Scitum

¿QUÉ ES LA CIBERSEGURIDAD?

TELMEX está contigo

¿QUÉ ES LA CÍBERSEGURIDAD?

INTRODUCCIÓN

Cada día escuchamos más hablar de ciberseguridad, al mismo tiempo que vemos en los medios de comunicación diversas noticias sobre *hackeos*, fugas de información, robos de identidad y otros ataques y amenazas.

Incidentes de cobertura mundial como los de *Wikileaks* elevan la conciencia sobre nuestros riesgos informáticos, pero poco ayudan en contestar la gran pregunta: ¿qué debemos hacer para tener una adecuada seguridad?

El propósito de este documento es contestar ésta y otras preguntas, como:

¿Qué es ciberseguridad?, ¿cuál es la diferencia entre ciberseguridad y seguridad informática?, ¿por qué es relevante para mi organización?, ¿qué papel juegan los ejecutivos en la ciberseguridad?, ¿es un tema que afecta a los usuarios, a las familias, a las organizaciones públicas o a las empresas privadas?, ¿debemos hacer algo distinto a lo que hemos venido haciendo?

Para contestar estas preguntas, revisaremos primero algunos hechos recientes sobre distintos ciberataques:

ALGUNOS HECHOS RECIENTES

- **Febrero 2013.** Una empresa de seguridad da a conocer un estudio muy completo sobre las intrusiones que un grupo de *hackers* chinos ha hecho en los últimos años a una multitud de empresas norteamericanas. El reporte prácticamente atribuye la autoría al Gobierno Chino, a través de un grupo de *hackers* que son empleados del Ejército para la Liberación del Pueblo (PLA, por sus siglas en inglés). El gobierno chino niega la evidencia.
- **Enero 2014.** Más de 100 millones de datos de clientes y tarjetas de crédito son robados de las tiendas departamentales Target. El incidente le costó a la empresa millones de dólares y la renuncia del director general (CEO) y el director de sistemas (CIO).

Durante todo ese mismo año, varias cadenas de tiendas (*Home Depot, Neimann-Marcus, Staple* y a la cadena de restaurantes *P.F. Chang* entre otras). En la mayoría de estos casos, a los pocos días del hackeo los datos comprometidos eran vendidos en el mercado negro a precios entre 2 y 5 dólares por tarjeta e incluían información sobre el código postal o el tipo de compras que los usuarios realizan típicamente (simplificando con esto su uso fraudulento por el crimen organizado).

» **Julio 2014.** Otra empresa de tecnología de seguridad libera un artículo documentando el trabajo del grupo "*Dragonfly*" (crimen organizado) que se ha dedicado desde el 2013 a comprometer equipos y redes de empresas de energía de España, Estados Unidos, Francia, Italia y Alemania. El mecanismo de infección es a través de un troyano llamado "*Havex*" que viene anexo a un correo electrónico que aparenta ser normal, y que infecta sistemas SCADA (control supervisorio) y de Control Industrial. En las mismas fechas, y tomando como base el referido reporte y las investigaciones de otro proveedor de seguridad, un organismo del gobierno americano publica una Alerta de Seguridad hacia las empresas de energía, explicando la forma de infección de "*Havex*".

» **Agosto 2014.** El banco *J.P. Morgan* sufre diversos ataques, incluyendo negación de servicio. Grupos nacionalistas de hackers rusos se atribuyen la autoría, argumentando acciones de represalia por las medidas del gobierno americano tomadas en contra de Rusia.

» **Junio 2015.** En un ataque ejecutado por otra nación, son robados los registros de 21 millones de personas de la Oficina Norteamericana de Administración de Personal (US-OPM por sus siglas en inglés), en un incidente que ha sido descrito como una de las mayores violaciones de seguridad de datos gubernamentales en la historia de los Estados Unidos.

» **Abril 2016.** El caso "*Panama Papers*" sale a luz en todo el mundo. Más de 2 Terabytes de información fueron obtenidos de los archivos del despacho Mossack Fonseca por una fuente desconocida y entregada a un periódico alemán quién la compartió, para su investigación, con 400 periodistas en todo el mundo. Los documentos detallan la creación de más de 200,000 empresas fantasmas en paraísos fiscales. Entre los dueños están muchos políticos y empresarios del mundo, incluyendo varias personas muy cercanas al presidente de Rusia, Vladimir Putin.

Estos hechos nos demuestran una nueva realidad:

» Hoy los ataques son más intensos

» Los atacantes tienen más recursos y nuevas motivaciones

» Los atacantes ya no son solamente *hackers* y grupos activistas, se les ha unido el crimen organizado, grupos extremistas (incluyendo terroristas) e incluso naciones

Por otro lado, las organizaciones tienen más interconectados todos sus sistemas y, por tanto, crece su nivel de riesgo tecnológico.

En la siguiente sección revisaremos con más detalle cada una de las aseveraciones anteriores.

LOS NUEVOS ATACANTES

El perfil de los atacantes ha cambiado, grupos organizados están generando ataques dirigidos, más complejos y muy difíciles de descubrir por medio de los mecanismos tradicionales. Los adversarios han creado un ecosistema completo que les permite contar con las capacidades y recursos (económicos, tecnológicos y humanos) necesarios para moverse con libertad. Sus principales motivaciones son económicas y políticas. En lo económico se han dado cuenta de que la venta de información sensible de las organizaciones es un negocio muy lucrativo, por lo que sus blancos principales son instituciones financieras y grandes comercios. En lo político se percatan de la importancia del ciberespionaje, que les permite robar información y secretos industriales (en general propiedad intelectual) y, eventualmente, tener capacidades para realizar operativos de ciber-ataque.

A estos nuevos atacantes ahora se les denomina como ciberactores, y podemos definirlos, de manera general, como aquellas personas u organizaciones que poseen un objetivo, motivación y recursos para hacer daño a través de buscar una oportunidad y explotar una vulnerabilidad. Se identifican los siguientes tipos:

- Grupos delincuentes (crimen organizado)
- Grupos terroristas
- Grupos subversivos ("*hacktivismo*")
- Gobiernos hostiles ("*rogue states*")
- *Hacker* independientes
- Organizaciones comerciales o grupos políticos competidores (ciberespionaje)

Las estrategias de ataque utilizadas son más complejas y de largo plazo, utilizan múltiples pasos previos para llegar a su objetivo, combinan diversas técnicas de explotación (*exploits*) y de evasión, emplean *malware* avanzado así como diversos mecanismos de pasar desapercibidos.

Estos ataques dirigidos se planean, articulan y ejecutan pensando en el perfil particular de la víctima de tal forma que sea mucho más factible tener éxito, lo anterior aunado al valor de la información que los atacantes buscan extraer provoca que su impacto, para las organizaciones, sea muy alto.

LAS NUEVAS AMENAZAS

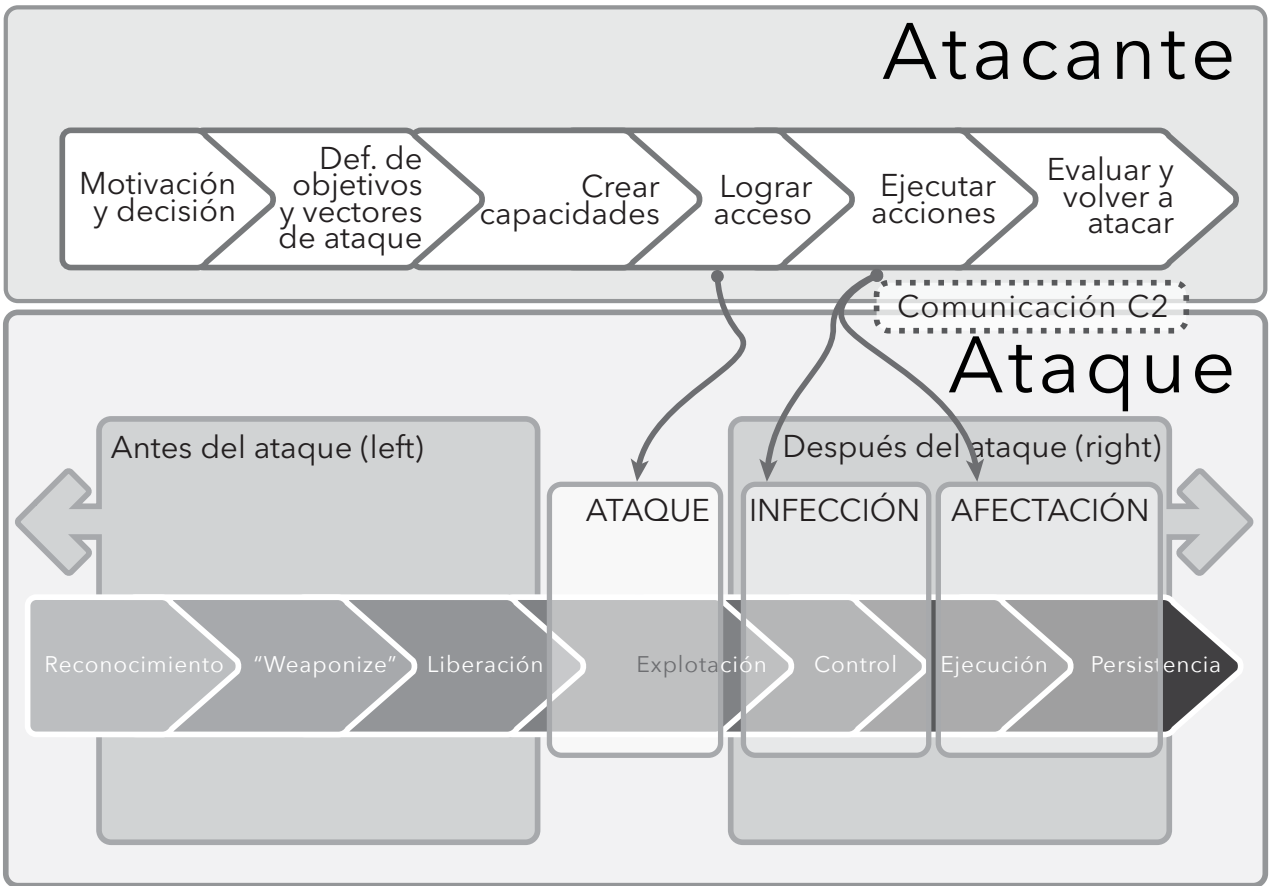
Una de las ciberamenazas más sofisticadas hoy en día son las Amenazas Persistentes Avanzadas (o APT por las siglas en inglés de *Advanced Persistant Threats*) cuyo objetivo es robar, por un tiempo prolongado, información valiosa de una organización determinada. Los atacantes utilizan múltiples métodos de ataque para vulnerar a la organización objetivo, uno de ellos es el spearphishing (campaña de phishing dirigida a un blanco específico, que a través de dirigirle un correo con un contexto que tiene sentido para esa persona u organización, la vuelve muy creíble y con un alta probabilidad de que el usuario lea el correo en cuestión y abra el anexo que previamente ha sido contaminado).

Una vez que el blanco es vulnerado se crean puertas traseras (*backdoors*) que permiten al atacante tener acceso continuo (a esto se le conoce como comunicación a un centro de comando y control o C2) hacia los sistemas comprometidos. El atacante, a continuación, busca expandir su alcance tomando control de más equipos para afianzar su permanencia (lograr su persistencia), con lo cual, si es exitoso, logra mantener el acceso a los sistemas del cliente por largos períodos, con el fin de recolectar más información sobre el blanco, realizar más ataques (movimientos laterales) hasta que logre tener acceso a la información objetivo y la extraiga (acción conocida como exfiltración).

Estos ataques típicamente se organizan a través de "campañas", las cuales pueden estar conformadas, a su vez, por una o más operaciones, y cada operación suele tener las siguientes fases:

1) Preparación
2) Infección
3) Expansión y consecución de la persistencia
4) Búsqueda y extracción de información
5) Limpieza

En el siguiente diagrama se muestra gráficamente la secuencia de pasos que el atacante sigue para realizar un ataque avanzado:



MAYORES VULNERABILIDADES

Recordemos que las vulnerabilidades son las debilidades de seguridad de nuestro sistema, entendiendo por sistema desde una PC o *Smartphone*, hasta toda una organización junto con su infraestructura de cómputo y comunicaciones, aplicativos y servicios del negocio, así como la información involucrada en lo anterior.

Uno de los elementos que ha cambiado rotundamente es nuestra superficie de exposición, lo cual significa que hoy tenemos muchos más elementos de *hardware* y *software* que proteger para evitar intrusiones. Dado que casi todas las vulnerabilidades tecnológicas están asociadas con el *software*, ahora:

1. Tenemos más piezas de *software* ejecutándose en servidores, PC, laptops, tabletas, teléfonos inteligentes, automóviles y, crecientemente en "las cosas" (lo que se ha llamado el Internet de las cosas: refrigerador, sistemas inteligentes y sensores en distintos dispositivos u objetos incluyendo relojes y ropa inteligente).
2. Todo está interconectado y es muy difícil, a veces imposible, distinguir dónde termina una red y empieza la otra, algo que se ha llamado el "perímetro borroso" de las nuevas redes.
3. La complejidad de las arquitecturas tecnológicas ha crecido: servidores (virtualizados y no) con distintas naturalezas (bases de datos, aplicaciones, servicios como DNS, Directorio Activo, etc.), enrutadores, *switches*, balanceadores, aceleradores de tráfico (distintos tipos), arquitecturas de nubes privadas y públicas, *software* intermediario (*middleware* de diversos sabores), aplicaciones móviles, etc.

Por todo lo anterior ahora es más difícil proteger nuestros ambientes. Mientras que una organización tiene que brindar seguridad a todos los elementos y sus interconexiones, un atacante sólo tiene que encontrar un camino por el que pueda entrar.

¿PERO ENTONCES QUÉ ES CIBERSEGURIDAD?

De manera general podemos definir Ciberseguridad como la habilidad de proteger o defender el uso del ciberespacio de ciberataques, con el fin de evitar el acceso, uso, alteración, modificación, extracción o destrucción no autorizada de la información almacenada electrónicamente.

Sin embargo, el foco de la Ciberseguridad (en contraposición con la seguridad informática "tradicional") ha estado más en la creación de nuevas tecnologías y procesos y en la preparación del personal para enfrentar los nuevos ciberriesgos.

En este nuevo entorno requerimos de nuevas tecnologías. De este modo han surgido, por ejemplo, herramientas para detectar malware avanzado (incluyendo los mencionados APT) o para poder encontrar anomalías e incidentes de seguridad dentro de millones de eventos de diversas bitácoras o, incluso, en miles de millones de paquetes de red. Este último caso, en donde se aplican los principios de "*big data*" a seguridad se denomina "analítica de seguridad".

Pero el reto de tener una estrategia de ciberseguridad es mucho mayor que la adquisición e implementación de nuevas herramientas, se vuelve muy importante fortalecer, entre otras, la capacidad de detectar que estamos siendo víctimas de un ataque avanzado; de analizar su estructura y comportamiento para poder contenerlos y remediarlos; así como de analizar los efectos o el impacto que se haya tenido.

La siguiente sección presenta, de una forma muy concreta, algunos de los elementos que necesitamos cambiar en nuestra manera de enfocar el reto. En pocas palabras los cambios de paradigmas que necesitamos hacer.

EL VERDADERO CAMBIO DE PARADIGMA

Un paradigma, en palabras simples, es la forma en que vemos el mundo, es el patrón mental que usamos para entender nuestro contexto. Entre más usemos un patrón mental, más compenetrado lo tendremos y más difícil será el cambio.

Un ejemplo rápido: en los años 80 en que empezaron a proliferar las computadoras personales (PC) y las redes locales (LAN) muchas personas informáticas se tardaron en aprovechar estas tecnologías porque seguían "aferradas" al paradigma de usar solamente equipos grandes.

Entonces de lo que se trata el verdadero cambio que propone la ciberseguridad es de modificar o actualizar algunos de nuestros paradigmas.

A continuación revisaremos los principales:

- **NO PODEMOS PENSAR EN QUE PROTEGEMOS PARA QUE NADIE PENETRE.** Para la mayoría de las organizaciones, la seguridad de la información se ha tratado de PROTEGER nuestras redes y sistemas para que no tengamos intrusiones. En una estrategia de Ciberseguridad, en cambio, partimos del hecho de que vamos a tener intrusiones, no importa que tan robusta sean nuestras medidas de seguridad. A partir de esa premisa, debemos diseñar nuestra seguridad para PROTEGER nuestra información (y, por tanto, reducir la posibilidad de intrusiones), para DETECTAR intrusiones (lo más pronto posible) y ACTUAR (para minimizar los impactos de una intrusión y tratar de que no se repita).
- **NINGUNA ORGANIZACIÓN (PÚBLICA O PRIVADA) PUEDE ENFRENTARLO SOLA.** La complejidad de los ataques, las capacidades crecientes de organizaciones criminales así como de los grupos y países hostiles, han hecho de que sea materialmente imposible para cualquier organización el poder enfrentarlo en forma independiente. Debemos movernos de pensar que una organización puede hacerlo sola, a actuar en colaboración con diversas organizaciones: con los centros de respuesta a incidentes (CERT-MX y CERT-UNAM en México), con el gobierno (p.ejem. en México con la División Científica, parte de la Policía Federal), con proveedores de tecnología y de servicios confiables y expertos e – incluso- con competidores del mismo sector (interesados en intercambiar información y prácticas de trabajo para beneficio mutuo).

» **LA INVERSIÓN EN SEGURIDAD NO PUEDE SER DIRIGIDA POR LA TECNOLOGÍA.** Aunque la seguridad siempre ha tenido que estar supeditada a los riesgos del negocio, muchas organizaciones han invertido en tecnologías de seguridad y se han olvidado de tener una estrategia completa de administración de riesgos, o dichos riesgos no han sido entendidos por los altos ejecutivos. En Ciberseguridad, la estrategia que definamos debe ser entendida y patrocinada por la alta dirección, tanto en organizaciones públicas como privadas, y debe partir de una evaluación completa de amenazas y vulnerabilidades. Para entender a fondo a los atacantes y sus "*modus operandi*", así como para tomar las acciones correspondientes (incluyendo el protegernos anticipadamente de algún nuevo ataque) son cada vez más necesarias actividades de inteligencia (y tecnologías de apoyo). En este sentido, el análisis de riesgos apoyado con "inteligencia" será cada vez más común. Todo ello es muy distinto a comprar *firewalls* y sistemas de prevención de intrusos (que siguen siendo necesarios) y pensar que, con ellos, estamos protegidos.

» **EL PERFIL Y FORMACIÓN DE NUESTRO PERSONAL DEBE DE AMPLIARSE.** Nuevamente, en los momentos actuales, para implementar adecuadamente una estrategia de Ciberseguridad necesitamos contar con gente que posea un grupo de conocimientos y habilidades mucho más amplio que antes. De contar con un grupo de especialistas súper-técnicos (sea personal nuestro y/o de nuestro proveedor de servicios) a tener consultores y especialistas con perfiles más completos e integrales que, además de ser súper-técnicos, entiendan el contexto del negocio, puedan anticipar escenarios de ataques avanzados y sean capaces de "cazar eventos" buscando pistas de esos ataques en bitácoras o tráfico directo de la red. Formar al personal en todas estas habilidades y conocimientos no será tarea fácil (Nota: Scitum está liberando una serie de talleres, cursos y servicios de transferencia metodológica para ayudar a las organizaciones en la formación de su personal en temas de ciberseguridad y ciberinteligencia).

LA RESPONSABILIDAD DE LA CIBERSEGURIDAD DEBE ESTAR EN LOS ALTOS EJECUTIVOS

La mayoría de empresas, públicas y privadas, ha dejado la responsabilidad de la seguridad al director de sistemas o CIO, o –en el mejor de los casos- al CISO (del inglés "*Chief Information Security Officer*"), pero recordemos que la seguridad informática está directamente asociada con los riesgos del negocio, en este caso los riesgos en el manejo de la información. En el caso de la ciberseguridad, debemos extender un poco los alcances de los riesgos y tomar muy en cuenta los riesgos de hacer negocios en el ciberespacio (que, como lo hemos comentado, tiene una gama cada vez más amplia de amenazas y actores).

Entonces, si nuestra visión está asociada totalmente con la administración de diversos riesgos del negocio, los responsables principales deben ser los altos ejecutivos. Por esa razón el actual presidente de los Estados Unidos, Barak Obama, comanda los esfuerzos de ciberseguridad en su país, habiendo lanzado su estrategia desde el 29 de mayo de 2009. En ese lanzamiento pudimos ver, quizás por primera vez, a un presidente hablando de "*hackeos*" y robos de información, de *malware* y *botnets*, mencionar a China como un país desde donde se realizan muchos de los ataques y, sobre todo, reconocer que los Estados Unidos no están preparados adecuadamente en términos de ciberseguridad.

Sigamos el ejemplo de Obama pero exijamos a los responsables técnicos (CIO, CISO y sus equipos de trabajo) que traduzcan el lenguaje técnico a un lenguaje de riesgos del negocio y medidas de seguridad (controles), que en vez de hablar de las inversiones hechas mejor nos presenten métricas claras (incluyendo indicadores clave de desempeño o KPI por sus siglas en inglés) y, preferentemente, tableros de mando (*dashboards*) donde se muestre el estado de riesgo que guarda el negocio.

LAS NUEVAS TECNOLOGÍAS Y SU INTEGRACIÓN

Los avances tecnológicos actuales han logrado que algunas de las técnicas de detección sean más robustas y den pie a nuevos modelos de detección y protección contra amenazas avanzadas. Han surgido nuevas técnicas tales como : *Indicator of Compromise (IoC), YARA Rules, Sink Holes, Security Analytics, Behavior and Anomaly Analysis, Dynamic Analysis, Sandboxing, Sandnet, Network Forensics, Static Analysis, Honeypots* y otras más. Para mayor detalle sobre estas técnicas consultar nuestro *white paper* **"Nuevas técnicas de protección ante amenazas avanzadas"**.

CONCLUSIONES

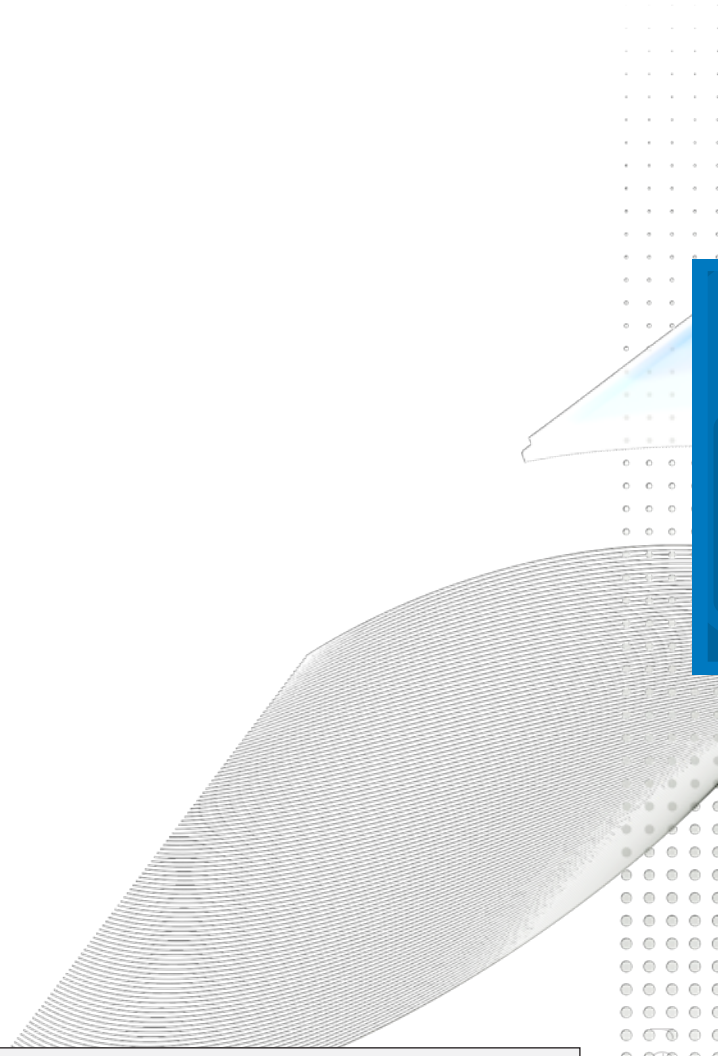
Podemos resumir las líneas anteriores en tres declaraciones importantes:

- Las cosas ya cambiaron. Los ataques son más intensos y sofisticados, los atacantes tienen mayores recursos, tenemos más elementos que cubrir y nuestra superficie de exposición ha crecido.
- Debemos entrar con otra mentalidad. No podemos pensar en defender como la estrategia básica. Hay que proteger pero también detectar y actuar.
- Buscar nuevas tecnologías no debiera ser el primer paso. Hay que considerar al personal que diseñará, implementará y administrará la seguridad (incluyendo el monitoreo, la detección y manejo de incidentes), así como los procesos y procedimientos necesarios.

Por ello, debemos entender nuestros ciberriesgos y crear una estrategia de proteger, detectar y actuar. Scitum, junto con su ecosistema de aliados (entre los que se cuentan los fabricantes líderes de tecnología de ciberseguridad así como empresas líderes en Estados Unidos e Israel en estas especialidades) le puede brindar diversos servicios de ciberseguridad y ciberinteligencia, de acuerdo a las necesidades de su organización.

M. en C. Ulises Castillo
Scitum
Fundador y Director General de Scitum S.A. de C.V., tiene una maestría en Seguridad de la Información y posee las certificaciones CISSP, CISM y CISA.

Marcos Polanco
Scitum
Director Ejecutivo de Iniciativas Estratégicas en Scitum, graduado como Ingeniero en Cibernética y Sistemas Computacionales cuenta con diversos programas de especialización en el IPADE e ITAM.Ostenta certificaciones tales como: ITIL Foundations, ITIL Practitioner (*Change Management y Configuration Management*), CISSP, CISA y CISM.



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