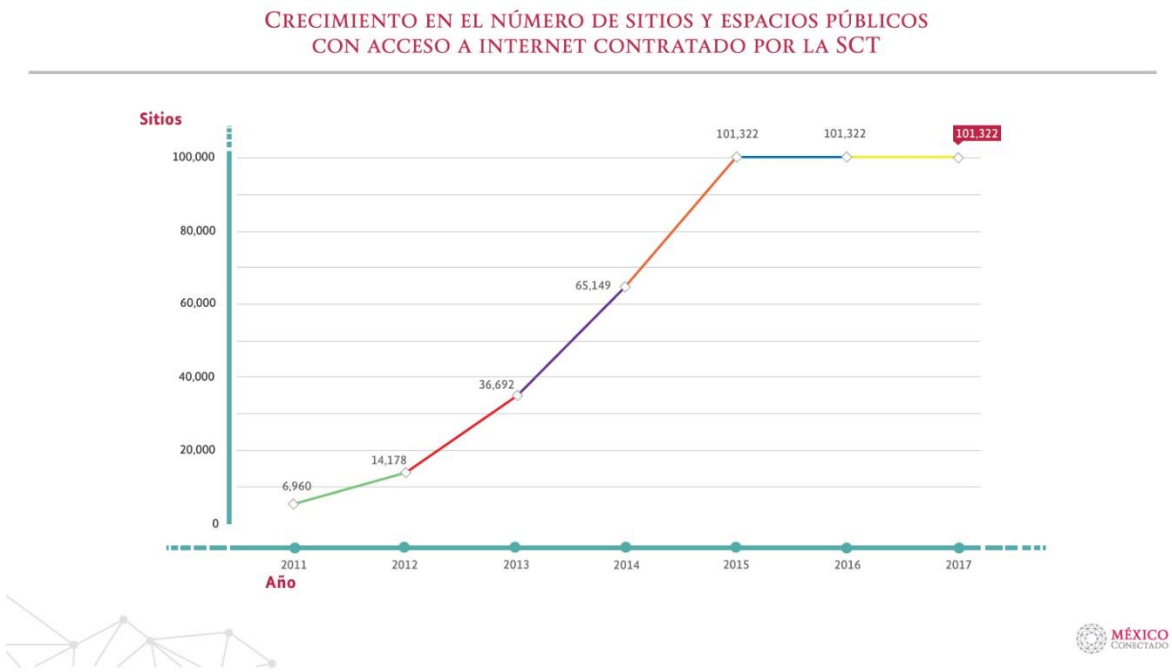


Gráfico 4.1: Crecimiento en el número de sitios y espacios públicos con acceso a internet contratado por la SCT[26]

Sin embargo, no se puede decir lo mismo de las políticas públicas emprendidas por el gobierno mexicano para generar una cultura digital en sus usuarios de internet. Tal es el caso que, para agosto de 2017, los sitios web de las principales políticas públicas en materia de conectividad (México Conectado y la Estrategia Nacional Digital) no proporcionaban a quienes las visitaba algún documento informativo, contenido multimedia o infografía que señale las buenas prácticas que debe seguir un usuario para mantenerse seguro en la red.

Los esfuerzos más destacables en este aspecto son los emprendidos por el IFT Sin embargo, es importante recordar que el IFT no es un organismo gubernamental orientado a la implementación de políticas públicas, sino que es un órgano regulador autónomo, y como tal, los alcances de sus esfuerzos en este aspecto no tienen la fuerza suficiente para generar un impacto profundo en las conductas digitales de la población.

[26] Secretaría de Comunicaciones y Transportes, 2017, Crecimiento en el número de sitios y espacios públicos con acceso a internet contratado por la SCT, Recuperado en agosto de 2017 de http://mexicoconectado.gob.mx/carousel.php?id=80&cat=80&id_carrusel=2

Discutir si la política pública en seguridad cibernética debe de ser llevada por una aérea especifica de la actual Secretaría de Comunicaciones y Transportes o por una nueva Secretaría con funciones específicas en seguridad cibernética, no obedecen a los objetivos de esta tesis. No obstante lo anterior, es indispensable que haya un órgano gubernamental encargado de emprender los proyectos de política pública que procuren mantener un elevado nivel de conciencia digital en los usuarios de internet en México.

Para lograr ese objetivo, dicha política pública debe enfocarse, en un inicio, en generar en el usuario de internet una cultura de prevención que pretenda, cuando menos, los siguientes puntos:

- Lectura de términos y condiciones (constituye una medida enfocada en hacer frente a esa gran cantidad de aplicaciones móviles y servicios digitales que roban la información del usuario y hacen mal uso de ella);

- Criterios para saber si se está infectado: enseñar al usuario a identificar cuando un dispositivo presente:
    - Lentitud;
    - Pérdida de información;
    - Mal funcionamiento del equipo;
    - Daño de información;
    - Actividad inusual como consumo de energía irregular, y/o
    - Detección del software de seguridad

- Explicar que todos los dispositivos conectados a la red pueden ser objeto de un ataque cibernético, y

- Medidas preventivas
    - Realizar respaldos de información
    - Actualización del sistema operativo
    - Verificar que las unidades exteriores no estén comprometidas
    - Revisión cuidadosa del correo electrónico
    - No instalar software de dudosa procedencia
    - Aprender a diferencia páginas fraudulentas y evitarlas
    - Ser intuitivo y desconfiado

- Académico

México enfrenta una creciente necesidad de profesionales en cuestiones relacionadas a la seguridad de la información y la seguridad cibernética, y a pesar de los esfuerzos emprendidos por algunas instituciones educativas, esta necesidad se mantiene.

Una estrategia mexicana de seguridad cibernética debe de incitar a la academia a producir profesionales en el sector, así como incentivar desde edad temprana a involucrarse en aspectos relacionados con la materia. Este último punto es muy importante, pues no existe una edad mínima para

involucrarte en el entorno digital, y prácticamente todas las conductas que reflejan los usuarios en el mismo fueron adquiridas de forma empírica. En ese sentido, se puede decir que los usuarios de internet son el eslabón más débil en la cadena se seguridad cibernética.

Los equipos digitales de los usuarios sin experiencia en seguridad de la información, son más propensos a ser infectados con malware y, consecuencia de eso, son más propensos a ser utilizados en ataques orquestados por delincuentes cibernéticos.

Por lo anterior, es fundamental que la academia se preocupe por impulsar el conocimiento de seguridad cibernética en todos los niveles educativos.

Fundamentalmente, una Estrategia Nacional en la materia debe impulsar e incentivar la formación de profesionales de la seguridad cibernética en las universidades públicas, y para ello el Estado Mexicano cuenta con instituciones sólidas y capaces como la propia Universidad Nacional y el Insultito Politécnico Nacional, entre otras.

Finalmente, es preciso agregar que las características de una perfecta estrategia de seguridad podrían no terminar de escribirse. Sin embargo, con base en el análisis hecho a lo largo de esta tesis, se considera que los puntos presentados con anterioridad señalan consideraciones esenciales en la formación de una estrategia de seguridad cibernética aplicable a México.

Para recalcar algunos puntos esenciales, se debe enfatizar en que las tecnologías digitales avanzan mucho más rápido de lo que la legislación, normalización y regulación pueden hacerlo hoy en día, es por ello que se considera que uno de los principales objetivos de una estrategia de seguridad cibernética es una política pública encaminada a educar, desde los niveles más básicos hasta la formación de profesionales de calidad, en cuestiones de la seguridad cibernética y las buenas costumbres del entorno digital. En imperativo recordar que el eslabón más débil en la cadena de seguridad de la información es el usuario mismo, y aquel usuario ignorante de las cuestiones de seguridad cibernética representa un peligro para él y para la sociedad misma.

Por último, me parece favorable hacer hincapié en que una óptima estrategia de seguridad nacional en México, y en cualquier parte del mundo, debe de obedecer a un principio de integración entre todas las partes interesadas. Principio en el que el Gobierno Mexicano tiene mucho por hacer, ya que ciertos errores de las administraciones que han gobernado la nación, han generado una desconfianza entre la sociedad civil y el gobierno, desconfianza que en nada ayuda a la formación de estrategias que impliquen la posibilidad de ejercer violaciones arbitrarias a la privacidad de las personas.

Bibliografía

Benoliel, D. (2015). *Towards a Cyber Security Policy Model – Israel National Cyber Bureau (INCB) Case Study.* Haifa: University of Haifa Faculty of Law.

Calder, A., & Watkins, S. (2008). *IT governance : a manager's guide to data security and ISO 27001/ ISO 27002.* Kogan page.

Clausius, R. (1865). *The Mechanical Theory of Heat with Its Aplications to the Steam-Engine and the Physical Properties of Bodies .*

Cooperative Cyber Defence Centre of Excellence (NATO). (2017). *National Cyber Security Organisation: ISRAEL.* Tallinn, Estonia: NATO CCD COE.

Instituto Colomabiano de Nomras Técnicas y Certificación, ICONTEC. (2013). *Compendio Seguridad de la Información .* Bogotá: Legis.

Jacobs, S. (2014). *Security management of next generation telecommunications networks and services.* Hoboken, Nueva Jersey.: IEEE.

Liskov, M., Rivest, R. L., & Wagner, D. (2010). Tweakable Block Ciphers. *Journal of Cryptology*, 588-613.

Muñoz, S. (2000). *La regulación de la red; Poder y Derecho en Internet .* Madrid, España : taurus.

Reziouk, A., Laurent, E., & Demay, J. C. (2016). Practical security overview of IEEE 802.15.4. *International Conference on Engineering & MIS* (págs. 1-9). IEEE.

Schmidt, E., & Cohen, J. (2012). *El futuro digital.* Nueva York: Anaya.

Suk Kim, P., & Chung, C.-S. (2016). Una revisión histórica del desarrollo del gobierno electrónico en Corea del Sur. *Gestión y Política Pública, vol. XXV, núm. 2*, 627-662.

The Software Alliance. (2015). *Asia-Pacific Cybersecurity Dashboard.* Washington: BSA.

The Software Alliance. (2015). *EU Cybersecurity Dashboard.* Washington: BSA.

WORKING GROUP 5: CYBER SECURITY INFORMATIONSHARING. (2017). *FINAL REPORT.* CSRIC.

WORKING GROUP 7: Cybersecurity Workforce. (2017). *Cybersecurity Workforce Development. Best Practices Recommendations.* CSRIC.

WORKING GROUP 9: Wi-Fi Security . (2017). *Final Report – Wi-Fi Security Best Practices .* CSRIC.