INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

“PLAN ESTRATÉGICO PARA LA CREACIÓN DE LA UNIDAD INTELIGENTE DE CIBERSEGURIDAD PARA LA ADMINISTRACIÓN PÚBLICA FEDERAL MEXICANA”

SOLUCIÓN ESTRATÉGICA
Que para obtener el grado de MAESTRO EN GESTIÓN DE INNOVACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Presenta:

Edgar Gutiérrez García

Asesor:

Dr. Ricardo Marcelín Jiménez

Ciudad de México, a 31 de agosto de 2020.

INFOTEC POSGRADOS

AUTORIZACIÓN DE IMPRESIÓN Y NO ADEUDO EN BIBLIOTECA

MAESTRÍA EN GESTIÓN DE INNOVACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Ciudad de México, 5 de noviembre de 2019
INFOTEC-DAIC-GCH-0513/19.

La Gerencia de Capital Humano / Gerencia de Investigación hacen constar que el trabajo de titulación intitulado

PLAN ESTRATÉGICO PARA LA CREACIÓN DE LA UNIDAD INTELIGENTE DE CIBERSEGURIDAD PARA LA ADMINISTRACIÓN PÚBLICA FEDERAL MEXICANA

Desarrollado por el alumno **Edgar Gutiérrez García** y bajo la asesoría del **Dr. Ricardo Marcelín Jiménez**; cumple con el formato de biblioteca. Por lo cual, se expide la presente autorización para impresión del proyecto terminal al que se ha hecho mención.

Asimismo se hace constar que no debe material de la biblioteca de INFOTEC.

Vo. Bo.

Mtra. Julieta Alcibar Hermosillo
Coordinadora de biblioteca

***Anexar a la presente autorización al inicio de la versión impresa del trabajo referido que ampara la misma.**

C.p.p Servicios Escolares

Agradecimientos

“Quiero agradecer a Patricia Libertad Castro Flores por su incondicional apoyo y por creer siempre en mí, me impulso a nunca rendirme y continuar con este proyecto. Por otra parte, quiero agradecer a mi madre María Elia García, mi tía Leticia García y al Dr. Jorge Aguilar Cortes quienes son mis pilares y que nunca han dejado de apoyarme y creer en mí. Así mismo, agradezco a INFOTEC y al CONACYT por el apoyo brindado”.

-Edgar Gutiérrez García

Dedicatoria

“Este proyecto se lo dedico a todas las personas que creen que la tecnología de la información es un medio que nos ayuda a hacer más fácil nuestras vidas, que nos impulsa a reinventarnos y ser mejores cada día. También a todas las personas que de forma directa o indirecta me ayudaron a terminar este proyecto”.

Tabla de contenido

Índice de figuras

Índice de gráficos

Índice de cuadros

Siglas y abreviaturas

APF: Administración Pública Federal.

ASI: Administración de Seguridad de la Información.

CERT: Equipo de Respuestas a Incidentes de Seguridad.

CESI: Comité Especializado en Seguridad de la Información.

CFO: Chief Finantial Officer.

CIDGE: Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico.

CIO: Chief Information Officer.

CISEN: Centro de Investigación y Seguridad Nacional.

CONACYT: el Consejo Nacional de Ciencia y Tecnología.

ENC: Estrategia Nacional de Ciberseguridad.

IFT: Instituto Federal de Telecomunicaciones.

INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

PGCM: Programa para un Gobierno Cercano y Moderno.

PGR: Procuraduría General de la Republica.

TIC: Tecnologías de la Información y la comunicación.

PND: Plan Nacional de Desarrollo.

UIT: Unión Internacional de Telecomunicaciones.

UIC: Unidad Inteligente de Ciberseguridad.

PF: Policía Federal.

SFP: Secretaría de la Función Pública.

Resumen Ejecutivo

Durante la última década, el Gobierno Mexicano ha elaborado estrategias conforme al Plan Nacional de Desarrollo 2013 - 2018 (PND.gob.mx, 2013) para abordar los problemas relacionados con la seguridad de la información, asociados con el uso y la rápida expansión de las tecnologías de la información y la comunicación (TIC).

Estas cuestiones de seguridad de la información se han convertido en un problema importante a nivel nacional que requieren una atención inmediata del Gobierno Mexicano, incluida la protección de los activos críticos, sistemas y redes vitales para el funcionamiento y la estabilidad del país.

Las amenazas contra estos activos críticos incluyen los delitos informáticos como el robo de identidad y fraude, "hacktivismo" ("Overview", 2017) por motivos políticos y espionaje sofisticado económico y militar.

Al día de hoy, no está publicada en el diario oficial de la federación una estrategia nacional de ciberseguridad que proteja tanto a las oficinas del gobierno mexicano, como a sus activos críticos que proporcionan servicios básicos y elementales como lo son: el acta de nacimiento, identificación oficial, licencia de manejo, pasaporte, entre otros servicios que se brindan a la ciudadanía mexicana.

Por lo que, en este proyecto se desarrolla una propuesta de un plan estratégico que permita la creación de un organismo regulador y/o unidad inteligente en materia de ciberseguridad que tenga como objetivo principal el aseguramiento de los activos críticos de todo el gobierno mexicano mediante la implementación de una estrategia de ciberseguridad respaldada por el primer mandatario de México.

Por otra parte, ayudar con la identificación de entidades educativas y del sector privado que sean claves para crear alianzas estratégicas que permitan

proveer tecnología e investigación, aportando recursos en investigación y desarrollo (I+D) al plan estratégico de este proyecto.

Por último, generar un plan de concientización para los mexicanos que les permita navegar de manera segura en el ciberespacio, mitigando posibles amenazas de fraude electrónico, robo de información, basado en las mejores prácticas en materia de seguridad de la información.

Introducción

Las tecnologías de la información están altamente integradas en nuestras vidas. Como una sociedad, estamos en una época digital en donde se aprende, se juega, se socializa, se comunica y se hacen negocios en línea. Mientras que el ciberespacio brinda grandes beneficios, así como nuestra incondicional confianza en él, crea nuevas y significantes vulnerabilidades que pudieran comprometer la información crítica para los usuarios finales. En línea con el compromiso del Gobierno Mexicano para mantener una nación segura y próspera se lanzó el Plan Nacional de Desarrollo 2013 – 2018 (PND.gob.mx, 2013), aprobado por decreto en el Diario Oficial de la Federación el 20 de mayo de 2013, el cual propone un "Programa para un Gobierno Cercano y Moderno (PGCM)" *("Programa para un Gobierno Cercano y Moderno (PGCM)", 2017)* que permita simplificar los procesos gubernamentales en México con el uso adecuado de los recursos públicos con el uso de las tecnologías de la información y comunicación.

¿Qué es la "Ciberseguridad"?
"Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados" (Azcona, 2018).

Cuadro 1 - Definición de Ciberseguridad – Fuente: (Azcona, 2018)

De acuerdo con lo anterior, El Gobierno Mexicano está consciente de la importancia de la seguridad de la información y que es necesario contar con un organismo que tenga las facultades para poder ayudar, promover y auditar las adquisiciones tecnológicas, así como los procesos y procedimientos en materia de seguridad de la información en

la Administración Pública Federal. Por otra parte, la “Ciberseguridad” se ha convertido en una prioridad del Gobierno Mexicano. La mayoría de los ciberataques, fuga de información y afectaciones de los sistemas públicos y privados han sido titulares en los diferentes medios de comunicación. Es clara la necesidad de tomar acciones para mejorar la ciberseguridad en el Gobierno Federal de México. Actualmente, la Administración Pública Federal en México cuenta con diversas unidades de inteligencia que funcionan de manera desconcentrada, pero no existe una colaboración eficiente entre las dependencias y que sea respaldada por el primer mandatario del Gobierno Mexicano. Por lo anterior, sería de gran beneficio para la Administración Pública Federal contar con un organismo que tenga las facultades anteriormente mencionadas y que pueda trabajar y apoyar de forma transversal con cada una de las dependencias del Gobierno Federal Mexicano.

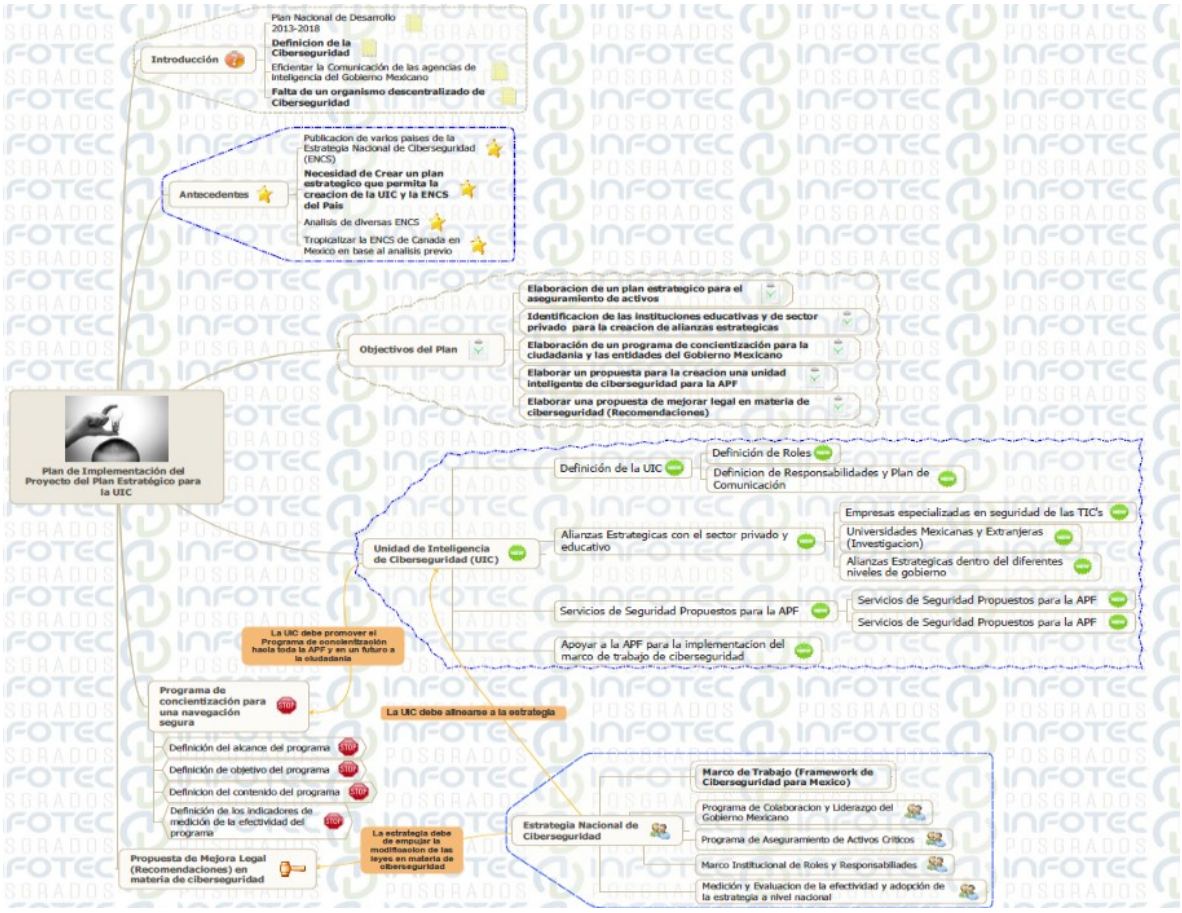


***Figura 1*- Mapa Mental del Proyecto Fuente: Elaboración Propia**

Objetivos del Proyecto

Objetivo General

Elaborar un plan estratégico para la creación de la unidad inteligente de ciberseguridad para la Administración Pública Federal Mexicana con base en las mejores prácticas de diversas estrategias nacionales de ciberseguridad, a través de la conformación de un plan de colaboración y liderazgo, perfiles especializados y adquisición de herramientas tecnológicas que permita cumplir con el objetivo estratégico de la misma, con la finalidad de asegurar los activos críticos del Gobierno Federal Mexicano.

Objetivos Particulares

Los objetivos particulares de este proyecto son los siguientes:

- Elaboración de un plan estratégico que permita el aseguramiento de los sistemas de información del gobierno.
- Identificación de entidades educativas y del sector privado que sean claves para crear alianzas estratégicas y poder asegurar los activos críticos del Gobierno Mexicano.
- Elaboración de un programa de concientización que permita ayudar a la ciudadanía para navegar de forma segura en el ciberespacio.
- Elaboración de una propuesta para la creación de la unidad inteligente de ciberseguridad que se encargará de la protección de los activos críticos de tecnologías de la información del Gobierno Mexicano.

Antecedentes

Durante el periodo de 2009-2011 varios países desarrollaron y publicaron su **estrategia nacional de ciberseguridad (ENC)**, la cual tiene como objetivo principal mitigar las amenazas cibernéticas y aunque se pensaría que tienen el mismo enfoque se ha encontrado que todas tienen al menos una definición y alcance de la ciberseguridad. Dentro del periodo mencionado, los países que destacaron con la publicación e implementación de su ENC son los siguientes: Canadá, Republica Checa, Francia, Alemania, Japón, Gran Bretaña, Holanda y Estados Unidos.

Por otra parte, para poder formalizar esta solución estratégica fue necesario realizar un análisis entre las diversas ENC que actualmente están vigentes y que han sido casos de éxito. A partir de esto, se propone tomar como base el análisis de estas ENC para la creación del plan estratégico de una unidad inteligente de ciberseguridad para la Administración Pública Federal en México. Una de las primeras acciones que se realizaron durante el análisis fue la de encontrar los objetivos y acciones comunes de cada una. Por otro lado, se hizo un comparativo de cada una de las estrategias. Para esto, se analizó trece puntos diferentes los cuales se detallarán más adelante. Para poder ejecutar este análisis, se eligieron cuatro ENC, las cuales son las siguientes: **Canadá, Republica Checa, Estados Unidos y Reino Unido**. Para esto, fue necesario revisar los siguientes puntos por cada estrategia:

1. ¿Qué significa el término de “Ciberseguridad” para estos países?
2. ¿Cuáles son las amenazas percibidas que enfrentan las diferentes ENC?
3. ¿Cuál es el alcance de las ENC?
4. ¿Existe una relación con otras estrategias nacionales?
5. ¿Cuáles son los objetivos estratégicos y principios rectores de la ENC?
6. ¿Qué grupos de interés se abordan y cómo se abordan?

7. ¿Cuáles son las líneas de acción clave y las acciones planificadas?

8. ¿Están cubiertas las nuevas amenazas?

9. ¿Cómo se institucionalizan las funciones nacionales de las ENC?

Una vez seleccionadas las ENC, se determinó el primer punto de este análisis, el cual se refiere a la definición o entendimiento de la ciberseguridad dentro de la ENC. A continuación, se detalla cada una de las definiciones encontradas:

País	¿Cuenta con una Definición?	La Ciberseguridad es…
Canadá	Si cuenta	"Un nivel apropiado de respuesta y / o mitigación a los ciberataques - el acceso, uso, manipulación, interrupción o destrucción intencionados o no autorizados (por medios electrónicos) de información electrónica y / o infraestructura física y electrónica utilizada para procesar, comunicar y/o almacenar esa información". (Bologna, Hämmerli, Gritzalis, & Wolthusen, 2011). Adicionalmente, Canadá cuenta con eslogan oficial que dice "La ciberseguridad es importante para todos, todos los días. Es importante para un Canadá más seguro y próspero." ("Canada's Cyber Security Strategy", 2010).
República Checa	Sin definición[1]	No está definida dentro de su ENC.
Estados Unidos	Utiliza un término Implícito	Un término implícito de seguridad de la información.
Reino Unido	Si cuenta	"La ciberseguridad abarca tanto la protección de los intereses del Reino Unido en el espacio cibernético, como la búsqueda de una política de seguridad con mayor alcance mediante la explotación de las oportunidades que ofrece el espacio cibernético". (Assets.publishing.service.gov.uk, 2011).

Cuadro 2 - Definiciones de ciberseguridad -Fuente: Elaboración propia

La primera observación que obtuvimos con este primer punto analizado, es que no existe un término único a nivel internacional, para la ciberseguridad. Cada país tiene su propia definición o interpretación de la misma. Esta observación, es un punto muy importante que se deberá permear dentro de todas las dependencias del Gobierno Federal de México.

Otro punto observado, es que Canadá y Reino Unido proveen una definición para la ciberseguridad e indica lo que para ellos significa. Por otra parte, la Republica Checa, no cuenta siquiera con una definición de lo que es para ellos la ciberseguridad. Estados Unidos simplemente hace una referencia implícita de este término como seguridad de la información.

A continuación, se identificó otro punto adicional que sirve para identificar las diferencias entre las ENC y es el siguiente: se detecta que existen países que publican su ENC en diferentes idiomas como es el caso de Canadá que publicó su ENC tanto en inglés como en francés. Por otra parte, la Republica Checa cuenta con dos versiones de su ENC, una en inglés y la otra en el idioma checo.

El siguiente punto a revisar es el alcance de las ENC, ya que algunas estrategias limitan su alcance únicamente a los activos conectados al ciberespacio (Internet), dejando fuera del alcance de la estrategia de ciberseguridad a otros activos de TIC's.

Otro punto de revisión importante es la relación de las ENC con las estrategias de seguridad nacional de sus países (si están referenciadas o se mencionan explícitamente). Las siguientes ENC que tienen esta relación son las siguientes: 1) Reino Unido; 2) Australia; 3) Canadá; 4) Republica Checa; 5) Francia; 6) Alemania y 7) Estados Unidos por mencionar algunas.

---

[1] **National Cyber Security Centre of Czech Republic (Govcert.cz, 2017) – "**La ciberseguridad comprende una suma de medidas y herramientas organizativas, políticas, legales, técnicas y educativas que permite proporcionar un ciberespacio seguro, protegido y resistente en la República Checa para el beneficio de los sectores público y privado, así como la ciudadanía en general".

Por otra parte, un análisis de riesgos y de amenazas a nivel nacional es el principal instigador para el desarrollo de cualquier ENC. Lo anterior, se debería integrar en un registro nacional de análisis de riesgos de forma anual. Como resultado de lo anterior, este registro podría ser un diferenciador que permita la actualización de cualquier ENC.

Aunque mayoría de las ENC's mencionadas previamente en la *"TABLA 1 DEFINICIONES DE CIBERSEGURIDAD"* mencionan explícitamente las posibles amenazas de ciberseguridad hacia las infraestructuras críticas (IC), la relación entre la ENC y las estrategias existentes que protegen las actuales IC no se mencionan claramente. Por otra parte, ninguna de las ENC's de origen europeo hace referencia al programa europeo sobre protección de las IC (EPCIP).

Aunado al punto anterior, las ENC's mencionadas en la *"TABLA 1 DEFINICIONES DE CIBERSEGURIDAD"* de origen europeo (Reino Unido y Republica Checa) abordan aspectos económicos referentes al ciberespacio. La ciberseguridad es considerada como un requisito mínimo para mejorar la prosperidad de la población y fomentar el bienestar económico.

La Agenda Digital de la Comunidad Europea deberá ser un motor de las actividades de ciberseguridad de los 28 países miembros europeos y solamente Alemania y Holanda hacen referencia a su agenda digital respectivamente.

Es importante mencionar que la mayoría de las ECNs revisadas en este documento se enfocan únicamente el cibercrimen[2] en general y el espionaje electrónico como una amenaza. Así como, solamente un pequeño grupo países consideran estas amenazas como temas de seguridad nacional. Finalmente, hay un aspecto que no se muestra dentro de las ENC's analizadas y es sobre el común entendimiento sobre la amenaza de terrorismo en el ciberespacio. A continuación, se muestra una tabla comparativa de las ENC's analizadas:

---

[2]**Cibercrimen –** se refiere al uso de las tecnologías globalizadas de la información y comunicaciones, poniendo especial énfasis al internet, para la comisión de actos delictivos de alcance transnacional (Unodc.org, 2018).

Características a comparar	Canadá	Republica Checa	Estados Unidos	Reino Unido
Idioma de la ENC Algún idioma adicional	Inglés Francés	Checo Inglés	Inglés	Inglés
Fecha de emisión de la ENC	Octubre del 2010	15 de julio del 2011	14 de febrero 2003	25 de junio del 2009
¿Es la primera versión de la ENC?	Si	Si	Si	Si
¿Todas las ciberamenazas dentro de la ENC están enfocadas hacia las TIC?	únicamente a los dispositivos conectados a internet	Si	Si	Implícitamente
¿La ENC tiene relación con la estrategia de seguridad nacional?	Si	Si	Si	Si
¿La ENC explícitamente describe la estrategia de protección de infraestructura crítica?	Si	No	SI	No
¿La ENC tiene relación con la agenda digital nacional de su país?	No	No	No	No
¿La ENC aborda las ciberamenazas a la infraestructura crítica?	Si	Si	Si	No
¿La ENC aborda las ciberamenazas a la prosperidad de la economía?	Si	Si	Si	Si
¿La ENC aborda las ciberamenazas a la seguridad nacional?	Si	Si	Si	Si
¿La ENC aborda las ciberamenazas a la confianza pública en materia TIC?	Si	No	No	No
¿La ENC aborda las ciberamenazas a la vida social de los ciudadanos?	Si	Implícitamente	Si	no

Características a comparar	Canadá	Republica Checa	Estados Unidos	Reino Unido
¿La ENC aborda las ciberamenazas provenientes de organizaciones activistas?	No	No	No	No

Cuadro 3 - Comparativa de estrategias nacionales de ciberseguridad – Fuente: Elaboración propia

Amenazas Identificadas dentro de la ENC	Canadá	Republica Checa	Estados Unidos	Reino Unido
¿La ENC aborda las ciberamenazas provenientes del crimen organizado?	Si	Si	Si	No
¿La ENC aborda las ciberamenazas provenientes del Espionaje?	Si	Si	Si	Si
¿La ENC aborda las ciberamenazas provenientes de países foráneos / guerra cibernetica[3]?	Si	Si	Si	Si
¿La ENC aborda las ciberamenazas provenientes de terrorismo[3]?	Si	Si	Si	Si
¿La ENC aborda las ciberamenazas provenientes de ataques a gran escala?	Implícitamente	No	No	Implícitamente
¿La ENC aborda las ciberamenazas provenientes de desarrollos incompatibles en materia de tecnologías y seguridad?	No	No	No	No

Cuadro 4 - Comparativa de amenazas encontradas en las ENC's – Fuente: Elaboración propia

Como se puede observar las cuatro estrategias de ciberseguridad analizadas tienen enfoques similares y con ciertas diferencias, indicándonos que estas han sido de gran utilidad para estos países, es claro mencionar que ninguna de estas iniciativas es mala, sino que cuentan con niveles de madurez que han ido evolucionando con el paso del tiempo. Las primeras diferencias encontradas en la tabla comparativa anterior, se refieren a la relación respecto a la protección de activos críticos, el cual es un punto medular para la estrategia. Canadá, por su parte, define dentro de su alcance, la protección de activos de su gobierno y toma en consideración un programa de concientización para sus ciudadanos, esto debido a la gran demanda de las iniciativas de gobierno electrónico generando un fuerte vínculo de confianza entre la ciudadanía y el gobierno, que a diferencia de México esto no existe.

Adicionalmente, el gobierno canadiense crea una delta de comunicación muy estrecha entre el gobierno, las universidades y la iniciativa privada mediante un plan de acción y de colaboración que ha permitido la comunicación transparente entre estos tres entes.

---

[3] ***Guerra Cibernética. – "****Se define como el conjunto de acciones llevadas por un Estado para penetrar en los ordenadores o en las redes de otro país, con la finalidad de causar perjuicio o alteración" – Richard Clarke, especialista en seguridad del gobierno estadounidense.*

[4] ***Terrorismo****. - "Cualquier acto destinado a causar la muerte o lesiones a un civil o un no combatiente cuando el propósito de dicho acto sea intimidar a una población u obligar a un gobierno o a una organización internacional a realizar un acto o abstenerse de hacerlo" - El secretario general de la ONU, Kofi Annan dentro de la cumbre de Madrid.*

Capítulo 1

Propuesta de una estrategia de liderazgo y colaboración entre dependencias del Gobierno Federal Mexicano

Capítulo I.- Propuesta de una estrategia de liderazgo y colaboración entre dependencias del Gobierno Federal Mexicano

Es claro que la comunicación entre las diferentes entidades de gobierno y la colaboración en materia de ciberseguridad es desigual. Lo anterior, se debe a los indicadores globales de ciberseguridad que muestra la Unión Internacional de Telecomunicaciones (UIT) colocando a México en el lugar 18 de 164 a nivel global en su ranking global de ciberseguridad, y por debajo de Canadá y Estados Unidos en el continente americano (ITU, 2015). Lo anterior, representa el nivel de preparación y/o compromiso de la ciberseguridad en estos países, mas no la capacidad ni las vulnerabilidades que actualmente cuentan.

Compartir la información de forma proactiva y segura entre las diferentes partes interesadas como lo son: sector privado (proveedor de tecnologías de TIC's) sector educativo (tanto público, como privado) y el mismo gobierno se ha convertido en un punto clave dentro del plan estratégico para la creación de la UIC y la generación de una estrategia de ciberseguridad efectiva para todo el Gobierno Mexicano y la ciudadanía. Un aspecto clave para generar una estrategia de liderazgo y colaboración es la comunicación bidireccional mediante la creación de un programa emblemático de intercambio de información entre los sectores público-privado y poder sumar esfuerzos para el intercambio de información de las dependencias de seguridad nacional.

El objetivo de esta propuesta es la creación de la UIC para que funcione como un centro de actividades de intercambio de información (hub) que permita aumentar la conciencia sobre las amenazas existentes.

La información compartida a través de este programa, permitirá a todas las partes interesadas asegurar de formar eficiente los activos críticos del Gobierno Mexicano, así como ayudar a respaldar la seguridad de los mismos. Por otra parte, este programa proporcionará un entorno de colaboración seguro donde los especialistas en materia de ciberseguridad podrán compartir conocimiento y así

obtener un mejor entendimiento sobre los riesgos emergentes de seguridad cibernética y las defensas efectivas.

Dentro del programa de intercambio de información, se deberá integrar de un grupo de confianza, donde todas las partes interesadas buscaran el beneficio mutuo de un sólido intercambio de información y colaboración. Por lo tanto, todas las empresas y/o universidades interesadas en participar en el programa de colaboración multilateral para el intercambio de información se podrán unir a dicho programa. Los aspectos claves que no se puede olvidar para el intercambio bidireccional de información son los siguientes:

- Los miembros o empresas que formen parte de este programa deberán presentar indicadores de identificación de amenazas cibernéticas las cuales deberán ser compartidas a todos sus miembros.

- Adicionalmente, deberán presentar información sobre incidentes cibernéticos y vulnerabilidades identificadas a la UIC, la cual tendrá la responsabilidad de compartir con todos los miembros de manera anónima y segura.

- Los miembros que formen parte de dicho programa deberán informar sobre alertas de ciberamenazas que pudieran afectar los activos críticos del gobierno o en su caso los ciudadanos mexicanos.

- Se deberá incluir dentro de este programa una propuesta de mejores prácticas en materia de seguridad de la información la cual deberá ser compartida hacia todos los miembros de dicho programa.

Cabe mencionar que la información compartida entre los miembros del programa debe ser entregada a través de un protocolo seguro, el cual deberá tener acceso únicamente las personas responsables de cada parte interesada. Específicamente, el Gobierno Mexicano debe considerar qué tipo de información se debe compartir entre las entidades gubernamentales, así como con el sector privado para obtener un intercambio recíproco.

También es necesario que haya espacio para el intercambio voluntario de información, especialmente con respecto al sector privado. Como parte del programa, la UIC deberá facilitar los eventos de colaboración con el gobierno y los socios de la industria, que permita crear un ambiente de confianza para compartir información sobre amenazas cibernéticas. Estos intercambios no están clasificados y se centran en las amenazas actuales o en la actividad reciente.

Gráfico 1 - Resumen de los hallazgos de la aplicación del Modelo de madurez cibernética para México – Fuente: (Hacia una Estrategia Nacional de Ciberseguridad, 2017)

1.1. Acciones para implementar una estrategia de liderazgo y colaboración para el Gobierno Mexicano

Las acciones que se deben de desarrollar para la implementación de una estrategia de liderazgo y colaboración entre las diferentes dependencias de gobierno, el sector educativo y el sector privado con el objeto de avanzar en la construcción del plan estratégico y promover la cultura de colaboración y cooperación entre las partes interesadas son las siguientes:

1. Con la ayuda de la UIC se podrá alinear las funciones y responsabilidades entre las diferentes dependencias del Gobierno Mexicano en relación con la ciberseguridad y respuesta a incidentes.

2. Cada una de las dependencias del Gobierno Mexicano deberán definir su mandato y autoridad con respecto a la ciberseguridad para que no existan dobles roles y/o funciones. Se deberá realizar un equilibrio adecuado de la asignación de las funciones y responsabilidades, así como mantener un enfoque estratégico coherente para todo el gobierno.

3. Para establecer un nivel de liderazgo y de colaboración entre las diferentes partes interesadas se debe definir estratégicamente el alcance del desarrollo y ejecución del plan estratégico, el cual deberá ser apoyada por el más alto nivel del Gobierno Mexicano.

4. Fortalecer y homologar las líneas de comunicación entre las diferentes dependencias de gobierno en materia de ciberseguridad. Por una parte, la formalización del proceso de comunicación y colaboración ya sea a través de un grupo de trabajo intersecretarial o en su caso un comité permanente.

5. Clarificar los roles del equipo de respuesta a incidentes versus las herramientas de aplicación de la ley. Lo anterior, debido a que el Equipo de Respuesta ante Amenazas Informáticas (CERT por sus siglas en ingles) en México depende de la policía federal y por lo tanto muchas dependencias del gobierno pueden ser reacias a colaborar. Por otra parte, generar nuevos convenios de colaboración con la UIC y fortalecer los convenios de colaboración que se han firmado al día de hoy entre la Policía Federal (PF) con la Secretaría de la Función Pública (SFP) que tiene como objeto capacitar a los servidores públicos en materia de ciberseguridad. Así como, el convenio con la empresa SCITUM que permitirá facilitar el intercambio de información para la detección de delitos cibernéticos y ciberamenazas.

6. Promover la colaboración internacional en temas de ciberseguridad y apegarse a convenios internacionales como lo es el de Budapest, el cual proporciona temas relacionados con el delito cibernético en la escena internacional, el cual se detallará más adelante. Por otra parte, continuar con los actuales tratados internacionales como el tratado integral y

progresista de asociación transpacífico (CPTPP), así como el T-MEC en sus apartados de comercio electrónico y comercio digital respectivamente, promueven la colaboración y desarrollo de capacidades de cooperación en la respuesta de incidentes.

1.2. Estrategia de Colaboración Intra-dependencias del Gobierno Mexicano

Aunque México no cuenta con un marco de trabajo oficial de cooperación y colaboración entre las diferentes dependencias del Gobierno México en materia de ciberseguridad, se creó el Comité Especializado en Seguridad de la Información (CESI) que fue el grupo encargado para la creación de la estrategia nacional de ciberseguridad. Lo anterior, fue retomado por la subcomisión de ciberseguridad que depende de la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (CIDGE). La cual fue integrada por un a un grupo multidisciplinario de los diferentes sectores públicos, privados y educativos, teniendo como resultado una primera y única versión de dicha estrategia.

Por otra parte, la división científica de la Policía Federal (PF) es la principal autoridad civil y que investiga delitos cibernéticos principalmente referentes a la prostitución infantil, robo de identidad, fraudes y robo de información mediante el uso de métodos como el phishing. Aunado a lo anterior, la Comisión Nacional de Seguridad (ahora Secretaría de Seguridad Pública y Protección Ciudadana) a través de su división de la policía federal y de autoridades locales han creado unidades especiales llamadas “policía cibernética”, las cuales tienen como objetivo primordial investigar la comisión de delitos informáticos y apoyar a las autoridades competentes (ministerio público o federal). Algunas de las policías cibernéticas son las siguientes:

1. Policía de Ciberdelincuencia Preventiva de la Ciudad de México (Data.ssp.cdmx.gob.mx, n.d.).

2. Unidad de Prevención e Investigación Cibernética del Estado de México (Sseguridad.edomex.gob.mx, n.d.).

3. La Policía Cibernética de Jalisco (Fge.jalisco.gob.mx, n.d.).

4. Unidad de Policía Cibernética de Hidalgo (Unidad de Innovación Gubernamental y Mejora Regulatoria, n.d.)

5. Unidad de Policía Científica Preventiva del Gobierno de Veracruz

No obstante, con la creación de estas unidades especializadas se creó el comité de ciberseguridad que permitirá la consolidación de un modelo homologado de policía cibernética, con el objeto de estandarizar la estrategia contra el combate de los ciberdelitos en todas sus formas. Así mismo, con este mecanismo se podrá brindar recursos para la operación, coordinación y vinculación con todas unidades de policía cibernéticas estatales y federales. Por otro lado, esto permitirá una mejor comunicación con autoridades de carácter internacional. Adicionalmente, la división científica es la encargada de manejar todos los asuntos de ciberseguridad de forma personalizada.

Por otro lado, existe el Instituto Federal de Telecomunicaciones (IFT), un organismo constitucional autónomo encargado de regular y supervisar el uso de las redes de telecomunicaciones, así como su prestación y radiodifusión en México. Adicionalmente, el IFT es la autoridad en materia de competencia económica de los sectores de telecomunicaciones y la radiodifusión. Lo anterior, permite tener un mercado de libre competencia, obteniendo un balance entre las ofertas y las demandas eliminando los agentes preponderantes.

Adicionalmente, el IFT estuvo liderando el grupo de trabajo correspondiente al sector objetivo estratégico de “Sociedad y Derechos” de la Estrategia Nacional de Ciberseguridad en México que indica: “Generar las condiciones para que la población realice sus actividades de manera responsable, libre y confiable en el ciberespacio, con la finalidad de mejorar su calidad de vida mediante el desarrollo digital en un marco de respeto a los derechos humanos como la libertad de

expresión, vida privada y protección de datos personales, entre otros" (Estrategia Nacional de Ciberseguridad, 2018).

Una de las acciones realizadas por el IFT en materia de ciberseguridad fue aprobar su Programa Anual de Trabajo 2018, indicando que entre los estudios e informes que tiene programados para este año destaca **el plan de acciones en materia de ciberseguridad.** Lo anterior, permitirá al IFT tener una mayor participación y colaboración en estudios e investigaciones que contribuyan a conocer el estado de la ciberseguridad en México, así como para propiciar desarrollos encaminados a generar capacidades propias en ciencia y tecnología para la misma.

Por otro lado, la Procuraduría General de la República (PGR) crea las unidades de investigaciones cibernéticas y operaciones tecnológicas, así la de combate al delito de secuestro, las cuales tienen como objetivo primordial fortalecer las acciones realizadas en materia de investigación y seguridad en materia de delitos relacionados con medios electrónicos bajo el mando del Ministerio Público de la Federación. Dentro de las facultades de estas unidades están las siguientes:

1) Determinar las herramientas y soluciones que permitan apoyar con las investigaciones.
2) Definir en conjunto con la Coordinación de Planeación, Desarrollo e Innovación Institucional los programas de capacitación para los servidores públicos para realizar las investigaciones a través de los medios electrónicos de la institución.
3) Monitoreo de las redes públicas para la identificación de actividades ilícitas relacionadas con las denuncias e investigaciones cibernéticas de la institución.
4) Establecer mecanismos de colaboración con otros organismos y autoridades internacionales relacionados con la investigación de delitos cometidos a través de medios cibernéticos y el uso de tecnologías de la información.

5) Auxiliar a las autoridades competentes en la investigación de delitos relacionados con medios cibernéticos y tecnológicos, entre otros que encomiende el director en jefe de la agencia de investigación criminal.

Lo anterior, se encuentra estipulado en el Diario Oficial de la Federación en el ACUERDO A/076/17 *"ACUERDO POR EL QUE SE CREA LA UNIDAD DE INVESTIGACIONES CIBERNÉTICAS Y OPERACIONES TECNOLÓGICAS, Y SE ESTABLECEN SUS ATRIBUCIONES"* (Dof.gob.mx, 2017).

Adicionalmente, refiriéndose a las entidades estatales. Se estipula que en el artículo 40 de la Constitución Política de los Estados Unidos Mexicanos establece que los estados son libres y soberanos en todo lo que concierne a su régimen interior, pero de forma limitada, ya que en el artículo 41 de la misma establece que las constituciones locales en ningún caso podrán contravenir las estipulaciones del pacto federal.

En otras palabras, los Estados de la Republica están sujetos a la soberanía federal porque depende de esta. Aunado a lo anterior, los estados han creado estrategias para el combate y concientización de sus habitantes con el apoyo de la policía cibernética que actualmente están presentes en 26 estados de los 32 estados. Las anteriores, prácticamente se dedican al patrullaje en las redes públicas, orientar al público sobre los riesgos del uso inadecuado del internet, así como apoyar a las autoridades competentes (Ministerio Público Federal o Local) con las investigaciones.

Actualmente, se encuentran en un proceso de homologación de una estrategia para unificar y fortalecer las policías cibernéticas en los estados. Los esfuerzos realizados por la Policía Federal han sido un gran avance y aunque las capacidades de los estados no son las mejores o en su caso no están debidamente focalizadas para fortalecer estas iniciativas y sean más efectivas con un programa permanente que se detallará en los siguientes capítulos.

Hasta ahorita hemos abordado a las diferentes autoridades y organismos que tienen atribuciones en materia de ciberseguridad a todos los niveles del gobierno. Por otra parte, falta mencionar las atribuciones que ha realizado el Consejo Nacional de Ciencia y Tecnología (CONACYT) que en apoyo con otros

organismos como el Instituto Nacional de Astrofísica, Óptica y Electrónica (INAOE) realizó la primera reunión de ciberseguridad para la Industria 4.0, la cual reunió investigadores, académicos y profesionales de la industria relacionados con el área de seguridad informática con el objeto de fortalecer la colaboración para la resolución de los problemas que ya han sido identificados en materia de ciberseguridad.

Así como este, el CONACYT firmó un convenio de colaboración con la Autoridad Israelí de Innovación (antes MATIMOP, parte del Office of the Chief Scientist, OCS, por sus siglas en inglés) para fomentar la investigación, desarrollo e innovación tecnológica e intercambio de tecnologías entre ambas entidades. Lo anterior, permitirá fomentar nuevos proyectos de alto impacto en corto tiempo.

Las instancias de seguridad nacional como lo es la Secretaría de la Defensa Nacional y la Secretaría de Marina han tomado acciones en materia de ciberseguridad en las que incluyen la creación de un Sistema Nacional de Inteligencia que permitirá integrar las inteligencias especializadas de la Administración Pública Federal, incluyendo la PGR, la PF, las Fuerzas Armadas y el órgano de inteligencia civil del Estado Mexicano.

Por otro lado, se encuentra el Centro de Operaciones del Ciberespacio el cual tiene como objetivos estratégicos el planear, coordinar, dirigir y ejecutar los esfuerzos del Ejército y Fuerza Aérea Mexicanos para identificar las amenazas provenientes del ciberespacio y mitigar sus efectos, así como prevenir y responder a incidentes que atenten contra la información e infraestructura crítica soportada en sus tecnologías de la información y comunicaciones.

Como se mencionó anteriormente, dentro de las acciones que ha tomado el Gobierno Mexicano en términos de ciberseguridad, hay que identificar de forma clara las diferencias entre la seguridad nacional, seguridad pública y la ciberseguridad, ya que parece que la línea que diferencia a estos términos es muy delgada. Por una parte, en el artículo 3 de la Ley de Seguridad Nacional establece que la seguridad nacional se entiende como “las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado

Mexicano que conlleven a: I. La protección de la nación mexicana frente a las amenazas y riesgos que enfrente nuestro país" (Diputados.gob.mx, 2005).

Por otro lado, la seguridad pública se enfoca a resolver problemáticas que atenten a la integridad de las personas. Lo anterior, establecido en el artículo 21 de la Constitución Política de los Estados Unidos Mexicanos (Diputados.gob.mx, 2016). Un ejemplo de lo anterior, son los casos de delitos de fuero común y algunos de fuero federal; prevención y acciones contra la incidencia delictiva; así como la investigación, persecución y penalidad ante actos criminales.

En contraste con lo que estipula la Ley de Seguridad Nacional que está enfocada hacia la protección del Estado (territorio, población y soberanía). Por último, tenemos el termino de ciberseguridad que se define como la "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados" (Azcona, 2018).

Ahora dentro de la Ley de Seguridad Nacional no se menciona en ninguna parte el termino de ciberseguridad, sino dentro del Plan Nacional de Desarrollo 2013 - 2018 de la administración del presidente Enrique Peña Nieto, en donde se estipula "impulsar, mediante la realización de estudios e investigaciones, iniciativas de ley que den sustento a las actividades de inteligencia civil, militar y naval, para fortalecer la cuarta dimensión de operaciones de seguridad: ciberespacio y ciberseguridad" (PND.gob.mx, 2013).

También se menciona el termino de ciberseguridad en el Programa para la Seguridad Nacional 2014-2018 establece que "…es necesario que el Gobierno de la República desarrolle una política de Estado en materia de ciberseguridad y ciberdefensa, para garantizar así la defensa de los intereses económicos, políticos y militares de México en el ciberespacio.

Es necesario generar y poner en marcha una estrategia que evite afectaciones a las capacidades nacionales de comunicación y a la funcionalidad de los sistemas de información estratégicos gestionados por las autoridades y el sector privado. El propósito central de la estrategia debe ser el fortalecimiento de la

cuarta dimensión de las operaciones de seguridad: la ciberseguridad y la ciberdefensa" (Programa para la Seguridad Nacional 2014 - 2018, 2014).

Con lo anterior, podemos hacer diferenciar lo que compete a la seguridad pública, seguridad nacional y la ciberseguridad, que hoy en día con la incursión de la Estrategia Nacional de Ciberseguridad se pretende o se tuvo la intención de que se ejecuten las acciones estipuladas tanto en el Programa Nacional de Desarrollo 2013-2018 y en el Programa para la Seguridad Nacional 2014 – 2018.

Aunque esto es un gran avance en materia de ciberseguridad, es necesario impulsar la implementación de iniciativas como la recién publicada Estrategia Nacional de Ciberseguridad (13 de noviembre 2017) y que no todos los asuntos de ciberseguridad se manejen a través de la División Científica de la Policía Federal y los organismos antes mencionados sino se haga a través de la UIC eventualmente.

Lo anterior, nos permitirá generar un marco de trabajo institucional con el objeto de asegurar que se tengan claras las responsabilidades y autoridad de cada una de las diferentes dependencias del gobierno federal mexicano, incluyendo un mecanismo de colaboración para lograr que se desarrollen y se apliquen las políticas públicas de todo el gobierno.

Uno de los grandes retos para la División Científica es la de incentivar a las personas a realizar las denuncias de los delitos e incidentes cibernéticos. Lo anterior, se debe a que se tienen registrados desde el 2012 al 2017 más de 176,029 incidentes, de los cuales únicamente el 30% son de denuncias realizadas por la ciudadanía, el resto se detectó mediante el "patrullaje cibernético" (Sánchez Onofre 19 de julio de 2017, 2017).

Como se puede observar, una de las principales causas de que la ciudadanía sea víctima de este tipo de delitos es la falta de la información. Aunque existen muchas iniciativas dentro del Gobierno Mexicano a todos los niveles y en diferentes sectores, hay un gran desconocimiento por parte de la ciudadanía en general de los riesgos que pueden ocurrir, así como el impacto que estos pueden tener como se ha mencionado previamente en este documento. Por otro lado, se

tiene que fortalecer las campañas de difusión de los medios de comunicación para realizar una denuncia, orientación y cualquier apoyo sobre tipo de delitos cibernéticos.

Así mismo, es necesario establecer un vínculo de confianza entre todas las dependencias del gobierno federal y autoridades competentes mediante el establecimiento de nuevos mecanismos de comunicación segura y generar un enfoque práctico que nos permita compartir información que es vital para este proyecto como: información sobre incidentes, amenazas, nuevas vulnerabilidades, mitigaciones, métodos e información sobre la concientización en materia de ciberseguridad, mejores prácticas y análisis estratégico.

Capítulo 2

Programa estratégico para el aseguramiento de los activos críticos del Gobierno Federal Mexicano

Capítulo II.- Programa estratégico para el aseguramiento de los activos críticos del Gobierno Federal Mexicano

Hay varias maneras de obtener acceso a la información en el ciberespacio. Los atacantes pueden explotar vulnerabilidades en el software y el hardware. Adicionalmente, se pueden aprovechar de dichas vulnerabilidades de seguridad para engañar a la gente para que abra correos electrónicos infectados o visitar sitios web corruptos que infectan sus computadoras con software malicioso. Los usuarios que navegan en el ciberespacio pueden llegar a ser víctimas de un fraude o incluso de un robo de identidad por desconocimiento de medidas básicas de seguridad de la información, como lo son: cambio periódico de sus contraseñas, actualización de su antivirus de forma regular, y el uso de redes inalámbricas protegidas solamente.

Es importante mencionar, que en el ciberespacio no es complicado conseguir herramientas sofisticadas y de fácil uso que pudieran comprometer los sistemas de información (ya sea públicos o privados) sin la necesidad de tener conocimientos avanzados en seguridad de la información. Por otra parte, la mayoría de los ataques informáticos comparten cuatro características en común las cuales se describen a continuación:

- Accesible – La mayoría de las herramientas de ataque se pueden adquirir a un precio modesto o descargar de forma gratuita a través de Internet (Canada's Cyber Security Strategy for a stronger and more prosperous Canada, n.d.).
- Fácil - Los atacantes con sólo habilidades básicas pueden causar un daño significativo (Canada's Cyber Security Strategy for a stronger and more prosperous Canada, n.d.).
- Eficaz- Incluso eficaces ataques menores pueden causar grandes daños (Canada's Cyber Security Strategy for a stronger and more prosperous Canada, n.d.).
- Bajo riesgo - Los atacantes pueden evadir la detección y procesamiento por ocultar sus pistas a través de una compleja red de ordenadores y explotar las

lagunas en los regímenes legales nacionales e internacionales (Canada's Cyber Security Strategy for a stronger and more prosperous Canada, n.d.).

Si bien hay cierta similitud en los objetivos y los métodos de atacantes cibernéticos, la naturaleza de la amenaza que representa cada uno se hace distinta por sus diferentes motivaciones e intenciones. Es importante mencionar, que las amenazas informáticas ocasionan pérdidas materiales, económicas, de información, y de prestigio a todas las organizaciones y las cuales se pueden clasificar en lo siguiente:

- Espionaje Cibernético patrocinado por el estado y actividades militares ("Cybercrime / Cybercrime / Crime areas / Internet / Home - INTERPOL", 2017).
- Espionaje Corporativo ("Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience", 2012).
- Abuso del uso del internet de parte de los terroristas ("Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience", 2012).
- Cibercrimen ("Cybercrime / Cybercrime / Crime areas / Internet / Home - INTERPOL", 2017).
- Hacktivismo ("Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience", 2012).
- Campañas de desinformación ("Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", 2017).

2.

2.1. Enfoque Estratégico para la Protección de los Activos Críticos del Gobierno Federal Mexicano

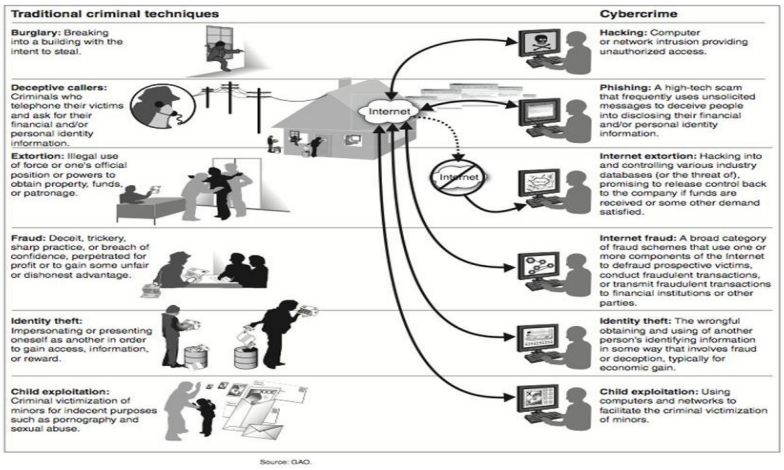


Figura 2 - Cibercrimen vs Crimen Tradicional – Fuente: ("U.S. Government Accountability Office (U.S. GAO)", 2019)

En los últimos años, los sistemas de gobierno se han convertido en blanco de diversos ataques cibernéticos, los cuales han perjudicado la imagen y la confianza de la ciudadanía en el uso de los servicios de gobierno electrónico. Es importante mencionar, que la ciberseguridad no es responsabilidad únicamente del gobierno federal, sino es una acción coordinada entre los diferentes niveles de gobierno (federal, estatal y municipal) junto con la iniciativa privada, la cual posee y opera aproximadamente el 85% de la infraestructura critica del Gobierno Mexicano. Lo anterior, es un punto clave para generar una estrategia para la protección de los activos críticos del gobierno y un vínculo de confianza entre las partes interesadas dentro y fuera del gobierno.

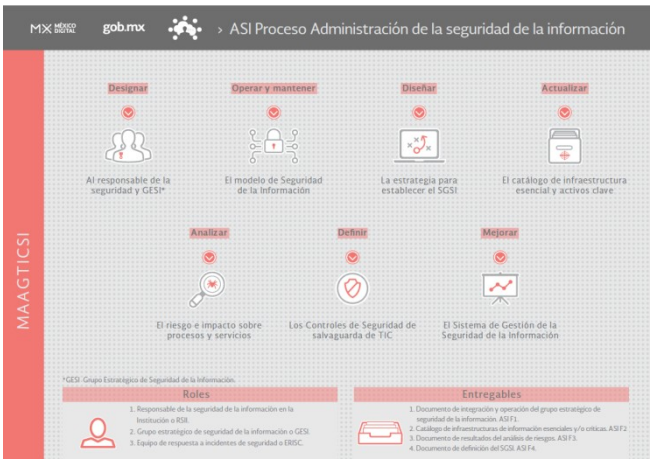


Figura 3 - Infografía del Proceso ASI - Fuente: (Electrónico, 2019)

El primer paso para iniciar con una estrategia, o en su caso la definición de un adecuado marco de trabajo para el Gobierno Federal Mexicano que permita la identificación y definición de las infraestructuras críticas. Actualmente, dentro del proceso de **ASI** (Administración de la Seguridad de la Información), el cual forma parte del **MAAGTICSI** (Manual Administrativo de Aplicación General en las materias de tecnologías de la información y comunicaciones, y en la de seguridad de la información) particularmente, en el entregable de **"Catálogo de Infraestructuras esenciales y/o críticas"** se especifica que todas las dependencias del Gobierno Federal Mexicano deben de contar con dicha información, la cual se encuentra descentralizada y muchas veces no se encuentra actualizada.

Debido a lo anterior, es necesario que se integre **un catálogo global de todos los activos críticos del gobierno,** comenzando con la identificación de los actuales catálogos de infraestructuras esenciales y/o críticas, así como los catálogos faltantes y los activos críticos que forman parte de los procesos de seguridad nacional[5]. Lo anterior, seguido de un análisis de riesgos de cada infraestructura crítica que tiene como objeto de definir la mejor forma de protegerlos eliminado las posibles amenazas, identificando los escenarios de riesgos, así mismo, definir los controles de seguridad que pudieran mitigar los riesgos identificados y salvaguardando la integridad, confidencialidad y disponibilidad de dichos activos críticos.

Otro punto importante, es la medición de la efectividad y seguimiento de la implementación de dichos controles de seguridad (mejora continua). Por otra parte, dentro del programa estratégico no debemos olvidar la fase de mitigación

cuando una amenaza se materializa y el equipo de respuesta a incidentes debe actuar, para lo cual es necesario contar con una mejor comunicación entre los centros de respuesta a incidentes (CERT) tanto de la UIC, como el de la CNS, UNAM, SCITUM-TELMEX, por mencionar algunos. Por último, es necesario hacer una reconstrucción de los eventos sucedidos y poder identificar ¿Qué fue lo pasó? ¿Quién fue el autor intelectual del ataque? ¿Cómo lo realizó? Lo anterior, es para tomar las medidas necesarias para que dicho evento no vuelva a pasar. El siguiente ciclo, ilustra de forma resumida un ciclo de eventos necesario para la protección de activos críticos.

Figura 4 - Ciclo de eventos para la protección de activos – Fuente: (Fas.org, 2018)

---

[5] **Proceso ASI –** Administración de la Seguridad en su actividad número 4 - Descripción: Elaborar y mantener actualizado un catálogo de infraestructuras de información esenciales y, en su caso, críticas, a fin de facilitar la definición de los controles que se requieran para protegerlas. Identificar, a partir de los procesos críticos identificados y enlistados en el factor crítico anterior, aquellos que se encuentren vinculados con la integridad, estabilidad y permanencia del Estado Mexicano, de acuerdo a lo que señalan los artículos 3 y 5 de la Ley de Seguridad Nacional. En caso de no identificarse este tipo de procesos críticos, no será necesario atender los factores críticos 5 al 14 siguientes, debiendo iniciar la actividad ASI 5.

Cabe mencionar que el Gobierno Mexicano es el responsable de emitir las mejores prácticas en materia de seguridad de la información basándose en los estándares internacionales como lo son: ISO27001, ISO20000, Risk Management of SANS, etc. Lo anterior, con el objeto de asegurar y coordinar todos los aspectos para la protección de la infraestructura critica del gobierno.

Es importante, no olvidar que se debe poner atención a la interconectividad de las infraestructuras y su interoperabilidad efectiva en casos de emergencia o desastre. Una estrategia efectiva es la clara definición del alcance del nivel de protección, así como la cooperación y coordinación entre todos los niveles de gobierno, sectores privados y educativos.

2.2. Definición de los Roles y Responsabilidades del Gobierno Mexicano, Sector Educativo y el Sector Privado

Uno de los puntos medulares de la estrategia para la protección de los activos críticos es asignar o en su caso definir las responsabilidades de cada parte interesada ya sea gobierno (en todos sus niveles), sector privado o educativo. Por otro lado, el hecho de darle más responsabilidades al sector privado no va a garantizar un mayor nivel de protección. Lo anterior plantea la creación de una estrategia de cooperación entre las partes interesadas mediante la instrumentación de canales de comunicación mediante la generación de una cultura de divulgación e información de incidentes que pudieran ayudar a la investigación y entendimiento de los mismos. La notificación oportuna de vulnerabilidades y el entendimiento de los diferentes vectores de ataques hacia los activos críticos, así como la correcta asignación de roles y responsabilidades de los sectores público, privado y educativo permitirá la disminución paulatina de los incidentes de ciberseguridad.

Así mismo, el sector privado puede responder de forma más rápida y efectiva ante una amenaza que las oficinas de gobierno, esto se debe que casi toda o al menos la mayoría de la infraestructura crítica es gestionada o administrada por el sector privado. Aunado a lo anterior, esto sería un esquema mal enfocado. Ahora, si se genera una cierta flexibilidad entre las partes interesadas, la respuesta ante cualquier amenaza en materia de ciberseguridad sería muy rápida y efectiva.

Adicionalmente, la relación de confianza entre el sector privado y el Gobierno Federal de México se ha visto dañada debido a que el mercado de oportunidades de compras de TIC’s han sido acaparado por 10 empresas durante el periodo 2013-2017 con recursos ejercidos por $29,248.77 millones de pesos y que son más del 40% de los procesos de adquisición ejercidos durante el periodo antes mencionado (Sites.google.com, 2019). Complementando lo anterior, debido a que los procesos para la adquisición de bienes y contratación de servicios de TIC’s son lentos, tediosos y largos, dicha situación retrasa la planeación de los

recursos provocando subejercicios, recontratación del mismo proveedor, así como el recorte de presupuesto. La generación de un plan de cooperación transversal entre los diversos sectores privados deberá ser una prioridad del gobierno para abrir el mercado y favorecer los procesos de licitaciones públicas y contratos marcos limitando las adjudicaciones directas.

Por otra parte, como se mencionó anteriormente, las empresas privadas proveedoras de servicios de TIC's gestionan o en su caso son dueñas de la mayoría de las infraestructuras críticas que pueden ser objeto de amenazas, las cuales pueden ser más peligrosas de lo que pueden ser hacia el mismo gobierno. En otras palabras, los ataques y la explotación de vulnerabilidades van enfocados en su mayoría hacia la infraestructura de TI, de la cual es responsable las empresas que gestionan dicha infraestructura y que por lo general deben de cumplir con niveles de servicio establecidos en los contractos o instrumentos legales entre los proveedores de servicio y el gobierno. Lo anterior, pone en tela de juicio la credibilidad y confianza del proveedor y la infraestructura de TIC's propuesta.

Es correcto asumir que las empresas del sector privado enfocadas en materia de TIC's vean las necesidades del Gobierno Mexicano no como un costo, sino como una oportunidad que beneficiará a ambas partes interesadas. Lo anterior plantea la posibilidad de generar nuevas estrategias financieras que permitan la inversión de proyectos claves de modernización de los servicios tecnológicos hacia la sociedad y el uso eficiente de las TIC's. Ahora, el gobierno por su parte debe garantizar que las empresas privadas cuenten y cumplan con las herramientas y niveles de servicio para el aseguramiento de los activos críticos del mismo. Sin embargo, es imposible para para el Gobierno Mexicano poder pagar todas y cada una de las tecnologías enfocadas en materia de seguridad de la información que actualmente son requeridas para poder mitigar las existentes amenazas. Para poder lograr esto, es necesario que se realice una evaluación de cada caso particular con el objeto de revisar cómo se pudiera adquirir. Lo anterior,

plantea la posibilidad del desarrollo de soluciones hechas en casa que permita el ahorro y mejor uso del presupuesto asignado a este rubro.

Por otra parte, si el sector privado no puede cumplir con los niveles de servicios comprometidos para la protección de los activos críticos del gobierno, este podría actuar de forma deliberada ejecutando y haciendo cumplir regulaciones más estrictas. Un claro ejemplo, sucedió en Estados Unidos con el atentado del 11 de septiembre de 2001, en el cual el gobierno de este país tuvo que intervenir en la industria de las líneas áreas implementando medidas más estrictas con los controles de seguridad, esto debido a que no hubo una respuesta rápida de parte del sector privado ante dicha amenaza.

Este proceso se puede volver muy tedioso para ambas partes interesadas si no existe un compromiso para cumplir con dichas responsabilidades, las cuales tienen como objetivo principal el aseguramiento de los activos críticos del Gobierno Mexicano. Es importante mencionar que, aunque esto lo podemos resumir a un tema de colaboración, la responsabilidad para implementar las mejores prácticas en materia de ciberseguridad recae en las partes interesadas que se han mencionado en este capítulo, usando al Gobierno Mexicano como fuente de guía y motivación.

La Administración Pública Federal con el apoyo del Congreso de la Unión deberán fortalecer y dar un mayor cumplimiento las actuales leyes en materia de acceso a la información (Ley General y Federal de Acceso a la Información Pública), protección de datos personales (Ley General de Protección de Datos en Posesión de Sujetos Obligaos) o en su caso crear una iniciativa legislativa que permita incrementar y asegurar los canales de comunicación sobre posibles amenazas cibernéticas como lo son: malwares, ransomware, algún tipo de amenazas persistentes avanzadas (APT, por sus siglas en ingles), vulnerabilidades del día “Zero” y entre otras, que pudieran comprometer algún activo critico tecnológico del Gobierno Mexicano y que dicha información este en posesión de los proveedores de servicio de tecnologías de la información, ya que

actualmente el proceso de comunicación de este tipo de información no es muy eficiente y lento.

Figura 5 - Publicación desde la cuenta oficial de Twitter del INE – 22 de abril 2016

Lo anterior, se debe a que diversas empresas privadas son renuentes a proporcionar información importante sobre sus posibles vulnerabilidades ya que temen que esta información pueda convertirse en pública y por lo tanto pueda afectar negativamente la confianza de los interesados. Tales temores constituyen importantes obstáculos para el diálogo de colaboración entre el sector privado, público y educativo reduciendo gravemente los niveles de cooperación.

La responsabilidad pública debe ser preservada, pero el acceso a la información de datos personales deberá estar alienado con base en lo que lo indica la Ley General de Datos Personales en Posesión de Sujetos Obligados para organismos gubernamentales y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares para

Un claro ejemplo, la información almacenada y asegurada por INE (Instituto Nacional Electoral) por ningún motivo deberá ser pública, ya que contiene información de datos personales de los ciudadanos mexicanos, salvo sus excepciones como los son los partidos políticos sustentados en la Ley en materia General de Instituciones y Procedimientos Electorales (art. 148 y demás relativos). Dicha información, se presume que fue filtrada dentro de la Deep web y se vendió a terceros para fines de lucro a través de la plataforma Amazon (Databreaches.net, 2016).

El INE dentro de sus acciones correctivas decidió dar de baja el portal donde se mostraba dicha información el día 22 de abril 2016 a través de su cuenta

de twitter. Debido a lo anterior, es primordial realizar una evaluación en materia de seguridad de los activos que hospedan la información presuntamente comprometida.

La cooperación en materia de protección de la infraestructura crítica y el intercambio de información debería estar debidamente regulada para proteger tanto a las empresas proveedoras de servicios de TIC's como el mismo gobierno a través de un canal seguro de comunicación y deberá ser compartida únicamente con las partes interesadas. Lo anterior, para que pueda funcionar deberá existir una iniciativa legislativa que establezca las medidas necesarias para la protección de infraestructuras críticas y poder crear un marco normativo, que sirva de base para la creación de un plan nacional de protección de infraestructuras y crear un catálogo global de infraestructuras críticas.

El Congreso de la Unión por su parte deberá analizar cuáles son las mejores opciones para permitir la apertura de mercado de la iniciativa privada en el gobierno, ya que actualmente se encuentra muy cerrado a los grandes competidores como lo son: Grupo Operbes, Telmex, Grupo Salinas, Axtel entre otros. Esto se debe, a que el requisito para poder competir en una licitación pública en su mayoría favorece a unos cuantos. Lo anterior, se puede revisar con la cantidad de procesos de adquisición que se dieron durante el periodo de enero 2013 a marzo 2017 que fueron alrededor de 12,000 según lo revisado en el sistema de COMPRANET.

Por otra parte, de acuerdo con el estudio de inversiones gubernamentales en tecnologías de la información y comunicación coordinado por la asociación de Internet.mx, durante la administración del presidente Enrique Peña Nieto, el 61% de los procesos de adquisición del gobierno federal fueron por adjudicación directa (User, 2018). Lo anterior, nos dice que un procedimiento de adquisición que debe ejecutarse únicamente como una excepción, se ha convertido en algo muy frecuente y por tal motivo es necesario hacer una revisión en la Ley de Adquisiciones y Arrendamientos y Servicios del Sector Público en donde exista

una mayor difusión de los procesos de licitación y se pueda regular las adjudicaciones directas y que sean únicamente por motivos de seguridad nacional.

La siguiente imagen muestra los porcentajes de ejecución de los procedimientos de adjudicación:

Gráfico 2 - Cantidad de procedimientos de adjudicación federal - Fuente: (User, 2018)

Las dependencias del Gobierno Federal Mexicano y proveedores de servicios de TIC's deberán fortalecer e incrementar los convenios de colaboración con universidades para desarrollar nuevos y mejorados estándares de seguridad que puedan ser utilizados para que puedan innovar los actuales como lo indica el artículo 1 fracción III y IV de la Ley de Ciencia y Tecnología. Lo anterior, promoverá un mayor uso de estándares en materia de seguridad de la información realizados en México.

Las agencias federales también deben ayudar en la creación de programas de evaluación de riesgos para las empresas del sector privado involucradas en la protección de la infraestructura. Aunque el gobierno puede asesorar a los propietarios y operadores de la infraestructura de una amenaza sospechosa, no puede evaluar el riesgo, la vulnerabilidad o la capacidad de supervivencia de cada activo.

Las dependencias del Gobierno Mexicano deben usar un modelo de mejores prácticas para trabajar con la iniciativa privada, lo cual les permitirá

realizar evaluaciones constantes. Este programa permitiría a los proveedores de servicios de TIC’s atender las necesidades de seguridad cumpliendo los estándares de seguridad con los requerimientos del Gobierno Federal Mexicano. Un ejemplo para cumplir con este programa se puede referenciar a lo aplicado dentro del pilar de “Liderazgo y Colaboración” de la Estrategia Nacional de Ciberseguridad del Gobierno Canadiense (Canada’s Cyber Security Strategy for a stronger and more prosperous Canada, n.d.).

Capítulo 3

Identificación de alianzas estratégicas con el sector privado y educativo en México

Capítulo III.- Identificación de alianzas estratégicas con el sector privado y educativo en México

Dando cumplimiento a los objetivos particulares de este proyecto, es de suma importancia el poder identificar cuáles son las alianzas estratégicas que el gobierno federal mexicano debe de afianzar con el sector privado en particular con las empresas especializadas en seguridad de la información. Al identificar dichas empresas, el gobierno mexicano podría tener acceso al estado de arte en soluciones especializadas de ciberseguridad con el fin de mitigar las amenazas existentes y permita el aseguramiento de sus activos críticos. Por otra parte, dentro de este capítulo, se identificarán las principales universidades y centros de investigación que deberán trabajar mediante un convenio de colaboración con el gobierno federal que permita la generación de nuevo conocimiento en la investigación y desarrollo de nuevas estrategias y soluciones para la mitigación de amenazas como lo son: la fuga de información, robo de identidades, malware persistente entre otras.

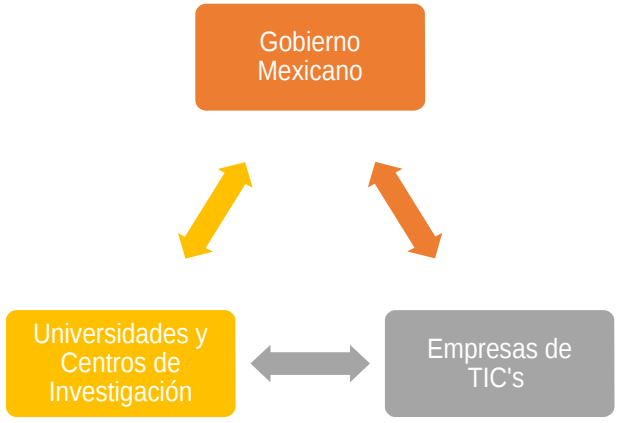


Figura 6- Identificación de las partes interesadas de la ciberseguridad – Fuente: Elaboración Propia

La identificación de las partes interesadas tanto en el sector privado, como en el educativo permitirá crear alianzas estratégicas las cuales tienen como objetivo crear un canal seguro de comunicación que permita compartir información confidencial sobre riesgos, impactos y amenazas existentes y emergentes, técnicas defensivas (seguridad ofensiva), así como las mejores prácticas de

ciberseguridad. Por otra parte, poder cumplir con los objetivos de seguridad nacional del país y mejorar la capacitación a través de programas de concientización entre los diferentes socios de la ciberseguridad. Con la práctica constante de dichas actividades se optimizarán los procedimientos para prevenir fallas de ciberseguridad. Otro punto medular de este capítulo, es la continuidad de las iniciativas entre el sector público y privado para identificar y compartir las mejores prácticas para el aseguramiento de la infraestructura crítica del gobierno mexicano.

3.

3.1. Identificación de los principales proveedores de ciberseguridad del sector privado

Dentro de la revisión y del estudio de mercado realizado sobre las principales tendencias en seguridad de la información encontramos las siguientes:

Figura 7 - Tendencias en ciberseguridad – Fuente: (M.isaca.org, 2018)

Como se puede observar en la tabla anterior, se tienen cuatro vectores tecnológicos a los cuales se debe poner especial atención y se recomienda al gobierno mexicano enfocar esfuerzos para mitigar ***las amenazas geopolíticas***, blindaje de las iniciativas de gobierno electrónico que nos permitirá ofrecer una ***"protección del negocio digital"***, generar mecanismos de protección y

concientización sobre el uso seguro del ***"Internet of Things (IoT)"***. Por otra parte, es importante la identificación de los principales proveedores de tecnologías en materia de ciberseguridad que pueden brindar la tecnología necesaria para la correcta implementación de las medidas de protección contra amenazas que puedan crear un valor agregado. ***"El 46% de las empresas invierte en seguridad de IoT"*** (M.isaca.org, 2018).

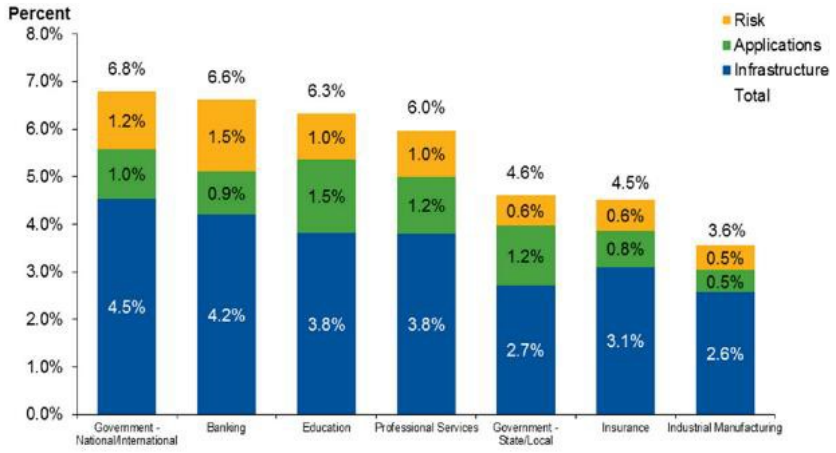


Gráfico 3 - Gasto asignado en seguridad de la información - Fuente: (Solís, 2019)

El presupuesto asignado en materia de seguridad de la información para México en comparación con otros países, por ejemplo, Canadá que tiene planeado la inversión de un billón de dólares asignado para ciberseguridad (Budget.gc.ca, 2019) es menor en comparación del gasto asignado en seguridad de la información (Solís, 2019). Por otra parte, cabe mencionar que en México no se le ha dado la prioridad y el presupuesto necesario para desarrollar nuevas iniciativas que permitan la protección de los activos de información del gobierno mexicano, así como a sus ciudadanos.

Aunado a lo anterior y en base en el análisis que se ha realizado durante este proyecto es necesario realizar la identificación de los principales proveedores que son innovadores en soluciones de ciberseguridad y que pueden tener la inteligencia necesaria para la prevención de amenazas latentes, mediante la identificación de los diferentes vectores de ataque previniendo la materialización de amenazas persistentes. A continuación, se enumeran las principales

compañías especializadas en ciberseguridad que han sido innovadoras y han dado un valor agregado a la industria de la tecnología de la información:

Núm.	Compañía	Descripción	URL	Soluciones Innovadoras
1	Arbor Networks	Arbor es una empresa de seguridad informática enfocada en la seguridad de red y monitoreo de actividad maliciosa en redes empresariales.	es.arbornetworks.com/	Protección contra ataques DDoS: Detecta y mitiga ataques DDoS con dispositivos físicos y en la nube. Amenaza Avanzada: Arbor Spectrum analiza tráfico en tiempo real para detectar amenazas críticas que ya están dentro de la organización.
2	Cisco	Cisco es una empresa líder en Tecnologías de la Información y Comunicación. Su principal enfoque son los equipos de conexión para redes informáticas, dispositivos de seguridad y telefonía IP.	www.cisco.com	Cisco Security Connector: Permite visibilidad del tráfico generado por dispositivos Apple y puede bloquear conexiones a sitios maliciosos sin importar el lugar donde vaya el usuario. Previene la conexión a redes celulares inseguras y redes públicas.
3	Fortinet	Es una empresa dedicada al software, dispositivos y servicios de seguridad informática.	www.fortinet.com	Virtualized Next Generation Firewall: Permite gran visibilidad y todas las funciones de un firewall tradicional en un ambiente virtual. Junto con todas las ventajas de este factor como gran

Núm.	Compañía	Descripción	URL	Soluciones Innovadoras
				rendimiento y escalabilidad sin límite. Sandbox: Protege contra amenazas avanzadas y emergentes en tiempo real sin necesidad de intervención humana.
4	CyberArk	Es una compañía de seguridad enfocada en eliminar ciber-amenazas.	www.cyberark.com	Cyberark DNA: Descubre cuentas privilegiadas locales, en la nube, y ambientes de desarrollo. Evalúa el riesgo de seguridad de cuentas privilegiadas. Identifica todas las cuentas con permisos de administrador. Identifica los equipos vulnerables a ataques de robo de credenciales.
5	Checkpoint	Es un proveedor de software y hardware para seguridad de Tecnologías de Información, seguridad de red, terminales móviles, datos y administración de seguridad.	www.checkpoint.com	Seguridad Móvil: Los empleados utilizan gran cantidad de dispositivos móviles en el trabajo, los cuales representan un riesgo potencial para la organización. Siguiente Generación de Prevención de

Núm.	Compañía	Descripción	URL	Soluciones Innovadoras
				amenazas: Ofrece una solución multicapa de defensa con un rango amplio de prevención, políticas comunes de monitoreo y máxima protección de amenazas emergentes.
6	RSA	Es una empresa dedicada a la criptografía y al software de seguridad. Algunos de sus productos destacan las bibliotecas criptográficas B-SAFE, mecanismos de autenticación SecurID y el algoritmo criptográfico RSA.	www.rsa.com	Prevención de Fraudes: Detecta y previene fraudes en tiempo real. Protege los activos y usuarios contra phishing, malware, rogue, y aplicaciones móviles. Permite transacciones seguras a través de la web y dispositivos móviles. Rastrea amenazas emergentes, tendencias de fraude y nuevas estrategias de fraude.
7	Symantec	Es una corporación que desarrolla y comercializa software para computadoras específicamente para seguridad informática.	www.symantec.com	Protección dispositivos móviles: Symantec ofrece protección multicapas para proteger a un dispositivo móvil de diferentes vectores de ataque como exploits de vulnerabilidad, apps maliciosas y

Núm.	Compañía	Descripción	URL	Soluciones Innovadoras
				ataques de red con protección automatizada. Protege activos sensibles de la organización. Se encuentra disponible para Android y iOS.
8	Absolute	Es una compañía canadiense especializada en la protección de equipos para usuarios finales, ya sea equipos de cómputo, móviles, tabletas y servidores	www.absolute.com	Plataforma Absolute permite el monitoreo completo del dispositivo de usuario final, con la capacidad de generar un inventario de hardware y software, geolocalización, análisis de riesgos, analítica sobre el comportamiento del dispositivo, concientización de la información y persistencia en las aplicaciones (cumplan con estándares).
9	Palo Alto	Es una compañía de seguridad que ayuda a evitar brechas de seguridad en las organizaciones.	www.paloaltonetworks.com.mx	La plataforma de seguridad de nueva generación de Palo Alto tiene 3 tecnologías integradas para reducir los ataques a la organización. Tiene Firewall Integrado para proteger terminales, centro de datos, la red,

Núm.	Compañía	Descripción	URL	Soluciones Innovadoras
				nubes públicas y privadas y entornos SaaS. Todo en tiempo real y se actualiza en su nube de inteligencia de amenazas.
10	FireEye	Es una compañía de ciber-seguridad que provee productos y servicios para protegerse contra amenazas avanzadas, persistentes y phishing.	www.fireeye.com	La solución de Fireeye de seguridad de red permite detectar rápidamente y actuar ante las últimas amenazas a través de los 3 principales vectores de ataque, red/web, correo y archivos de sistema. Correlaciona toda la actividad en redes locales y remotas para identificar vulnerabilidades de día cero.
11	Norse	Es una empresa que ofrece servicios de inteligencia de seguridad informática en tiempo real.	www.norse-corp.com	Detecta nuevos tipos de ataques sofisticados, tiene su propia red de Inteligencia. Bloquea conexiones inseguras en tiempo real, botnets y URL's. Trabaja con conexiones encriptadas. Detiene el filtrado de información que pasa por proxies

Núm.	Compañía	Descripción	URL	Soluciones Innovadoras
				anónimos.

Cuadro 5 - Empresas Innovadoras de ciberseguridad – Fuente: Elaboración propia

La relación anterior servirá de referencia para poder crear contratos macro que sean realmente rentables y que la intención de esta estrategia sea proveer servicios dicha tecnología a todas las dependencias del gobierno mexicano, iniciando a nivel federal y con el paso del tiempo llegar con los diferentes municipios. Con la ayuda del sector privado, el gobierno mexicano seguirá actualizándose en términos de tecnología de la información a través de la UIC, la cual podrá brindar servicios de ciberseguridad efectivos y costeables a toda la Administración Pública Federal.

Es cierto que la tecnología no es barata y que se debe de crear un modelo de economía a escalas que no sea limitado al tiempo a seis años (periodo presidencial en México), sino que se pueda garantizar la continuidad de los servicios mediante convenios de colaboración entre la UIC y las diferentes oficinas federales, estatales y municipales. Un ejemplo de un convenio de colaboración podría ser la creación de un programa permanente y actualizado de concientización en materia de ciberseguridad para el gobierno mexicano, en el cual se apliquen las diferentes mejores prácticas como lo especifica la NIST SP 800-50 Building an Information Technology Security Awareness and Training Program ("Building an Information Technology Security Awareness and Training Program", n.d.) las cuales se detallarán en los siguientes capítulos de este documento. La idea de crear servicios de ciberseguridad efectivos y costeables se debe negociar con la industria privada para generar diferentes soluciones escalables horizontalmente y verticalmente que a diferencia de cómo se venden hoy en día en el mercado van enfocados únicamente hacia las necesidades de una dependencia. Lo que se quiere plasmar es generar servicios que cumplan con las necesidades de la mayoría de las dependencias y personalizar servicios para los casos muy particulares como la Comisión Nacional de Hidrocarburos que pudiera utilizar tecnología especializada como Scada. Lo anterior, nos sirve para

crear un vínculo estratégico y con ello abatir el rezago del gobierno mexicano, en materia de tecnología para la seguridad de la información.

3.2. Identificación de las universidades y centros de investigación en materia de ciberseguridad

Una vez identificadas las principales compañías innovadoras de ciberseguridad es necesario voltear al sector educativo y buscar las principales universidades que han impulsado la investigación, desarrollo, capacitación y proyectos en materia de ciberseguridad. Por otra parte, están los centros de investigación que mediante sus proyectos e iniciativas para la protección de los mexicanos en el ciberespacio a través de diversas líneas de investigación como lo son: ***criptografía, seguridad en las redes, forense digital, análisis de malware, aseguramiento del internet de las cosas (IoT) y entre otras,*** han creado diversas iniciativas y alianzas con múltiples organizaciones y entidades del gobierno tanto federal como extranjero.

Cabe mencionar que la incursión y el trabajo de colaboración entre el gobierno federal con el sector educativo privado y público es fundamental para que la actual estrategia nacional de ciberseguridad pueda cumplir cabalmente con sus objetivos estratégicos. Como se mencionó las universidades y centros de investigación en México con el paso del tiempo se han desarrollado diversos programas especializados en materia de ciberseguridad como el **Laboratorio de Ciberseguridad del Centro de Investigación de Computación del Instituto Politécnico Nacional.**

Como se ha mencionado previamente en otros capítulos, dentro del plan estratégico de este proyecto es fortalecer estas iniciativas como el CIC con el apoyo del gobierno federal y de la iniciativa privada para obtener mejores y mayores resultados. Lo anterior, nos estará llevando a la creación de un programa de concientización en materia de ciberseguridad que no solamente servirá para los funcionarios públicos, sino para los usuarios que navegan en el ciberespacio y que puedan tener la certeza que estarán navegando de forma segura.

Adicionalmente, se pretende que otro objetivo de estas iniciativas sea colaborar con el conocimiento obtenido de los diferentes proyectos y líneas de investigación con la unidad inteligente de ciberseguridad para que sean un centro de respuestas a incidentes, como lo es actualmente la **UNAM CERT-MX, Mnemo-CERT y Scitum-CERT.**

A continuación, se detallan las universidades y centros de investigación que han sido participe o que tienen líneas de investigación en materia de ciberseguridad. Así mismo, se incluye dentro de la tabla los proyectos de navegación segura, protección contra malware, etc. Por otra parte, se incluye una pequeña descripción de los proyectos y/o líneas de investigación, así como la URL de la universidad y/o centro de investigación.

Núm.	Universidad / Centro de Investigación	Descripción	URL	Proyectos y/o Líneas de Investigación
1	Centro de Investigación de Computación (CIC) del Instituto Politécnico Nacional (IPN).	Laboratorio de Ciberseguridad	http://www.conacytprensa.mx/index.php/tecnologia/tic/15236-laboratorio-ciberseguridad-vigilando-ciberespacio-mexico	criptografía, seguridad en redes, seguridad en host, forense digital, malware, el internet de las cosas, ciudades inteligentes, esteganografía, sistemas detectores de intrusos, aplicación de los algoritmos evolutivos para la ciberseguridad, biometría, entre otros.
2	Universidad Nacional Autónoma de México	CERT – Centro de Respuesta a Incidentes de Seguridad	https://www.seguridad.unam.mx/proyectos	➢ Proyecto Honeynet UNAM Chapter. • Plan de Sensores de Tráfico Malicioso. • Proyecto Malware. • Red Distribuida de Honeypots.
3	Centro Iberoamericano para el Desarrollo e	Centro de capacitación, investigación, previsión de	http://ceidic.org/	➢ Sirena - campañas de sensibilización, alianzas estratégicas, persecución criminal y

Núm.	Universidad / Centro de Investigación	Descripción	URL	Proyectos y/o Líneas de Investigación
	Investigación de la Ciberseguridad	menores, propuesta de estándares y legislación en materia de ciberseguridad.		atención a casos existentes. ➢ Poseidón - es la rama de capacitación y certificación del CEIDIC en los temas que este Centro trata en toda la región iberoamericana a nivel empresarial, educativo y gubernamental. ➢ Nautilius - marcos de protección relacionados con la Ciberseguridad en cada uno de los países miembros de la red del CEIDIC, mismos que van desde la creación de políticas públicas, legislación y hasta la investigación, todos ellos relacionados a la ciberseguridad. ➢ Kraken - es una red de inteligencia sobre ciberamenazas para la prevención de amenazas con la ayuda de diferentes sectores públicos y privados.
4	Universidad de la Salle	Programa de posgrado en ciberseguridad	http://www.lasalle.mx/oferta-educativa/maestria/facultad-de-ingenieria/maestria-ciberseguridad/	➢ Maestría en Ciberseguridad

Núm.	Universidad / Centro de Investigación	Descripción	URL	Proyectos y/o Líneas de Investigación
5	Universidad Autónoma de Nuevo León	Programa de licenciatura en ciberseguridad	http://www.uanl.mx/oferta/licenciatura-en-seguridad-en-tecnologias-de-informacion.html	➢ Licenciatura en Seguridad en Tecnologías de Información
6	UNITEC	Programa de posgrado en ciberseguridad	https://issuu.com/unitecmexico/docs/maestria_seguridad_informacion	➢ Maestría en Ciberseguridad
7	ESIME Culhuacán	Programa de posgrado en ciberseguridad	http://www.posgrados.esimecu.ipn.mx/index.php?option=com_content&view=category&layout=blog&id=26&Itemid=144	➢ Maestría en Ingeniería en Seguridad y Tecnologías de la Información
8	Centro de Estudios Superiores Navales (CESNAV)	Programa de posgrado en seguridad de la información	https://cesnav.uninav.edu.mx/cesnav/links_acc_progr/seginfor_site/seginfor_index.html	➢ Maestría en seguridad de la información
9	Universidad de la Salle	Programa de posgrado en seguridad de la información	http://www.lasalle.mx/oferta-educativa/	➢ Maestría en Ciberseguridad

Núm.	Universidad / Centro de Investigación	Descripción	URL	Proyectos y/o Líneas de Investigación
			maestria/ facultad-de-ingenieria/ maestria-ciberseguridad/	
10	Universidad Autónoma de Nuevo León	Programa de licenciatura en seguridad de la información	http:// www.uanl.mx/content/ licenciado-en-seguridad-en-tecnologias-de-informacion	➢ Licenciatura en Seguridad en Tecnologías de Información
11	Universidad Nacional Autónoma de México	Programa de diplomado en ciberseguridad	http:// redyseguridad.fi-p.unam.mx/ Dipciber/ index.html	➢ Diplomado en ciberseguridad

Cuadro 6 - Centros de investigación y universidades en México con proyectos y programas en ciberseguridad – Fuente: Elaboración propia

Las anteriores universidades y centros de investigación han impulsado programas y líneas de investigación en materia de ciberseguridad en México. La investigación de campo realizada nos permite darnos cuenta que existen pocos programas, licenciaturas, posgrados y líneas de investigación en materia de ciberseguridad. En base a lo revisado durante este trabajo, es claro que es necesario impulsar los programas y líneas de investigación con el apoyo del gobierno federal y de las empresas especializadas en ciberseguridad.

Haciendo un programa de colaboración eficiente entre la triada identificada (gobierno, sector educativo y el privado). Por otra parte, es necesario generar un marco de trabajo en materia de ciberseguridad que incluya la habilitación del sistema de gestión de seguridad de la información a nivel transversal en los tres

niveles de gobierno, la aplicación de las mejores prácticas, controles, técnicas y estándares específicos. Así mismo, la definición de servicios especializados, procesos, plataformas tecnológicas, monitoreo, analítica y reporteo. Lo anterior, va a servir para establecer la forma de trabajo, gobernanza y comunicación entre los diferentes actores principales que forman parte del plan estratégico del presente documento.

Figura 8 - Arquitectura empresarial de ciberseguridad - Fuente: (Slideshare.net, 2018)

Capítulo 4

Propuesta de definición de la Unidad Inteligente de Ciberseguridad (UIC) para el Gobierno Federal Mexicano

Capítulo IV.- Propuesta de definición de la Unidad Inteligente de Ciberseguridad (UIC) para el Gobierno Federal Mexicano

Durante los primeros capítulos de este proyecto se ha elaborado una propuesta de estrategia de liderazgo y colaboración, las acciones necesarias para su implementación y un marco de colaboración entre las diferentes dependencias del gobierno en sus diferentes niveles. Lo anterior, nos ha permitido tener una visibilidad que nos permita generar una estrategia de protección de los activos críticos con la ayuda de una clara definición de roles y responsabilidades de cada parte interesada. Por otra parte, se han identificado a los principales proveedores de tecnología e investigación en materia de ciberseguridad con el objeto de contar con el estado del arte de las medidas preventivas, equipamiento, mejores prácticas para la protección de los activos críticos del gobierno mexicano contra amenazas persistentes, espionaje industrial, daños a la reputación, filtración de datos y disponibilidad de los activos junto con sus datos.

Actualmente, la Administración Pública Federal en México cuenta con diversas unidades de inteligencia que funcionan de manera desconcentrada, pero no existe una colaboración eficiente entre las dependencias y que sea respaldada por el primer mandatario del Gobierno Mexicano. Por lo anterior, sería de gran beneficio para la Administración Pública Federal contar con un organismo que tenga las facultades anteriormente mencionadas y que pueda trabajar y apoyar de forma transversal con cada una de las dependencias del Gobierno Federal Mexicano.

Aunado a lo anterior, es fundamental la creación de una secretaría para este proyecto, por lo que se propone una Unidad Inteligente de Ciberseguridad (UIC), la cual tendrá como objetivo funcionar como un hub central (centro único) para el asesoramiento, prestación de servicios de ciberseguridad, auditoria, ciber inteligencia, análisis normativo en materia de ciberseguridad y que pueda trabajar mediante un marco de trabajo basado en riesgos para la protección de activos críticos alineando los objetivos estratégicos del gobierno con las actividades de

ciberseguridad. Lo anterior nos permitirá desarrollar un “lenguaje común” que permita la colaboración y cooperación internacional en infraestructura y mejores prácticas de ciberseguridad.

Una vez que hemos definido el alcance de esta Unidad Inteligente de Ciberseguridad para la Administración Pública Federal es necesario primero identificar todas las secretarías del gobierno federal, entidades de gobierno, estados y municipios, así como las embajadas y consulados que conforman el poder ejecutivo, lo cual se muestra a continuación:

Gráfico 4 - Resumen del Poder Ejecutivo – Fuente: (Gob.mx, 2019)

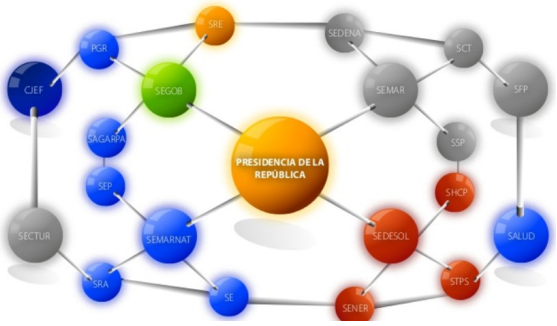


Gráfico 5 - Resumen de la estructura del gobierno federal mexicano – Fuente: (Gob.mx, 2019)

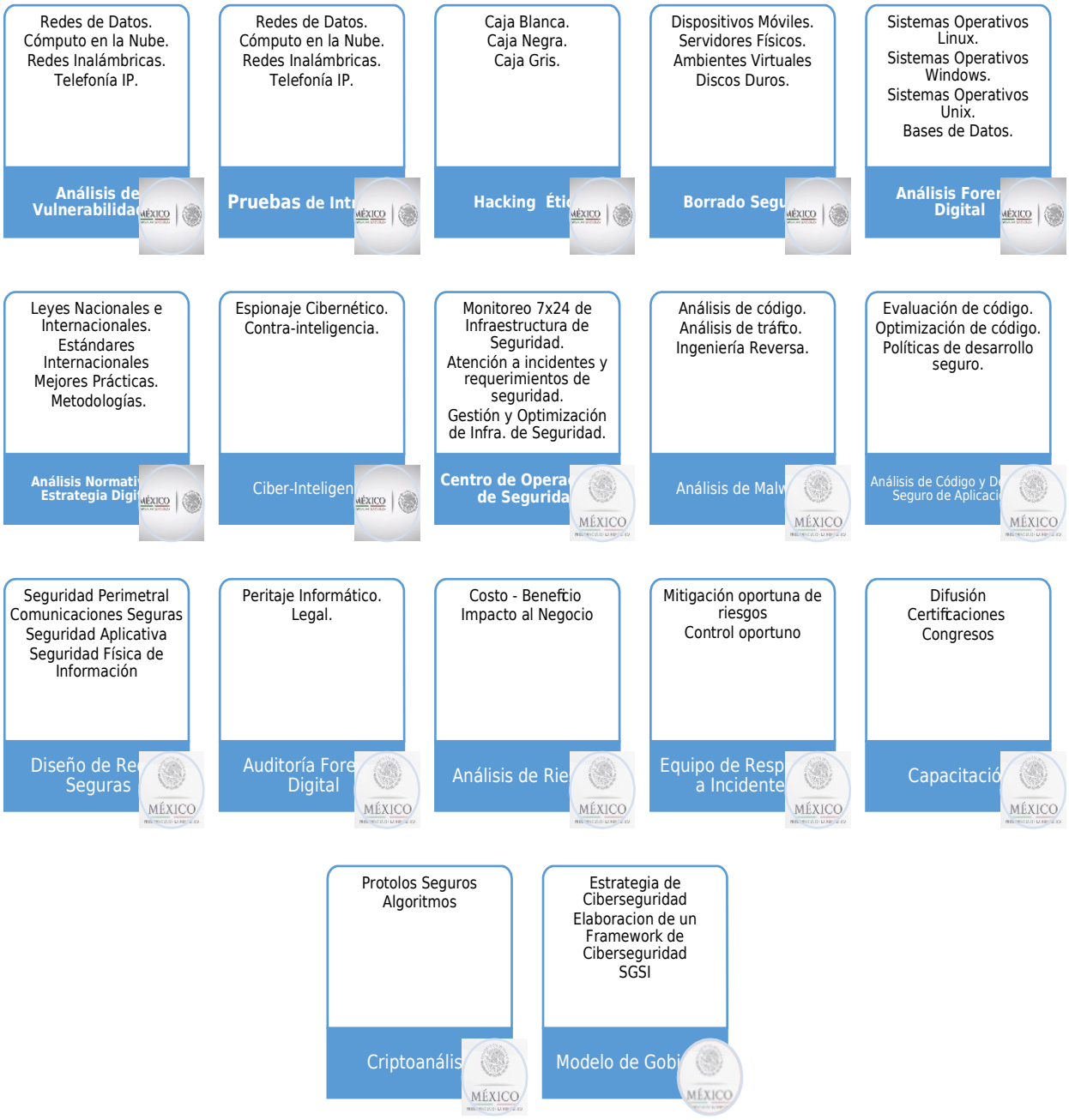
Lo anterior, muestra la estructura general del actual gobierno federal mexicano y las secretarías de los diferentes sectores. Adicionalmente, es necesario ubicar dentro de la estructura del Gobierno Federal a la UIC a nivel de secretaría para que pueda cumplir con los objetivos establecidos anteriormente en este documento. Por otra parte, es necesario definir sus funciones, responsabilidades y la forma de trabajar con todas las secretarías, gobiernos

estatales y municipales. La UIC deberá tener al menos un enlace de alto nivel con poder de toma de decisión que tenga conocimientos o al menos experiencia en ciberseguridad de cada secretaría.

Una de las responsabilidades de la UIC es contar con un centro de respuesta a incidentes centralizado para todo el gobierno federal mexicano. El cual deberá coordinar las acciones necesarias y será la encargada de la ejecución del programa estratégico de concientización de ciberseguridad y navegación segura. Lo anterior, deberá ser enfocado en primer lugar a todas las oficinas de nivel federal y posteriormente a los diferentes niveles de gobierno y oficinas descentralizadas. La unidad será encargada intercambiar conocimiento y experiencia a través de programas integrales de capacitación para el gobierno y la ciudadanía. Utilizar el conocimiento y experiencia del sector privado y educativo para fortalecer las capacidades en materia de ciberseguridad y reducir de forma significativa los riesgos protegiendo los activos y redes de datos del gobierno, así como las redes públicas de uso común de los ciudadanos.

4.1. Servicios Propuestos de la Unidad Inteligente de Ciberseguridad (UIC) para el Gobierno Federal Mexicano

A continuación, se detalla un pool de servicios estratégicos de ciberseguridad para apoyar a toda la estructura del gobierno mexicano:



Cuadro 7 - Servicios integrales de la Unidad de Inteligencia de Ciberseguridad – Fuente: Elaboración propia

Los servicios mencionados anteriormente están preparados para ser modulares y adecuarse a las necesidades de las entidades del gobierno federal, paraestatales, descentralizadas, estatales y municipales. La forma de trabajo de UIC deberá ser de forma transversal y será a través de los diferentes enlaces de gobierno que serán los encargados de transmitir y recibir retroalimentación de las necesidades y del seguimiento a cualquier servicio solicitado a la UIC. Cabe mencionar que el modelo de funcionamiento será muy similar a los convenios marcos que actualmente cuenta el gobierno con la iniciativa privada como lo es Microsoft, Oracle y Google por mencionar algunos. La diferencia con esta propuesta es que la UIC podrá atender directamente a cada oficina de gobierno sin la necesidad de algún intermediario, fungirá como centro único de respuesta a incidentes y tendrá la obligación de atender y apoyar a la oficina para la mitigación de los riesgos en caso de presentarse.

Por otra parte, la UIC tendrá las facultades para poder proveer de tecnología de ciberseguridad aquellas oficinas que no cuenten con ninguna infraestructura de ciberseguridad. Por otro lado, la unidad tendrá la capacidad de poder generar análisis de necesidades a cada una de las dependencias con el objeto de poder identificar brechas de seguridad, vulnerabilidades, riesgos latentes y hacer recomendaciones de como poder cerrar dichas brechas sin la necesidad de recurrir a un tercero y que pueda generar gastos excesivos y los cuales podrán ser auditables ante las autoridades competentes en materia de transparencia y gasto del gobierno mexicano.

Los servicios propuestos para la UIC podrán ser proporcionados a todas las dependencias del gobierno a través de convenios de colaboración entre la unidad y las diferentes dependencias. Cabe destacar, que la UIC será el punto de contacto de intercambio de información de forma segura con las diferentes universidades, centros de investigación, proveedores de servicios de ciberseguridad, entidades internacionales y sociedades anónimas las cuales deberán de ser registradas a través de un punto único dentro del proyecto de la ventanilla única del gobierno mexicano (www.gob.mx).

La UIC tendrá la obligación de generar conocimiento en materia de ciberseguridad con el apoyo de las diversas universidades y centros de investigación el cual deberá estar disponible para todos. Adicionalmente, deberá gestionar y organizar los recursos tanto de infraestructura como operacionales de ciberseguridad dando cumplimiento a la estrategia de ciberseguridad que actualmente rige al país. Como en otros países, la UIC deberá por una parte estudiar e investigar las amenazas en materia de ciberseguridad y por otro lado estratégicamente deberá responder ante cualquier amenaza que pudiera ser materializada y que afectará a los activos críticos y/o ciudadanos.

Capítulo 5

Programa Transversal para la Concientización en materia de Ciberseguridad para la APF

Capítulo V.-Programa Transversal para la Concientización en materia de Ciberseguridad para la APF

En este capítulo se diseñará un programa de concientización en materia de ciberseguridad, el cual estará enfocado para todos los usuarios finales que trabajan dentro de la Administración Pública Federal, incluyendo contratistas externos, personal de outsourcing y proveedores de servicios. Actualmente, el Gobierno Mexicano ha implementado diversas medidas y acuerdos de cooperación entre diversas dependencias con el objeto de capacitar, formar y mantener actualizados a los servidores públicos en materia de ciberseguridad.

Lo anterior, como medida preventiva contra abusos y delitos electrónicos. Este acuerdo, fue firmado entre la Comisión Nacional de Seguridad y la Secretaría de la Función Pública el día 25 de noviembre del 2017. Así como este acuerdo, se han implementado diversas medidas de concientización como las pláticas en escuelas públicas y privadas sobre los riesgos que pueden tener los menores con el uso de las redes sociales y en el ciberespacio durante la semana anual de ciberseguridad que preside la Policía Federal. Lo anterior, nos muestra que las autoridades del Gobierno Mexicano están tomando acciones preventivas en materia de ciberseguridad y que han empezado a concientizar tanto a los servidores públicos como a la ciudadanía.

También la Comisión Nacional de Seguridad (ahora llamada secretaría de seguridad y protección ciudadana) creó un comité nacional de ciberseguridad con el objeto de que todas las policías cibernéticas de México puedan operar bajo los mismos estándares y con una visión unificada, homologando sus procesos. Aunque, existen muchas iniciativas de concientización en materia de ciberseguridad, es necesario impulsar los actuales programas y convenios de colaboración. Lo anterior, a través de una estrategia permanente mediante un programa transversal que sea gestionado por la UIC junto con el apoyo de la división científica que es la única autoridad oficial.

Un punto esencial para que esta estrategia funcione es la comunicación y difusión efectiva del programa hacia todos los servidores públicos. El punto anterior y falta de información han sido el eslabón más débil de las propuestas de concientización en materia de ciberseguridad, por lo que se estará creando una nueva estrategia para mitigar estos puntos. El programa transversal incluirá al menos los siguiente: 1) El programa deberá ser adoptado como una medida preventiva para todas las dependencias del gobierno federal de forma inicial; 2) teniendo como base la actual Estrategia Nacional de Ciberseguridad ("Estrategia Nacional de Ciberseguridad", 2018) poder desarrollar una política general de ciberseguridad que esté alineada con los objetivos estratégicos del gobierno federal; 3) generar una estrategia de comunicación de las mejores prácticas a cada una de las dependencias del gobierno federal; y 4) establecer los procesos para el monitoreo y medición de la efectividad del programa transversal.

Es importante mencionar que este programa es crucial para este proyecto ya que será un *“vehículo”* que permite la comunicación de los requerimientos de seguridad a través de todas las oficinas del gobierno y a todos los usuarios finales. La efectividad de este programa permitirá explicar las reglas y normas para uso adecuado de los sistemas e información de TIC’s. Este programa transversal difundirá las políticas de seguridad y los procedimientos que deberán seguirse. Así como, las sanciones impuestas en caso de incumplirse. Por otra parte, la responsabilidad de la ejecución del programa deberá ser derivada de un grupo de trabajo especializado plenamente informado, entrenado y consciente del alcance del mismo. Dicho grupo, deberá ser parte de la Unidad Inteligente de Ciberseguridad. El programa deberá ser diseñado y alineado a las necesidades del negocio o en este caso de las funciones y objetivos estratégicos del gobierno federal. Así como ser parte fundamental de la cultura organizacional y de la arquitectura en TIC’s. Por otra parte, los programas más éxitos son aquellos en los que los usuarios se sientan parte del programa y de los problemas presentados.

El primer paso para desarrollo del programa transversal de concientización es el diseño del programa el cual incluye lo siguiente:

- Definición del alcance.
- Identificación de las necesidades del gobierno.
- Elaboración de un plan efectivo de implementación.
- El aseguramiento de la aceptación del programa dentro de la organización.
- Establecimiento de las prioridades del programa.
- Definir una “Barra de Ajuste” (Nivel de Complejidad de los temas).
- Identificar las opciones para fondear el programa de concientización.

Una vez establecido lo anterior, es necesario definir la estructura y el modelo de implementación del programa. Dicho modelo deberá establecer las actividades de supervisión e implementación del programa transversal, así como contemplar al menos lo siguiente:

- El tamaño y la dispersión geográfica de las diferentes oficinas de gobierno
- Definición de los roles y responsabilidades con base en lo estipulado en el Capítulo II en la sección de “Definición de los Roles y Responsabilidades del Gobierno Mexicano, Sector Educativo y el Sector Privado”.
- Asignación y control presupuestal.

Como parte importante del diseño del programa transversal es necesario detallar el modelo de implementación, análisis de necesidades, plan estratégico para el desarrollo del material del programa, las técnicas para la entrega del material y la medición de efectividad del programa.

5.

5.1. Modelo de Implementación del Programa Transversal

Una parte importante para el éxito del programa transversal de concientización es la definición de un modelo operacional que nos sirva para definir la estructura de cómo se va a diseñar, desarrollar e implementar dicho programa, siempre

basándonos en las mejores prácticas. Para este caso, utilizaremos la metodología definida por el Instituto Nacional de Estándares y de Tecnología (NIST, por sus siglas en inglés). Una vez que hemos establecido la necesidad de tener un modelo operacional, es necesario decidir cuál es el mejor modelo que pueda acoplarse o en su caso redefinir el modelo de gobierno de las dependencias tanto federales, estatales y municipales de México. Para esto hay que considerar al menos lo siguiente:

- La gran variedad de dependencias del gobierno federal.
- La descentralizada estructura de cada oficina con específicos roles y responsabilidades asignadas por el primer mandatario.
- Existen oficinas como la de comunicaciones y transporte que tiene oficinas en todo el país brindando servicios a toda la ciudadanía.
- Las oficinas federales como lo son: SCT, IMSS, ISSSTE, SRE y la SEDESOL cuentan con unidades organizacionales independientes en cada estado con objetivos estratégicos bien definidos como funcionan los gobiernos estatales. Debido a lo anterior, la estrategia de concientización que se deberá aplicar a dichas oficinas se deberá gestionar de forma diferente.

Figura 9 - Modelo Descentralizado del Programa de Gestión de Seguridad – Fuente: Elaboración Propia

En este modelo propuesto, se permitirá la diseminación de las políticas de seguridad y los requerimientos sobre el programa de concientización y la capacitación en materia de ciberseguridad. Por otra parte, se da la responsabilidad de la ejecución e implementación del programa transversal a cada una de las oficinas del gobierno Federal Mexicano.

Para este modelo se va integrar un grupo distribuido conformado con servidores públicos con el poder de toma de decisión dirigidos por la UIC. Lo anterior, permite crear un subsistema de CIO's y directores de TIC's de todas las dependencias los cuales estarán reportando a la UIC y formarán parte indispensable del modelo de gobierno de este programa transversal. Este subsistema ejecutará el programa en cada una de las oficinas federales, estatales y municipales.

Por otra parte, el análisis de necesidades será responsabilidad de cada oficina, esto debido a que la estrategia de concientización y del programa de entrenamiento recae exclusivamente en cada dependencia del Gobierno Mexicano. Aunado a lo anterior, cada oficina desarrollará el material del programa de concientización, así como la estrategia de implementación basada en el modelo de operación de cada dependencia. La UIC podrá orientar a cada dependencia sobre la creación del material del programa transversal de concientización.

La comunicación entre las dependencias y la UIC como unidad responsable del programa transversal deberá ser bilateral. Tanto las dependencias como la UIC van a poder realizar el intercambio de la información teniendo como fundamento la estrategia de colaboración especificada en el Capítulo II del presente documento. La UIC será la encargada de difundir las políticas de seguridad en materia de concientización y de capacitación para todas las oficinas del Gobierno México. Por otra parte, una de las atribuciones de la UIC será la de emitir y comunicar dichas políticas, así como un presupuesto asignado a cada dependencia el cual será entregado por los canales que actualmente cuenta la SHCP. Adicionalmente, la UIC podrá asistir a cada una de las oficinas para

realizar el análisis de necesidades, así como el desarrollo de la estrategia de implementación, programas de capacitación y la implementación del mismo.

La UIC será retroalimentada de los avances actuales, presupuesto asignado, material desarrollado, así como del resultado del análisis de necesidades realizado en las dependencias y los indicadores de efectividad y eficacia del programa. A continuación, se detallará un borrador de un análisis de necesidades que podrá ser utilizado como base para su implementación en las diversas oficinas del Gobierno Mexicano.

5.2. Análisis de Necesidades del Programa Transversal

En esta sección, se definirá un boceto del análisis de necesidades del programa transversal, el cual estará dirigido a cada una de las diferentes oficinas del gobierno federal y organismos descentralizados, el cual servirá como línea base para la creación del programa de concientización en materia de ciberseguridad para todo el gobierno federal:

ANTECEDENTES				
En el caso de que la respuesta sea SI o No sombrear la respuesta de la siguiente manera				
1	¿Realiza actualmente deberes como administrador de Sistemas?	SI	NO	
1a.	En caso afirmativo, ¿realiza el trabajo de tiempo completo?	SI	NO	
1b.	Si es menos de tiempo completo, ¿qué porcentaje de tiempo pasa haciendo deberes de administración de sistemas?		%	
2	¿Cuánto tiempo ha trabajado como administrador del sistema?	_____Años	_____Meses	
3	¿Tiene administradores de sistemas que trabajan para usted?	SI	NO	
4	¿Usted trabaja para un administrador de sistemas?	SI	NO	
5	¿Ha tenido capacitación formal en la administración de los sistemas?	SI	NO	
	(En caso afirmativo, especifique a continuación)	_____	_____	_____
		Escuela/proveedor	Título del Curso	Duración
		_____	_____	_____
		Escuela/proveedor	Título del Curso	Duración

6	¿Ha tenido entrenamiento formal en la seguridad del sistema? (En caso afirmativo, especifique a continuación)	SI	NO	
		_____	_____	_____
		Escuela/proveedor	Título del Curso	Duración
7	Por favor indique el número de años de educación formal que ha completado	_____	años	
8	¿A cuántos seminarios o conferencias relacionadas con la administración o la información de sistemas, y/o seguridad de la Información ha asistido en el último año?	_____		
9	¿Lee regularmente redes / revistas informáticas de software / o revistas? (En caso afirmativo, especifique a continuación)	SI	NO	

DESEMPEÑO DE TAREAS Y FORMACIÓN

	Para cada tarea en la columna A, Ponga en negrita si es: N - Nunca, V - menos de una vez al mes, M - mensual, S- semanal o D - diario		Ponga una X que indique la forma principal en que recibió su capacitación para realizar esta tarea. Si es "Otro", especifique (por ejemplo, talleres, prueba y error, etc.).	Ponga una X que indique el nivel de entrenamiento que sientas que necesitas. B (Básico) I (Intermedio) y A (Avanzado)
Manejo de Hardware				
	Instalar Hardware	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Adquirir el Hardware	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Coordinar la Instalación de Red	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Programar mantenimiento preventivo	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Coordinar la reparación del Hardware	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Revisar Sistemas de arranque	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Mantener el inventario de Hardware, el sistema de consumibles actualizado	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Ejecutar Diagnósticos	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Reubicar el hardware	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
Manejo de Software				
	Optimizar los parámetros del SO	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A

	Cambios en el SO	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Establecer valores predeterminados del Sistema	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Mantener los procedimientos de Inicio/apagado del Sistema	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Probar las actualizaciones	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Instalar Sistemas Operativos	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Mantener el inventario de los Software	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Instalar los cambios del Sistema	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Instalación especifica del software por el proveedor de hardware	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Instalar actualizaciones del sistema o parches	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Mantener la documentación del Software	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
Almacenamiento de Datos				
	Planificar el diseño de almacenamiento de datos	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Planificar procedimientos de respaldo	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Implementar procedimientos de respaldo	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Controlar el uso de almacenamiento de datos	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Mantener la integridad del sistema de archivos	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Gestionar la Seguridad del sistema de archivos de auditoría	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Eliminar archivos innecesarios	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Administrar archivos de registro	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Mantener el diseño de almacenamiento de datos	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Formatear los medios de	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A

	almacenamiento			
	Conocimientos en Discos de partición	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Crear un sistema de archivos	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Cargar datos	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Restaurar datos desde una copia de seguridad	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
Administración del Software				
	Evaluar el efecto de los programas	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Optimizar los parámetros de la aplicación	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Asegurar la compatibilidad entre las aplicaciones	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Asignar recursos del sistema a las aplicaciones	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Validar la integridad de las aplicaciones antes de la instalación	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Validar de la prueba de la instalación del software	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Instalar software de la aplicación	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Mantener el inventario	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Mantener la documentación de la aplicación	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Instalar actualizaciones de las aplicaciones	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Plan de conectividad de red	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Solicitar conectividad del host	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Obtener la dirección de Internet	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Construir cables de red	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Configurar líneas TTY	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Configurar líneas periféricas	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Configurar servidores de archivos y clientes	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A

	Configurar firewalls	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Monitorear la actividad	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Administrar servicios de red	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Administrar routers	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Administrar servidores de impresión	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Administrar servidores de terminal	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Administrar topología de red	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Asignar direcciones a nodos	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Instalar software de red	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Establecer permisos de acceso	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Restablecer la conectividad del host	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Ayudar a establecer pautas de auditoría	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Ayudar a escribir planes de seguridad del sistema	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Asistir en la acreditación de la red de host	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Asegurar los procedimientos de etiquetado de salida	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Asegurar los procedimientos de etiquetado de datos	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Ayudar a probar los mecanismos de seguridad	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Ayudar en el análisis de pistas de auditoría	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Ayudar en el manejo de incidentes	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Hacer cumplir los procedimientos de seguridad	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Ayudar a mantener la seguridad física del sistema	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A
	Ayudar a mantener los controles de acceso del dispositivo	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___I ___A

	Informar incidentes de seguridad	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
Cuentas de administración				
	Establecer entornos de inicio de sesión de usuario	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Administrar privilegios de cuenta	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Agregar nuevas cuentas	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Ayudar a establecer la lista de control de acceso de la cuenta	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Explicar los procedimientos operativos básicos	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Ayudar en la modificación de contraseñas	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Eliminar cuentas	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
Troubleshooting				
	Recrear escenarios de problemas	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Interpretar mensajes de error	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Aislar problemas	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Mantener registro de problemas y soluciones	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Recuperarse de las fallas del sistema	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Responder a los problemas identificados por el usuario	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Recopilar información de la solución del problemas	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Usar herramientas de diagnóstico	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A
	Iniciar acción correctiva	N V M S D	__Escuela ___ En el Trabajo __ Por su cuenta ___ Otro_____	___B ___ I ___A

DISCUSIÓN DE TAREA DE TRABAJO			
1	¿Se le exige a:	_____	Instalar firewalls
		_____	Operar Firewalls
		_____	Mantener firewalls
2	Si marcó alguna respuesta en la pregunta 1, especifique:	La cantidad de Firewalls	
		El tipo de Hardware	
		Software con que se trabaja	
3	¿Se le exige a instalar:	_____	Cables de red

		_____	PC's / Estaciones de trabajo
		_____	Routers
		_____	Hardware relacionado con la seguridad
		_____	Software relacionado con la seguridad
		_____	Otro software
4	¿Su trabajo requiere que sepa cómo programar o escribir scripts de shell?	SI	NO
	¿En qué idioma (s)?	_____	
5	¿Administra usted más de una red?	SI	NO
6	¿Qué sistemas operativos y versiones usa?	_____	
7	¿Es responsable de la seguridad del sistema?	SI	NO
8	¿Qué programas específicos usa para cada uno de los siguientes puntos (para cada uno, indique si su uso es opcional (O) o requerido (R) para la Institución):	Mapeo de red	_____
		Detección de intrusión	_____
		Registro del sistema	_____
		Comprobación o mejora de la contraseña	_____
9	¿Es usted ingeniero certificado?	SI	NO
	En caso afirmativo, ¿qué cursos de capacitación específicos tomó para obtener la certificación?	_____	
10	¿Cree que son importantes los cursos de capacitación en seguridad de sistemas de información?		
	¿por qué?		

Cuadro 8 - Modelo Descentralizado del Programa de Gestión de Seguridad – Fuente: Elaboración propia

5.3. Estrategia de Implementación del Programa Transversal

Una vez desarrollado el análisis de necesidades es necesario definir una estrategia para la implementación y puesta a punto del programa, el cual al menos deberá integrar lo siguiente:

- En caso de existir, las políticas de seguridad de cada una de las dependencias en materia de concientización. Integrarlas con los ejes transversales de la actual estrategia nacional de ciberseguridad.

- Definir el alcance del programa transversal, el cual tendrá como objetivo incursionar en una primera fase en las dependencias de la Administración Pública Federal (APF).
- Definición de roles y responsabilidades del personal asignado con un nivel jerárquico alto que pueda tomar decisiones y dar seguimiento para la planeación, diseño, implementación, puesta a punto y monitoreo del programa transversal en cada una de las dependencias del Gobierno Mexicano.
- Definición de Metas y objetivos específicos, el cual tendrá como principal hito la definición de la estrategia y difusión de las políticas de seguridad. Seguido del plan de implementación y medición de los primeros avances a través de indicadores como lo pueden ser: número de funcionarios públicos inscritos en el programa, cantidad de materiales generados, cantidad de objetivos alcanzados, entre otros.
- Hacer del programa transversal una estrategia necesaria y mandatorio dentro de la actual estrategia nacional de ciberseguridad.
- Definición de los temas a desarrollar dentro del material de concientización.
- Evaluación y actualización frecuente del material
- Definición del tipo de personal o funcionario público (técnico, alta dirección y/o externo).
- Definición de las prioridades de la implementación del programa, no se puede hacer todo en una fase. Tiene que estar bien definida las prioridades las cuales se pueden determinar teniendo en cuenta los siguientes factores críticos:
    - Disponibilidad de Recursos (Material)
    - Impacto Organizacional y de Roles
    - Cumplimiento de las actuales normativas que tiene el Gobierno Mexicano (MAAGTICSI – Procesos ASI y OPEC)
    - Revisión de dependencias del programa transversal.
- Definición de la barra de ajuste. La cual se refiere a la complejidad que se le va a dar a los temas que se van a exponer dentro del programa transversal de concientización en materia de ciberseguridad. Lo anterior con base en los siguientes criterios:

- ¿Cuál es la posición de los funcionarios públicos y personal externo a los cuales va a estar dirigido el programa transversal?
- ¿Cual deberá ser el nivel de conocimiento en materia de seguridad de la información de los funcionarios públicos o personal a los cuales se le estará dirigiendo el programa transversal?

- Definir una estrategia para poder fondear el programa transversal. Es claro que este tema depende de muchos factores como lo es el tipo de dependencia federal, no es lo mismo el presupuesto asignado a la SCT que la Oficina de la Presidencia de la República. La SCT cuenta con un presupuesto mucho mayor que la Oficina de la Presidencia. El objetivo de crear una Unidad Inteligente de Ciberseguridad es para que tenga un presupuesto que no tenga conflicto de interés con las demás dependencias esto debido a la rígida y vieja estructura de TIC's en el gobierno. La UIC será la encargada de manejar este presupuesto el cual deberá ser asignado por el primer mandatario y el cual tendrá las siguientes consideraciones:
  - Determinar un porcentaje promedio del presupuesto asignado para el plan de entrenamiento de los funcionarios públicos.
  - Determinar un presupuesto promedio por tipo de funcionario público (técnico, alta dirección y externo).
  - Determinar un porcentaje del presupuesto de las direcciones generales de TIC de las dependencias para el programa (en caso de ser necesario).
- Una vez realizado el análisis de necesidades se puede determinar las áreas de oportunidades del programa en cada una de las dependencias y saber qué áreas se deben reforzar y cuales son habilidades necesarias para permear. Existen un sinfín de temas que se pueden utilizar como lo son:
  - Manejo y uso de contraseñas
  - Protección contra amenazas (virus, malware, troyanos, códigos maliciosos, amenazas persistentes, etc.)
  - Políticas de Seguridad.
  - Uso del navegador de internet

- Identificación de SPAM
- Ingeniería Social.
- Respuesta contra incidentes, ¿Qué hacer en estos casos?
- Cambios dentro de la organización
- Uso de dispositivos personales
- Entre muchos otros.

5.4. Implementación del programa transversal

Antes de poder iniciar con la implementación del programa transversal es necesario tener al menos lo siguiente:

- Haber ejecutado y obtener el resultado del análisis de necesidades de cada una de las unidades organizacionales incluidas (al menos las 18 secretarías de la Administración Pública Federal).
- La estrategia de implementación del programa transversal debe estar definida y comunicada a cada una de las dependencias del Gobierno Mexicano.
- El plan de implementación del programa transversal debe de estar terminado
- Haber elaborado el material del programa transversal (Material para la estrategia de concientización y del programa de entrenamiento para los funcionarios públicos).

Figura 10 - Factores claves para la implementación del programa transversal – Fuente: Elaboración Propia

5.5. Plan de Comunicación de la Implementación del Programa

Para que un programa de concientización basado en un modelo completamente descentralizado tenga éxito y funcione de forma transparente entre todas las partes involucradas, es muy importante tener un plan de comunicación efectivo entre la Unidad Responsable (en este caso la UIC) con las demás unidades organizacionales (en este caso dependencias del gobierno federal, estatal y municipal), lo anterior nos ayudara para poder tener todo el apoyo de la alta dirección y que tengan muy claro el alcance del programa y las expectativas del mismo, así como el costo del mismo y los beneficios que este programa va a traer no solamente a todas las oficinas del gobierno sino a toda los ciudadanos mexicano, en otras palabras crear una cultura organizacional de concientización en materia de ciberseguridad para que los usuarios puedan usar el ciberespacio de forma segura.

En este modelo se plantea tener un grupo de CIO's y gerentes o directores de seguridad de la información que puedan permear dentro de todas las dependencias las políticas de seguridad en materia de concientización del programa transversal. Por otra parte, los encargados de TI y de seguridad de la

información serán los responsables de la ejecución del análisis de necesidades y de la implementación del mismo programa. Así mismo, estas personas estarán reportando al CIO de cada dependencia los avances los cuales serán entregados a la UIC para el monitoreo del avance del programa. Cabe mencionar y es muy importante tener en mente que una vez que tengamos comunicado y aceptado el plan de implementación se podrá iniciar actividades de ejecución del programa.

5.6. Medición de la Efectividad del Programa

Una vez que el programa ya fue implementado es necesario poder identificar la efectividad del mismo ya que si este no es mejorado de forma continua se puede volver obsoleto. La mejora continua siempre es un tema principal del programa transversal de concientización. Es importante hacer ver a los CIO's y Gerente/Director de Seguridad del problema que pudiera existir si no existiera un programa de concientización que permita dar cumplimiento a los objetivos estratégicos del Gobierno Mexicano.

Una vez que el programa ha sido implementado es necesario desplegar un sistema de monitoreo que permita capturar la información clave respecto a la actividad del programa (ej.: cursos, fechas, audiencias, costos, etc.) el monitoreo del sistema se debe realizar a nivel de cada dependencia, el cual deberá realizar un análisis y reporte del seguimiento de concientización y las iniciativas educativas. Se deberá integrar en una base de datos las necesidades de los diferentes tipos de usuarios como lo pueden ser:

- CIO's
- Gerente / Director de Seguridad (Área o Adjunto)
- Departamento de Recursos Humanos
- Gerentes / Directores Funcionales
- Auditores

- Oficiales Mayores (CFO’s)

Los mecanismos de evaluación de efectividad y eficacia del programa se deben generar mediante una estrategia que incorpore diferentes elementos que deberán ser enfocados hacia la calidad, el alcance, métodos de desarrollo, nivel de dificultad, facilidad de uso, duración de las sesiones, sugerencias, etc. Existen diferentes métodos para la evaluación del programa como lo son:

- Formas de Evaluación / Cuestionarios.
- Foros de Discusión.
- Entrevistas Seleccionadas.
- Análisis Independientes.
- Reportes de Estatus.
- Evaluación Comparativa del Programa.

Una vez elegido el método de medición es necesario definir el uso de métricas que nos permitirá tener un valor cuantitativo y cualitativo de los indicadores definidos en conjunto con la UIC. Uno de los ejemplos de las métricas que se pueden utilizar son los siguientes: 1) La disminución en incidentes o violaciones de seguridad; 2) La brecha entre la conciencia existente la cobertura de capacitación y las necesidades identificadas se está reduciendo; 3) El porcentaje de usuarios que están expuestos al material del programa transversal de concientización; 4) el porcentaje de funcionarios públicos y personal tercero que tiene toma de decisión en temas de seguridad siendo entrenados apropiadamente.

Capítulo 6

Propuesta de Mejoramiento del Marco legal y Jurídico para la protección de los mexicanos en el Ciberespacio

Capítulo VI. -Propuesta de Mejoramiento del Marco legal y Jurídico para la protección de los mexicanos en el Ciberespacio

En capítulos anteriores, se ha definido las estrategias de colaboración y liderazgo de las diferentes dependencias del gobierno federal que permitan generar las alianzas estratégicas necesarias para la creación de la unidad inteligente de ciberseguridad (UIC), para la cual ya se ha definido sus roles y responsabilidades, así mismo los servicios que unidad va a ofrecer al gobierno federal.

Aunado a lo anterior, falta definir un marco legal que permita sustentar legalmente la creación de esta UIC y por otro lado fortalecer las actuales leyes (de las cuales se detallaran después) que permita la lucha con la creciente amenaza cibernética como: a) el robo de la identidad, b) estafas en línea y fraude, c) distribución de malware, d) integridad y disponibilidad de la información y e) distribución en línea de contenidos ilegales.

Hoy en día, con la incursión y la creciente cobertura de acceso del servicio de internet en la ciudadanía mexicana se han incrementado de forma exponencial la cantidad de los dispositivos conectados a internet, como se muestra a continuación:

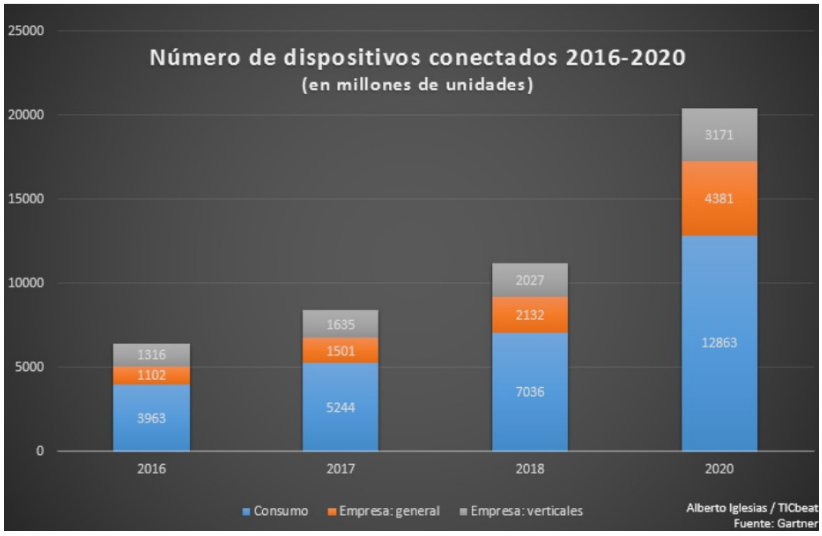


Gráfico 6 - Numero de Dispositivos Conectados 2016-2020 – Fuente: (Fraga, 2018)

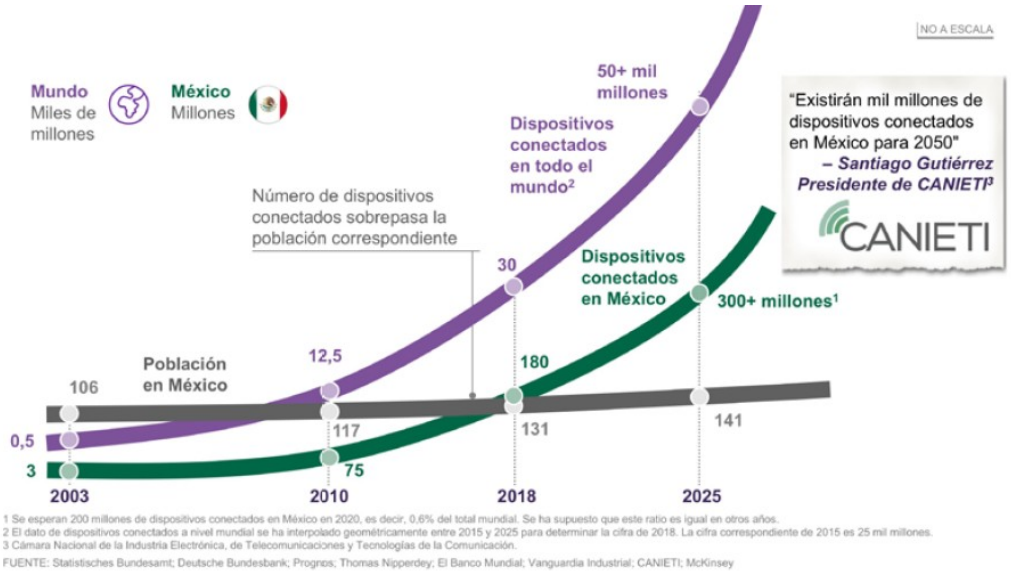


Gráfico 7 - Cada vez más Dispositivos Conectados – Fuente: CANIETI

Lo anterior, nos ha enseñado que el creciente número de dispositivos conectados a internet ha provocado el incremento de ataques más grandes y complejos poniendo en riesgo la seguridad, disponibilidad y resiliencia de los mismos. Por otra parte, se han integrado diversos grupos hacktivistas que ejecutan dichos ataques desde otros países teniendo consecuencias devastadoras para las empresas, gobierno y la ciudadanía que hace uso de las TIC's. La naturaleza de estos ataques va más allá de las leyes y regulaciones nacionales, sino que trascienden a varios países. Por lo que es necesario adaptar las leyes de México para que se puedan perseguir a los cibercriminales sin importar en donde se encuentren.

Es importante mencionar que los delitos informáticos se encuentran tipificados en el Código Penal Federal en los artículos 211 (bis 1 al 5 y 7), 424 bis y 429; en la Ley General del Sistema Nacional de Seguridad Pública, Artículo 139; y en 21 legislaciones estatales. Aunque los delitos informáticos estén *"definidos"* en las leyes mexicanas no existe una claridad efectiva para perseguir un ciberdelito. Por ejemplo, cuando un ciberdelito se lleva acabo se tiene que demostrar a un juez que el activo tecnológico en cuestión se encontraba protegido. Cada perito puede tener una definición diferente sobre el activo tecnológico protegido por un mecanismo de seguridad, lo anterior es uno de los principales

problemas que tiene México en ese sentido. Poniéndolo de otra forma, si el dispositivo tecnológico no contaba con un mecanismo de autenticación o protección a los ojos del perito o juez significa que no existe un delito que perseguir.

Es necesario tener bien definido y claro los diferentes tipos y vectores de los ciberdelitos con el objeto de asegurar que la investigación y fiscalización de los mismos sea eficiente. Aunado a lo anterior, es visto que los ciberdelitos abarcan una gran cantidad de actividades o conductas que pueden afectar no solamente aspectos tecnológicos, sino financieros e incluso hasta el robo de identidad y/o la trata de personas. Adicionalmente y desafortunadamente estos se clasifican como figuras legales como lo es: a) robo, b) falsificación y/o c) fraude.

La complejidad y su diversidad de los ciberdelitos han dificultado su definición y por ende la persecución y evaluación de las sanciones correspondientes al daño ocasionado. Es importante tener en cuenta que es necesario mantener un marco legal regulado y actualizado que no impacte en el ejercicio de los derechos humanos y/o en la criminalización a quienes su profesión sea el análisis y entendimiento de los ciberataques.

6.

6.1. Situación Actual del Marco Legal en México

Actualmente, en México existe un documento oficial liberado el 13 de noviembre de 2017, el cual da vida a la Estrategia Nacional de Ciberseguridad y dentro de su séptimo eje transversal “Marco jurídico y autorregulación” estipula lo siguiente: “las acciones orientadas a la adecuación del marco jurídico nacional y el desarrollo de mecanismos de autorregulación en la era digital son vitales para el desarrollo de la digitalización en el mundo y clave para para la prevención de riesgos y amenazas, la investigación y sanción de los delincuentes en la era digital”. Por lo anterior, es necesario que se construyan los instrumentos legales y regulatorias que permitan erradicar los ciberdelitos.

Por otro lado, se han creado organismos como el CISEN, el CERT-MX de la División Científica de la Policía Federal y se está consolidado un centro de operaciones del ciberespacio de la (SEDENA), y la actual creación de la dirección de ciberseguridad del Banco de México (Banxico) los anteriores tienen como objetivos mantener la estabilidad y seguridad del gobierno mexicano, entre otras funciones. Lo anterior, han sido estrategias de mecanismos de respuesta a incidentes informáticos. Existen en México tres autoridades en respuestas de ciberataques y son las siguientes: a) Unidad de Investigaciones y Operaciones Tecnológicas (PGR) b) Policía Federal a través de la División Científica y c) Centro de Investigación y Seguridad Nacional (CISEN).

Dentro del marco legal en México, existe dos mecanismos para la protección de datos personales, uno es aplicable a los organismos no gubernamentales (***Ley Federal de Protección de Datos Personales en Posesión de los Particulares***) y la segunda aplica únicamente a los organismos gubernamentales (***Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados***). Las anteriores, tienen como objetivo proteger la información personal contra algún daño, pérdida, destrucción, uso, acceso o tratamiento no autorizado. Así mismo, estas leyes obligan a dichos organismos (gubernamentales y no gubernamentales) que manejan datos personales a garantizar la confidencialidad y manejo/transferencia de los datos con otras entidades.

Por otro lado, para implementar los mecanismos de seguridad y protección de los datos personales es necesario que se tengan en consideración todos los posibles riesgos que se han mencionado previamente. Es necesario que se implementen un sistema de gestión de protección de datos personales (SGPDP). El cual permitirá la identificación y clasificación de los datos, análisis de riesgos, controles/mecanismos de seguridad, seguimiento y medición de la efectividad de los mismos y la mejora continua del SGPDP.

El ***Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*** (INAI), desarrolla y publica material para asistir

a organismos que manejan datos personales, y así cumplir sus responsabilidades. Cualquier organización que no se apegue a este marco legal está sujeta a sanciones, pero estas pueden atenuarse si la autoridad considera que la organización siguió las recomendaciones del INAI.

Lo anterior, nos muestra que el gobierno mexicano ha realizado grandes esfuerzos para combatir los ciberdelitos, pero el avance de la tecnología y su creciente demanda han sobrepasado dichos esfuerzos, y como se ha mencionado previamente en este proyecto la complejidad, diversidad y el alto impacto de estos ciberdelitos pudieran tener graves consecuencias, incluso para el estado mexicano.

Esto nos ha llevado a generar una propuesta general en el marco legal que permita la protección de los activos críticos, así como de la ciudadanía en general creando una estrategia de resiliencia la cual se detallará a continuación.

6.2. Propuesta de Mejora

Como se ha mencionado previamente en este capítulo, es necesario que se haga una revisión y una actualización de las leyes penales y procesales permitiendo tipificar, dar seguimiento y fiscalización de los actuales y emergentes ciberdelitos sin obstaculizar la innovación ni la adopción de nuevas tecnologías de la información, respetando siempre los derechos humanos y la privacidad de los datos. Lo anterior, se puede alcanzar si se otorga a los jueces, fiscales y unidades de investigación policial recursos humanos especializados en la materia de ciberseguridad.

Por otro lado, es necesario fortalecer y autorregular la industria de forma voluntaria basándonos en las mejores prácticas, como la mejor práctica 38 BCP “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing” y la mejor práctica 84 BCP” Ingress Filtering for Multihomed Networks” del grupo de trabajo de ingeniería de internet (IETF, por sus siglas en inglés). Las anteriores, no son las únicas que existen, pero las anteriores hacen referencia a las mejores prácticas referente a la protección del

uso del internet y que están respaldadas por un grupo de expertos multidisciplinarios que forman parte del IETF. Existen diversas mejores prácticas que pueden ser aplicables y que han sido presentadas por la sociedad de internet a través del programa de *Deploy360 Programme.*

Adicionalmente, se debe fortalecer las capacidades de las autoridades legales y fiscales del país, el poder contar con abogados especialistas en materia de ciberdelitos es muy complicado y por consiguiente caro. De acuerdo al informe técnico – Destrezas en Materia de Redes en América Latina, en México se pronostica que casi 148 mil puestos en tecnologías de redes no se podrán ocupar para el 2019; cerca de 36 mil de estos puestos de trabajo estarán relacionados con ciberseguridad (Pineda and González, 2016). Los esquemas de educación en materia de derecho cuentan con asignaciones o talleres especializados en materia de ciberseguridad, pero desafortunadamente en las universidades estos son opcionales/optativos o en el peor de los casos no existen. Hoy en día, México carece de oficiales de policía, fiscales, jueces, investigadores judiciales y expertos forenses en los diferentes niveles de gobierno como lo son: federal, estatal y municipal que tengan entendimiento del delito cibernético y puedan procesar y enjuiciar a criminales con éxito. Es clara la necesidad de aumentar la capacidad profesional en temas relacionados con la ciberseguridad. El nivel técnico de estos temas deberá ser el necesario para que sea de un entendimiento a nivel público.

Otro punto a considerar, es la adopción de leyes que permitan ser compatibles con la incorporación de México con convenios y/o tratados internacionales que permita eliminar los refugios seguros para los ciberdelincuentes y que en coordinación con otros países a través de la cooperación bilateral se les pueda perseguir sin importar donde se encuentren. Adicionalmente, con lo anterior se podrá minimizar riesgos cuando existen intermediarios y otras partes inocentes que se encuentran sujetos a obligaciones o responsabilidades contradictorias. Una medida que se puede considerar es la posible integración de México en el convenio de Budapest.

El Convenio de Ciberdelincuencia, también conocido como el Convenio de Budapest, es el primer tratado internacional sobre delitos cometidos a través de internet y otras redes informáticas. Se ocupa especialmente de infracciones sobre derechos de autor, fraude informático, pornografía infantil y violaciones de la seguridad de la red. Su principal objetivo es perseguir una política criminal común, dirigida a la protección de la sociedad contra el delito cibernético. Esto, mediante la adopción de una legislación apropiada y el fomento de la cooperación internacional por la naturaleza transnacional del tema.

A la fecha, el Convenio de Budapest ha sido ratificado por 57 países, de los cuales, 14 no son miembros del Consejo de Europa, incluyendo Estados Unidos, Canadá, Chile, Costa Rica y República Dominicana (Abusaid et al., 2018). La adhesión a este tipo de tratados permitirá a los diferentes gobiernos articular las políticas públicas de seguridad nacional con el ciberespacio y las TIC’s generando un marco de normas, conductas y principios relacionados con el manejo de las TIC’s garantizando la seguridad nacional y económica del país.

Ahora, para que México pueda adherirse al convenio es necesario cumplir principalmente con dos puntos principales, el primero es tipificar ciertas conductas enlistadas y definidas dentro del convenio como delitos del orden nacional, para este caso hacer las modificaciones o un nuevo apartado al Código Penal Federal (CPF), segundo, dotar a las autoridades en materia de procuración de justicia penal de las facultades y herramientas procedimentales necesarias para realizar la investigación de dichos delitos, fortaleciendo las capacidades de inteligencia y vigilancia. Para el primer punto es necesario definir de forma clara, precisa, así como los máximos y mínimos de pena aplicable para una de las conductas especificada en el convenio.

Si bien el convenio establece que en lo que respecta al mismo, se deberá “garantizar el debido equilibrio entre la acción penal y el respeto de los derechos humanos fundamentales”. Lo anterior, genera una interesante controversia, ya que en México no puede aplicarse algún tipo de pena cuya tipificación sea vaga, imprecisa, vaga o amplia, lo cual se sustenta en los artículos 14 y 16 de la

Constitución Política de los Estados Unidos Mexicanos, donde se estable el principio de legalidad o irretroactividad de la ley, lo cual implica que nadie podrá ser juzgado por un delito que no esté previsto en una ley anterior a la comisión del hecho en cuestión, así como la definición clara y precisa del delito. Por lo tanto, el convenio impone las modificaciones en la legislación nacional, tipificando los delitos que el tratado prevé de conformidad con el principio de exacta aplicación de la ley penal. Por otro lado, llevar a cabo dicho proceso de implementación con absoluta transparencia, partiendo desde una perspectiva de derechos humanos que incorpore en todo momento los comentarios y observaciones de las múltiples partes interesadas, particularmente de la sociedad civil.

Con base en lo anterior, si se hacen las adecuaciones a la legislación nacional, por una parte, se podrá tener una base para poder dar seguimiento y persecución a los ciberdelitos, por otro lado, esto puede ser un proceso muy lento ya que existen cerca de 300 leyes federales, lo que nos da a pensar que, entre más leyes, el grado de especialización de los jueces para su correcta ejecución de las mismas deberá ser mayor y más si se trata de tratados internacionales. Una posible solución, es tipificar de forma dispersa cada delito cibernético en los diferentes apartados del CPF o generar un apartado exclusivo donde se detalle cada delito que especifica el convenio.

Es importante mencionar que se tiene que generar nuevos enfoques que permita la persecución de los ciberdelincuentes, para lo cual la OEA realizó una recomendación a la Oficina de la Presidencia de la Republica que fue la de “participar en un programa piloto de la policía de Londres junto con algunas firmas privadas de abogados que utilizan tribunales civiles para confiscar los activos tecnológicos de los ciberdelincuentes” (OEA, 2017). Otra recomendación, y que es aplicable a esta iniciativa fue “la apertura de comunicación e intercambio de información de forma segura entre las fuerzas del orden público y el sector privado generando un ambiente de confianza y de cooperación voluntaria” (OEA, 2017).

La UIC, dentro de sus funciones deberá liderar y coordinar el desarrollo de estas normas y ser el frente único para la comunicación de las mismas tanto a

nivel nacional como a nivel internacional en los foros y convenciones. Cabe mencionar que el desarrollo de las normas en materia de ciberseguridad es una tarea a largo plazo y la cual se deberá ir madurando poco a poco y con la ayuda de organismos internacionales como la OEA poder hacer realidad este marco legal y jurídico.

Las agencias policiales deberán integrarse a asociaciones internacionales como la Red Cumplimiento de las Comunicaciones No Solicitadas (UCENet), la cual tiene programas muy completos para combatir el correo SPAM (Correo no deseado que pudiera contener software malicioso). Lo anterior, permitirá a estas agencias estar a la vanguardia y tener conocimiento de primera mano de las últimas amenazas y permitirá la conexión con otros organismos policiales de alrededor de 27 países para el intercambio de información y experiencias.

En México, existen organismos policiales a nivel federal que se encargan de los ciberdelitos, sin embargo, se ha detectado que a nivel estatal y municipal existen muy pocas o casi nulas unidades policiales especializadas en materia de ciberseguridad y ciberdelitos. Lo anterior, nos lleva a que los estados no tienen experiencia en cómo darle seguimiento a este tipo de delitos que han causado pérdidas millonarias no solamente al gobierno sino también al sector privado que hace uso de las TIC’s. Los estados al encontrarse en esta situación piden apoyo a la policía federal para que les brinde el apoyo y atención, lo cual genera una sobrecarga de solicitudes a la división científica de la policía federal.

Por otra parte, es sabido que en México no contamos un organismo fiscal que se dedique únicamente a la atención de los ciberdelitos. Anteriormente, se había externado que si tipificamos los ciberdelitos como simple delitos estaríamos desperdiciando esfuerzos que actualmente hacen los organismos federales que se encargan de la mitigación de la ciberdelincuencia.

Dentro de este proyecto se propone atender las necesidades detectadas y crear estas unidades especializadas en ciberdelincuencia que permitan atender y dar seguimiento a los ciberdelitos y la persecución de los autores de dichos

ciberataques. Aunado a lo anterior, se deben crear los grupos de fiscales e investigadores especializados en materia de ciberseguridad que atiendan no únicamente a nivel federal, sino que trabajen a nivel estatal y municipal. Para complementar esta recomendación se deben crear los canales y métodos de comunicación segura entre la policía federal, estatal, municipal, unidades especializadas de ciberdelincuencia e incluso el sector privado para el intercambio y conocimiento en materia de ciberseguridad.

El plan de comunicación especificado anteriormente deberá ser propuesto por el gobierno mexicano quien es el que deberá definir y en caso de ser necesario hacer las modificaciones necesarias para que las leyes permitan este intercambio de información. No se puede obviar que los participantes en este plan de comunicación deberán tener obligaciones y roles que en caso de no cumplirse estos deberán ser sancionados con base al impacto que pudiera tener si la información se fugará, se modificara, no esté disponible o llegara usarse para fines distintos de los autorizados.

Será necesario hacer un análisis de identificación de las áreas de oportunidad dentro de las jurisdicciones donde haya mayor actividad de ciberdelincuencia, así como la identificación de las áreas en donde se pueda encontrar la mayor evidencia posible para el correcto enjuiciamiento y ejecución de las leyes que castiguen la ciberdelincuencia en México. Lo anterior, deberá estar alineado con la estrategia nacional de ciberseguridad del país dentro del eje transversal “Marco jurídico y autorregulación”.

Conclusiones

Conclusiones

Dentro del alcance del documento se habla de la creación de una unidad inteligente de ciberseguridad (UIC) para la Administración Pública Federal del gobierno mexicano, la cual tiene como objetivo principal la protección de los activos tecnológicos del gobierno federal. Lo anterior, nos enseñó que antes de iniciar con cualquier definición es necesaria proponer una estrategia de liderazgo y de colaboración entre las diferentes oficinas del gobierno mexicano las cuales al día de hoy trabajan de forma descentralizada en materia de ciberseguridad.

Se definieron las acciones necesarias para que todas las dependencias queden alineadas mediante una iniciativa del ejecutivo federal y la cual deberá ser de carácter mandatorio. Entre las principales acciones se detallan las funciones y atribuciones que deberá tener la UIC, así como la creación de canales y métodos de comunicación e intercambio de información de forma segura.

Por otro lado, para que la colaboración e intercambio de información sea eficiente se deberá generar una estrategia de colaboración que permita crear un vínculo de confianza no únicamente entre las diferentes oficinas del gobierno federal sino hacia los diferentes niveles de gobierno estatal y municipal, así como el vínculo hacia la ciudadanía mexicana que hace uso de las diferentes iniciativas de comercio electrónico (E-Commerce) del gobierno y del uso apropiado del servicio de internet de los ciudadanos.

En un segundo punto, antes de implementar cualquier mecanismo y control de ciberseguridad, es necesario realizar una estrategia que permita la identificación de las diferentes infraestructuras de tecnologías de la información que tienen que ser protegidas, para esto se definió un enfoque estratégico que permita identificar cada uno de los diferentes activos de TIC’s, así como los diferentes sectores y subsectores del gobierno. Por otra parte, es necesario la identificación de los diferentes procesos críticos y a su vez poder medir la criticidad de cada uno de los activos de TIC’s. Lo anterior, nos va a permitir

generar un catálogo general de infraestructuras críticas de TIC’s, el cual al día de hoy se encuentra de forma descentralizada en el mejor de los casos y en el peor no existe. Aunado a lo anterior, es necesario definir los diferentes roles y responsabilidades que van a tener cada uno de los interesados de esta iniciativa para que puedan trabajar de forma transparente y eficiente.

Sin perder el objetivo principal de la creación de la UIC tuvimos que detallar los primeros pasos para que se abriera el camino para la creación de esta unidad que deberá trabajar de forma transversal con todas las diferentes dependencias del gobierno federal y la cual deberá ser apoyada por el primer mandatario del poder ejecutivo. Por otro lado, se tiene que hacer la identificación de lo que se va a proteger y realizar una definición de los roles y responsabilidades de cada uno de los diferentes actores que formarán parte de este plan estratégico.

Para que exista un modelo de gobierno de ciberseguridad de TIC’s que trabaje de forma transversal deberá existir una estrategia nacional de ciberseguridad que sea el modelo y vincule no solamente la tecnología entre los diferentes niveles de gobierno, sino que enlace los diferentes sectores privados, educativos, judiciales, penales e incluso se respete los derechos humanos de los ciudadanos mexicanos.

Para esto se debe construir una delta de alianzas estratégicas entre el sector privado que es líder en las TIC’s, por otro lado, tenemos que incorporar al sector educativo quien nos estará brindando la investigación y desarrollo en materia de ciberseguridad y finalmente el sector público quien tiene como obligación la protección de los activos críticos de TIC’s de todo el gobierno en los diferentes niveles de México. Cabe mencionar que la responsabilidad de la ciberseguridad no es únicamente del sector público sino de todos. Por eso desde un inicio se trabajó en las estrategias de liderazgo, colaboración entre dependencias y con los diferentes sectores y subsectores de México que forman y hace uso de las TIC’s.

Se identificaron diferentes empresas, universidades y centros de investigación que son líderes en ciberseguridad y que, si se abre ese canal de comunicación e intercambio de información, podemos reducir de forma considerable las brechas de seguridad que tienen o pudieran tener los diferentes activos críticos de TIC’s.

Hasta este punto ya tenemos todos los elementos necesarios para la definición de la UIC que servirá como una secretaría de ciberseguridad, la cual deberá trabajar en conjunto con los diferentes organismos que actualmente persiguen y enjuician a los ciberdelincuentes. La UIC podrá apoyar de forma transversal y brindará servicios de seguridad de la información, podrá realizar análisis para la identificación de las brechas de seguridad de los activos críticos de las dependencias.

También la UIC deberá ser el líder para la elaboración de las normas y modificaciones en conjunto con los diferentes organismos jurídicos y legales que actualmente dictan las leyes en materia de ciberdelitos. La UIC se encargará de darle seguimiento y continuidad a la actual estrategia nacional de ciberseguridad y apoyar a la creación de un modelo de ciberseguridad de TIC’s para todo el gobierno mexicano.

Lo anterior no podría funcionar si no mejoramos y capacitamos a todos los servidores públicos que hacen uso de las TIC’s, recordemos que el eslabón más de la cadena de protección de los activos es el factor humano, el cual es impredecible y no podemos controlar. Lo que sí se puede hacer es evangelizarlo y crearle conciencia sobre los diferentes riesgos y consecuencias que pueden ser catastróficas y que han causado una pérdida millonaria a muchos ciudadanos mexicanos, no olvidemos al inicio del año, el robo de aproximadamente 300 millones de pesos que sufrió la banca mexicana debido a la explotación de brechas de seguridad.

Se definió un modelo de implementación de un programa de concientización de ciberseguridad para todas las oficinas del gobierno a través un

modelo de gestión descentralizado que fue seleccionado por la naturaleza, roles y funciones del gobierno. Se estableció un análisis de necesidades para la identificación de las áreas de oportunidad que se tienen actualmente, se definió una estrategia de implementación basada en la metodología NIST que permite tener el gobierno y seguimiento del avance de la implementación.

Así mismo, se definió un plan de comunicación para dar a conocer o en su caso definir las políticas de ciberseguridad a cada una de las diferentes oficinas. Y finalmente, generar las métricas e indicadores necesarios para la medición de la efectividad del programa y poder identificar qué, no está funcionando o está dando los resultados esperados y tomar una decisión y hacer los cambios necesarios.

Por último, para que tenga un sustento legal el proyecto fue necesario hacer una revisión del actual marco legal y jurídico del país, se identificaron varios retos en los cuales se tienen que ajustar las actuales leyes para que los ciberdelitos puedan ser perseguido no importando donde se realizó. Por otro lado, México se tiene que adherir a convenios y tratados internacionales como el de Budapest para que el intercambio y las facilidades se puedan dar.

Así mismo, es necesario generar la capacidad de conocimiento y apoyo a las diferentes instancias legales y jurídicas para que puedan atender los asuntos de ciberdelincuencia. Ahora, se puede tener la mejor ley del mundo, hecha por los mejores especialistas del planeta, pero si no se tiene a la gente capacitada en México para entender, interpretar y ejecutar esa ley no sirve absolutamente de nada. No sólo falta mejorar la ley mexicana sino tener protocolos de investigación y tener autoridades capaces que entiendan del tema. El reto de la próxima administración en materia de ciberseguridad será enlazar la Estrategia Nacional de Ciberseguridad, con el marco jurídico mexicano para que haya obligatoriedad de cumplirla.

Bibliografía

1. Abusaid, D., Cristofori, A., Fernández, R. and Waisser, S. (2018). Perspectiva de ciberseguridad en México - PDF. [en línea] Docplayer.es. Disponible en: https://docplayer.es/85016373-Perspectiva-de-ciberseguridad-en-mexico.html [Consultado el 14 agosto 2018].
2. Assets.publishing.service.gov.uk. (2011). The UK Cyber Security Strategy. [en línea] Disponible en: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf [Consultado el 28 nov. 2018].
3. Azcona, J. (2018). Definición de ciberseguridad y riesgo. [en línea] ICEMD. Disponible en: https://www.icemd.com/digital-knowledge/articulos/definicion-ciberseguridad-riesgo/ [Consultado el 26 Nov. 2018].
4. Bologna, S., Hämmerli, B., Gritzalis, D., & Wolthusen, S. (2011). Critical Information Infrastructure Security (6th ed., pp. 1-17). Lucerne, Switzerland: Springer Heidelberg NewYork Dordrecht London. Disponible en: http://www.springer.com
5. Budget.gc.ca. (2018). Budget 2015 - Chapter 4.3: Protecting Canadians. [en línea] Disponible en: https://www.budget.gc.ca/2015/docs/plan/ch4-3-eng.html [Consultado el 31 Jan. 2018].
6. Budget.gc.ca. (2019). Equality + Growth - Strong Middle Class. [en línea] Disponible en: https://www.budget.gc.ca/2018/docs/plan/budget-2018-en.pdf [Consultado el 21 enero 2019].
7. Building an Information Technology Security Awareness and Training Program. Consultado en: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-50.pdf
8. Buyandsell.gc.ca. (2018). Procedures for invoking a national security exception. [en línea] Disponible en: https://buyandsell.gc.ca/policy-and-guidelines/supply-manual/section/3/105/10 [Consultado el 17 enero de 2019].

9. Canada's Cyber Security Strategy For a stronger and more prosperous Canada. (n.d.). 1st ed. [Libro Electrónico] Ottawa, p.4. Disponible en: http://publications.gc.ca/site/eng/9.693830/publication.html [Consultado el 17 diciembre de 2018].
10. Canada's Cyber Security Strategy. (2010). Public safety Canada. Retrieved 24 February 2017, disponible en: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-en.aspx
11. Cybercrime / Cybercrime / Crime areas / Internet / Home - INTERPOL. (2017). Interpol.int. Consultado el 24 enero 2017 en: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
12. Data.ssp.cdmx.gob.mx. (n.d.). SSP | Secretaría de Seguridad Pública. [en línea] Disponible en: http://data.ssp.cdmx.gob.mx/ciberdelincuencia.html [Consultado el 19 Feb. 2019].
13. Databreaches.net. (2016). Personal info of 93.4 million Mexicans exposed on Amazon (UPDATED). [en línea] Disponible en: https://www.databreaches.net/personal-info-of-93-4-million-mexicans-exposed-on-amazon/ [Consultado el 8 enero 2019].
14. Diputados.gob.mx. (2005). [en línea] Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LSegNac.pdf [Consultado el 22 febrero 2019].
15. Diputados.gob.mx. (2016). Constitución Política de los Estados Unidos Mexicanos. [en línea] Disponible en: http://www.diputados.gob.mx/LeyesBiblio/htm/1.htm [Consultado el 22 febrero 2019].
16. Estrategia Nacional de Ciberseguridad. (2018). Disponible en: https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf
17. Fas.org. (2018). Critical Infrastructure Protection (PDD 63). [en línea] Disponible en: https://fas.org/irp/offdocs/pdd/pdd-63.htm [Consultado el 20 diciembre 2018].

18. Fge.jalisco.gob.mx. (n.d.). Policía cibernética | Fiscalía General del Estado. [en línea] Disponible en: https://fge.jalisco.gob.mx/policia-cibernetica [Consultado el 19 febrero 2019].
19. Fraga, A. (2018). Internet de las Cosas: 8.400 millones de dispositivos conectados.... [en línea] TIC beat. Disponible en: http://www.ticbeat.com/innovacion/internet-de-las-cosas-8400-millones-dispositivos-conectados-2017/ [Consultado el 10 agosto 2018].
20. Govcert.cz. (2017). The Czech Republic opened National Cyber Security Center. [en línea] Disponible en: https://www.govcert.cz/en/info/events/2456-the-czech-republic-opened-national-cyber-security-center/ [Consultado el 12 Feb. 2019].
21. Infografías del MAAGTICSI. [en línea] gob.mx. Disponible en: https://www.gob.mx/cidge/documentos/infografias-del-maagticsi [Consultado el 5 de febrero 2019].
22. ITU. (2015). Índice mundial de ciberseguridad y perfiles de ciberbienestar. [en línea] Disponible en: http://www.itu.int/pub/D-STR-SECU-2015/es [Consultado el 30 enero 2019].
23. M.isaca.org. (n.d.). Estudio de la Seguridad de la Información en México 2017. [en línea] Disponible en: https://m.isaca.org/chapters4/Mexico-City/Documents/Estudio%20de%20la%20Seguridad%20de%20la%20Informaci%C3%B3n%20en%20M%C3%A9xico%202017.pdf [Consultado el 30 enero 2018].
24. OEA. (2017). Hacia una Estrategia Nacional de Ciberseguridad [Ebook] (1st ed.). Ciudad de México. Disponible en: https://www.gob.mx%2Fmexicodigital%2Farticulos%2Fhacia-la-estrategia-nacional-de-ciberseguridad%3Fidiom%3Des&usg=AOvVaw3JYbDYwNbiPaZKha2LKmbm
25. Overview. (2017). Alexandrasamuel.com. Consultado el 25 enero 2017 en: http://www.alexandrasamuel.com/dissertation/index.html

26. Pineda, E. and González, C. (2016). INFORME TÉCNICO - Destrezas en materia de redes en América Latina. [en línea] cisco.com. Disponible en: http://www.bing.com/cr?IG=6DF5C404D388465CB22C2899D9EC08CA&CID=160AE4FD2F8F64B6371BE8B62E7265D7&rd=1&h=3M9taOUHmDMkKCfecpPHk33wXe4zldysiM7KuM9S9HU&v=1&r=http%3a%2f%2fcsrinfo.cisconetspace.com%2frs%2f059-VFZ-834%2fimages%2fCisco-Skills-Gap.pdf%3fpdf%3dSkills-Gap&p=DevEx.LB1,5041.1 [Consultado el 14 agosto 2018].
27. Pnd.gob.mx. (2013). Plan Nacional de Desarrollo (PND) 2013-2018. [en línea] Disponible en: http://pnd.gob.mx/ [Consultado el 22 Feb. 2019].
28. Programa para la Seguridad Nacional 2014 - 2018. (2014). Programa para la Seguridad Nacional 2014 - 2018. [en línea] Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5342824&fecha=30/04/2014 [Consultado el 22 febrero 2019].
29. Programa para un Gobierno Cercano y Moderno (PGCM). (2017). gob.mx. Consultado el 24 enero 2017 en: http://www.gob.mx/sfp/acciones-y-programas/programa-para-un-gobierno-cercano-y-moderno-pgcm
30. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. (2017). Disponible en: https://www.enisa.europa.eu/events/enisa-cscg-2017/presentations/boratynskiElectrónico C. (2019).
31. Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience. (2012). Disponible en: http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf
32. Sánchez Onofre 19 de julio de 2017, J. (2017). Policía Federal quiere un Consejo Nacional de Ciberseguridad. [en línea] El Economista. Disponible en: https://www.eleconomista.com.mx/tecnologia/Policia-Federal-quiere-un-Consejo-Nacional-de-Ciberseguridad-20170719-0101.html [Consultado el 22 febrero 2019].

33. Slideshare.net. (2018). Enterprise Security Architecture for Cyber Security. [en línea] Disponible en: https://www.slideshare.net/OpenGroupSA/enterprise-security-architecture-for-cyber-security [Consultado el 1 marzo 2018].
34. Sseguridad.edomex.gob.mx. (n.d.). Policía Cibernética | Secretaría de Seguridad. [en línea] Disponible en: http://sseguridad.edomex.gob.mx/seguridad-publica-transito/policia-cibernetica [Consultado el 19 febrero. 2019].
35. U.S. Government Accountability Office (U.S. GAO). (2019). Disponible en: https://www.gao.gov/
36. Unidad de Innovación Gubernamental y Mejora Regulatoria. (n.d.). Gobierno del Estado de Hidalgo. [en línea] Disponible en: http://policiacibernetica.hidalgo.gob.mx/ [Consultado el 19 febrero 2019].
37. Unodc.org. (2018). 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. [en línea] Disponible en: https://www.unodc.org/documents/congress//Documentation/A-CONF.222-12_Workshop3/ACONF222_12_s_V1500666.pdf [Consultado el 28 Nov. 2018].
38. User, S. (2018). Estudio de Inversiones Gubernamentales en TIC's. [en línea] Asociaciondeinternet.mx. Disponible en: https://www.asociaciondeinternet.mx/es/estudios [Consultado el 17 enero 2019].

Glosario de Términos

1. **Activo de información**

   - Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

2. **Amenaza**

   - Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad.

3. **Análisis de riesgos**

   - Es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para tratar el riesgo.

4. **Auditoría de seguridad**

   - Es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales en tecnologías de la información con el objetivo de identificar, enumerar y describir las diversas vulnerabilidades que pudieran

presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones, servidores o aplicaciones.

5. **Ataque de fuerza bruta**

   - Un ataque de fuerza bruta es un procedimiento para averiguar una contraseña que consiste en probar todas las combinaciones posibles hasta encontrar la combinación correcta.

6. **Autenticación**

   - Procedimiento para comprobar que alguien es quién dice ser cuando accede a un ordenador o a un servicio online. Este proceso constituye una funcionalidad característica para una comunicación segura.

7. **Aviso Legal**

   - Un aviso legal es un documento, en una página web, donde se recogen las cuestiones legales que son exigidas por la normativa de aplicación.

8. **Bluetooth**

   - La tecnología Bluetooth es una tecnología inalámbrica de radio de corto alcance, cuyo objetivo es eliminar los cables en las conexiones entre dispositivos electrónicos, simplificando así las comunicaciones entre teléfonos móviles, ordenadores, cámaras digitales y otros dispositivos informáticos operando bajo la banda de radio de 2.4 GHz de frecuencia.

9. **Botnet**

   - Una botnet es un conjunto de ordenadores (denominados bots) controlados remotamente por un atacante que pueden ser utilizados en conjunto para realizar actividades maliciosas como envío de spam, ataques de DDoS, etc.

10. Certificado digital

- Un certificado digital es un fichero informático generado por una entidad denominada Autoridad Certificadora (CA) que asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital en Internet.

11. CIO

- Chief Information Officer. Es el director encargado del área de tecnologías de la información. Tiene a su cargo la planeación de la estrategia del uso y apropiación de las TIC's.

12. Cloud Computing

- El término "C*loud Computing"* o computación en la nube se refiere a un paradigma que permite ofrecer servicios de computación a través de una red, que usualmente es Internet. Esta tendencia permite a los usuarios almacenar información, ficheros y datos en servidores de terceros, de forma que puedan ser accesibles desde cualquier terminal con acceso a la nube o a la red, resultando de esta manera innecesaria la instalación de software adicional (al que facilita el acceso a la red) en el equipo local del usuario.

13. Confidencialidad

- Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.

14. Denegación de servicio (DoS)

- Se entiende como denegación de servicio o como DoS (Denial of Service, por sus siglas en inglés), en términos de seguridad informática, a un conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca sobrecargar un servidor y de esta

forma impedir que los usuarios legítimos puedan utilizar los servicios prestados por él.

15. Disponibilidad

- Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.

16. Exploit

- Secuencia de comandos utilizados para, aprovechándose de un fallo o vulnerabilidad en un sistema, provocar un comportamiento no deseado o imprevisto.

17. Firma electrónica

- La firma electrónica (o digital) se define como el conjunto de datos electrónicos que acompañan o que están asociados a un documento electrónico y la debe cumplir las siguientes propiedades o requisitos:

  - ✓ Identificar al firmante.
  - ✓ Verificar la integridad del documento firmado.
  - ✓ Garantizar el no repudio en el origen.
  - ✓ Contar con la participación de un tercero de confianza.
  - ✓ Estar basada en un certificado electrónico reconocido.
  - ✓ Debe de ser generada con un dispositivo seguro de creación de firma.

18. Fuga de datos

- La fuga de datos o fuga de información es la pérdida de la confidencialidad de la información privada de una persona o empresa. Información que, a priori, no debería ser conocida más que por un grupo de personas, en el ámbito de una organización, área o actividad, y que termina siendo visible o accesible para otros.

19. Incidente de seguridad

- Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

20. Informática forense

- La informática forense consiste en un proceso de investigación de los sistemas de información para detectar toda evidencia que pueda ser presentada como prueba fehaciente en un procedimiento judicial.

21. Ingeniería social

- Las técnicas de ingeniería social son tácticas utilizadas para obtener información datos de naturaleza sensible, en muchas ocasiones claves o códigos, de una persona. Estas técnicas de persuasión suelen valerse de la buena voluntad y falta de precaución de la víctima.

22. Integridad

- La Integridad es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales.

23. Malware

- Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de software malintencionado: malicious software.

24. Metadatos

- Los metadatos son el conjunto de datos relacionados con un documento y que recogen información fundamentalmente descriptiva del mismo, así como información de administración y gestión. Los metadatos son información que enriquece el documento al que está asociado.

25. No repudio

- El no repudio en el envío de información a través de las redes es la capacidad de demostrar la identidad del emisor de esa información. El objetivo que se pretende es certificar que los datos, o la información, provienen realmente de la fuente que dice ser.

26. Parche de seguridad

- Un parche de seguridad es un conjunto de cambios que se aplican a un software para corregir errores de seguridad en programas o sistemas operativos. Generalmente los parches de seguridad son desarrollados por el fabricante del software tras la detección de una vulnerabilidad en el software y pueden instalarse de forma automática o manual por parte del usuario.

27. Pruebas de Intrusión

- Una prueba de penetración es un ataque a un sistema software o hardware con el objetivo de encontrar vulnerabilidades. El ataque implica un análisis activo de cualquier vulnerabilidad potencial, configuraciones deficientes o inadecuadas, tanto de hardware como de software, o deficiencias operativas en las medidas de seguridad.

28. Phishing

- *Phishing* es la denominación que recibe la estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de

usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta.

29. Plan de contingencia

- Un Plan de Contingencia de las Tecnologías de la Información y las Comunicaciones (TIC) consiste en una estrategia planificada en fases, constituida por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación, encaminados a conseguir una restauración ordenada, progresiva y ágil de los sistemas de información que soportan la información y los procesos de negocio considerados críticos en el Plan de Continuidad de Negocio de la compañía.

30. Plan de continuidad

- ✓ Un Plan de Continuidad de Negocio es un conjunto formado por planes de actuación, planes de emergencia, planes financieros, planes de comunicación y planes de contingencias destinados a mitigar el impacto provocado por la concreción de determinados riesgos sobre la información y los procesos de negocio de una compañía.

31. Política de seguridad

- Son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riesgos a los que están expuestos.

32. Puerta trasera

- Se denomina backdoor o puerta trasera a cualquier punto débil de un programa o sistema mediante el cual una persona no autorizada puede acceder a un sistema.

33. Ransomware

- El ciberdelincuente, toma control del equipo infectado y «secuestra» la información del usuario cifrándola, de tal forma que permanece ilegible si no se cuenta con la contraseña de descifrado. De esta manera extorsiona al usuario pidiendo un rescate económico a cambio de esta contraseña para que, supuestamente, pueda recuperar sus datos.

34. SGSI

- Un Sistema de Gestión de la seguridad de la Información (SGSI) es un conjunto de políticas de seguridad de la información que siguen la norma ISO/IEC 27001. Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

35. SLA

- Un acuerdo de nivel de servicio o ANS (en inglés Service Level Agreement o SLA), es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.

36. Spoofing

- Es una técnica de suplantación de identidad en la Red, llevada a cabo por un ciberdelincuente generalmente gracias a un proceso de investigación o con el uso de malware. Los ataques de seguridad en las redes usando técnicas de spoofing ponen en riesgo la privacidad de los usuarios, así como la integridad de sus datos.

37. Spyware

- Es un malware que recopila información de un ordenador y después la envía a una entidad remota sin el conocimiento o el consentimiento del propietario del ordenador.

38. Troyano

- El troyano es un software malicioso que engaña al usuario presentándose como un programa normal, una vez instalado, permite la entrada de usuarios externos al equipo infectado, con el objetivo de obtener información, instalar virus o bien para controlarla remotamente.

39. Suplantación de identidad

- Es la actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude, acoso (cyberbulling).

40. Vulnerabilidad

- Fallos o deficiencias de un programa que pueden permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota.

41. XSS

- Se trata de una vulnerabilidad existente en algunas páginas web generadas dinámicamente en función de los datos de entrada). XSS viene del acrónimo en inglés de Secuencias de comandos en sitios cruzados (Cross-site Scripting). Dado que los sitios web dinámicos dependen de la interacción del usuario, es posible insertar en un formulario un pequeño programa malicioso, ocultándolo entre solicitudes legítimas y hacer que éste se ejecute. Los puntos de entrada comunes incluyen buscadores, foros, blogs y todo tipo de formularios alojados en una página web.

42. Zero-day

- Son aquellas vulnerabilidades en sistemas o programas informáticos que son únicamente conocidas por determinados atacantes y son desconocidas por los fabricantes y usuarios. Al ser desconocidas por los fabricantes, no existe un parche de seguridad para solucionarlas.