Scitum

UNIDADES CIBERNÉTICAS ESTATALES

SCI LABS
SCITUM CYBER INTELLIGENCE LABORATORIES

TELMEX
está contigo

LAS UNIDADES CIBERNÉTICAS ESTATALES EN MÉXICO

EL INCREMENTO DEL USO DE INTERNET EN MÉXICO

La era digital se caracteriza por el crecimiento acelerado de internautas a nivel mundial. De acuerdo con las cifras de la Unión Internacional de Telecomunicaciones (UIT)[1], en el mundo existen alrededor de 3,366 millones de cibernautas (41% de la población mundial), con una tasa de crecimiento anual aproximada de 18%.

Aunado a lo anterior, se espera que en nuestro país exista un incremento considerable en el número de usuarios de internet a nivel nacional derivado del decreto publicado en el Diario Oficial de la Federación el pasado 11 de junio de 2013, el cual indica que se garantizará el derecho de acceso a las tecnologías de la información y comunicación así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet.

México es uno de los países en Latinoamérica con más actividad en la red según un reporte emitido por la Organización de los Estados Americanos (OEA); hasta el momento, el escenario en nuestro país resalta un notable incremento en la cifra de cibernautas, pasando de 34.9 millones en 2010 a 65 millones en 2015 (59.8% de la población nacional2). Es muy importante destacar que para el 2018 se espera llegar a un 98% de la población conectada a internet mediante la implementación del proyecto "México Conectado" a cargo de la Secretaría de Comunicaciones y Transportes.

Un dato revelador del estudio sobre hábitos del Internet en México 2016, realizado por la Asociación Mexicana de Internet (AMIPCI), es que 22 millones (34%) de cibernautas son personas menores de edad, lo que muestra un gran número de posibles víctimas de delitos en contra de menores.[2]

Asimismo, este estudio muestra que el tiempo promedio de conexión a Internet de los cibernautas en México es de más de siete horas al día, incrementándose una hora más con respecto al año 2015. Es de destacar que el principal dispositivo de conexión es el smartphone y que el uso primordial es para acceder a redes sociales, correo electrónico, envío/recepción de mensajes instantáneos y búsqueda de información, en ese orden.

La AMIPCI identificó que en México se incrementó el comercio electrónico en 2014, llegando a movilizar más de 12 MDD, lo que representa un 34% más que en el año inmediato anterior.

Otro dato relevante es la importancia de las micro, pequeñas y medianas empresas (MIPYMES) en el desarrollo económico y social de la nación, ya que datos de Promexico refieren que existen cerca de 4.2 millones de MIPYMES que generan el 52% del Producto Interno Bruto (PIB) y el 72% de los empleos formales. El 95% de ellas son particularmente Pequeñas y Medianas e impulsan de manera relevante el crecimiento económico digital del país con el fortalecimiento de sus infraestructuras tecnológicas[3].

De acuerdo a cifras del INEGI[4], la Ciudad de México es la entidad con más hogares conectados a internet, seguidas por Nuevo León, Baja California Sur, Sonora, Quintana Roo, Colima, Jalisco, Yucatán y Tamaulipas; entre las menos conectadas se encuentran Chiapas, Oaxaca, Tabasco, Guerrero, Tlaxcala, Michoacán, Puebla, Veracruz, Durango y Zacatecas.

LOS AVANCES TECNOLÓGICOS UN NUEVO NICHO PARA LOS DELITOS CIBERNÉTICOS EN MÉXICO.

Los delitos que utilizan como medio o fin la tecnología (ciberdelitos), ofrecen un panorama cada vez más complejo que involucra a personas, empresas y gobiernos de todos los tamaños. Los recientes avances tecnológicos sin duda han sido beneficiosos para el desarrollo económico y social de todas las naciones, pero también han abierto la puerta a una creciente ola de delitos informáticos. El ciberespacio es una zona virtual donde converge una enorme cantidad de fuentes de información por lo que su uso en actividades cotidianas como el comercio electrónico, manejo de finanzas personales, mensajes o elementos difundidos en redes sociales, entre otros, pueden derivar en el menoscabo del patrimonio, la reputación, el honor o la actividad profesional de los individuos y de las organizaciones.

Dadas las tendencias nacionales e internacionales, las autoridades en nuestro país observarán un incremento constante en las incidencias delictivas cometidas a través de internet, tales como el acoso, el contacto a través de redes sociales con fines de trata de personas o pornografía infantil, fraudes, suplantación de identidad, entre otros; las cuales son conductas nocivas que están presentes cada vez más en nuestra sociedad digital. El incremento de los ciberdelitos va en estricta relación con el crecimiento exponencial del número de usuarios de internet, y en un futuro cercano, la ciberdelincuencia también irá de la mano con la capacidad de conexión considerada dentro del Internet de las Cosas (IoT por sus siglas en inglés).

Un estudio realizado por la firma de software Symantec señala que la cifra de víctimas del cibercrimen a nivel mundial es de aproximadamente 594 millones de usuarios al año.

En Latinoamérica, conforme a un estudio realizado por la Organización de los Estados Americanos (OEA) en colaboración con la firma Trend Micro[5], se observa un incremento en los delitos cometidos a través de la banca en línea.

Es de resaltar que, tomando como referencia las cifras publicadas por la Policía Federal en el 2015[6], los principales delitos cibernéticos a los que se enfrentarán las autoridades en las entidades federativas son:

- Fraude
- Extorsión
- Robo de contraseñas
- Infección por código malicioso
- Ramsomware (Criptoloker)
- Amenazas contra menores
- Pornografía infantil

El panorama anterior nos permite observar que las nuevas tecnologías y la alta demanda del servicio de Internet por parte de los ciudadanos, resultan un campo fértil para la delincuencia que ha encontrado nuevas formas para consumar delitos a través de dichos medios provocando que sea primordial que cada Entidad Federativa conozca el comportamiento nacional y local de este tema, lo que le permitirá definir las capacidades que requiere su Estado para atender el fenómeno de la ciberdelincuencia.

CAPACIDADES DE LAS UNIDADES CIBERNÉTICAS

Como hemos mencionado existe un notable incremento en el número de usuarios de internet, así como en las actividades que se realizan en el ciberespacio, entre las cuales destacan el comercio electrónico y las redes sociales; por lo que los ciudadanos mexicanos se encuentran cada vez más expuestos a ser víctimas del robo de información personal que deriva en fraudes, extorsiones, suplantación de identidad, entre otras afectaciones ocasionadas por la ciberdelincuencia.

Las autoridades no pueden dejar al azar la prevención, investigación y persecución de estos delitos, por lo que se requiere contar con recursos humanos especializados dentro de las instituciones encargadas de la seguridad pública que puedan hacer frente con eficacia a las actividades delictivas cometidas a través de dispositivos informáticos e Internet, siendo necesario para ello la creación o fortalecimiento de Unidades Cibernéticas en el país.

Para llevar a cabo lo anterior, el Programa Nacional de Seguridad Pública (PNSP) ha establecido en su estrategia 2.7.6 el desarrollo de un Modelo de Policía Cibernética para las Entidades Federativas cuya creación se encuentra a cargo de la Policía Federal, el cual sentará las bases de coordinación entre la Policía Federal y las Policías Estatales para la especialización de los elementos activos con los que cuenta cada entidad en materia de Ciberseguridad, con el objetivo de prevenir, atender e investigar en conjunto los delitos cibernéticos que afectan a la ciudadanía y la infraestructura crítica del Estado Mexicano.

La creación y fortalecimiento de las Unidades Cibernéticas, responde a la demanda ciudadana de atender los delitos cometidos a través de medios tecnológicos que afectan su patrimonio y seguridad, asimismo, tiene el objetivo de especializar al personal designado por las Entidades Federativas, con el fin de incrementar sus capacidades de prevención y atención a la ciudadanía.

MODELO DE CREACIÓN Y FORTALECIMIENTO PARA LAS UNIDADES CIBERNÉTICAS

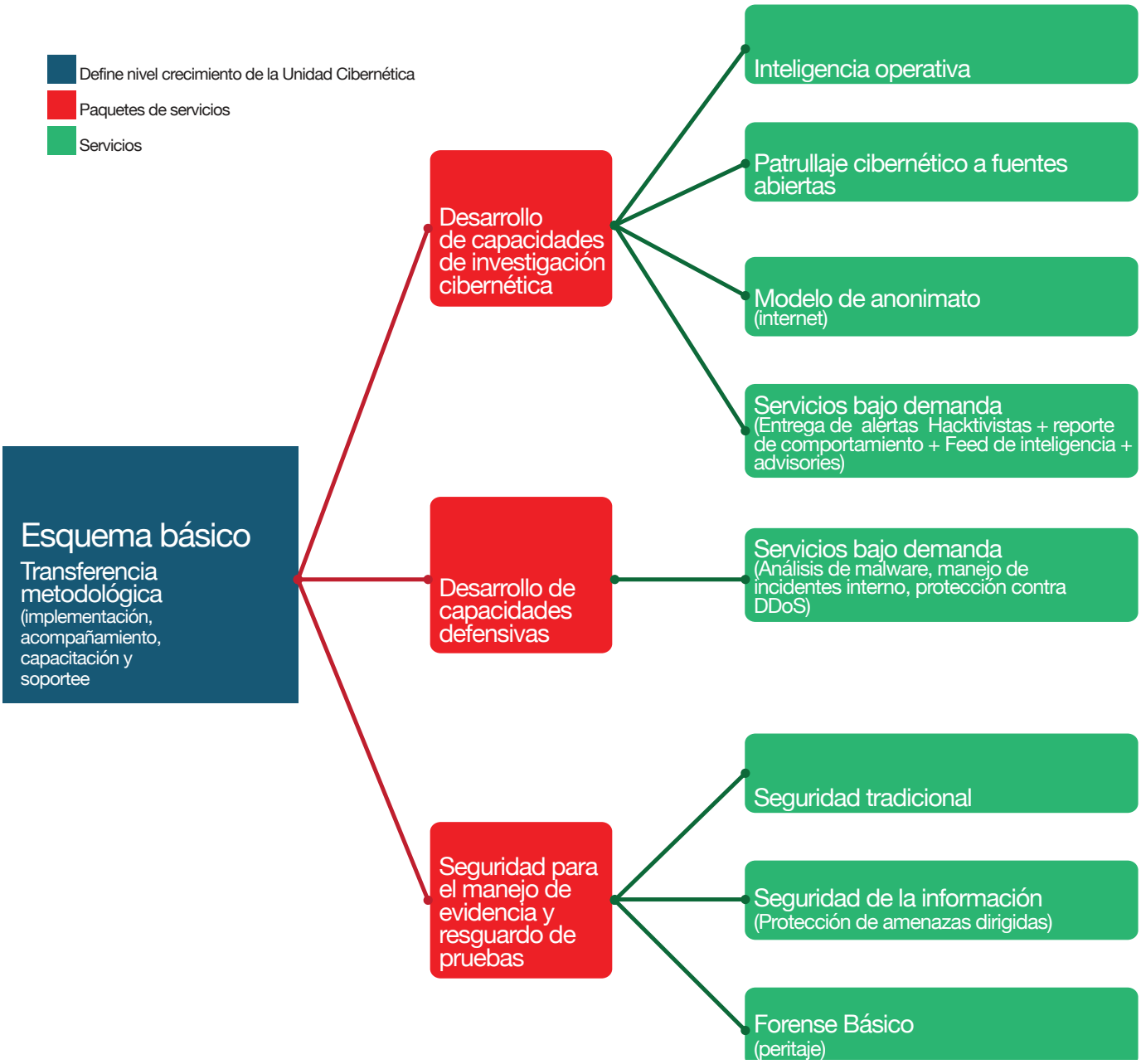
Para cumplir estas funciones, las Unidades Cibernéticas Estatales requieren contar con soluciones, servicios, procesos, herramientas tecnológicas y capacitación que les permitan llevar a cabo acciones de prevención, atención e investigación de delitos cibernéticos a fin de disminuir y prevenir la incidencia delictiva cibernética en sus entidades.

Consciente de la situación nacional, SCITUM ha diseñado un esquema de crecimiento en tres niveles para crear o fortalecer las Unidades Cibernéticas Estatales, brindando servicios que pongan a la vanguardia a los estados en materia de ciberseguridad, investigación, inteligencia para la prevención y persecución de delitos cibernéticos, asegurando en todo momento el adecuado manejo de evidencia, la seguridad de la información y el resguardo de pruebas.

1. Unidades Cibernéticas de reciente creación.

Las Entidades Federativas requieren de una transferencia metodológica adecuada, que considere la implementación de tecnología, capacitación y transferencia de conocimientos para su personal, así como soporte y acompañamiento, lo que les permitirá realizar funciones primordiales como patrullaje cibernético e inteligencia policial bajo un modelo de anonimato basado en estándares de seguridad de la información, que resguarde las evidencias y pruebas obtenidas para la judicialización correspondiente.

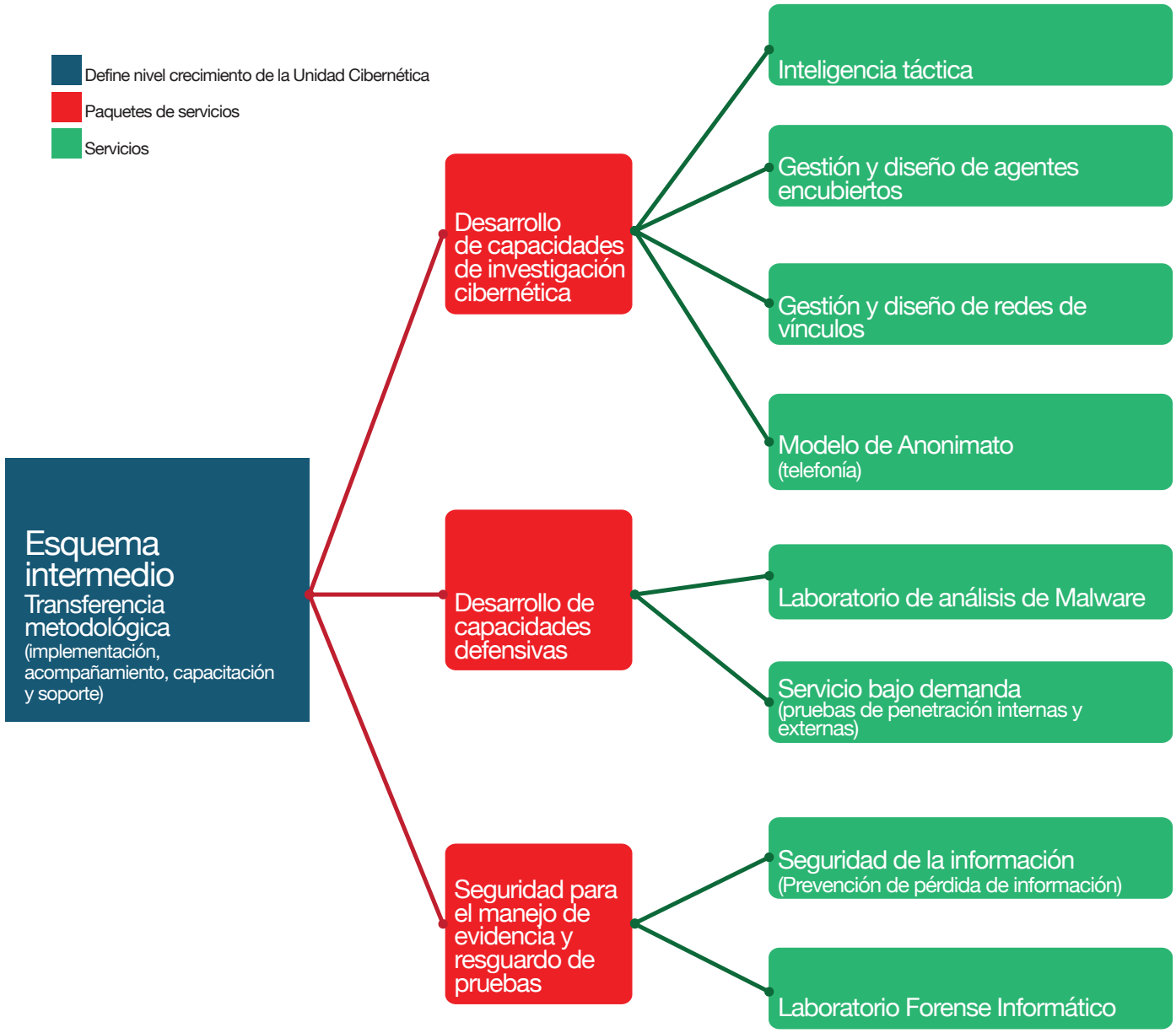
Unidad cibernética
Reciente creación



2. Unidades de madurez intermedia

Los Estados que cuentan con Unidades Cibernéticas requieren consolidar y extender sus capacidades de investigación y respuesta, con el objetivo de hacer frente al incremento y constante evolución en los modos de operación utilizados por los ciberdelincuentes. Con apoyo de la inteligencia táctica, laboratorios y personal especializado incrementarán las capacidades para realizar sus funciones de una manera más ágil y proactiva.

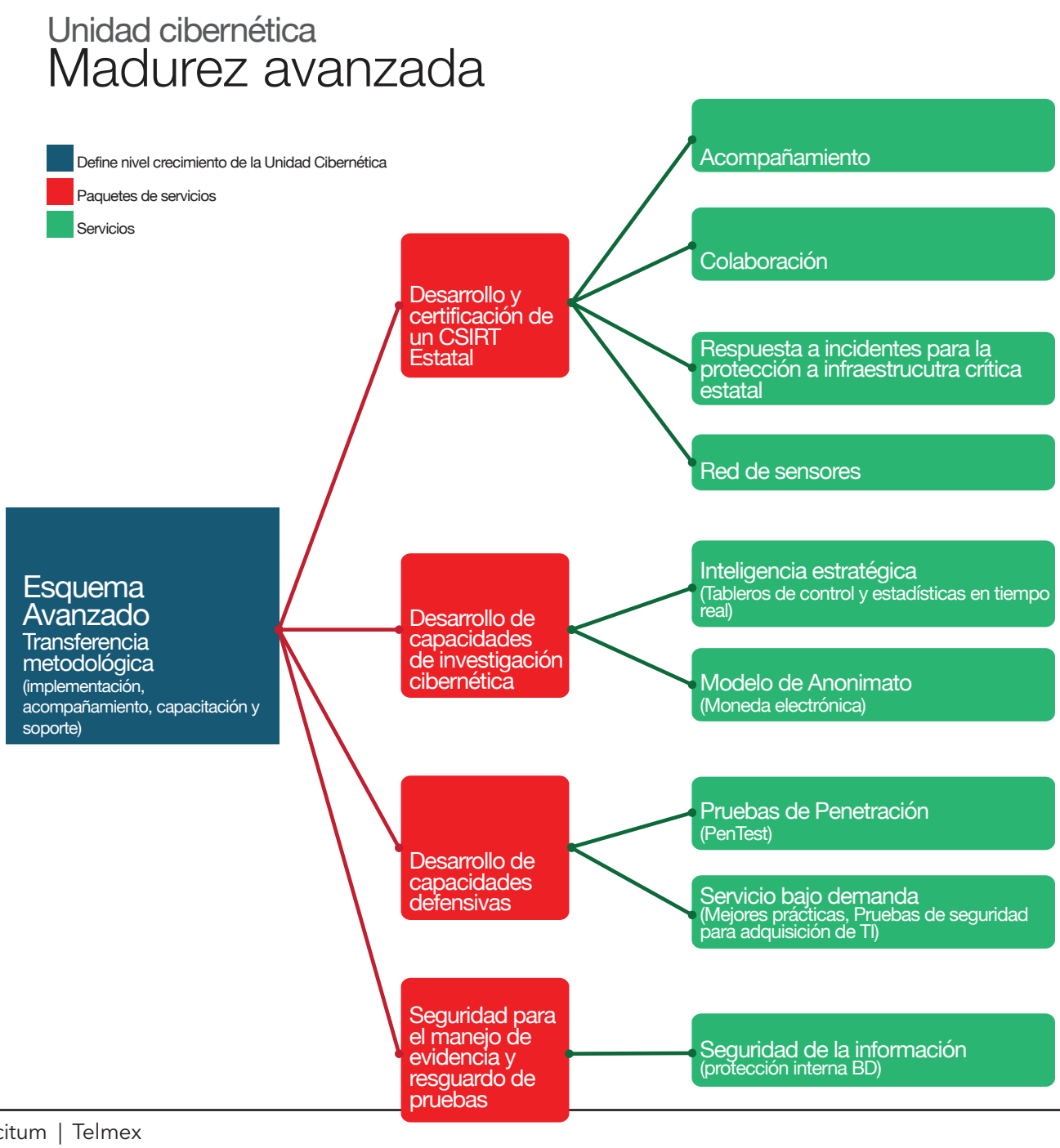
Unidad cibernética
Madurez intermedia



3. Unidades de madurez avanzada

Las Unidades Cibernéticas cuyo tamaño, experiencia y nivel de especialización de su personal les permite atender un mayor número de afectaciones e incidentes cibernéticos, así como llevar a cabo investigaciones mucho más detalladas que incluyan redes profundas, colaboración internacional, transacciones con monedas electrónicas y pruebas de penetración, bajo un modelo de seguridad de la información robusto, requieren mantener un constante fortalecimiento técnico y estratégico de la unidad que considere la actualización de sus conocimientos y habilidades a través de una constante capacitación.

Asimismo con base en la experiencia internacional, es de considerar que estas Unidades robustas pueden evolucionar y formar parte de una comunidad de colaboración transnacional, al implementar en su Entidad Federativa un Equipo de Respuesta a Incidentes de Seguridad Informáticos (por sus siglas en inglés CSIRT) para la protección de su infraestructura crítica local.



PROPUESTA SCITUM

Scitum con base en la experiencia desarrollada a través de los servicios de Ciberseguridad y Ciberinteligencia que entrega a sus clientes, puede ayudar a las unidades cibernéticas en la transferencia de metodología donde además de la entrega de herramientas se brinde capacitación a los analistas para fortalecer sus capacidades de investigación, adicionalmente acompañarlos para garantizar la aplicación y seguimiento de las mejores prácticas en sus investigaciones a fin de disminuir la curva de aprendizaje de los nuevos integrantes de los equipos con la adquisición de conocimientos teórico-prácticos avalados por el equipo de SCILabs (Scitum Cyber Intelligence Laboratories) el cual entre sus principales funciones tiene a cargo el monitoreo del ciberespacio para la detección de diversos tipos de amenazas.

En resumen, lo que obtendrán las Entidades Estatales de manera general a través de una transferencia metodológica basada en implementación, acompañamiento, capacitación y soporte es lo siguiente:

- Adquirir conocimientos que ayuden a obtener información de valor para las actividades relacionadas con investigaciones.
- Disminuir el tiempo de investigación en los casos relacionados con ciberdelitos.
- Contar con un punto de apoyo para resolución de dudas en temas de investigación.
- Conocer y aplicar las mejores prácticas para realizar investigaciones de manera anónima sin poner en riesgo la identidad y la información de la organización.
- Tener un modelo de protección de seguridad para el manejo de casos, evidencia y las pruebas que requieran ser resguardadas por la unidad cibernética.
- Realizar investigaciones seguras y asertivas dentro de la Darknet que puedan ligarse a actividades y objetivos de interés para la organización.

Notas y referencias

[1]Unión Internacional de Telecomunicaciones (2015).

[2]https://www.amipci.org.mx/images/Estudio_Habitosdel_Usuario_2016.pdf

[3]ProMéxico es el organismo del Gobierno Federal encargado de coordinar las estrategias dirigidas al fortalecimiento de la participación de México en la economía internacional, apoyando el proceso exportador de empresas establecidas en nuestro país y coordinando acciones encaminadas a la atracción de inversión extranjera. Sitio web https://www.promexico.gob.mx/es/mx/home

[4]Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares INEGI 2015

[5]http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbeancybersecurity-trends-and-government-responses.pdf

[6]http://www.senado.gob.mx/sgsp/gaceta/63/1/2015-10-27-1/assets/documentos/Inic_PRI_Ley_Delitos_Informaticos.pdf, p.5.

Imelda Flores
SCILABS - Scitum

Es Ingeniero en Comunicaciones y Electrónica por el Instituto Politécnico Nacional. Posee cursos en áreas vinculadas a la gestión de seguridad de la información por organizaciones internacionales de respuesta a ciberincidentes. Es miembro del equipo de SCILabs (Scitum Cyber Intelligence Laboratories) y responsable de los proyectos de ciberinteligencia para clientes en México y Latinoamérica, ha participado en paneles de discusión en temas de ciberseguridad y ciberinteligencia tanto en México como en el extranjero. Actualmente lidera la unidad de ciberinteligencia de Scitum, desde donde se prestan los servicios de monitoreo y vigilancia del ciberespacio basados en inteligencia y se coordinan las investigaciones sobre eventos en redes sociales, operaciones hacktivistas, ciberextorsión y malware avanzado.

Samantha Moreno
SCILABS - Scitum

Samantha Moreno es especialista en administración de proyectos de TI, ha colaborado en diversas organizaciones federales de seguridad en el área de Tecnologías tales como la SSP, PGR y Policía Federal, participó en la integración del Modelo de Policías Cibernéticas y la Estrategia Nacional de Seguridad de la Información. Actualmente colabora en SCITUM como Gerente en Ciberecosistemas de Colaboración.

SCI LABS

SCITUM CYBER INTELLIGENCE LABORATORIES

POWERED by Scitum

Ciudad de México
Plaza Inbursa / Torre Telmex
Av. Insurgentes Sur No. 3500 Piso 2, Col. Peña Pobre
C.P. 14060 Del. Tlalpan, México, D.F.
Conm.: +52 (55) 9150.7400
Fax: +52 (55) 9150.7478

E-mail: **ventas@scitum.com.mx**

www.scitum.com.mx