Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Maestría en Gestión Estratégica de Sistemas y Tecnologías de la Información

Trabajo Final de Maestría

Centro de operaciones de seguridad.
Estrategia, diseño y gestión.

Autor: Patricio Hernán Biggeri

Director: Raúl Horacio Saroka

Marzo 2018

Este trabajo culmina un ciclo de aprendizaje y crecimiento profesional que sólo fue posible gracias a la ayuda, el apoyo y el impulso de mis familiares, amigos, compañeros y profesores.

A todos ellos, mi sincero agradecimiento.

I. Resumen

Los centros de operaciones de seguridad se constituyen como un área de gestión capaz de articular procesos, personas y tecnologías con el fin de proteger los activos de la organización. El objetivo del trabajo será demostrar que los centros de operaciones de seguridad (COS) son una efectiva solución de gestión a la problemática de la ciberdefensa.

Serán objetivos secundarios del trabajo presentar una introducción a las operaciones de seguridad y explicar la tríada de procesos, personas y tecnologías identificando los procesos que lo soportan, los perfiles de personal idóneo y las tecnologías que habilitan el análisis en tiempo real de datos y flujos de red. Luego se concluirá delineando los hitos y consideraciones que debería contemplar una estrategia para la conformación de un COS.

El trabajo se desarrollará entendiendo los desafíos de la ciberseguridad para las organizaciones, el surgimiento de los centros de operaciones de seguridad con sus modelos de madurez, la descripción de las tecnologías y sistemas sobre las que operan los COS. Asimismo, se incluirán observaciones empíricas en un Ministerio de la Administración Pública Nacional en el camino hacia la constitución de un COS.

Se aplicará una metodología de investigación exploratoria descriptiva sobre el estado del arte de los centros de operaciones de seguridad. Se realizará un estudio exploratorio sobre la teoría existente y la descripción de las buenas prácticas, modelos y arquitecturas de los centros de operaciones de seguridad.

El Trabajo Final de Maestría será de utilidad y aportará conocimiento a aquellas personas que se encuentran ante el desafío de abordar la ciberseguridad en el entorno corporativo, presentándoles el estado actual de este tema en el mundo y explorando una solución de gestión que les permita dar respuesta mediante la articulación de procesos, personas y tecnologías.

Palabras clave: seguridad informática, gestión por procesos, tecnología, estrategia.

II. Índice

Tabla de contenidos

I. Resumen 1
II. Índice 2
Tabla de contenidos 2
Tabla de figuras 4
1. Introducción 5
2. Planteamiento del tema 7
Objetivos 8
Hipótesis 8
3. Marco teórico 9
Los desafíos de ciberseguridad en las organizaciones 9
Centros de operaciones de seguridad 10
Gestión orientada a procesos 11
Tecnologías y sistemas 12
Estrategia del centro de operaciones de seguridad 13
4. Metodología 14
5. Desarrollo 15
Ciberseguridad 15
Una muestra de realidad 15
Cambio de paradigma 16
La era de la ciberseguridad 17
Seguridad en el ciberespacio 19
Operaciones de seguridad 21
Colaboración e inteligencia sobre amenazas 21
Evolución de los centros de operaciones de seguridad 24
Primera generación 24
Segunda generación 26
Tercera generación 27
Cuarta generación 28
Operaciones de los centros de operaciones de seguridad 30
Servicios de valor agregado 30
Factores de éxito 31
Tríada: procesos, personas y tecnologías 34

Procesos 34
Gestión de servicios corporativos 35
Gestión de servicios de seguridad 36
Ingeniería de servicios de seguridad 37
Operación de los servicios de seguridad 37
Monitoreo de seguridad 38
Investigación y respuesta a incidentes de seguridad 39
Gestión de registros de auditoría 39
Gestión de vulnerabilidades 40
Inteligencia de seguridad 41
Gestión de reportes de seguridad 41
Personas 42
Roles 44
Funciones y estructura 45
Dimensionamiento 46
Aprovisionamiento 48
Tecnologías 49
Redes de datos 50
Seguridad de red 51
Sistemas 53
Plataformas de seguridad 54
Planificación y puesta en marcha 58
Evaluación de capacidades 58
Objetivos 58
Capacidades 59
Recolección de información 61
Modelos de madurez 61
Informe final 62
Estrategia 63
Misión y alcance 63
Servicios 64
Modelo de operaciones 65
Hoja de ruta 67
6. Conclusiones 69
Conclusiones generales 69
Experiencia profesional 70
7. Bibliografía 73

Tabla de figuras

Figura 1. Objetivo general y objetivos específicos. 8
Figura 2. Generaciones de los centros de operaciones de seguridad. 29
Figura 3. Servicios del centro de operaciones de seguridad. 31
Figura 4. Factores de éxito de un centro de operaciones de seguridad. 33
Figura 5. Representación de la metodología de evaluación de capacidades. 58

1. Introducción

Los centros de operaciones de seguridad deben ser analizados como una herramienta de gestión para la continuidad y calidad de las operaciones de las organizaciones. Su inclusión en la estructura orgánica de las organizaciones permitirá que éstas alcancen sus objetivos estratégicos. Debe tenerse en cuenta que la difusión del uso de las Tecnologías de la Información y las Comunicaciones (TIC) ha modificado nuestras actividades cotidianas y la forma en que interactuamos entre nosotros como personas y también con las empresas, organizaciones y entidades gubernamentales.

Este mayor uso de sistemas, tecnologías y comunicaciones conlleva un aumento de las amenazas cibernéticas que se aprovechan de las vulnerabilidades para la obtención de un beneficio económico a través del robo de dinero o un beneficio intelectual por la violación de patentes. En función de esta problemática ha surgido de la mano de la informática el área de estudio de la seguridad informática, cuyo objetivo es garantizar la integridad, confidencialidad y disponibilidad de los datos y sistemas de procesamiento.

La seguridad informática requiere combinar conocimientos técnicos sobre todo tipo de plataformas informáticas y conocimientos de gestión para lograr articular dispositivos, tecnologías, sistemas avanzados de detección, procesos y personas. De esta forma, se logrará proteger efectiva y sustentablemente los activos de interés para la organización.

La estrategia de sistemas y tecnologías de la información debe contemplar como pilar la gestión de la seguridad de la información, ya que, de lo contrario, los sistemas podrían sufrir afectación en la disponibilidad o calidad y, por lo tanto, esto impediría alcanzar los objetivos estratégicos planteados por la Alta Dirección. Evidencia de la importancia es que la Maestría en Gestión Estratégica de Sistemas y Tecnologías de la Información contempla la asignatura de Gestión de Seguridad de la Información. Los conocimientos adquiridos en la Maestría permiten comprender y presentar a los centros de operaciones de seguridad como una solución de gestión y no sólo como un elemento tecnológico. La combinación de conocimientos técnicos y de gestión, aportarán un enfoque particular para abordar la gestión de la seguridad.

La bibliografía existente sobre los centros de operaciones de seguridad es diversa y con niveles de abstracción distantes, encontrándose, por un lado, información técnica y especializada sobre aspectos puntuales de las tecnologías y aspectos de la seguridad informática. En cambio, por otro lado, existen buenas prácticas que apuntan a la construcción de sistemas de gestión de seguridad de la información, por lo que resulta difícil encontrar una

visión integral que pueda relacionar ambos extremos a través de un área de gestión que vincule los procesos, las personas y las tecnologías.

El desarrollo del Trabajo Final de Maestría comienza en su primer capítulo analizando la situación actual de la ciberseguridad[1]. Casos recientes ilustran las debilidades de las organizaciones a ataques cibernéticos, lo que a su vez representa un cambio de paradigma en materia de seguridad informática. En el segundo capítulo se describe en qué consisten las operaciones de seguridad informática, cómo han tomado forma en unidades organizativas y cómo han evolucionado en el tiempo. Se presenta a los centros de operaciones de seguridad como un área de gestión que brinda servicios corporativos.

En el tercer capítulo se explora la tríada de procesos, personas y tecnologías que conforman los centros de operaciones de seguridad. Se identificarán los procesos, la estructura orgánica junto con los perfiles de personas necesarias y la tecnología requerida para operar. El sistema conformado entre estos elementos, principalmente por la interacción que se representa en sus vínculos, es lo que permitirá alcanzar el éxito. En el cuarto capítulo se hace una descripción de la metodología de evaluación de capacidades y los elementos que conforman la estrategia, incluyendo las alternativas del modelo de operación. Ambos aspectos son clave para la planificación y puesta en marcha de un centro de operaciones de seguridad.

Por último, las conclusiones del trabajo validan la concreción de los objetivos planteados y el autor aporta su experiencia profesional en la conformación de un centro de operaciones de seguridad en función de los conceptos vertidos en el desarrollo del trabajo.

[1] Ciberseguridad: entiéndase como referencia de las prácticas y concepto de seguridad informática aplicados al espacio cibernético.

2. Planteamiento del tema

Los centros de operaciones de seguridad se están constituyendo como un área de gestión para proteger eficazmente la información de las organizaciones. A lo largo del tiempo, las responsabilidades del área de la seguridad informática fueron asumidas por distintas áreas de los departamentos encargados del desarrollo y mantenimiento de sistemas e infraestructura informática. Esta diseminación inicial y natural de responsabilidades como forma de responder a las necesidades de la operación impide la sinergia de combinar factores y aunar criterios de decisión para responder con efectividad a los desafíos que afronta una organización en relación con la seguridad de la información.

El modelo de gestión y la estrategia de sistemas que defina una organización deben contemplar como pilar la gestión de las operaciones de seguridad de forma centralizada, coordinando las tecnologías, los procesos y las personas para alinear la propia estrategia de seguridad con la estrategia de sistemas y contribuir por lo tanto al modelo de negocio.

Entonces, es necesario descubrir qué puntos debe contemplar la estrategia de un centro de operaciones de seguridad, cuál es la hoja de ruta para su conformación y cuáles serán las funciones y responsabilidades primarias. En función de estos lineamientos se podrá identificar qué procesos soportarán la gestión y qué perfil de personal es el idóneo. Asimismo, la gestión de las tecnologías de la información toma un rol esencial para esta área, cuya materia prima serán registros de auditorías con un volumen, variedad y velocidad cada vez mayor.

Si bien esta problemática aplica a organizaciones de todo tipo y tamaño, cada una con sus propios desafíos y requerimientos legales, el autor relacionará este tema con aplicabilidad en un ministerio bajo la órbita de la Administración Pública Nacional (APN). En este contexto existe normativa que obliga a los ministerios y otros entes de la APN a gestionar la seguridad la información, aunque no establezca la estructura organizacional para llevar a cabo esta tarea.

Objetivos

El objetivo general del trabajo consiste en demostrar que un centro de operaciones de seguridad (COS) es una solución de gestión a la problemática de la ciberdefensa[2].

Para alcanzar el objetivo general será necesario abordar el primer objetivo específico que es introducir las operaciones de seguridad, incluyendo los motivos que impulsan la conformación de un COS y los servicios prestados por este.

Luego se avanzará con el segundo objetivo específico que es explicar la tríada de procesos, personas y tecnologías, cuya sinergia e interacción soportan la gestión de un COS.

Por último, se desarrollará el tercer objetivo específico que es delinear la estrategia para la conformación de un COS exponiendo los elementos que deben considerarse.

Figura 1. Objetivo general y objetivos específicos.

Hipótesis

Se plantea como hipótesis orientativa que a partir del desarrollo del trabajo y alcanzados los objetivos específicos se arribará a la conclusión de que **los centros de operaciones de seguridad representan una solución de gestión a la problemática de la ciberdefensa** logrando alinear objetivos estratégicos, procesos, recursos humanos y recursos tecnológicos.

[2] Ciberdefensa: entiéndase como referencia de las prácticas de defensa de seguridad informática aplicadas al espacio cibernético.

3. Marco teórico

Los desafíos de ciberseguridad en las organizaciones

En la primera parte del trabajo se hará una introducción a los desafíos que enfrentan las organizaciones respecto a la ciberseguridad. La difusión y uso intensivo de las tecnologías de la información y comunicaciones traen consigo riesgos que podrían afectar la disponibilidad, confidencialidad o integridad de la información. Por lo tanto, una organización que sufre la afectación en alguno de los aspectos mencionados puede perder la confianza de sus clientes por mala reputación, como así también puede verse afectada económicamente al tener que suspender la provisión de los bienes o servicios que ofrece.

Eventos imprevistos a lo largo del tiempo han forzado a los gobiernos a generar normativas que establezcan requerimientos mínimos para el cuidado de la información. En algunos países estos requerimientos son obligatorios sólo para entes gubernamentales, mientras que en otros se hacen extensivos a organizaciones privadas. En este sentido, el gobierno argentino ha considerado al Estado como el mayor ente productor o tomador de información del país (Poder Ejecutivo Nacional, 2005) y ha impuesto a los entes que forman parte de la Administración Pública Nacional requerimientos mínimos sobre la seguridad a través un modelo de políticas de seguridad de la información (Oficina Nacional de Tecnologías de la Información, 2015).

A nivel mundial se han confeccionado normas como la serie ISO 27000 con guías de buenas prácticas y modelos de gestión de la seguridad de la información. Estas normas pueden ser utilizadas por las organizaciones como referencia de mejor práctica mundial y hasta pueden certificarse, lo que puede representar en ciertos casos una ventaja competitiva frente a otras organizaciones que no estén certificadas.

Los controles que establecen la norma ISO 27002 abarcan la gestión de los activos, la seguridad en la gestión de los recursos humanos, la protección física, la seguridad en la gestión de las operaciones y las comunicaciones, el control de accesos, buenas prácticas en la gestión de software, la gestión de incidentes de seguridad, la continuidad del negocio y la verificación del cumplimiento (International Organization for Standardization, 2013). Esta diversidad de temáticas y sobre tantos aspectos representa un desafío para las organizaciones que deben implementar por voluntad propia o de forma obligatoria controles que disminuyan al mínimo los riesgos en el uso de las tecnologías de la información y las comunicaciones.

Centros de operaciones de seguridad

El camino andado hasta la existencia actual de normas y leyes ha sido un camino forzoso, ya que las normas surgieron de forma reactiva ante eventos no deseados en vez de surgir proactivamente. Del mismo modo, las responsabilidades que actualmente tiene un centro de operaciones de seguridad son el fruto de años de evolución y reorganización en las responsabilidades de las áreas que componen un departamento encargado de los sistemas y las telecomunicaciones.

Así como a lo largo del tiempo se han creado áreas específicas para gestionar la seguridad informática, cuyas responsabilidades se podrían encontrar originalmente entre las de un administrador de redes de datos o servidores, observando en retrospectiva se pueden identificar distintas generaciones o niveles de madurez de los centros de operaciones de seguridad (Cisco Systems, 2015).

La primera generación de lo que hoy conocemos como un centro de operaciones de seguridad (COS) era en realidad un conjunto de responsabilidades diseminadas entre áreas del departamento de sistemas ejercidas por personas cuya tarea principal era otra y que por lo tanto no estaba capacitada ni concientizada en seguridad. Sus tareas consistían básicamente en monitorear los dispositivos de red y servidores para garantizar la disponibilidad de los servicios, administración básica de los sistemas antivirus y una recolección de registros de auditoría limitada a los dispositivos de red. La reacción ante los incidentes de seguridad era por lo tanto lenta y reactiva.

Las siguientes generaciones que serán descriptas en el cuerpo del trabajo agregan funciones y consolidan responsabilidades hasta llegar a los centros de operaciones de seguridad (COS) de última generación en los que las capacidades se han sofisticado a la par de la sofisticación de los ataques. Gestión proactiva de vulnerabilidades e incidentes, análisis de regresión sobre eventos en tiempo real, soluciones de tipo *big data*[3] y servicios de reputación globales son algunos de los componentes que se encuentran en lo que hoy se constituye como un COS de última generación.

[3] Big Data: es un término para describir conjuntos de datos que son tan grandes o complejos que hacen inadecuados para su tratamiento a los programas tradicionales de procesamiento de datos. El desafío de este tipo de conjuntos de datos es poder capturarlos, almacenarlos, analizarlos, consultarlos, visualizarlos, entre otros (Wikipedia, 2011).

Gestión orientada a procesos

Es importante que la conformación de un centro de operaciones de seguridad se sustente en la gestión orientada a procesos a los fines de garantizar la calidad de los servicios brindados por el área logrando estandarizar las tareas y proveyendo entonces siempre el mismo nivel de servicio. El entramado de procesos es un pilar fundamental para brindar una respuesta adecuada en tiempo y forma, sin embargo, también es de gran importancia contar con un equipo humano capaz de ejecutar procesos y tener al mismo tiempo la capacidad de ser flexibles y reaccionar ante situaciones imprevistas.

Es común que la gestión de incidentes de seguridad, que abarca la detección, investigación, contención y respuesta, sea el servicio más conocido de un centro de operaciones de seguridad. Esta situación es natural ya que es la respuesta reactiva a los problemas que se suceden cotidianamente y teniendo en cuenta la diseminación de responsabilidades entre las distintas áreas, aparece la figura del COS como coordinador de la gestión de incidentes.

También la gestión de vulnerabilidades se lleva a cabo de forma centralizada por parte del COS cuando la organización toma conciencia de la importancia de la prevención como un método efectivo para disminuir el riesgo al que se encuentra expuesta la información. Este proceso proactivo en el que la propia organización busca, identifica, reporta y remedia las vulnerabilidades permitirá que se alcancen mejores niveles de protección y por lo tanto disminuirá la probabilidad de ocurrencias.

En tercer lugar, se encuentra el proceso encargado de adquirir datos y procesarlos para convertirlos en información. Este proceso que a priori parece trivial es en realidad un sofisticado proceso de recolectar, normalizar y analizar registros de auditoría, flujos de tráfico y otros eventos. Todos ellos de gran variedad y volumen necesitan ser analizados en tiempo real y de forma sostenible en el tiempo. Sin este proceso base será difícil brindar los servicios esperados.

Por otra parte, resulta clave la formación de los recursos humanos. Los operadores, analistas y supervisores deben tener funciones definidas que eviten la dispersión y desorganización ante un incidente de seguridad. Lograr que el personal desarrolle capacidades y se complemente mutuamente es quizás el desafío más importante en la conformación de un COS.

La contratación, el desarrollo y mantenimiento del personal de un COS se lo considera como un problema en la industria (HP Enterprise, 2015) dada la alta rotación de personal. Esto se debe a que el perfil requerido para estas posiciones es difícil de encontrar y mantener, ya que no existen estudios profesionales que provean este perfil de trabajador, sino que se trata, por el

contrario, de una combinación de perfiles y conocimientos que enriquecen el análisis y entendimiento de la problemática abordada. La estrategia de gestión de recursos humanos toma entonces un rol preponderante en la conformación de un COS.

Tecnologías y sistemas

La diversidad de dispositivos, marcas y versiones que encontramos en las redes de datos actuales representa un desafío para poder ejecutar los procesos y brindar los servicios que se esperan de un centro de operaciones de seguridad. Dispositivos de red, sistemas operativos, servidores, software estándar, software desarrollado a medida y flujos de red dejarán registros que necesitarán ser recolectados y almacenados eficientemente.

En un inicio, las organizaciones mantendrán registros de auditoría locales en cada sistema o dispositivo, dificultando el análisis en conjunto e impidiendo la sinergia del análisis de regresión en tiempo real. El mercado de soluciones de software ha tomado nota de esta deficiencia y se ofrece software específico capaz de recolectar e interpretar prácticamente cualquier tipo de registro en cualquier método de almacenamiento.

Estos sistemas son conocidos como gestores de información y eventos de seguridad o SIEM[4] por sus siglas en inglés. Por la variedad de formatos, volumen de datos y velocidad con la que se necesita procesar los eventos, los SIEM se despliegan sobre plataformas de *big data* que posibilitan este tipo de análisis. Además, no sólo permiten recolectar datos de interés de la organización, sino que también son capaces de incluir información provista por servicios de seguridad globales, como reputación y categorías de sitios de internet, listas negras de direcciones de red IP, dominios de mail maliciosos o conocidos por el envío de correo no deseado y otros.

En su conjunto, la arquitectura tecnológica de un COS tendrá amplios alcances, incluyendo redes internas, externas y otras, además de distintas técnicas de inspección. Servidores de navegación, sistemas detección de intrusiones, sistemas de prevención de fuga de información, sistemas para la protección ante correo no deseado o ante denegaciones de servicios y otros tantos, formarán parte de la arquitectura del COS.

Por otra parte, será importante disponer de un software para gestionar casos internos mediante el que los analistas del COS puedan tanto derivar requerimientos al resto de las áreas

[4] SIEM: Security Information and Event Management.

como así también llevar registro de las tareas y de esta forma proveer de información útil para la medición de los procesos.

Estrategia del centro de operaciones de seguridad

El camino hacia la construcción de un centro de operaciones de seguridad es en sí mismo un proceso en el que se incrementan las capacidades a medida que se alcanzan los objetivos planteados y se redefinen las prioridades de la organización en su contexto. La planificación de un COS debería implementarse como mejoras continuas que tiendan a resolver las necesidades identificadas y proveer mejores niveles de servicio a lo largo del tiempo.

La combinación de recursos humanos, la tecnología y los procesos debe articularse con colaboración y comunicación para responder a las necesidades identificadas (SANS Institute, 2015). Encontrar el equilibrio entre la conformación de un COS según las prácticas mundiales y al mismo tiempo brindar los servicios que en lo inmediato necesita la organización será una tarea constante por parte de los mandos medios y altos.

El plan del centro de operaciones de seguridad se deberá alinear al plan estratégico de sistemas y tecnologías de la información, que a su vez debe estar alineado al plan estratégico de la organización para sustentar el modelo operativo determinado por la Alta Dirección. Este alineamiento garantizará que se destinen los recursos humanos y financieros a proteger los activos que resulten de interés para la organización. Sin esta guía se puede crear una falsa sensación de seguridad.

Los centros de operaciones de seguridad tendrán entonces en cada etapa sus propios alcances, misiones, modelos de operación y desarrollo que devendrán de los planes estratégicos. Esbozar estos lineamientos servirá como guía para cada etapa de planificación y para la operación diaria de los analistas. Teniendo en cuenta las restricciones presupuestarias y que los recursos son finitos, la gestión de riesgos aparece como un elemento útil para la priorización y asignación de recursos.

Delinear la estrategia de un centro de operaciones de seguridad implicará conocer los desafíos de ciberseguridad que enfrenta la organización, cuáles son las funciones y responsabilidades de un COS, qué procesos se deben confeccionar y sobre qué tecnologías se soportará la gestión.

4. Metodología

Se aplicará una metodología de investigación exploratoria descriptiva sobre el estado del arte de los centros de operaciones de seguridad. Se realizará un estudio exploratorio sobre la teoría existente y la descripción de las buenas prácticas, modelos y arquitecturas de los centros de operaciones de seguridad. Existe bibliografía con distintos niveles de abstracción, desde lo técnico hasta lo gerencial de lo que se realizará una interpretación propia del maestrando.

Asimismo, se acompañará el estudio teórico con la observación empírica y experiencias de la conformación de un centro de operaciones de seguridad en un Ministerio de la Administración Pública Nacional cuya identificación será reservada por cuestiones de confidencialidad.

Las experiencias resultan útiles en tanto son consistentes con la teoría y los modelos de madurez de los COS y podrán ser incorporadas tanto como descripciones de hechos análogas a la teoría como también en forma de opiniones y puntos de vistas expresados por especialistas y profesionales que hayan participado en la construcción y desarrollo de un centro de operaciones de seguridad.

5. Desarrollo

Ciberseguridad

Una muestra de realidad

"*Paralización total en grandes multinacionales*" (Segu-Info, 2017). Con estas palabras comienza el artículo del sitio especializado en seguridad informática para informar sobre el impacto mundial de un nuevo virus informático. "*Algunas empresas ceden y pagan a los 'hackers' para liberarse del ciberataque*" (El País, 2017) titula el periódico generalista español al accionar de algunas organizaciones afectadas por el virus informático *Petya*.

La recompensa exigida por los atacantes para descifrar los archivos digitales y permitir a los usuarios recuperar su información asciende a 300 dólares. *Petya* es el segundo programa malicioso que se hace famoso mundialmente en menos de un mes por cifrar computadoras personales y de organizaciones públicas o privadas, sean pequeñas o grandes, interrumpiendo las operaciones y poniendo en duda la capacidad de defensa, contingencia y recuperación.

Los atacantes detrás del virus logran tomar control de las terminales al ingresar software malicioso por correos electrónicos no deseados o al engañar a los usuarios para acceder a un vínculo de internet que permite su descarga. Una vez dentro del equipo, el programa entra en ejecución, aprovecha deficiencias del sistema operativo para tomar control de este e intenta infectar computadoras ubicadas dentro de la misma red.

La consecuencia es conocida. Los archivos en la computadora empiezan a verse de forma extraña y el usuario ya no puede acceder al contenido. Aparece en pantalla una ventana en primer plano exigiendo el pago de una recompensa para obtener la llave que permitirá, con suerte, descifrar los archivos. Si se dispone de copias de resguardo, se podrá hacer caso omiso a la advertencia e iniciar el proceso de restauración. Si no se han tomado medidas de protección previas, probablemente los atacantes habrán logrado su objetivo y contarán con un cliente más.

El portavoz de Kaspersky, empresa especializada en seguridad, informa que se identificaron al menos 2.000 ciberataques concentrados en un 60% en Ucrania y 30% en Rusia. Microsoft estima que se infectaron al menos 12.500 equipos y observa ataques en 64 países. Empresas de renombre internacional se han visto afectadas por el virus (El Cronista, 2017). Entre ellas podemos encontrar a la naviera Moller-Maersk, el banco BNP Paribas, la empresa de alimentación Mondelez, el laboratorio Merk y la petrolera rusa Rosneft.

Un mes antes, el software malicioso denominado *WannaCry*, con un vector de ataque similar a *Petya*, ya había expuesto la deficiencia de las organizaciones en sus posturas de seguridad. Hospitales de Inglaterra y Escocia tuvieron que interrumpir la atención de casos que no fueran críticos (Wikipedia, 2017). La misma suerte tuvo la empresa alemana de transporte ferroviario Deutsche Bahn y el Ministerio de Interior de Rusia, por mencionar algunos ejemplos de los más de 230.000 equipos infectados en más de 150 países.

Ambos programas maliciosos, *WannaCry* y *Petya*, se aprovechan de los defectos del obsoleto sistema operativo Microsoft Windows XP, que quedó fuera de soporte en el año 2014. Tres años después, en mayo de 2017, Microsoft se vio obligado a tomar cartas en el asunto ante el impacto masivo y lo expresa de la siguiente forma: "*Estamos tomando el altamente excepcional paso de proveer a nuestros clientes una actualización de seguridad para proteger la plataforma Windows […], incluyendo Windows XP […]*" (Microsoft, 2017).

Cambio de paradigma

Evidentemente nos encontramos ante un nuevo modelo de seguridad y la compañía Tenable Network Security lo sintetiza con las siguientes palabras en su reporte global sobre ciberseguridad: "*Con una moderna red corporativa compuesta de dispositivos móviles, nube, aplicaciones web, máquinas virtuales, internet de las cosas, BYOD*[5] *y contenedores los días de un perímetro de red bien definido, que se puede asegurar y defender, han quedado atrás*" (Tenable, 2017).

En los últimos años la influencia de las tecnologías de la información y las comunicaciones han transformado la forma de hacer negocios y gestionar. Los modelos de operación de las organizaciones se han convertido incorporando tecnología para procesar información, innovar en los servicios ofrecidos y establecer nuevas vías de comunicación, en especial con sus clientes y proveedores.

Por su parte, las personas han incorporado la tecnología en sus actividades diarias modificando costumbres y cambiando la forma en que solían hacer ciertas tareas, como realizar transacciones bancarias, efectuar consultas médicas o estudiar una carrera. Esto se puede apreciar en los individuos de todas las sociedades, independientemente del rol que asuman, sean empleados, ciudadanos, estudiantes, profesores, médicos, pacientes, etc.

[5] BYOD: siglas de las palabras *Bring Your Own Device*. Conceptualiza la tendencia de que los empleados utilicen cada vez más sus propios dispositivos personales para acceder a la red y aplicativos corporativos.

En este nuevo contexto, en el que las organizaciones y las personas adoptan nuevas tecnologías para gozar de nuevas funcionalidades y servicios, toman preponderancia ciertos desafíos como la privacidad y la continuidad operativa. Esto se debe fundamentalmente a que se cambia el espacio en el que se interacciona, pasando de un entorno local o cerrado a un entorno global o abierto, con los riesgos que ello implica.

Según la norma ISO 27032 el ciberespacio es "*un entorno complejo resultante de la interacción de personas, software y servicios en Internet, soportado globalmente por dispositivos distribuidos físicamente y redes conectadas*" (International Organization for Standardization, 2012). El instituto NIST lo define como "*un dominio global dentro del entorno de información que consiste en la red interdependiente de infraestructuras de sistemas de información incluyendo Internet, redes de telecomunicaciones, sistemas informáticos y procesadores y controladores integrados*" (National Institute of Standards and Technology, 2013).

Se desprende de las definiciones precedentes que en el ciberespacio resulta decisiva la interacción con otras redes y actores, lo que en la práctica es facilitado por la conexión a internet y el consumo de servicios almacenados en la nube. Esto es clave para explicar el cambio de paradigma respecto a la gestión de la seguridad tradicional, en la que el perímetro se encontraba bien definido y las organizaciones se focalizaban en proteger activos ubicados localmente bajo su dominio, en sus propios centros de cómputos.

Ahora, los activos de la organización y los recursos con los que opera pueden encontrarse diseminados internacionalmente, incluso fuera de nuestro dominio y por lo tanto fuera de nuestro control. Es decir que se transita de un modelo de seguridad en el que se tenía control hacia un modelo de ciberseguridad donde ya no lo tendremos. Esto implica que se debe cambiar el modelo de gestión de seguridad pasando de decisiones de única vez, como permitir o denegar, a un enfoque de monitoreo continuo de riesgo y confianza.

La era de la ciberseguridad

"*Las amenazas cibernéticas son uno de los más serios desafíos económicos y de seguridad nacional que enfrentamos como nación*" afirmó el presidente de los Estados Unidos de América en un discurso del año 2009 (The New York Times, 2009). La ciberseguridad definitivamente toma relevancia en un mundo cada vez más interconectado y en el que los ataques evolucionan sofisticándose y adquiriendo mayor complejidad.

Las organizaciones han actuado en consecuencia y se puede observar en la actualidad cómo se implementan tecnologías de defensa y procedimientos de gestión de riesgos. Por

ejemplo, no resulta difícil encontrar organizaciones con servidores de control de navegación en internet, servidores de protección de correos no deseado o sistemas de detección de intrusiones.

La consultora McKinsey realizó una serie de entrevistas con líderes de seguridad de la información de 25 de las empresas más importantes a nivel global y concluyeron que los cambios en las formas en que las organizaciones usan las tecnologías han hecho más difícil la protección de los entornos corporativos al mismo tiempo que ha aumentado la importancia de protegerlos. En el trabajo *Meeting the cybersecurity challenge* (McKinsey, 2011) exponen que han logrado identificar cuatro tendencias comunes.

La primera tendencia consiste en que el valor continúa migrando al mundo en línea −entiéndase internet− y que los datos digitales han profundizado su penetración. Esto se debe a que la información digital tiene valor, incluso monetario, y por lo tanto se convierte en un blanco atractivo. Los servicios en la nube no sólo dan potencia de procesamiento, sino que también permiten a usuarios con menores conocimientos técnicos disponer de aplicaciones funcionando en poco tiempo, prescindiendo de las tradicionales áreas administradoras de sistemas.

La segunda tendencia identificada es que se espera que las corporaciones sean más abiertas que nunca. Esta tendencia está fuertemente vinculada a la filosofía *Bring Your Own Device* (BOYD) que representa el concepto de que los empleados utilizan sus propios dispositivos personales para acceder a la red corporativa y los aplicativos. La heterogeneidad de dispositivos, en su mayoría fuera del control de los departamentos de sistemas corporativos, abre la puerta a vulnerabilidades y pueden convertirse en vectores de ataque. Esta filosofía entra a su vez en contraposición con el mayor control de las terminales que se tiende a implementar en entornos corporativos cuando las terminales pertenecen a la organización. Por ejemplo, la restricción de uso de puertos USB o la restricción de instalar software no homologado previamente.

La tercera tendencia está asociada la mayor integración en la cadena de proveedores, ya que las organizaciones buscan obtener beneficios de la interconexión e integración de sus sistemas informáticos y redes de datos. Un ejemplo de ello es la integración de aplicativos informáticos como *Supply Chain Management Systems* (SCMS) mediante los que las organizaciones pueden gestionar pedidos a sus proveedores automáticamente y en línea en función de las ventas que realizan. Naturalmente, esta apertura de lo que previamente eran redes cerradas conlleva riesgos informáticos ya que el intercambio de información y la interacción entre las partes podrían convertirse en una vía de ingreso de intrusiones.

La cuarta tendencia es que los atacantes se sofistican, trabajan en equipo o incluso conforman organizaciones. Los grupos de atacantes han incorporado tecnología de avanzada y en ciertos casos han superado en habilidades y recursos a los equipos de seguridad corporativos. En el último tiempo se han visto ataques cada vez más complejos, con software malicioso difícil de identificar y rastrear. Es importante observar que, mientras la misión de los criminales justamente es lograr un ataque exitoso, las funciones de seguridad corporativa representan tareas de soporte y por lo tanto dispondrán de menores recursos y atención que la misión crítica del negocio.

Seguridad en el ciberespacio

En la sección "Una muestra de realidad" se presentó dos ejemplos concretos, recientes y masivos que permiten ilustrar el nivel de exposición al riesgo cibernético de organizaciones y personas comunes. El perímetro de las organizaciones se ha vuelto difuso o hasta inexistente y las organizaciones se encuentran en la actualidad desenvolviéndose en el ciberespacio, enfrentando ataques cibernéticos y respondiendo a incidentes.

El instituto NIST define un ciberataque como "*un ataque, a través del ciberespacio, con destino al uso del ciberespacio por parte de una organización y con el objetivo de interrumpir, inhabilitar, destruir o controlar maliciosamente un entorno o infraestructura computacional; o destruir la integridad de los datos o robar información bajo control*" (National Institute of Standards and Technology, 2013).

Es decir, que al catálogo de ataques que enfrenta cualquier organización en el entorno local se agregarán más atacantes y vías de ataques al operar en el ciberespacio. Seguiremos gestionando para proteger la confidencialidad, integridad y disponibilidad de la información, pero abriendo ahora el espectro de potenciales atacantes, tipos de ataques y elevando consecuentemente el riesgo de incidentes. Por lo tanto, será necesario optimizar las protecciones de seguridad implementadas o tradicionales y trabajar en la incorporación de nuevos mecanismos que se mencionarán más adelante.

Es importante remarcar que en este nuevo escenario de ciberseguridad sigue siendo un factor crítico mantener los controles clásicos de seguridad, como concientizar a los usuarios, disponer de un inventario de activos, clasificar la información, actualizar los sistemas operativos y aplicaciones, desplegar un sistema antivirus, realizar copias de resguardo, y otras medidas tradicionales. *WannaCry* y *Petya* demostraron que hay organizaciones que aún no logran una postura de seguridad adecuada en el modelo de gestión clásico.

En mayo del año 2000 un gusano informático denominado *ILOVEYOU* se había distribuido masivamente por correo electrónico (Wikipedia, 2006). Consistía en un archivo ejecutable que viajaba adjunto en los correos electrónicos y que, al ser ejecutado por usuarios desprevenidos, permitía al atacante robar información local y dejar fuera de funcionamiento a las computadoras. En aquel entonces, las medidas como concientización, resguardo, antivirus y actualizaciones también hubieran disminuido el impacto del virus. 17 años después nos encontramos con el mismo patrón de ataque y las mismas falencias, como se observó en el caso de *WannaCry* y *Petya*.

Al abordar la temática de la ciberseguridad, la guía contenida en la norma ISO 27032 plantea dos focos. Por un lado, presenta los desafíos que incorpora la ciberseguridad en relación con la seguridad tradicional como la falta de comunicación entre las partes intervinientes o afectadas en los ciberataques. Es importante visualizar que, al tratarse del ciberespacio, podemos encontrarnos con múltiples dueños o responsables de los activos, cada uno abocado a su propio negocio, con su modelo de operación propio y con sus correspondientes regulaciones. Como se mencionó anteriormente, ahora la información no yace únicamente dentro de nuestro perímetro ni se encuentra exclusivamente bajo nuestro único control.

Entonces, es importante entender los riesgos inherentes a la operación en el ciberespacio, como los ataques web, la denegación distribuida de servicios (DDoS), la infección por software malicioso como los casos mencionados, el engaño por correo electrónico (*phishing*), entre otros. Para esto, las organizaciones deberán estar preparadas y en condiciones de detectar y responder a los ataques aún fuera del perímetro.

El segundo foco sobre el que se desarrolla la norma ISO 27032 es en la necesidad de intercambiar información en tiempo y forma, como así también la interacción y coordinación entre las partes afectadas o con capacidad de acción en la respuesta a incidentes. En el ciberespacio este es un factor clave para proteger la información, teniendo en cuenta que se puede enfrentar un ataque de origen desconocido y puede resultar necesario que la respuesta se dé desde ubicaciones físicamente distantes, incluso entre continentes.

Operaciones de seguridad

Colaboración e inteligencia sobre amenazas

Alineado a los dos focos planteados por la norma ISO 27032 sobre la necesidad de comunicación entre los actores que intervienen en el espacio cibernético y la necesidad de contar con información en tiempo y forma para responder exitosamente a ciberataques, el reporte *Key findings from the Global State of Information Security® Survey 2017* (PwC, 2017) expone cómo las organizaciones están abordando las tareas de inteligencia sobre amenazas y las actividades de compartir información.

El reporte identifica cuatro áreas clave para responder a ciberataques. Primero, incorporar y procesar información de inteligencia en tiempo real. Segundo, evaluar el impacto organizacional de esas novedades. Tercero, identificar acciones para mitigar las amenazas detectadas. Cuarto, ejercer prontas acciones técnicas, legales y operativas.

Para llevar a cabo estas actividades no sólo será necesario contar con un equipo experto y multidisciplinario entre especialistas de informática, consejeros legales, administradores de riesgo y las unidades de negocio. Además, será necesario contar con una plataforma tecnológica capaz de procesar con la velocidad necesaria, la variedad y el volumen de información relacionada.

En el reporte se propone utilizar la capacidad de procesamiento de computación en la nube para monitorear y analizar los eventos y crear un repositorio centralizado y unificado de información en tiempo real. La potencia disponible en servicios en la nube permitirá implementar técnicas de aprendizaje automático e inteligencia artificial, al mismo tiempo que correlacionar esta información con bases de datos globales de amenazas.

Sin embargo, no todas las organizaciones pueden o quieren trabajar con esquemas de computación en la nube y eligen, en cambio, desplegar soluciones locales. De esta forma, la organización tendrá dentro de su perímetro el control integral de la información que utiliza para la ciberdefensa. Como contrapartida, la organización deberá incorporar y retener especialistas capaces de analizar, entender y actuar a partir de la información, al mismo tiempo que la organización deberá disponer de equipamiento capaz de procesar y almacenar el volumen de información en cuestión.

Independientemente del esquema, el reporte revela que aproximadamente la mitad de las organizaciones tienen sistemas de detección de intrusiones, monitorean y analizan información de inteligencia de seguridad; o realizan evaluaciones de vulnerabilidades y amenazas; o disponen de sistemas de gestión de información y eventos de seguridad (SIEM); o

se encuentran suscriptos a servicios de información de amenazas; o realizan pruebas de penetración. Por lo tanto, hay otra mitad de las organizaciones encuestadas que no realizan alguna o ninguna de las actividades arriba mencionadas.

El concepto de inteligencia sobre amenazas hace referencia a que la organización o el equipo encargado de la ciberdefensa cuenten con información sobre amenazas nuevas o desconocidas, que pueden estar surgiendo en otra parte del mundo y que podrían llegar a afectar a la organización, si es que aún no estuviesen siendo afectadas. Existen servicios de reputación o bases datos globales que proveen información de seguridad y pueden ser consumidas por los sistemas de ciberseguridad dentro de la organización para mejorar las protecciones, permitiendo identificar ataques desconocidos o activando barreras ante potenciales ocurrencias.

Asimismo, la inteligencia sobre amenazas abarca la aplicación de técnicas avanzadas como el aprendizaje automático y la inteligencia artificial, para identificar amenazas desconocidas a partir del estudio del comportamiento. Es difícil que esta tarea sea realizada por un humano, dado el volumen, variedad y velocidad de los eventos que se generan y fluyen por la organización, por lo que la tecnología de avanzada cumple un rol fundamental para procesar y analizar los eventos de seguridad.

Una vez que una organización es capaz de identificar una amenaza o bien de encontrar una forma efectiva de responder a una amenaza, es importante que este nuevo conocimiento se distribuya para que otras organizaciones, de la misma rama de actividades o de otras, puedan responder de igual forma y evitar ser afectadas. A esto hace referencia el concepto colaborativo para compartir información y tornando la comunicación entre organizaciones en un desafío para la ciberseguridad.

Si se observa la metodología aplicada por los cibercriminales, se podrá identificar que trabajan en grupos colaborativos compartiendo información, metodologías y herramientas. Existen redes para compartir información sobre ciberataques donde los miembros aportan datos sobre vulnerabilidades en sistemas, distribuyen herramientas para perpetrar ataques o hasta aúnan esfuerzos y se coordinan para actuar.

Del mismo modo, las organizaciones deben imitarlos y abrirse a compartir conocimiento entre ellas. Las plataformas para compartir información son claves para lograr este acuerdo, aunque aún no se encuentran estandarizadas y hay reticencias por parte de muchas organizaciones para compartir información sobre ataques que hayan sufrido, quizás porque podría afectarse su imagen. Sólo el 55% de las organizaciones colabora recíprocamente y comparte información para mejorar la ciberseguridad (PwC, 2017).

Otro obstáculo en este aspecto es que si la información no se logra estandarizar es probable que resulte de poca utilidad para las organizaciones que forman parte de la comunicación y, en vez de ser información valiosa, se convertiría en un cúmulo de alertas con poco valor real para prevenir o responder a nuevas amenazas. Por esto y por la importancia de colaborar y compartir información entre las organizaciones, se generaron a partir del año 2015 las Organizaciones para Compartir y Analizar Información (ISAO) en función de la Orden Ejecutiva 13691 de los Estados Unidos de América (The White House, 2015).

Mediante ese instrumento, el presidente de los Estados Unidos de América impulsó la creación de estas organizaciones para compartir información y enfrentar los ciberataques con mejores herramientas. Desde entonces se han generado los Centros para Compartir y Analizar Información o *Information Sharing and Analysis Centers* (ISAC) según su denominación original en inglés (ISAO SO, s.f.).

En la misma línea, la Unión Europea aprobó en 2016 la *Directiva de Redes y Seguridad Informática* (Comisión Europea, 2016) mediante la que obliga a las naciones a formar Centros de Respuesta a Incidentes de Seguridad Informática y que las organizaciones relacionadas a infraestructuras críticas a su vez les notifiquen a las autoridades nacionales la ocurrencia de incidentes. Al mismo tiempo, les encomienda a esas organizaciones a formar grupos para cooperar en el intercambio sobre información de riesgos.

En la Argentina se formó el grupo de trabajo ICIC CERT (Oficina Nacional de Tecnologías de la Información, 2013), que es el Centro de Respuesta a Emergencias Informáticas y que tiene entre sus objetivos administrar la información sobre reportes de incidentes de seguridad en el Poder Ejecutivo Nacional, asesorar técnicamente a los miembros para dar respuesta a los incidentes y difundir información útil para incrementar los niveles de seguridad.

Por ejemplo, si un Ministerio de la República Argentina detecta un ataque a su infraestructura informática, debe informar dicha situación al ICIC CERT y éste puede difundir la información a los demás Ministerios para que estén preparados ante la potencial amenaza, o bien, sepan cómo responder a partir de la experiencia del otro organismo. De esta forma, se logra compartir conocimiento y trabajar colaborativamente en la ciberdefensa.

Las organizaciones ISAO o similares permiten la creación de redes confiables para fortalecer las capacidades de identificar y mitigar ataques cibernéticos por parte de las organizaciones individuales que forman parte. También proveen información de inteligencia útil y rápida para mejorar la postura de seguridad.

Evolución de los centros de operaciones de seguridad

Los centros de operaciones de seguridad han ido evolucionando a lo largo del tiempo incorporando capacidades, brindando nuevos servicios y especializándose. Esta evolución acompaña a su vez la sofisticación de los ataques y las nuevas metodologías de defensa que necesitan implementar las organizaciones. Una mirada en retrospectiva permite distinguir cuatro generaciones en las que han evolucionado los COS en los últimos 15 años (Cisco Systems, 2015).

Esta evolución a lo largo del tiempo puede a su vez identificarse y desarrollarse internamente dentro de cada organización. Es decir, que es una forma de entender el nivel de madurez en cuanto a gestión de las operaciones de seguridad que tiene cada organización, pudiendo algunas encontrarse en la primera generación y otras en la cuarta. Por lo tanto, si bien el análisis en retrospectiva permite identificar generaciones, es importante destacar que en la actualidad aún hay organizaciones iniciando el camino.

Primera generación

Los servicios de los centros de operaciones de en un principio se encuentran embebidos dentro las funciones generales del área responsable por la tecnología informática. El personal en esta generación no necesariamente está preparado ni capacitado para gestionar eventos e incidentes de seguridad. Las operaciones de seguridad no se brindan a través de un área dedicada y formalmente establecida, sino que son gestionadas entre un cúmulo de otras tareas por una persona o por un equipo tradicional que administra las operaciones de informática.

Las actividades básicas tienen que ver con el monitoreo de salud de dispositivos y enlaces de comunicaciones, administrar el sistema de protección contra software malicioso en la organización y una incipiente colección de registros de seguridad. Sin embargo, esto último sólo está acotado a los dispositivos que son capaces de generar registros de auditoría, probablemente en un nivel básico configurado por defecto por el fabricante. Por ejemplo, los firewalls, el servicio de directorio o el propio cliente de antivirus.

Estos registros en general se almacenan localmente en cada dispositivo, como el servidor de directorio o en la consola local de antivirus en cada terminal. Alternativamente y principalmente en los dispositivos de red, los fabricantes proveen protocolos por defecto para

centralizar los registros, tales como SNMP[6] o Syslog[7]. Los registros son rara vez analizados de forma proactiva, sino que se consultan por el administrador en la medida que un dispositivo estuviese involucrado en un incidente.

En esta generación no hay una concepción de procedimientos de respuesta a incidentes de seguridad en el que se encuentren establecidas las responsabilidades y los pasos a ejecutar. La identificación, comunicación y respuesta a incidentes de seguridad es lenta, a demanda y variable según la persona que toma el caso y lo lleva adelante.

Un ejemplo clásico para ilustrar esta primera generación de centros de operaciones de seguridad puede ser la expansión de software malicioso o virus. En este escenario, las terminales tienen un cliente antivirus instalado, que se actualiza autónomamente de internet y con políticas configuradas localmente, pudiendo éstas variar de una terminal a otra. No existe una consola central donde un administrador despliega políticas y reciba en tiempo real información sobre el estado de seguridad de cada terminal. Por lo tanto, la organización no tiene visibilidad en caso de que un mismo virus esté afectando múltiples terminales. Sólo se enterará en la medida que los usuarios reporten inconvenientes y luego de que los técnicos intercambien información sobre lo que está sucediendo.

Del mismo modo, en el caso que exista un servicio de directorio que registre los eventos de inicio de sesión de los usuarios, aun estando centralizados los registros, el personal no los analizará proactivamente para identificar situaciones de riesgo. Probablemente el servidor esté configurado con los parámetros que viene por defecto, generando registros de poco valor para la organización, que a su vez tapan y complican el análisis de los eventos que sí interesan, como los intentos fallidos de inicio de sesión. Por lo tanto, si en este escenario un atacante intenta tomar control de una cuenta y genera intentos fallidos al ingresar contraseñas incorrectas, no habrá nadie observando e intentando identificar este comportamiento para adelantarse al ataque y responder de forma acorde.

---

[6] SNMP: es un protocolo simple para la administración de redes, "Simple Network Management Protocol" en inglés. Popularmente utilizado en redes IP para la administración de dispositivos de red, la colección de información, la configuración de dispositivos de red como servidores, impresoras, hubs, switches, enrutadores (Microsoft Corporation, 2003).

[7] Syslog: es un estándar para los mensajes sobre registros de auditoría. Permite la separación entre los dispositivos que generan los registros, los sistemas que los almacenan y los sistemas que los analizan. Cada mensaje es etiquetado con código de instalación, indicando el tipo de software que genera el mensaje, y se le asigna una etiqueta de seguridad (Wikipedia, 2006).

Esta generación puede representar a las organizaciones pequeñas, que disponen de un área de informática con poco personal cuyas funciones son variadas y están orientadas más bien a dar servicio básico de funcionamiento que de calidad corporativa. En este contexto no hay aún responsabilidades de seguridad asignadas ni roles dedicados a la temática.

Segunda generación

En esta generación entran en escena los sistemas de gestión de información y eventos de seguridad (SIEM). Las primeras versiones de SIEM eran provistas por fabricantes como netForensics, Network Intelligence o Cisco con su producto MARS (*Security Monitoring, Analysis, and Response System*). Estos sistemas prometían detectar amenazas de red quitándole a los administradores la responsabilidad de analizar manualmente enormes volúmenes de información. Estos proveedores se enfocaban más bien en los gestores de amenazas de red o STM por sus siglas en inglés (*Security Threat Management*), similar a lo que se conoce en la actualidad como gestor de eventos de seguridad o SEM (*Security Event Management*) que proveen análisis en tiempo real para la detección de amenazas.

Estas herramientas reciben registros de auditoría generados por múltiples dispositivos en diferentes formatos y permiten acelerar el proceso de detección de potenciales incidentes. El concepto de SEM es la agregación de registros de auditoría provenientes de distintos dispositivos como aplicaciones, sistemas operativos o dispositivos de red. Luego, las herramientas realizan un análisis de regresión sobre los eventos para identificar posibles relaciones entre ellos, lo que podría indicar un posible incidente de seguridad. Los operadores consumen esta información a visualizando tableros de control especialmente diseñados.

Las funciones de los SEM se consolidan con las de los sistemas de gestión de información de seguridad o *Security Information Management* (SIM) para alcanzar lo que hoy se conoce como SIEM. Los productos SIM se focalizan en realizar búsquedas sobre grandes volúmenes de registros de auditoría previamente colectados y almacenados. Esta información histórica puede ser luego analizada con distintos fines, como el análisis forense, investigaciones sobre incidentes o asegurar el cumplimiento de políticas de retención de registros de seguridad.

Otro aspecto importante que se introduce en esta segunda generación de los centros de operaciones de seguridad es la administración de casos. Los operadores de los SIEM pueden generar casos y asignarlos a partir de las detecciones realizadas por los productos. Estas herramientas pueden estar integradas con el sistema de tiques tradicionalmente utilizado por el área de informática para la gestión de casos.

Los productos SIEM consolidan las funciones de recolectar o recibir registros de auditoría, analizar gramaticalmente los registros para identificar columnas o pares de valores, normalizar los datos asociándolos a etiquetas estándar y luego aplicar las reglas de correlación para identificar las situaciones de riesgo.

Tomando como referencia las situaciones mencionadas en la primera generación, un SIEM tendría la capacidad de recibir los eventos de infección de los clientes de antivirus en las terminales para alertar tempranamente sobre la propagación de un software malicioso. O bien, identificar los intentos fallidos de inicio de sesión tanto en el servidor de directorio como en otros dispositivos y alertar sobre un posible intento de intrusión o robo de credenciales. Ante estas alertas que aparecen en tiempo real en la consola, los operadores pueden generar un caso y reaccionar rápidamente desplegando nuevas firmas de antivirus, aislando terminales o advirtiendo a los usuarios sobre un potencial riesgo.

Tercera generación

La tercera generación de los centros de operaciones de seguridad se caracteriza principalmente por incorporar la gestión de vulnerabilidades técnicas, además de alcanzar un estado de madurez mayor en cuanto a la formalización de los procedimientos en la respuesta a incidentes. Es decir que al mismo tiempo que se perfecciona el proceso de gestión de incidentes de seguridad, se incorpora la gestión de vulnerabilidades dentro de los servicios brindados.

Probablemente en esta etapa ya se encuentre conformada una pequeña área o al menos un grupo de individuos tengan asignadas responsabilidades específicas en asuntos de seguridad para atender las alertas del SIEM, responder incidentes y controlar la colección de eventos de seguridad.

La gestión de vulnerabilidades en sí misma se refiere a la práctica en la que las vulnerabilidades técnicas se descubren y confirman, se evalúa su impacto, se identifican y aplican medidas correctivas, y se le da un seguimiento del estado de las vulnerabilidades hasta que se verifica su cierre.

Un factor determinante en esta gestión es que la evaluación del impacto de las vulnerabilidades detectadas esté alineada a la gestión de riesgos de la organización. Esto implica que todo el proceso se encuentre alineado y que no sea un mero escaneo de vulnerabilidades sobre dispositivos de red. La fase del escaneo es una actividad que forma parte del proceso global y se lleva a cabo durante el descubrimiento, confirmación y seguimiento.

Los productos que sustentan esta gestión han evolucionado de simples escáneres a productos que automatizan la gestión integral del proceso. El equipo encargado del COS podría

operar directamente las herramientas de descubrimiento o podría sólo serle asignada una parte del proceso. Este es el caso cuando se trabaja con proveedores o servicios de consultorías especializados, que se encargan de realizar el descubrimiento, confirmar las vulnerabilidades, descartar falsos positivos y luego remitir los hallazgos al equipo del COS para que encomiende la remediación a la respectiva área administradora y realice el seguimiento.

El área o estas personas podrían actuar como interlocutores con los CERT o ISAO para intercambiar información tanto sobre ataques como sobre vulnerabilidades que afectan a tecnologías similares. En el caso de la Administración Pública Nacional de la Argentina, el grupo de trabajo ICIC CERT distribuye alertas entre los organismos asociados para advertir sobre nuevas vulnerabilidades de fabricantes como Microsoft, Apple o Cisco, al mismo tiempo que envía información sobre ataques que podrían afectar a los organismos públicos.

Cuarta generación

Esta generación es la que alcanza el mayor nivel de sofisticación en las tareas de inteligencia de los COS y puede encontrarse en grandes organizaciones que priorizan la seguridad dentro de sus planes estratégicos. En esta generación se incorporan servicios avanzados de seguridad que buscan prevenir los nuevos tipos de amenazas.

El primer concepto que se destaca de esta generación es transcender el análisis clásico de regresión sobre los eventos de los productos SIEM para incorporar funcionalidades de *big data*. Estas plataformas se despliegan en la actualidad para consumir datos de cualquier origen, a gran velocidad y en grandes volúmenes, al mismo tiempo que permiten consultar y analizar los datos en tiempo real o fuera de línea.

Un ejemplo desde la perspectiva de seguridad sería recibir todo tipo de registros de auditoría con variedad de formatos, en grandes volúmenes, procesarlos con alta velocidad y poder realizar análisis de regresión incluyendo información externa provista por fuentes especializadas. De esta forma se logra mayor capacidad de detección de ataques y rapidez de reacción al expandir las fronteras del análisis interno y disponer de resultados inmediatos. Naturalmente este tipo de arquitectura tendrá sentido en organizaciones de medianas a grandes donde el volumen de registros de auditorías tome tal dimensión que torne obsoletas las plataformas tradicionales de análisis.

Otro concepto que incorpora la cuarta generación de COS es el enriquecimiento de datos a través de la geolocalización de eventos, la incorporación de datos sobre los nombres de dominios involucrados en los eventos, información provista por sistemas de control de accesos y servicios de reputación. La telemetría es a su vez otro componente para enriquecer el análisis

ya que permite analizar el comportamiento a partir de los propios registros que producen los dispositivos de red, convirtiéndolos de esta forma en sensores adicionales.

La integración de la plataforma de seguridad toma especial protagonismo para lograr efectividad en la respuesta de incidentes de modo tal que, en caso de que un sensor detecte cierta situación, pueda accionar de forma automática aplicando una regla restrictiva que impida la continuidad de lo que potencialmente podría ser un ataque. Puede compararse este accionar al de un sistema de prevención de intrusiones (IPS) pero con la diferencia de que la acción no se aplica a partir del análisis de un único dispositivo y en un único punto, sino que la detección puede prevenir de un conjunto de sensores o dispositivos y la acción puede tomarse en uno o más puntos de control.

Esta transversalidad es característica de la cuarta generación de COS y demuestra el dominio del equipo tanto en conocimiento como en acción para operar la respuesta a incidentes en el menor tiempo posible como así también en prevenir incidentes detectando a tiempo brechas de seguridad y aplicando su remediación automáticamente.

Figura 2. Generaciones de los centros de operaciones de seguridad.

Operaciones de los centros de operaciones de seguridad

Los centros de operaciones de seguridad agregan valor a la organización a través de los servicios que brindan. En línea con la sección anterior, a lo largo de las generaciones han ido concentrando y asumiendo responsabilidades con el fin de brindar servicios de seguridad eficientes y eficaces.

Servicios de valor agregado

De acuerdo con las funciones esenciales identificadas por la empresa IBM, entre los servicios principales que debe brindar un COS se encuentra la gestión de incidentes de seguridad, abarcando las acciones como la detección, el análisis y la respuesta a incidentes (IBM Corporation, 2013). Este servicio se materializa mediante la ejecución del proceso de gestión de incidentes y tendrá como objetivo la rápida y eficaz contención y respuesta a incidentes para minimizar el impacto.

Para sustentar la gestión de incidentes es intrínseco a los COS que brinden el servicio de colección, análisis y almacenamiento de registros de auditoría y eventos de seguridad. Esto permitirá llevar a cabo la detección de incidentes de seguridad y el análisis forense en caso de resultar necesario. Si bien parte de estas actividades pueden estar delegadas en otras áreas, continuará siendo responsabilidad del COS asegurar que se encuentren habilitadas las auditorías y monitorear la disponibilidad de esos registros mediante la colección y almacenamiento.

Otro servicio de los centros de operaciones de seguridad es la gestión de vulnerabilidades. En caso de que el COS realice la gestión completa, incluyendo el descubrimiento y la remediación, entonces el servicio es brindado íntegramente por éste. Alternativamente, el COS puede actuar como nexo con proveedores que suministren información sobre vulnerabilidades descubiertas en la organización, como también actuar como nexo con los administradores encargados de implementar las medidas correctivas.

El monitoreo para asegurar el cumplimiento tanto de normativa interna como externa en materia de seguridad informática es un servicio que puede ser asignado a los centros de operaciones de seguridad y que contribuye tanto a la disminución del riesgo como también a la prevención de ser multados, con el impacto financiero y de reputación que podría conllevar.

El personal del COS puede brindar el servicio de concientización para la educación en materia de seguridad informática. Estas actividades serán útiles para capacitar al personal sobre la detección de potenciales incidentes, cómo reportarlos y cómo reaccionar ante una situación de riesgo.

La investigación forense es un servicio brindado por el centro de operaciones de seguridad, actuando como referente técnico ante eventuales cuestiones legales. Por ello el personal del COS debe estar capacitado para actuar en los casos utilizando tecnología dedicada y preservando al mismo tiempo la cadena de custodia.

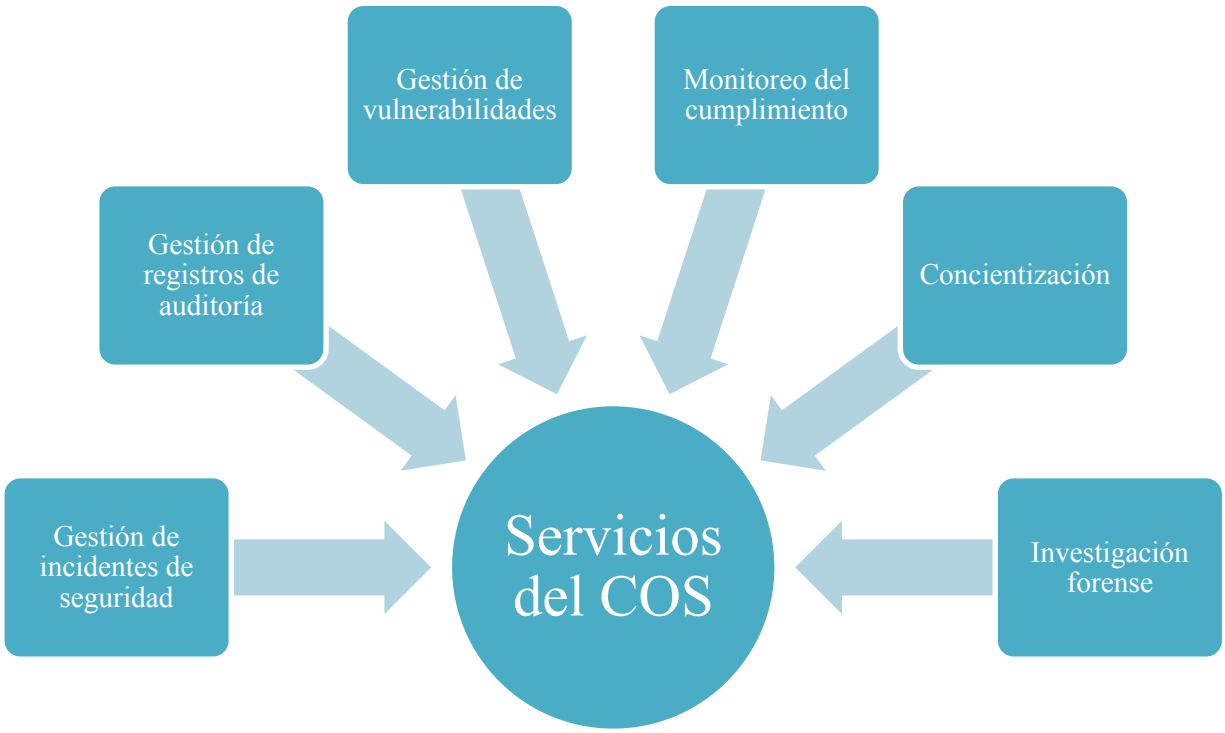

Figura 3. Servicios del centro de operaciones de seguridad.

Factores de éxito

Para que las operaciones se desarrollen con éxito y se puedan brindar los servicios con los niveles esperados, se deben dar factores de éxito que son característicos de los centros de operaciones de seguridad efectivos (Cisco Systems, 2015). En primer lugar, resulta esencial contar con apoyo ejecutivo que puede materializarse mediante la aprobación de la misión del COS por parte la Alta Dirección y el correspondiente reporte de métricas por parte del equipo. El rol del patrocinador puede ser asumido por el director ejecutivo (CEO), el director de información (CIO) o por los directores de tecnología o de gestión de riegos según la dependencia jerárquica del COS.

El gobierno es el segundo factor de éxito y se lleva a cabo eficazmente mediante el establecimiento de métricas que permitan medir la efectividad del COS. Las métricas deben

proveer visibilidad a la dirección sobre la performance del COS y a su vez deben permitir identificar los puntos débiles que requieren optimización o inversión.

El COS debe ser operado como un programa y no como un proyecto individual. Esto se debe a la criticidad y la cantidad de recursos necesario que implica diseñar y poner en ejecución un centro de operaciones de seguridad. Es importante para ello tener una estrategia con objetivos intermedios en función de las prioridades establecidas e ir incrementando las capacidades a medida que se alcanzan los objetivos (SANS Institute, 2015).

La colaboración entre las áreas de la organización es un factor de éxito clave a lo largo de las fases de planificación, diseño, construcción y operación del COS. La colaboración debe ser definida formalmente al comienzo del programa para garantizar el apoyo y evitar conflictos de intereses por superposición o incertidumbre sobre las responsabilidades de cada área.

Un COS será exitoso en la medida que pueda tener visibilidad sobre los datos y los sistemas. Para ello se debe garantizar el acceso a los datos y los sistemas de modo que el COS pueda obtener la información necesaria para operar. El alcance del acceso debe definirse en la etapa de diseño e incluirse en la estrategia, y puede abarcar también a las configuraciones de los sistemas además de los registros de auditoría. Asimismo, el acceso a la información puede incluir la asignación de permisos de lectura sobre una parte del sistema donde se almacenan los registros de auditoría.

La operación y entrega de servicios debe sustentarse sobre procesos y procedimientos establecidos en la etapa de diseño. La gestión por procesos evidenciará la necesidad de conocimiento por parte del equipo del COS como así también la necesidad de contar con determinadas herramientas. Los procesos creados durante el diseño y construcción deberían contemplar las capacidades actuales y deseadas.

Las habilidades y la experiencia son otro factor de éxito para el COS, ya que le permitirá al equipo operar las herramientas tecnológicas y dar curso a las investigaciones de incidentes. Asimismo, con el correr del tiempo el equipo irá adquiriendo experiencia en términos del negocio de la organización y en la gestión de seguridad específicamente. La organización, a través de las áreas específicas, deberá apoyar el crecimiento, desarrollo y capacitación del equipo mediante cursos de capacitación y entrenamiento en la gestión de sus habilidades personales.

El presupuesto asignado al programa será determinante para dar impulso y alcanzar los niveles esperados de servicio. Para definir el presupuesto adecuado se deben considerar múltiples variables, como el modelo de operación que se elija, los servicios que se esperan según cada etapa, el nivel de habilidad del personal y la hoja de ruta del COS.

Los factores de éxito descriptos se interrelacionan entre sí y la falta de uno de ellos puede afectar significativamente al resto de los factores comprometiendo la efectividad del COS. Por ejemplo, si no se cuenta con apoyo de la Alta Dirección, podrían aparecer inconvenientes en la interacción con las demás áreas y esto podría afectar la visibilidad que tiene el COS, lo que a su vez le impediría gestionar incidentes de seguridad.

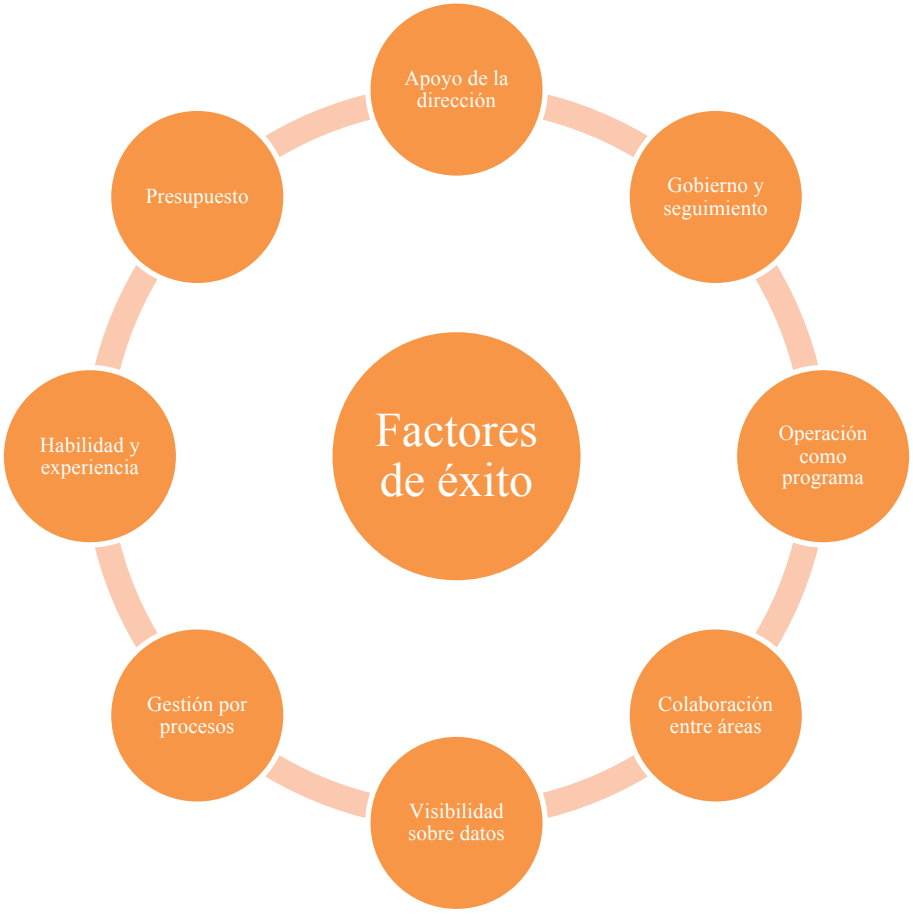

Figura 4. Factores de éxito de un centro de operaciones de seguridad.

Tríada: procesos, personas y tecnologías

Procesos

La gestión por procesos definirá el modo de administrar las operaciones de los COS incorporando el concepto de cadena de valor, permitiendo la estandarización de las actividades y dando lugar a la mejora continua. Estas características propias de gestionar por procesos son factores de éxito para los centros de operaciones de seguridad y facilitarán el entendimiento de las actividades por parte de la Alta Dirección y su consecuente apoyo tanto corporativo como financiero.

El concepto de cadena de valor referencia al entramado de instrumentos como políticas, reglas de gestión, procesos, procedimientos y otros, que aseguran que las actividades llevadas a cabo por el personal agreguen valor para la organización al implementarse de forma ordenada y dentro de una jerarquía. Esto se logra ya que el trabajo se organiza, por un lado, cumpliendo con las reglas impuestas por los directivos a través de políticas y reglas de negocio. Por otro lado, evaluando si las actividades contenidas en procesos y procedimientos aportan valor para los objetivos que buscan satisfacer.

Es importante resaltar que los centros de operaciones de seguridad tendrán que cumplir con requerimientos legales como legislación nacional o estándares internacionales, y a su vez tendrán que cumplir con las políticas y reglas de negocio determinadas por la Alta Dirección. Esta normativa interna o externa, nacional o internacional, debe regir y a su vez ser cumplimentada con la implementación de procesos y procedimientos que regulen las actividades del personal.

La estandarización que se alcanza por la implementación de procesos agrega calidad a la operación en dos sentidos. Por un lado, la tarea de estandarizar procesos busca reducir y eliminar la variabilidad del resultado de las actividades llevadas a cabo; es decir, se espera que el producto o servicio que entregan los procesos sea siempre mismo. Por otro lado, el camino hacia la estandarización implica que se efectúen relevamientos de la situación actual, se identifiquen las herramientas y personas involucradas, se consensuen las actividades y su secuencia y todo esto se vuelque en un documento formal.

Documentado el proceso, se podrá efectuar sobre él la mejora continua a través de la medición y análisis de indicadores. El resultado de este análisis será una fuente fiable y objetiva para evaluar cambios en el proceso, como, por ejemplo, cambiar el orden de las actividades, agregar o suprimir actividades, incorporar tecnología o personal, optimizar el vínculo con otras partes interesadas.

Hasta aquí se ha referenciado al término de procesos exclusivamente, pero es importante aclarar que los puntos descritos arriba aplican de igual forma a los procedimientos y que éstos son muy importantes para la operación. Ambos artefactos consisten en una serie de actividades que llevadas a cabo de forma ordenada permiten alcanzar un entregable. Ahora bien, los procesos buscan entregar un determinado servicio o producto e incluyen a distintas áreas, como puede ser la gestión de incidentes en la que interviene el COS y también áreas administradoras, entre otras.

En cambio, los procedimientos son ejecutados por un único individuo y describen la forma correcta en que esa persona debe hacer esa tarea. El resultado del procedimiento puede ser la entrada a una actividad del proceso, por lo que un proceso puede componerse de múltiples procedimientos, pero no al revés. Los procedimientos tienen un nivel de abstracción menor a los procesos.

Los procesos y procedimientos pueden resultar perjudiciales para la operación si se documenta en exceso o si se intentan documentar situaciones que requieren creatividad o libertar de acción. Los procesos y procedimientos son herramientas para mejorar la operatoria y deben utilizarse en situaciones que los requieran, como en la integración de las áreas, cuando se necesita consistencia en los resultados o en actividades que tienen impacto directo en el nivel de servicio.

A continuación, se presentan los procesos y procedimientos que pueden formar parte de la gestión del COS, de acuerdo con el agrupamiento por aspecto o funcionalidad propuesto por especialistas de seguridad (Cisco Systems, 2015). Es común que las organizaciones no tengan documentados todos los procesos y procedimientos que identifican los especialistas, sin embargo, resulta útil su identificación y presentación para ilustrar las tareas y operaciones que se pueden llevar a cabo en un COS. Muchas de estas tareas seguramente se lleven a cabo de forma natural y por requerimiento propio de la operatoria cotidiana, sin estar siendo ejecutadas y medidas en el marco formal de gestión por procesos.

Gestión de servicios corporativos

Existen procesos corporativos que pueden ser reutilizados por los centros de operaciones de seguridad al estar posiblemente implementados por el área encargada de administrar la infraestructura tecnológica. Estos procesos se desprenden o soportan directamente la entrega de servicios de tecnologías de la información (TI) y pueden estar basados en el conjunto de prácticas como *Information Technology Infrastructure Library* (ITIL).

Entre los procesos existentes o asociados a la operación de TI se encontrará el proceso de gestión de eventos, que abarca la administración y monitoreo de registros de auditoría de los dispositivos de red y sistemas informáticos. Estos registros pueden ser usados con fines de monitorear los niveles de servicio o con fines de seguridad.

También se encontrará el proceso de gestión de incidentes que puede estar implementado y siendo ejecutado por las áreas de mesa de ayuda, soporte técnico, administración de servidores y otras áreas operadoras de la infraestructura tecnológica. A su vez, el proceso de gestión de problemas, cuyo objetivo es identificar el inconveniente que subyace y genera reiterados incidentes sobre el mismo aspecto. Ambos procesos pueden ser implementados por el COS ya que se pueden identificar incidentes y problemas de seguridad.

Otro proceso existente puede ser el proceso de gestión de vulnerabilidades, cuyas actividades pueden estar siendo implementadas por las áreas operadoras de TI, a través de la instalación de parches o el análisis de seguridad de los propios dispositivos que administran o como resolución de defectos reportados por los usuarios.

Dependiendo el nivel de administración que efectúa el COS sobre las plataformas tecnológicas que utiliza, puede ser que sean de interés los procesos de gestión del cambio, gestión de configuraciones o gestión de versiones.

Gestión de servicios de seguridad

Los procesos de gestión de servicios de seguridad abarcan las tareas generales asociadas a la seguridad y pueden estar relacionados con un sistema de gestión de seguridad de la información. Entre estos se pueden encontrar el proceso para el desarrollo de procesos o procedimientos, que establece quiénes se deben involucrar y cómo se confeccionarán y aprobarán nuevos documentos. También se encuentra el proceso de medición y soporte, cuyo objetivo es la recolección de métricas de los procesos y la realización de reportes periódicos o a demanda. A su vez, se encuentra el proceso de mejora continua, cuyo objetivo es la implementación de mejoras en los procesos a partir del análisis de los indicadores de performance.

Dentro del mismo agrupamiento se encuentra el proceso de entrega de servicios de seguridad, cuyo objetivo es establecer cómo los usuarios acceden a los servicios de seguridad. Aquí se puede encontrar la gestión de tiques, de llamados, de correos electrónicos y cualquiera otra vía de contacto. También forman parte los procesos de retención, archivo y purgado de registros de auditoría, y el proceso de auditoría y soporte al cumplimiento, cuyo objetivo es responder a los requerimientos de informes.

El proceso de entrenamiento de personal, el proceso de continuidad de operación y el proceso de recuperación a desastres forman parte del agrupamiento. Del mismo modo que el proceso de gestión de proveedores y el proceso de reporte financiero y operacional, cuyo objetivo es informar sobre estos aspectos a los directos y a los interesados.

Ingeniería de servicios de seguridad

Si se está ante un COS de gran envergadura se pueden encontrar procesos asociados al mantenimiento de la plataforma tecnológica, donde los cambios toman relevancia por el riesgo operacional que implican y el impacto que pueden generar. En este tipo de COS se puede encontrar el proceso de administración del ciclo de vida, cuyas actividades pueden ser el análisis, la planificación, el diseño de alto y bajo nivel, el despliegue, prueba, y hasta la remoción de productos tecnológicos.

También se encuentra el proceso de gestión de cambios y versionados al desarrollar y migrar tecnologías, o procedimientos de gestión de configuraciones, que establecen los pasos y buenas prácticas para aplicar cambios en los sistemas y dispositivos.

En los centros de operaciones de seguridad, que administran registros de auditoría de variados orígenes y tipos, el proceso de gestión de orígenes de eventos puede resultar útil para administrar con consistencia la incorporación de nuevas fuentes y su actualización a lo largo del tiempo. Esto es importante porque un nuevo producto en la red de datos generará registros de auditoría que deben ser integrados e interpretados por los sistemas de seguridad, como así también, la mera actualización de un producto puede requerir cambios de configuración por parte del COS.

Operación de los servicios de seguridad

Este agrupamiento contiene los procesos y procedimientos que dan mantenimiento a los sistemas y a la información utilizada por el COS. Entre ellos se encuentra el proceso de monitoreo de sistemas, cuyo objetivo es identificar posibles problemas que impidan alcanzar los niveles de servicio deseados. También se encuentra el proceso de monitoreo de licenciamiento, que permite identificar licencias próximas a caducar. Este proceso toma especial relevancia en redes que contienen múltiples productos, versiones y proveedores, como así también cuando el proceso de renovación de licencias requiere largos periodos y por lo tanto es importante adelantarse al vencimiento.

El proceso de mantenimiento de la plataforma es importante para el COS cuando debe dar soporte a la plataforma tecnológica además de dar soporte a las aplicaciones. En este escenario el COS deberá soportar el hardware y el sistema operativo base. Surge entonces

adicionalmente el proceso de pruebas sobre la plataforma, cuyo objetivo es asegurarse que la plataforma es adecuada para soportar una nueva versión de los sistemas o un nuevo sistema directamente.

En la capa más abstracta de este agrupamiento se encuentra el proceso de gestión de contenido, cuyas actividades abarcan la creación de reglas, casos de usos, filtros, alertas y monitores del software que actúa como SIEM. Los procedimientos deben abarcar la puesta en producción de estos elementos sin que afecten la operación del SIEM y evitando cualquier tipo de incompatibilidad que pudiera detener el análisis en tiempo real que efectúa el sistema.

Monitoreo de seguridad

Este agrupamiento contiene los procesos y procedimientos para gestionar los eventos, reportes de incidentes y alertas recibidas de modo que sean adecuadamente tratadas y escaladas. El proceso de monitoreo de seguridad y escalamiento establece cómo se efectuará el monitoreo de seguridad, cómo se investigarán y cómo se escalarán los casos.

Los procedimientos asociados pueden estar confeccionados por plataforma afectada y deberán contener el detalle suficiente para ser ejecutados por analistas iniciales. Estos procedimientos se desarrollan principalmente para alertas comunes, para las que ya se sabe cómo responder y qué pasos se deben ejecutar.

El proceso de gestión de casos regula cómo se abrirán, actualizarán y cerrarán los casos administrados por el COS, donde se incluye la información asociada. Cada acción tendrá a su vez el correspondiente procedimiento que establecerá cómo se hace y qué se debe incluir. Si se utiliza un sistema de casos compartido en el área de operaciones de TI, estos procedimientos ya pueden existir y podrán reutilizarse.

El proceso de gestión de alertas de terceros tiene como objetivo administrar y dar el tratamiento adecuado a las alertas recibidas desde fuera de la organización. Entre los emisores pueden estar las ISAO, los CERT, los proveedores de tecnología o los proveedores de servicios subcontratados, entre otros. Según cada remitente, se pueden confeccionar distintos procedimientos.

El proceso de gestión del conocimiento es de suma utilidad para el COS ya que cada analista irá explorando y adquiriendo información por su cuenta, en la operación misma, y es importante compartir ese conocimiento en el equipo. Por tal motivo, gestionar el conocimiento y establecer el ciclo de vida de los artículos que compongan la base será importante para una buena dinámica en la operación.

Investigación y respuesta a incidentes de seguridad

La respuesta a incidentes es una de las tareas del COS más conocidas y visibles, y realizar esta tarea de forma consistente, efectiva y repetitiva requiere de procesos y procedimientos. El proceso de gestión de incidentes de seguridad, emparentado con el proceso de gestión de incidentes de TI, abarca las actividades de detección, investigación, contención y recuperación, siempre con los objetivos de minimizar el impacto y asegurar la continuidad operativa.

Los procedimientos de investigación, dependientes del proceso de gestión de incidentes de seguridad, establecerán los pasos a ser efectuados por los analistas según el tipo de incidente del que se trate. Estos procedimientos son importantes para asegurar la calidad de la evidencia forense que se recolecte. Es importante redactar los procedimientos una vez que se hayan podido modelar los tipos de incidentes e identificar la mejor respuesta; caso contrario, los procedimientos pueden resultar obsoletos, teniendo en cuenta que es difícil anticiparse a la variedad de incidentes y las condiciones en la que se producen.

El proceso de análisis de software malicioso forma parte de este agrupamiento y es necesario tenerlo previsto ya que se tienen que saber los pasos a seguir por las personas intervinientes cuando se detecta una infección de este tipo. En caso de que las herramientas antivirus sean administradas por otras áreas, es importante definir qué área recolecta la muestra de software malicioso, cómo las almacena y transporta y cómo son reportadas a los proveedores de firmas antivirus.

Como no todos los incidentes son detectados por casos de usos previamente configurados por el personal del COS, se puede confeccionar un proceso de retroalimentación, cuyo objetivo sea actualizar el contenido del SIEM, como casos de usos, alertas, etc., que permita detectar a futuro las situaciones previamente no detectadas. Asimismo, esto puede servir para reconfigurar y optimizar los dispositivos de detección existentes, como los sistemas de detección de intrusiones.

Gestión de registros de auditoría

La gestión de los registros de auditoría es una actividad crítica para los centros de operaciones de seguridad, ya que a partir de ellos podrá efectuar la detección y respuesta a incidentes, como así también responder a requerimientos de informes. El proceso de análisis de orígenes de registros de auditoría tiene como actividades el análisis de los distintos orígenes de datos y la determinación de si debe ser incorporado en la plataforma de colección.

Determinado que el origen será integrado, el procedimiento de colección establecerá los pasos y condiciones en que esos registros de auditoría serán incorporados en la solución SIEM. Luego entra en acción el procedimiento para almacenamiento de registros que establece cómo asignar los registros de cierta tecnología a la base de almacenamiento correspondiente según las necesidades operativas. Por último, el procedimiento de normalización establece los pasos y la lógica con que cada registro será procesado y normalizado. Estos procedimientos pueden ser confeccionados para cada tecnología, dada la diversidad con que cada producto y proveedor generan registros de auditoría.

En centros de operaciones de seguridad de gran tamaño pueden ser necesarios procedimientos para la consulta de registros, teniendo en cuenta no sólo la complejidad que implica realizar una consulta en grandes volúmenes de datos, sino que el consumo de recursos que puede afectar la consulta. El procedimiento de purgado de registros de auditoría establecerá los pasos y explicitará los criterios con que los registros de auditoría colectados serán luego eliminados. Cada tecnología puede tener procedimientos específicos, que establezcan pasos y tiempos de retención individuales.

Gestión de vulnerabilidades

La gestión de vulnerabilidades es el segundo servicio principal que ofrece un centro de operaciones de seguridad en conjunto con la gestión de incidentes de seguridad. Si bien el COS generalmente no es responsable de la gestión integral, es decir, por ejemplo, no suele ser responsable de aplicar las medidas de remediación, sí participa en la gestión, coordinando y realizando seguimiento.

El proceso de gestión descubrimiento de vulnerabilidades tiene entre sus actividades la realización de escaneos, el análisis de los resultados preliminares y el reporte de estos hallazgos a quien corresponda. Puede a su vez incluir procedimientos para la recepción de reportes efectuados por terceros. Esta tarea puede formalizarse en un proceso, ya que su realización puede requerir la intervención y la coordinación con otras áreas, como las áreas de desarrollo y las áreas de operación de TI.

El proceso de gestión de alertas de vulnerabilidades abarca la recepción y tratamiento de reportes automáticos provistos por servicios de reputación u organizaciones especializadas. En estos se incluyen los avisos de los proveedores cuando liberan una nueva versión de un producto o cuando proveen actualizaciones. Puede no ser necesario el escaneo de vulnerabilidades y resultar mejor en relación costo beneficio aplicar el parche liberado por el proveedor, por lo que en ese caso se deben gestionar estos avisos y remitirlos al área pertinente.

El proceso de seguimiento abarca las actividades de administración de los hallazgos una vez confirmados. Este proceso toma como entrada a la salida de los dos procesos mencionados anteriormente. El área de seguridad revisa la situación actual de los hallazgos reportados, verifica los tiempos transcurridos, colabora en la remediación de ser necesario y eleva a las autoridades los desvíos o aquellos casos que presentan dificultades.

El proceso de seguimiento puede tener interfaces con los procesos corporativos de gestión de riesgos, en lo que el COS participa evaluando el riesgo técnico de las vulnerabilidades detectadas y no remediadas e informa esta situación a los directivos.

Inteligencia de seguridad

Este agrupamiento incluye los procesos y procedimientos necesarios para consumir información de inteligencia y darle sentido en el contexto de la organización. De igual forma sirve para la producción de información que tendrá como destinatarios organizaciones externas. Los servicios reputación y las organizaciones específicas como las ISAO o los CERT producen información que puede no tener aplicabilidad en la organización y por lo tanto es importante procesar estos reportes.

El proceso de identificaciones de amenazas tiene como objetivo procesar la información de inteligencia e identificar amenazas reales que puedan afectar la operatoria de la organización. El proceso de modelado de amenazas y vulnerabilidades identifica la probabilidad, relevancia y severidad de estas en el contexto de la organización. De este modo se podrán identificar riesgos y establecer prioridades para aplicar medidas de protección.

El modelado en sí mismo es una actividad enriquecedora que se debe realizar en los equipos de trabajo cuando la información o los datos son críticos, confidenciales o sensibles y se desea darles mayor seguridad a los sistemas de información. En ese ejercicio se identifican las amenazas, los vectores de ataque, los activos involucrados y se buscan las vulnerabilidades que podrían ser aprovechadas para afectar la confidencialidad, integridad o disponibilidad de la información.

El proceso de instrucción y notificación establece cómo se comunican los resultados del análisis efectuado anteriormente sobre la información de inteligencia. Este proceso toma relevancia al regular el vínculo entre áreas y la definición de tareas y responsabilidades.

Gestión de reportes de seguridad

Uno de los servicios del COS es la emisión de reportes basados en el cúmulo de datos e información que consolidan. Los reportes son emitidos tanto para usuarios finales que requieran cierta información como para autoridades y el mismo personal del COS.

El proceso de recolección de datos tiene como fin identificar qué datos y de qué forma se colectarán para estar a disposición de la plataforma de análisis. Los datos pueden provenir del mismo origen, o bien, ser procesados por los mecanismos de colección que utiliza en común con el SIEM. El enfoque que se le da a estos datos es que tengan fines de análisis y reporte.

De este proceso dependerán el procedimiento de gestión de requerimientos, que analiza la solicitud e identifica el reporte correspondiente para resolverla, y el procedimiento de formateo y entrega, que le da el formato necesario al reporte y lo entrega al requirente.

Por el volumen de datos y en línea a lo mencionado en apartados anteriores, existen procedimientos para la gestión de consultas que se efectúan sobre el repositorio de información. Estos procedimientos establecen cómo se generan nuevas consultas de datos e incluyen el diseño, prueba y puesta en producción. Eventualmente pueden incluir la programación de tareas para que se ejecuten de forma periódica o planificada.

El repositorio de datos requerirá procedimientos de minería de datos, que se encarguen de modelar los datos y procesarlos para el almacenamiento a largo plazo. Este almacén de datos puede existir en paralelo al SIEM, que contiene los datos operativos. Es decir, existirán dos repositorios, uno para sustentar la operación y otro con fines analíticos.

Personas

"*Los chicos malos están por todos lados y nuestra superficie atacable se expande a una tasa alarmante. La tecnología por sí sola no puede combatir este desafío. Necesitamos los chicos buenos en forma de analistas de seguridad en nuestros COS y Centros de Ciberdefensa para proteger y defender nuestras organizaciones, nuestros clientes y nuestros activos*" (HP Enterprise, 2015). De acuerdo con el reporte *Growing the Security Analyst* de la empresa HP Enterprise, diseñar una estructura acorde y contar con las personas adecuadas es un factor clave y a su vez un desafío difícil de alcanzar. Las personas que formarán parte del centro de operaciones de seguridad deberán contar con un balance de aptitudes técnicas, sociales y de auto superación que es complicado encontrar y mantener.

La cotidianeidad de la operación de los centros de seguridad puede sintetizarse como largos períodos de tareas rutinarias junto con cortos períodos de crisis. Por un lado, se encuentran momentos de preparación y mantenimiento, donde se llevan actividades de análisis de registros de auditoría, mejora de procesos y procedimientos, configuración de tecnologías y aprendizaje individual. Por otro lado, cuando las alertas se disparan y el COS tiene que iniciar la respuesta a incidentes, aumenta la presión para responder rápida, efectiva y consistentemente.

La capacitación individual juega un rol fundamental en el perfil del personal, porque no existe una formación orientada especialmente al rol de un operador o analista de COS ni en cursos, carreras terciarias, carreras universitarias ni de posgrado, pero también, por la diversidad de conocimientos que debe adquirir el personal.

Es esta diversidad de conocimientos y la predisposición por explorar fuera de la zona de confort de las personas, que requiere una capacitación constante por parte del personal. Todo el tiempo se implementan nuevos productos, se descubren nuevas vulnerabilidades, se detectan nuevos ataques sobre dispositivos de red, personas, redes, aplicaciones informáticas y cuanto activo de la información pueda encontrarse en una organización. Es ese entorno único el que exige conocimientos específicos por parte del personal que no podrán encontrar en una única formación.

Sin embargo, no será suficiente ser autodidacta y flexible, sino que además se deberán tener habilidades sociales para poder desenvolverse en equipos de trabajo e interactuar tanto con otros miembros del COS como con otras personas de la organización o incluso externas. Es importante poder comunicarse con los demás, transmitir un mensaje, en el momento exacto y utilizar un léxico acorde al destinatario del mensaje. En una situación de crisis, cuando el equipo entra en acción deberá poder informar a superiores con un lenguaje poco técnico y más abstracto, y, al mismo tiempo, interactuar con áreas administradoras de TI siendo específicos en términos técnicos.

Los procesos y procedimientos, desarrollados en la sección anterior, pueden tener un efecto negativo en los niveles de servicio del COS al limitar la capacidad de acción del personal en términos de creatividad. Es decir, procesos y procedimientos maduros pueden tornar burocrática la operación y restringir el accionar del personal, por lo tanto, deben implementarse de forma tal que representen un beneficio en mejora de la calidad y tiempo de respuesta.

Del mismo modo, la tecnología puede tener un efecto negativo en los niveles de servicio del COS tanto por la configuración que se aplique como por el nivel de atención que demande. Por ejemplo, si un SIEM descarta ciertos registros de auditoría o directamente no los recolecta, los analistas no podrán incluir ese aspecto en su análisis. O bien, si, por ejemplo, el COS debe administrar íntegramente las plataformas que opera, deberá en desatender el servicio de respuesta a incidentes para dedicarse a instalar parches de seguridad del sistema operativo.

En conjunto, las personas, los procesos y la tecnología se deberán alinear detrás de la misión que se le asigne al COS y los servicios que de él se demanden. Para ello se le deberán asignar los recursos necesarios para contar con los perfiles de personas necesarios para brindar los servicios de COS y dar soporte tanto a la tecnología como los procesos que se implementen.

Serán distintos los roles y la cantidad de personas que se necesiten si se desean implementar todos los procesos y procedimientos identificados en el apartado anterior o si el COS deberá ser responsable de administrar todos los mecanismos de seguridad de la organización, en contra posición a los roles y cantidad de personas que requeriría la mera administración de un SIEM y la gestión de respuesta a incidentes.

Roles

Los roles que se identifican a continuación según la bibliografía (Cisco Systems, 2015), consolidan las distintas aptitudes que se requieren del personal para dar soporte a los servicios que la organización espera del COS. Estos roles pueden encontrarse en otras áreas de la organización por lo que, en ese caso, el COS puede consumir ese servicio de otra área o bien incorporar los recursos para ser autosuficiente.

Roles de liderazgo pueden encontrarse en posiciones de director o gerente del centro de operaciones de seguridad, como así también en las sub áreas en los roles de jefe de departamento o supervisor. En los distintos niveles jerárquicos, los líderes asumen la responsabilidad de ordenar el equipo de trabajo y canalizar los esfuerzos para alcanzar los objetivos planteados. La estructura, en términos de departamentos y cantidad de posiciones de liderazgo, dependerá de lo que se establezca en cada organización en función del presupuesto, los servicios que se desean brindar, el tamaño de la organización, el modelo operacional y otros factores condicionantes.

Los roles analíticos conforman el núcleo del centro de operaciones de seguridad. De acuerdo con cada nivel, los analistas iniciales, intermedios y avanzados se desenvuelven en distintas tareas y trabajan conjuntamente para combinar conocimientos. Los analistas abarcan todas las áreas de conocimiento del COS, incluyendo gestión de incidentes, vulnerabilidades, monitoreo de seguridad, inteligencia de amenazas, investigación forense, y otras. Cada rama de conocimiento tiene sus particularidades y su profundidad, por lo que es enriquecedor contar con un equipo interdisciplinario y con grados de conocimiento. La diversidad se consolidará como una fortaleza para el COS.

Con foco en el ecosistema tecnológico propio del centro de operaciones de seguridad, las posiciones de ingeniería pueden encontrarse dentro o fuera COS. Según la división de tareas establecida en cada organización, las tareas de ingeniería pueden ser satisfechas por otras áreas dedicadas. Aunque por la especificidad de las herramientas utilizadas en el COS, puede ser el mismo COS quien se encargue de administrarlas. Comúnmente, estas posiciones suelen ser cubiertas por proveedores especializados, ya que as tareas de ingeniería están asociadas más

bien a la puesta en marcha de nuevas soluciones y requieren de conocimientos específicos para integrar y configurar los productos de seguridad en el entorno de TI.

En cambio, los roles operativos se encargan de dar mantenimiento a la tecnología para garantizar la disponibilidad y estabilidad de los servicios del COS. Los operadores trabajan sobre soluciones desplegadas aplicando cambios menores en las configuraciones. Si se necesitara aplicar un cambio mayor, entonces intervendrían nuevamente los ingenieros. Este rol suele ser cubierto por personal de la organización, salvo que los servicios estuvieran subcontratados, caso en el que es responsabilidad del proveedor del servicio. Ocasionalmente puede estar repartido entre áreas de TI y del COS. Por ejemplo, los operadores de TI pueden dar mantenimiento al sistema operativo de igual modo que se realiza con el resto de los servidores, mientras que el COS puede abocarse a dar soporte a las aplicaciones de seguridad.

En función de la estructura, el tamaño, la complejidad y variedad de servicios brindados, el centro de operaciones de seguridad puede tomar gran dimensión y requerir entonces de roles que comúnmente son corporativos pero que por las necesidades puntuales se replicarán dentro del COS. Entre estos roles se pueden encontrar los gestores de proyectos, personal de finanzas, auditoría y cumplimiento, personal abocado al armado de procesos, capacitadores, especialistas en comunicación y gestores de proveedores, entre otros.

Funciones y estructura

Tomando como referencia el modelo propuesto por Cisco (Cisco Systems, 2015) y adaptándolo a la experiencia profesional del maestrando, las funciones de un centro de operaciones de seguridad pueden agruparse de forma general en cuatro ramas, a saber, las operaciones, la ingeniería de servicios, la inteligencia de seguridad y la gestión de soporte.

La función principal es la operación, que en sí misma se identifica por los servicios prestados por el COS, que toman visibilidad a través de la gestión de incidentes y gestión de vulnerabilidades. Estas funciones abarcan el monitoreo, investigación y respuesta a incidentes, como así también el descubrimiento, seguimiento y remediación de vulnerabilidades.

La función de ingeniería de servicios agrupa aquellas tareas de administración y configuración de mecanismos de seguridad que se encuentran implementados en la organización. Estos mecanismos podrían ser sistemas antivirus, antispam, sistemas para la prevención de fuga de información, dispositivos cortafuegos, servidores para el control de la navegación. Del mismo modo, la ingeniería de servicios puede proveer las tareas de administración y configuración de las tecnologías que utiliza el mismo COS en su operación.

La inteligencia en seguridad es una función que actúa como observatorio de amenazas externas, como interfaz con organismos externos para el intercambio de información y así también como un proveedor interno de reportes. Estos reportes combinan información interna y externa que permiten agregar valor en la identificación de brechas de seguridad para luego ser analizadas por el equipo de operaciones.

Por último, se encuentran las funciones de soporte que suelen ser comunes en grandes centros de operaciones de seguridad, que por su tamaño requieren abastecerse de sus propios servicios de soporte, como gestores de proyectos, auditores, gestores financieros o de recursos humanos.

Dependiendo de los servicios, capacidades y funciones, la organización deberá diseñar la estructura organizacional que mejor se adapte a sus necesidades. Un COS pequeño podría iniciar sus actividades gestionando incidentes, vulnerabilidades y con una simple ingeniería se servicios internos (MITRE Corporation, 2014).

A medida que se incorporan funciones y se expanden las capacidades, tal como se expuso en la sección "Evolución de los centros de operaciones de seguridad", se irá adaptando la estructura para agregar analistas, técnicos y líderes que permitan hacer una entrega completa de los servicios y funciones mencionadas anteriormente.

Dependiendo de cada organización, el centro de operaciones de seguridad puede depender de la dirección de tecnologías y sistemas (CTO), de la dirección de seguridad informática (CISO) o de la dirección de información (CIO). Es poco común encontrar al COS dependiendo directamente de la gerencia general (CEO).

Dimensionamiento

Una vez determinada la estructura que dará forma al centro de operaciones de seguridad, es necesario estimar la cantidad de personal necesario para completarla. La estimación es una tarea difícil y que debe contemplar múltiples factores a lo largo del tiempo. En aquellos aspectos que es posible calcular de antemano la carga de trabajo y las horas hombre necesarias, será entonces una tarea más sencilla, pero no será así cuando se trate de tareas de investigación y de las que no se tiene una base de consulta histórica sobre la frecuencia de los sucesos.

Para empezar, se debe definir el horario de servicio y los días en que se prestará el servicio de COS. Los rangos tradicionales son 24x7, es decir, las 24 horas de los 7 días de la semana; o bien, 5x8, cinco días hábiles por semana durante ocho diarias. Este factor debe tenerse en cuenta en clave regional, ya que las horas hábiles variarán en función del huso horario de los distintos países donde se consuman los servicios del centro de operaciones de seguridad.

Dependiendo del país en el que se opere el servicio, entran en consideración las horas hábiles, días de descanso, días feriados o no laborables, licencias por vacaciones o estudio, tasa de ausencias por enfermedad, etc. Del tiempo que quede disponible se debe descontar tiempos de descanso, tiempo de almuerzo, tiempo destinado a tareas administrativas y cualquier otra tarea con el fin de obtener el tiempo real disponible para la operación.

Otro factor importante es la cantidad promedio de eventos a gestionar por intervalos de tiempo, es decir, cuántos eventos deberán ser atendidos por un individuo en un intervalo, como, por ejemplo, 30 minutos. Del mismo modo, resultará útil conocer cuánto tiempo promedio le demanda a un analista tratar un evento. Al ser un promedio, se tiene que considerar que hay alertas de fácil resolución y otras que requieren más esfuerzo.

Se deberá definir cuál es el tiempo en cola que se acepta para que un analista tome una alerta y defina si le da tratamiento de inmediato o si en cambio la deriva a la pila de pendientes. En consecuencia, se debe definir cuál es el tamaño aceptable de la lista de pendientes que se irá acumulando por día, mes, trimestre o año. La gestión de los casos estará atada al nivel de servicio que se desea brindar, el que generalmente es ronda los porcentajes de 90%, 95% o 99%.

Estos parámetros y mediciones pueden encontrarse en bases de información de recursos humanos de la organización, o bien, se puede acudir a datos de referencia en el rubro o en el mercado. Con estos datos será fácil estimar la cantidad de personas necesarias para los servicios que se desean brindar. Esta información será útil como guía para empezar, pero es probable que la estructura y tamaño se deba ir adaptando no sólo en función de los servicios que se brinden, sino que también en función de la curva de experiencia de los equipos de trabajo. En caso de que exista en la organización un centro de monitoreo de redes, denominadas en inglés como *Network Operations Center* (NOC), se dispondrá entonces de una base de datos y experiencia muy valorable y que puede resultar análoga al COS.

Ciertas actividades como investigación forense e investigación de software malicioso serán difíciles de traducir en cantidad de personas necesarias. Del mismo modo, la cantidad de personal necesario para operar y mantener software que todavía no ha sido desplegado en la organización y del que no se tiene conocimiento previo. La organización deberá identificar los distintos proyectos que conformarán el programa, y las fases que conforman los proyectos para poder identificar los perfiles y cantidad de personal que demandará cada etapa.

Aprovisionamiento

Con una estructura definida y habiendo calculado la cantidad de personal necesario para integrarla, se debe definir el método de aprovisionamiento, pudiendo ser interno, externo o subcontratado. La retención del personal toma especial relevancia en el COS ya que es un rubro donde hay alta rotación entre empresas, por la alta demanda de este perfil en el mercado del trabajo. Retener al personal es importante porque los servicios brindados tienden a ser personalizados para cada organización y por lo tanto requiere que le personal conozca a la organización, sus activos críticos y cómo gestionar los eventos interactuando con el resto de las áreas (MITRE Corporation, 2014).

Suele considerarse como una buena estrategia contratar personal inicial, ingenieros y técnicos recién graduados, para luego capacitarlos y que se desarrollen dentro de la organización. Sin embargo, esto resulta una estrategia equivocada ya que el personal generalmente tenderá a abandonar la organización cuando consiga experiencia que sea reconocida en el mercado para una mejor o más interesante posición.

Una estrategia más adecuada es la de realizar búsquedas internas de personal que ya esté trabajando en la organización, que la conoce y que desea un cambio en sus funciones y responsabilidades. Si bien el personal interno que presta servicios en otras áreas como soporte técnico, mesa de ayuda, redes, etc., no esté capacitado en seguridad, es valioso el conocimiento de la organización y las funciones de las áreas, así como también el conocimiento de cómo tratar con el resto de las personas. Además, será posible tener referencias reales de cómo es la personalidad y su dedicación al trabajo.

Otra alternativa, no excluyente e incluso complementaria con la estrategia mencionada en el párrafo anterior, es la de recurrir a consultoras especializadas que pueden proveer perfiles específicos que se requieren para cubrir demandas puntuales o conocimientos carentes en el personal existente. Asimismo, las consultoras podrían proveer de personal en momentos críticos para los que hay mayor demanda y luego liberarlos, sin incurrir en ese entonces de incorporaciones y desvinculaciones.

La desventaja de las consultoras es que el personal no tendrá conocimiento de la organización y que, si bien se puede disponer de individuos, los mismos pueden ser rotados, perdiendo entonces el conocimiento adquirido. En este punto, es importante si está en las posibilidades, requerir contractualmente que se mantengan asignadas a la organización las mismas personas mientras dure el contrato.

La subcontratación es una alternativa más que puede complementarse también con los servicios brindados internamente y suele utilizarse tanto para brindar servicios que requieren

alta capacidad y baja complejidad, como el monitoreo continuo 24 horas los siete días de la semana. Por el contrario, la subcontratación puede ser conveniente para brindar servicios de baja capacidad y alta complejidad, como las investigaciones forenses, el análisis de malware o el soporte puntual de ciertos casos o tecnologías.

Puede resultar útil diferenciar el grado de subcontratación, siendo posible sólo la de provisión de personal, pero con infraestructura propia; o bien, la subcontratación completa del servicio quedando a cargo del proveedor la disponibilidad del personal y la infraestructura necesaria. La subcontratación, además, no agregará valor por sí misma en los casos donde se requiera alto conocimiento de los activos críticos de la organización, de las redes internas o de los sistemas y aplicativos. En esos casos conviene combinar personal interno que actúe de interfaz con el proveedor.

Tecnologías

Los dos pilares desarrollados hasta aquí, los procesos y las personas, serán complementados por la implementación de tecnología específica para los centros de operaciones de seguridad. Esta tecnología será utilizada por las personas para poder llevar a cabo los procesos definidos, actuando por un lado como posibilitadora y por otro lado como facilitadora. Es decir, por un lado, hará posible siquiera que se puedan llevar a cabo ciertos procedimientos, como podría ser la inspección de paquetes en la red. En otras palabras, sin tecnología no sería posible inspeccionar en línea todos los paquetes que fluyen en una red de datos.

Por otro lado, la tecnología actuará como facilitadora para mejorar la operación de los procesos y permitir que las personas puedan dedicarse a la tomar decisiones y agregar valor a partir del análisis de información. Ejemplo de esto podría ser la tecnología SIEM, que procesa diversos datos y expone información a través de tableros, reportes, alertas u otros elementos que facilitan el análisis por parte de las personas. La tecnología forma parte de un círculo virtuoso, ya que un COS no es posible sin ella y a su vez la tecnología optimiza el funcionamiento de este.

Sin adentrarse en esta sección sobre las decisiones de subcontratación, es menester destacar que, al aprovisionarse de servicios brindados por terceros, habrá también decisiones por tomar en términos de tecnología. Si no se subcontrata, entonces la organización deberá adquirir, desplegar y mantener tecnología específica del COS. En cambio, si se subcontrata completamente la provisión de servicios del COS, igualmente habrá tecnología, que se deberá implementar dentro de los perímetros de la organización. Del mismo modo, si dentro de la

estrategia hay está planificada la migración de servicios desde la subcontratación hacia la prestación completamente interna, este camino será de igual forma acompañado por la tecnología.

Redes de datos

Las redes de datos son esenciales para los centros de operaciones de seguridad, por dos motivos. Por un lado, representan el ambiente en el que se despliega un COS, ya que son condición necesaria para la existencia de este. Sin red de datos, no se puede implementar un COS. Por otro lado, representan el objeto de atención de cualquier centro de operaciones de seguridad; es decir, sin red de datos a monitorear, no hay sentido de existencia del COS. Por lo tanto, las redes de datos definen dónde se montará el COS y qué alcance tendrá su servicio.

Las redes de datos se pueden concebir de forma general en tres particiones, a saber, la red interna, la red externa y la red desmilitarizada (DMZ). La red interna tiene un nivel de confianza alto, la red externa tiene un nivel de confianza nulo y la red desmilitarizada tiene un nivel de confianza bajo. La organización tiene control sobre los activos en la red interna y la DMZ, pero no lo tiene sobre los activos de la red externa, por ello el nivel de confianza es bajo sobre los activos que no puede controlar.

La DMZ es un ambiente donde se alojan sistemas de la organización que necesitan ser accedidos por agentes externos, por lo que estará expuesto a agentes externos desconocidos en el espacio cibernético. Sin embargo, es un ambiente controlado y donde se aplican medidas de seguridad, pero se lo considera un ambiente de confianza baja, dado que un atacante podría eventualmente tomar control de esos activos e intentar luego acceder a otros sistemas.

Las redes suelen subdividirse en segmentos de red que sean representativos del subconjunto de activos que alojan y sirven para facilitar las operaciones de los administradores y los controles de seguridad. Una subdivisión clásica puede consistir en definir un segmento de red para cada piso de cada edificio donde la organización opera. O bien, en el caso del centro de cómputos, se puede segmentar la red en función del tipo de ambiente, por ejemplo, la red de desarrollo, la red de prueba, la red de producción.

Las redes privadas virtuales son redes externas o equipos individuales para los que se establece un nivel de confianza superior y que se conectan con la organización a través de mecanismos de seguridad específicos. Estas redes suelen ser útiles para empleados que trabajan de forma remota y necesitan que sus computadoras accedan a servicios que se encuentran en la red interna de la organización. Del mismo modo pueden necesitarse para conectarse de forma

segura con distintas sedes de la organización o con otras organizaciones, como proveedores o clientes.

Al momento de definir el alcance del COS es posible que por restricciones presupuestarias se deban priorizar las áreas de monitoreo y, entonces, se tome la decisión de no prestar ciertos servicios para ambientes de desarrollo o redes de piso de empleados. En cambio, destinar todos los esfuerzos disponibles a brindar servicios de seguridad en redes de producción y sólo los servicios básicos o de menor demanda para los demás segmentos.

Conocer las redes en las que opera el COS y las redes con las que se relaciona la organización es importante para saber qué alcance se le dará al COS y en qué segmento se instalará el centro de operaciones. Por ejemplo, si la organización subcontrata servicios de publicación y almacenamiento en la nube, es necesario definir si esa red será alcanzada por el COS. Por otro lado, si se subcontrata el servicio del COS, es necesario definir el enlace entre la red de datos interna y la red de datos donde se encuentra ubicado el centro de operaciones.

Seguridad de red

La seguridad es un aspecto que se debe implementar en cualquier ambiente donde se despliegue un centro de operaciones de seguridad. En el apartado anterior se han descripto las redes y características que conformaran la red de datos de la organización. Estos segmentos de red se tornan aún más importante cuando se implementan listas de control de accesos (ACL) para restringir o permitir el tráfico y acceso por parte de sistemas y usuarios a determinados recursos. Los cortafuegos o *firewalls* en inglés son los dispositivos encargados de hacer cumplir las políticas definidas por los administradores.

Sin embargo, el control de acceso no se limita a los cortafuegos, sino que se perfecciona con otras herramientas. Para empezar, se deben implementar mecanismos de seguridad física para prevenir el acceso de personas a zonas restringidas. Esto aplica tanto para el ingreso a las instalaciones de la organización, como así también para el ingreso a las zonas específicas donde el COS opera. La seguridad física está relacionada con la infraestructura edilicia, el personal de seguridad y los mecanismos de autenticación que una persona debe accionar para obtener un acceso permitido. Entre estos dispositivos se pueden encontrar molinetes, dispositivos biométricos, tarjetas de acceso, etc. Comúnmente, la seguridad física queda fuera del alcance de los COS tradicionales, aunque sí se consume la información generada por los dispositivos que autentican las personas, ya que puede ser información útil para detectar situaciones de riesgo.

En cuando a la seguridad lógica, profundizando y complementando las funciones de un cortafuego, existen mecanismos que pueden prevenir la conexión de terminales a puertos de red, evitando que los usuarios conecten distintos equipos o múltiples equipos de forma simultánea en las bocas de red dispersas en las instalaciones. Esta protección, conocida como *port security* o seguridad de puertos, puede resultar insuficiente o burocrática según el dinamismo de la organización y teniendo en cuenta las tendencias de BYOD.

Surgen entonces soluciones más avanzadas de autenticación de red que permiten identificar la identidad de la persona y configurar de forma dinámica los accesos para ese usuario según el lugar donde está llevando a cabo el inicio de sesión. Este tipo de soluciones avanzadas se complementan con los cortafuegos ya que pueden identificar quién y desde dónde se conecta y determinar, en función de las políticas definidas, si ese acceso está permitido o no. El protocolo que permite esta operatoria es *802.1X* y puede implementarse por medio de distintos productos disponibles en el mercado.

Un caso de uso podría ejemplificarse como un empleado que intenta acceder a un sistema crítico desde un espacio común del edificio, como la cocina o lugar de almuerzo. El sistema de control de acceso a la red prevendría ese acceso, pero permitirlo si esa misma persona accede al sistema crítico desde una oficina que sí tiene aplicada restricciones de seguridad física. Del mismo modo, podría tomar decisiones en función del dispositivo que utiliza la persona diferenciando si se trata de su teléfono móvil o su estación de trabajo; o bien, en función del horario laboral, evitando el acceso a sistemas críticos en horarios fuera de lo normal.

Un repositorio centralizado de identidades es un factor clave en estos tiempos donde hay diversidad de sistemas aplicativos y de distintos proveedores, en el que cada uno puede manejar su propia base de usuarios y métodos de autenticación. Centralizar las credenciales mediante un sistema de gestión de identidades conectado con el repositorio de recursos humanos evitará la proliferación de credenciales obsoletas o cuya identidad no puede determinarse. Esto sirve también para mantener la trazabilidad de las acciones de los usuarios ya que se podrá identificar quién es la persona que realizó determinada acción.

En las redes de datos se deben desplegar dispositivos y sensores como sistemas de detección de intrusiones, filtros de contenido, detectores de brechas, administrador de aplicaciones, software para la protección contra virus informáticos, que permitan detectar, prevenir o corregir situaciones de seguridad. Estos mecanismos no sólo aplicarán cambios en las redes para contener los incidentes, sino que también reportarán información de valor para al SIEM.

Otro aspecto importante de la seguridad es el cifrado del tráfico. Por un lado, cifrar el tráfico es una herramienta importante para prevenir ataques que vulneren la confidencialidad y que eviten el robo de identidad. Por otro lado, el cifrado del tráfico de red representa un problema para el COS ya que impide analizar el tráfico de red y por lo tanto es un vector de ataque que podría ser aprovechado. Existen mecanismos de seguridad capaces de descifrar el tráfico y enviarlo a los sistemas de detección de intrusiones para que lo inspeccionen y alerten si está fluyendo tráfico malicioso. Por el esfuerzo de procesamiento que requiere esta actividad, es recomendable definir qué tráfico se descifrará, priorizando el descifrado de accesos a los sistemas propios de la organización y los sitios web externos que revistan poca confianza.

Sistemas

Los aplicativos informáticos serán objeto de monitoreo por parte del COS ya que la información que procesan es de valor para la organización y por lo tanto su afectación podría ocasionar un perjuicio para las partes interesadas. El COS puede tener la responsabilidad de aplicar medidas de seguridad en los sistemas, o, en cambio, puede solamente asumir un rol de monitoreo para lo que se debe garantizar la recolección de registros de auditoría que permitan brindar los servicios de seguridad.

En caso de que el COS tome un rol en el que implementa medidas de seguridad, como ser la instalación de actualizaciones de software o la aplicación de configuraciones de seguridad, debe tender a aplicar medidas de seguridad de forma homogénea. Para ello, idealmente es una ventaja disponer de software y hardware del mismo tipo, para evitar la diversidad de productos.

Si se tuviera que afrontar la decisión de seleccionar un sistema operativo, se recomienda elegir un producto estándar de gran distribución y reputación en el mercado, como Microsoft Windows o Apple Mac OS. En cambio, se desaconseja la implementación de sistemas operativos personalizados o desarrollados internamente, salvo en ambientes que tuvieran requerimientos específicos, como podría ser un entorno militar o de alta seguridad.

Es importante que el proveedor de la plataforma priorice la seguridad distribuyendo actualizaciones que permitan corregir vulnerabilidades e introducir nuevas protecciones. Este tipo de software incluye mecanismos de seguridad como antivirus, firewalls y administración centralizada. Por otro lado, los proveedores de soluciones de seguridad más conocidos como Symantec, McAfee, Cisco, Trend y otros, disponen de productos compatibles con ambos sistemas operativos, lo que es un punto a favor para tener flexibilidad al momento de diseñar una arquitectura de seguridad.

El COS debe evaluar y configurar o requerir la configuración de los registros de auditoría en terminales, dispositivos móviles y servidores. Estos registros colectados de forma centralizada le darán visibilidad al centro de operaciones de seguridad para identificar situaciones de riesgo. Si los sistemas son del mismo proveedor o al menos no hay gran diversidad, se facilitará la tarea de configuración e interpretación de los eventos.

Especial atención requerirán los aplicativos informáticos desarrollados por o para la organización, ya que este tipo de sistemas suelen implementarse para dar soporte a la gestión sustantiva de la organización. Por lo tanto, procesarán y almacenarán información crítica para la operación del negocio y esto le dará más relevancia a la aplicación de medidas de seguridad. El análisis de seguridad del código fuente, la revisión de los derechos de accesos, la integración con los sistemas centrales de servicios como los directorios de identidades y el servicio de correo electrónico, son puntos en el que el COS deberá focalizar esfuerzos.

Plataformas de seguridad

A continuación, se presentan las tecnologías principales que se encuentran en un COS y sustentan su operatoria. Subcontratadas o implementadas internamente, es importante contar con ellas para tener visibilidad efectiva y poder operar la seguridad implementando las políticas definidas en la organización.

Sistemas de gestión de eventos e información de seguridad

En el centro neurálgico del COS se encontrará tecnología de gestión y análisis de eventos e información de seguridad, los SIEM. Estos productos se nutren de información provista por otros dispositivos y permiten efectuar análisis mediante técnicas de aprendizaje autómata o análisis de *big data*. En términos de monitoreo, los SIEM agregan valor a las tareas llevadas a cabo por los analistas de seguridad e incluso permiten efectuar ciertos análisis que no serían factibles sin esta tecnología.

Cortafuegos, enrutadores y switches

Los cortafuegos, enrutadores y *switches* son dispositivos tecnológicos necesarios para las operaciones de seguridad. Tanto para implementar políticas de seguridad en términos de filtrado y segmentación, como así también para remitir información al SIEM sobre lo que está sucediendo en la red. Posibilitan la captura de paquetes de red y la aplicación de técnicas de telemetría o transmisión los eventos de interés.

Sistemas de control de acceso a la red

Sistemas de control de acceso a la red y sistemas de directorio permitirán implementar las políticas de seguridad y obtener información sobre los accesos e inicios de sesión la red. Estos eventos serán de utilidad para los casos de uso del SIEM y se podrán tomar medidas preventivas o reactivas sobre los usuarios y los dispositivos; por ejemplo, inhabilitar un usuario para que opere en la red luego de detectarse un comportamiento anómalo.

Servidores de navegación

Los servidores de navegación en internet, conocidos en inglés como *proxy*, toman relevancia en el contexto actual donde los usuarios acceden constantemente a servicios en internet. La navegación por la red de redes es uno de los vectores más frecuentes de infección de software malicioso, como *ransomware*[8]. Asimismo, la organización puede determinar la aplicación de restricciones en el uso como política corporativa, por ejemplo, prohibir el acceso a redes sociales, juegos o bloquear sitios de pornografía. La tecnología habilita este tipo de protección y genera registros de utilidad para los SIEM.

Sistemas de detección de intrusiones

Los sistemas de detección de intrusiones se consolidan como una tecnología necesaria para las operaciones de seguridad. La base de firmas y técnicas de inspección alertarán y remitirán eventos al SIEM y de esta forma, en conjunto con otros eventos e información, el COS podrá detectar situaciones de riesgo o brechas de seguridad. Los sistemas de prevención a su vez pueden ser operados por el COS para evitar ataques en línea, ya que detectan ataques y bloquean tráfico en tiempo real, impidiendo a los atacantes alcanzar el activo objetivo.

Sistemas de protección de correo electrónico

El correo electrónico sigue siendo una herramienta de uso diario por la mayoría de los empleados de la organización y como un medio de comunicación esencial entre la organización y las partes interesadas. Por lo tanto, sigue siendo un medio de interés para los atacantes. La protección contra correos no deseados, sean de tipo publicitarios o maliciosos, es vital para cualquier organización. Tecnología *antispam*, combinada con antivirus, permitirá sanear el correo electrónico y reportar al SIEM posibles ataques de relevancia.

[8] Ransomware: es un tipo de software malicioso que exige al usuario una recompensa para devolverle el acceso a la información secuestrada.

Sistemas de protección de aplicativos webs

Al exponer aplicaciones internas hacia internet, las organizaciones han abierto la puerta a agentes desconocidos. Los cortafuegos de aplicaciones se especializan en sanear el tráfico web que ingresa a las aplicaciones, previniendo que los atacantes aprovechen vulnerabilidades y puedan obtener accesos no autorizados o afectar tanto la integridad como la confidencialidad y la información de la organización. Estos sistemas permitirán filtrar tráfico malicioso y alertar al SIEM sobre situaciones de riesgo.

Servicios de reputación

Los servicios de amenazas o reputación suelen consumirse como suscripción y se encuentran embebidos en los productos que lo requieren. Por ejemplo, un servidor de navegación puede consultar a su proveedor de servicio de reputación si el sitio al que el usuario intenta acceder es de buena o mala reputación. Lo mismo sucede con los sistemas de detección de intrusiones o los productos *antispam*; todos se conectan con una base central que agrega información sobre los orígenes y destino de las comunicaciones.

Sistemas de protección contra software malicioso

Sistemas de protección contra software malicioso, sea antivirus o *antimalware*, es una barrera básica y que aún sigue siendo necesaria implementar tanto en las terminales de los usuarios como en los servidores. Los dispositivos móviles también requieren de este tipo de protección. Un enfoque central y corporativo es necesario para poder detectar y responder a incidentes de seguridad antes de que se afecte la organización completa. El SIEM podrá consumir los registros y alertas de los clientes para destacar situaciones de riesgo.

Sistemas de detección de brechas

Las tecnologías de detección de brechas permiten identificar situaciones de riesgo con un enfoque alternativo. Los tarros de miel o *honeypot* como se conocen en inglés, son trampas que la organización planta de forma premeditada para detectar ataques. Sirven justamente para tentar a los atacantes y poder recabar información de estos. Los areneros o *sandbox* en inglés, permiten emular el comportamiento de una pieza de software en un ambiente aislado y seguro. Así es posible detectar software malicioso para el que aún no hay firmas antivirus en el mercado. El SIEM podrá combinar esta información con el resto de los eventos y detectar de este modo situaciones que hubieran pasado desapercibidas.

Sistemas de prevención de fuga de información

La información es valor y por lo tanto se debe prevenir que la misma sea fugada fuera de los límites de la organización o hacia personas no autorizadas. Los sistemas de prevención de fuga de información analizan el tráfico de red para detectar situaciones representativas de fuga. Al mismo tiempo, permiten llevar registro de las operaciones de los usuarios en un nivel de abstracción que no sería posible para dispositivos de red, como la apertura, modificación, eliminación o impresión de archivos ofimáticos, o el grabado de archivos a dispositivos externos o adjuntarlos a un correo web privado. Los registros serán de utilidad para el SIEM.

Sistemas de descifrado

Tecnología para descifrar tráfico será vital para ganar visibilidad y poder operar en línea. Si bien existen productos individuales que reciben tráfico y los descifran, es común en la actualidad encontrar esta funcionalidad embebida en cada producto que la requiera. Así, los servidores de navegación, los detectores de intrusiones, los sistemas de detección de fuga de información y otros productos que necesitan descifrar tráfico para inspeccionarlo, cuentan con esta funcionalidad embebida y permiten ser selectivos al momento de definir cuáles flujos se descifrarán y cuáles no.

Sistemas de detección de vulnerabilidades

Sistemas de detección de vulnerabilidades son ahora parte de los COS modernos y alcanzan tanto a los dispositivos de red y servidores, como así también a los aplicativos informáticos. Sea de forma periódica o continua, los sistemas escanean los activos de la organización y pueden reportar esta información al SIEM. De este modo, ante una alerta el SIEM podrá priorizarla en caso de que ese activo sea vulnerable y susceptible a cierto ataque. En cambio, puede descartarla si el activo está protegido.

Software y hardware de investigación forense

Software de investigación forense complementado con hardware dedicado, será requerido cuando suceden incidentes de seguridad que requiere análisis profundo sobre lo sucedido. No suele conectarse este software con el SIEM ya que la operatoria es atemporal, fuera de línea y bajo demanda. Es importante disponer de este tipo de software para recabar evidencia y encontrar información que pudo haber sido eliminada.

Planificación y puesta en marcha

Evaluación de capacidades

El punto de partida para gestionar un centro de operaciones de seguridad que requiere mejoras o qué está próximo a construirse, es la evaluación de capacidades de los procesos, las personas y las tecnologías en función de los objetivos a alcanzar. Conocer lo existente, determinar su nivel de madurez y contrastarlo con el estado deseado, permitirá definir la estrategia y confeccionar una hoja de ruta para iniciar el camino.

La evaluación de capacidades suele ser llevada a cabo por consultores externos con experiencia en la materia y que a su vez puedan aportar una visión imparcial sobre la situación con la que se encuentran. Esta tarea se debe realizar aplicando una metodología ordenada, documentada y repetible, que abarque la identificación de objetivos, la recopilación de datos, el análisis y la confección de un informe final.

Al plantearlo como un proceso y no como un simple servicio de única vez, se podrán obtener novedades y actualizar la información recolectada previamente, como así también realizar la evaluación nuevamente luego de cierto tiempo y contrastar los resultados de ambas instancias. Como todo proceso con sus actividades, la evaluación de capacidades inicia identificando los objetivos de la organización y los objetivos de TI. A partir de ello identifica las capacidades que se esperan encontrar en el centro de operaciones de seguridad. Luego se recolectará información de las personas, procesos y tecnologías existentes. Finalmente se analizarán las brechas entre lo que es y lo que debe ser, formalizando los hallazgos en un informe final.

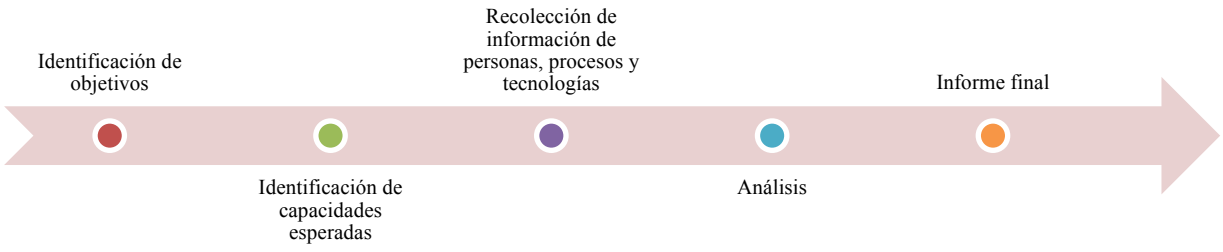

Figura 5. Representación de la metodología de evaluación de capacidades.

Objetivos

El primer paso consiste en identificar los objetivos de gestión de la organización y los objetivos para la tecnología de la información. Este punto es central ya que la madurez de un centro de operaciones de seguridad y la evaluación de su funcionamiento dependerá del alineamiento final que tenga con los objetivos de la organización.

Es posible que no estén definidos los objetivos para la tecnología de la información, por lo que en ese caso se deben identificar personas clave y que tengan interés en la materia para luego obtener sus opiniones y visiones sobre la tecnología. Resulta conveniente incluir a personas de distintos departamentos y rangos jerárquicos. Se podrá recabar información tal como el valor que agregan las tecnologías de la información, si se observan oportunidades en ella, qué tan críticas resultan para la gestión, cómo se gobierna y cómo se toman decisiones.

Utilizando el marco de referencia COBIT[9], se pueden asociar objetivos de las tecnologías de la información con los aspectos de gestión tales como lo financiero, el cliente, cuestiones internas y el crecimiento y aprendizaje. Es común encontrar estos cuatros aspectos cubiertos en los tableros de control corporativos o *balanced scoreboard* según su terminología en inglés, por lo que probablemente ya esté siendo utilizado como una forma de dar seguimiento a los indicadores de gestión.

Finalizada esta etapa, se dispondrá de una lista de objetivos corporativos asociados a los objetivos de tecnologías de la información que le darán sustento. De este mapa de objetivos se podrán identificar los procesos necesarios y los niveles de servicio requeridos que permitan dar cumplimiento a los objetivos de TI y, por lo tanto, a los objetivos corporativos.

Capacidades

El segundo paso consiste en identificar las capacidades requeridas para dar cumplimiento a los objetivos de TI. Como los objetivos se alcanzarán mediante la ejecución de uno o más procesos, se deben listar los procesos involucrados y las capacidades requeridas para que esos procesos se lleven a cabo satisfactoriamente. Identificar el nivel de madurez de los procesos que soportan un objetivo, permitirá saber qué tan efectivo se está siendo en el cumplimiento de los objetivos.

De acuerdo con la tríada de elementos presentada en este trabajo, la evaluación de capacidades debe considerar aspectos sobre los procesos, las personas y la tecnología. Por medio de esta actividad se podrá identificar cuál es el nivel de habilidad o aptitud que se requiere para que los servicios del COS puedan satisfacer los objetivos de TI. Por ejemplo, si un proceso se encuentra documentado y se cuenta con tecnología correcta, la falta de capacitación de las

[9] COBIT (Control Objectives for Information and Related Technologies) se define como Objetivos de Control para Tecnología de Información y Tecnologías relacionadas es un modelo para auditar y controlar la gestión de los sistemas de información y la tecnología.

personas puede provocar que ese proceso no entregue los resultados esperados y por lo tanto que no se alcance el objetivo de TI.

Personas

Las capacidades esperadas de las personas pueden ser evaluadas considerando el modelo de gobierno corporativo, la estructura orgánica, la experiencia y el entrenamiento. En términos de gobierno, es importante identificar el nivel de entendimiento e involucramiento por parte de la Alta Dirección sobre las funciones y servicios que brinda el centro de operaciones. De igual forma, qué nivel de apoyo, seguimiento y atención se le brinda al COS.

La estructura de la organización y la conformación orgánica del COS es otro factor para tener en cuenta. La experiencia de las personas, su capacidad de trabajo en situaciones críticas y de alta presión y su entendimiento de las diversas formaciones que intervienen en la seguridad dará cuenta de personal capacitado para la tarea. Esto puede estar acompañado de la educación formal, cursos de capacitación y certificaciones que ostenten.

Procesos

Los procesos ordenan las actividades y articulan la operación entre las personas y la tecnología. En cuanto a los procesos que lleva a cabo el COS, se debe indagar sobre la existencia de estos, si se encuentran documentados, si la documentación refleja la realidad, si se miden, si se reportan métricas y si se practica la mejora continua. Hay procesos que pueden estar delegados en otras áreas, por lo que es importante considerarlo al momento de establecer cuál es el estado del COS con relación a las cuatro generaciones identificadas en la sección "Evolución de los centros de operaciones de seguridad".

Los procesos principales que se buscará evaluar estarán asociados a la gestión de incidentes y la gestión de vulnerabilidades, sin embargo, como se han identificado en la sección "Procesos", habrá otros que serán de interés para la operación de seguridad. Entre estos procesos de interés se encontrará la gestión de registros de auditoría, la gestión de cambios de la tecnología del COS, la gestión de inteligencia de seguridad, etc.

Los procesos planteados pueden tomarse como referencia y adaptarlos a las necesidades de la organización, removiéndolos, simplificándolos o profundizándolos para conseguir un nivel mayor de especialización.

Tecnología

La tecnología, estrictamente relacionada a los procesos, debe evaluarse si se encuentra implementada, atendida por el personal, con contratos de soporte vigentes. A su vez, es posible identificar tecnologías faltantes que impiden al COS brindar los servicios esperados o con los

niveles deseados por la Alta Dirección. Disponer de un diagrama de arquitectura del COS, o en su defecto, generarlo, es importante para dar visibilidad a este aspecto.

La tecnología por evaluar estará asociada a las redes de datos, la gestión de eventos e información de seguridad, la administración de registros de auditoría, el monitoreo, la detección, el descubrimiento de vulnerabilidades, la gestión y reportes.

Recolección de información

A este punto ya se dispondrá de los objetivos del negocio, su descomposición en objetivos de tecnologías de la información y los procesos de TI que los soportan. Asimismo, se dispondrá de una visión sobre las capacidades necesarias del COS y las capacidades reales que se encuentran implementadas.

La recolección de información es un paso importante para poder confeccionar el informe final. Es aconsejable que quienes realicen el asesoramiento incorporen especialistas en las distintas temáticas que aborda un centro de operaciones de seguridad, esto incluye gestores de proyectos, especialistas en recursos humanos, especialistas en procesos, administradores de tecnologías, desarrolladores, etc. De esta forma, el resultado estará enriquecido y agregará aún más valor, evitando conflictos que se podrían producir por desconocimiento en la temática analizada.

La recopilación de información puede llevarse a cabo en paralelo con la identificación de capacidades del paso anterior, en el que probablemente se realizan entrevistas desde el gerente general hasta técnicos y operadores. Por lo tanto, en este punto ya se dispondrá de información valiosa que será complementada con requerimientos precisos de información.

Entre la documentación complementaria se puede solicitar el inventario de activos, diagramas de red, documentación de seguridad, archivos de configuración, procesos y procedimientos, listas de controles de seguridad implementados, etc. Con esto ya se estará en condiciones de pasar a la siguiente etapa.

Modelos de madurez

En este paso se debe estimar el nivel de efectividad del proceso en relación con los objetivos de TI y del negocio que tiene asociados. Para esto se debe calcular el nivel de madurez de los procesos, promediándolos en caso de que dos procesos de distinto nivel de madurez hagan al mismo objetivo de TI.

Los modelos de madurez según COBIT abarcan seis niveles. El nivel cero representa la inexistencia absoluta de procesos e incluso que la organización no reconoce que hay un problema al respecto. El nivel uno representa que la organización sí reconoce que hay un

problema que requiere resolución, pero los procesos se ejecutan a demanda y la forma de ejecutarlo como así también el resultado, varían caso por caso o persona por persona.

El nivel dos representa una situación donde las personas con mismas responsabilidades llevan a cabo procedimientos similares, sin embargo, el resultado dependerá del nivel de habilitad, experiencia y conocimiento de la persona, lo que provocará que el resultado sea variable. El nivel tres representa una situación donde los procedimientos se han estandarizado, documentado y comunicado. En este nivel la ejecución de los procesos queda a criterio de las personas, por lo que se producen desvíos.

En el nivel cuatro se incorporar la medición del cumplimiento con los procesos y se puede reaccionar ante desvíos. Al mismo tiempo, ya se empiezan a implementar herramientas automáticas, aunque de forma aislada. En el nivel cinco se completan el círculo de mejora continua y los procesos se encuentran optimizados y prácticamente automatizados. La organización adquiere eficiencia, eficacia y flexibilidad.

Informe final

El informe final debe reflejar el estado actual del centro de operaciones de seguridad. Es imperativo que se incluya la relación entre los objetivos de la organización, los objetivos de tecnologías de información, los procesos de TI y su respectivo nivel de madurez. El informe debe invocar la visión y estrategia de la organización y presentar cómo la inclusión de seguridad o la falta de ella pueden afectar a la organización. De esta visión y estrategia organizacional se despenderá la visión y estrategia del departamento de tecnologías de información. La seguridad debe embeberse tanto en este nivel como así también los procesos y procedimientos de TI.

Si se han identificado requerimientos de cumplimiento externo, tanto de normas financieras como regulatorias, se debe incluir un apartado que las identifique y exponga, ya que será un factor decisivo al momento de definir una estrategia. Por otro lado, el riesgo al que se expone la organización conformará un segundo factor de interés que debe explicarse, para que los directivos estén conscientes del escenario y puedan capitalizar la inversión en seguridad como una forma de agregar valor al producto o servicio que ofrecen.

La organización puede haber experimentado incidentes de seguridad en primera persona, por lo que es conveniente mencionarlos y destacar los aspectos de esas situaciones que se verían mejorados en caso de que la organización decidiera avanzar en la implementación o mejora de un centro de operaciones de seguridad. Esto facilitará la necesidad de identificar un patrocinador del programa y su correspondiente asignación presupuestaria.

En el desarrollo del informe se podrán incluir los hallazgos de la evaluación realizada, preferentemente incorporando gráficos, información resumida y bien estructurada que haga fácil su lectura e interpretación. Es recomendable identificar qué aspecto de la tríada de elementos son los que requieren revisión en los temas que se aborden.

Estrategia

Mediante la metodología de evaluación de capacidades del apartado anterior se han identificado los objetivos, el estado actual del COS, el estado deseado y los elementos faltantes o brechas entre ambos extremos. Ahora se debe formalizar una estrategia y para ello es necesario definir aspectos clave que den pautas claras hacia las partes interesadas.

Para que una estrategia tenga el apoyo necesario es importante contar con la intervención del gerente general o del directorio como avales del programa. Se debe tener presente que la implementación de un centro de operaciones de seguridad implicará cambios en las formas de trabajar y acceso a información sensible, por lo que es frecuente encontrar resistencia en las áreas o personas afectadas. Por lo tanto, arquitectos de seguridad, el responsable por la información, el responsable por la seguridad y el sponsor del COS son personas necesarias para esta fase en la que se forjará una estrategia de alto impacto para la organización. Jefes de TI, de las unidades de gestión, finanzas y recursos humanos serán también parte importante de las definiciones que se tomen.

Misión y alcance

En este ámbito se propondrá, adecuará y validará la definición de la misión del COS, alineada naturalmente a la misión de TI y la misión de la organización. En conjunto con la misión se definirá el alcance del COS recordando que, a mayor alcance, mayor será el presupuesto y esfuerzo requerido. Definiciones del alcance incluyen el período en el que se alcanzarán los objetivos del COS, las ubicaciones y redes de datos que estarán bajo su alcance, los sistemas de información cubiertos, el nivel de servicio y horarios.

A continuación, se transcribe una misión y el alcance de un centro de operaciones de seguridad. Como misión ejemplifica "*el COS monitorea la postura de seguridad de las redes, sistemas y aplicaciones operadas por TI, con el objetivo de detectar y reaccionar a incidentes de seguridad que pueden impactar negativamente la operación de la organización.*"

Como alcance ejemplifica "*el COS alcanza todos los sistemas que son administrados y operados por TI, incluyendo aquellos ubicados en oficinas nacionales o internacionales. Los servicios del COS son ofrecidos en todo horario e incluyen la recolección y correlación de eventos de seguridad, el tratamiento de ataques de denegación de servicios, la detección de*

actividades maliciosas internas o externas, la respuesta a incidentes de seguridad informática, la coordinación del equipo de respuesta a incidentes y la concientización cuando sea requerida." (Cisco Systems, 2015).

Servicios

El definir la misión y el alcance, se deben definir los servicios que brindará el COS. Mientras más claros y definidos sean los servicios, menor será la posibilidad de conflicto en puntos grises donde pudiera prestarse a confusión un solapamiento de responsabilidades con otras áreas. Recuérdese que los COS evolucionaron en generaciones y con el correr del tiempo asumen tareas que hasta ese momento estaban asignadas a otras áreas. Por lo tanto, se debe gestionar el cambio organizacional en caso de que haya transferencias de funciones y responsabilidades.

Los servicios principales que brinda un centro de operaciones de seguridad han sido definidos en el apartado "Servicios de valor agregado", por lo que la organización debe definir qué servicio espera del COS siendo consistente con el presupuesto, estructura y experiencia del área. Puede definirse una ampliación de servicios a lo largo del tiempo para acompañar el desarrollo y curva de experiencia del COS.

En caso de que se opte por un modelo de operación subcontratado, se debe acordar el nivel de servicio (SLA) con el proveedor. El documento deberá incluir los criterios de clasificación de criticidad de los casos y los tiempos de respuesta acorde a los niveles de criticidad definidos. Convenios de confidencialidad deben ser firmados entre las organizaciones y por el personal, teniendo en cuenta el nivel de visibilidad y conocimiento de vulnerabilidades de seguridad que puede tener un operador de COS.

Es importante presentar los servicios del centro de operaciones de seguridad como facilitadores y de valor agregado. Para esto se debe poder materializar o hacer visible de qué forma el usuario puede consumir los servicios del COS y de qué forma estos lo ayudan cotidianamente. Por ejemplo, la implementación de un sistema de protección de correo electrónico evita que los usuarios reciban cientos de correos basura que deberían revisar y eliminar personalmente. En cambio, la existencia de un COS y sus servicios de monitoreo mediante procesos, personas y tecnología ahorran tiempo a los usuarios y permiten que dediquen esfuerzo a otras tareas que hagan a los objetivos de la organización. Sólo el 20% de los centros de operaciones de seguridad expresan que reciben actualizaciones anuales por parte de las áreas de negocio para entender y resolver sus inquietudes y riesgos (EY, 2014).

Modelo de operaciones

Al momento de planificar la estrategia para la construcción o mejora de un centro de operaciones de seguridad, se debe evaluar cuál es el modelo de operación que mejor se adapta a las necesidades y posibilidades de la organización. Entre las alternativas de operación se encuentra el despliegue de un COS completamente propio, la subcontratación integral de los servicios, o bien, un esquema híbrido que combine ambos extremos.

Para tomar la decisión de la arquitectura y modelo se deberán tener en cuenta aspectos como los costos de desarrollo, despliegue, mantenimiento, contratación y entrenamiento de procesos, personas y tecnología. No deben considerarse sólo los costos iniciales, sino que todos los costos en que se incurrirán hasta que se alcancen los niveles deseados de servicio. También se debe tener en cuenta si en el mercado hay proveedores que satisfagan las necesidades de la organización. Es posible que existan restricciones legales que impidan la subcontratación de un centro de operaciones de seguridad, por lo que, en tal caso, no sería un camino posible.

Al igual que los costos, alcanzar los niveles deseados de servicios de seguridad implicará identificar, documentar y poner en marcha procesos; contratar, capacitar y mantener personas; adquirir, desplegar y mantener tecnologías. La planificación de un COS debe contemplar este tiempo al momento de elegir el modelo de operaciones.

La operación interna de un COS se caracteriza por ser responsabilidad de la organización le entrega de los servicios. Esto quiere decir que eventualmente se pueden incluir sistemas en la nube o aprovisionarse de personal subcontratado. Sin embargo, será la organización quien tome decisiones y gestione las tecnologías y las personas. Como contrapartida, en el caso de la subcontratación, la organización sólo percibirá los servicios y no podrá, salvo que se establezca en los contratos, incidir en la gestión de la tecnología ni de las personas.

En el caso de la subcontratación de servicios, la organización sí deberá disponer de un equipo interno que haga de interfaz con el o los proveedores, valide los niveles de servicio y haga un seguimiento interno de los reportes que provienen de los proveedores. En este contexto la organización probablemente tenga acceso a un aplicativo donde puede visualizar la información de seguridad y el estado de los casos. De igual modo, este equipo podrá visualizar los casos iniciados por el personal de la organización y que deben ser resueltos por el proveedor.

Las ventajas de un COS interno residen principalmente en disponer de personal dedicado a la seguridad de la organización, el conocimiento del entorno que adquiere el personal al mismo tiempo del conocimiento sobre la estructura orgánica, la propiedad sobre la tecnología y el poder que eso conlleva para la organización para la toma de decisiones. Como

desventaja, un COS interno requiere amplias partidas presupuestarias para su puesta en marcha, necesita mucho esfuerzo en reclutar, entrenar y gestionar al personal, y carece de información de inteligencia de seguridad que en cambio podría tener una empresa subcontratada por el sólo hecho de operar sobre redes de múltiples compañías.

Las ventajas de un COS subcontratado consisten en el bajo costo de entrada para disponer de un alto nivel de servicio, mejor respuesta a incidentes por contar con información de múltiples redes, aportan un punto de vista imparcial por encontrarse fuera del contexto de la organización, pueden ser escalables y flexibles y disponen de personal especializado que de forma individual no sería posible incorporar en funciones de un COS interno. Como contrapartida, las desventajas de un COS externo son principalmente el poco conocimiento sobre la organización, las personas y la dinámica corporativa, la posible distracción por tener que atender distintas cuentas, inconvenientes de confidencialidad por la información que se debe exportar fuera de los límites de la organización y por lo tanto la mayor probabilidad de fuga de información.

Como alternativa a ambos extremos existen los COS híbridos, en los que ciertos aspectos se desarrollan internamente y otros se subcontratan. Es un esquema óptimo cuando se desea construir un COS interno, pero se deciden consumir servicios externos hasta tanto la organización haya podido adquirir la experiencia necesaria para alcanzar los niveles de servicios deseados. Incluso disponiendo de un COS interno, ciertos servicios son económicamente más viables al subcontratarse, tal como el caso de los servicios de protección contra denegaciones distribuidas de servicio. De igual modo, la investigación forense, que es intensiva en conocimientos y requiere software y hardware específico, puede ser cubierta con profesionales externos que sólo se convoquen cuando una situación los requiere.

En el caso que se opte por un esquema híbrido como acompañante y guía en el camino hacia la construcción de un COS interno, es importante incluir en la estrategia esta planificación y determinar los tiempos e hitos que requieren alcanzar para dar por finalizado cierto servicio y que el mismo se empiece a brindar internamente. Estas transiciones deben ser planificadas con anticipación para que el servicio se brinde de forma continua.

Al subcontratar los servicios, es importante que los hallazgos o incidentes que se reporten tengan una baja tasa de falsos positivos. Es común, por la falta de conocimiento de la organización y por falta de acceso interno, que tanto los escaneos de vulnerabilidades como los reportes de incidentes, tengan mayor cantidad de falso positivos si provienen de terceros. Un servicio efectivo para la organización incluirá la depuración de casos con el objetivo de brindar información cierta y precisa sobre lo que esté información.

Hoja de ruta

La estrategia del centro de operaciones debe contener una hoja de ruta que ubique en el tiempo la evolución del COS mediante la incorporación de nuevos servicios, la transición en entre los modelos de operaciones si los hubiera, la implementación de nuevas tecnologías, los cambios en la estructura y todos los elementos que mediante su realización permitan alcanzar la misión definida. Se describen a continuación cuatro tramos estimativos desde la puesta en marcha hasta el funcionamiento pleno (MITRE Corporation, 2014).

Desde la fundación y durante los primeros seis meses, algunas prioridades que se deben contemplar son la obtención de confirmación de las partes interesadas y las autoridades sobre la misión, funciones, responsabilidades, alcance y todo aquello que dé fuerza al cambio que sobrevendrá. Del mismo modo, la formación del equipo humano y su ubicación en un espacio físico integrado, junto con el despliegue de tecnología y la identificación de los procesos críticos serán las tareas prioritarias iniciales. Analizar la organización e incluir todo aquello que ya se encuentre implementado y que a partir del cambio corresponderá al COS, es una alternativa útil para reutilizar lo existente y aprovecharlo en el contexto de seguridad.

En el segundo tramo que toma lugar desde los seis meses hasta el primer año, el COS empezará a operar y brindar servicios. Se debe establecer contacto con otros centros de respuesta a emergencias y centros de operaciones de seguridad para poder recibir información sobre inteligencia de seguridad. Se establecerán los requerimientos de compra de nueva tecnología que aún no se encuentra disponible en la organización y se obtendrá experiencia en la operación y monitoreo de las herramientas existentes. Es momento de iniciar el proceso de reclutamiento en mayor volumen para alcanzar el 50% del personal deseado.

En el tercer tramo que ocurre desde los 12 hasta los 18 meses, ya se dispondrá del lugar físico acorde para la estructura del COS y se estarán haciendo efectivas las contrataciones cursadas anteriormente permitiendo alcanzar ahora el 90% del plantel. Se despliega nueva tecnología, se activan los sensores y los procesos de monitoreo continuo. El área interactúa con jefes y responsables de otras áreas y se hace visible a través de un sitio web interno que le permite interactuar con los usuarios y ofrecer sus servicios.

A partir de los 18 meses el COS debería alcanzar el funcionamiento pleno abarcando todo el alcance que fue establecido en la misión. Es momento, si no hubiera ocurrido con anterioridad y si es un requerimiento de la organización, de brindar servicio durante el día completo. Se debe focalizar en las personas para captar sus necesidades de crecimiento profesional y desarrollo organizacional. Los procesos deberán ser revisados y ya deberían estar en condiciones de alcanzar altos niveles de madurez. Los servicios de monitoreo se pueden

profundizar al mismo tiempo que es posible refinar las técnica de recolección de datos y análisis. El COS debe alcanzar al usuario final por medio de campañas de concientización y también convertirse en productor de información de calidad de inteligencia de seguridad que puede compartir con otras organizaciones.

En caso que el COS sea subcontratado, probablemente desde un inicio la organización tenga acceso a altos niveles de servicio y esto sea alcanzado en un período máximo de un año. Es importante destacar, que, aún siendo los servicios prestados por un externo, será necesaria la aplicación de configuraciones en los dispositivos, sistemas y aplicativos del organismo. Se requerirá configurar reglas de acceso y permisos a los usuarios, por lo que, si bien es más rápido, aún insumirá tiempo alcanzar profundos niveles de visibilidad. En caso que el COS opere de forma híbrida, la hoja de ruta debe contemplar los hitos y puntos temporales en los que se harán las transiciones de operación de los servicios.

6. Conclusiones

Conclusiones generales

Mediante el desarrollo del presente trabajo se han podido alcanzar el objetivo general y los objetivos específicos para confirmar la hipótesis orientativa. Los centros de operaciones de seguridad (COS) representan una solución de gestión a la problemática de la ciberdefensa.

El primer objetivo específico de introducir las operaciones de seguridad, incluyendo los motivos que impulsan la conformación de un COS y los servicios prestados por este, ha sido alcanzado mediante el desarrollo del primer y segundo capítulo. En el primero, denominado "Ciberseguridad", se ha presentado el panorama actual sobre la seguridad en el espacio cibernético, la apertura de las organizaciones a operar en el ciberespacio y los riesgos que esto conlleva. En el segundo capítulo, denominado "Operaciones de seguridad" se ha hecho una introducción a estas operaciones y se han idenfiticado los servicios que esta área de gestión puede ofrecer para la organización.

El segundo objetivo específico que es explicar la tríada de procesos, personas y tecnologías, cuya sinergia e interacción soportan la gestión de un COS, fue alcanzado mediante la descripción y exploración de cada uno de estos elementos, tal como se puede observar en el tercer capítulo denominado "Tríada: procesos, personas y tecnologías". Estos tres elementos conforman un sistema que funciona de forma óptima si se articulan en pos de un objetivo común. Entenderlos permitirá administrarlos eficientemente y vincularlos efectivamente de en función de la misión de la organización.

El tercer objetivo específico que es delinear la estrategia para la conformación de un COS exponiendo los elementos que deben considerarse fue logrado mediante el desarrollo del cuarto capítulo denominado "Planificación y puesta en marcha". Disponer de una metodología para evaluar las capacidades existentes y analizarlas en función de las capacidades deseadas, permitirá delinear una estrategia para planificar la hoja de ruta e iniciar las operaciones.

Fue cumplido el objetivo general del trabajo sobre demostrar que un centro de operaciones de seguridad (COS) es una solución de gestión a la problemática de la ciberdefensa. La tecnología o las personas por sí solas no podrán brindar una solución efectiva. Se requiere gestionar por procesos y siempre alienados a los objetivos de TI (tecnologías de la información) y los objetivos de la organización. La construcción o mejora de un COS requiere de conocimientos de gestión que permitan entender que la misión de un COS está supeditada y tiene que estar a disposición de la misión de la organización y los servicios que esta requiere.

En caso de producirse desalineamiento, se percibirá que el COS no agrega valor, que resulta una traba y que es un gasto sin sentido.

Experiencia profesional

El maestrando ha participado profesionalmente en la conformación de un centro de operaciones de seguridad en un Ministerio de la República Argentina. En ese proceso de construcción pudo visualizar cómo el área de gestión y las funciones distribuidas dentro de la organización han evolucionado de acuerdo con las generaciones que se identificaron en el presente trabajo en la sección "Evolución de los centros de operaciones de seguridad".

Cuando el maestrando tomó funciones en el área, observaba que las tareas de seguridad se encontraban diseminadas entre las áreas que prestaban servicios de soporte de TI. Existía tecnología de seguridad, aunque desatendida y con el solo fin de aplicar medidas básicas y necesarias de seguridad como separar redes, filtrar tráfico mediante cortafuegos, proteger la instalación contra software malicioso en computadoras y filtrar correo no deseado. La respuesta a incidentes era llevada a cabo de forma exclusiva por el área que daba soporte a la TI y había conflictos en el equipo humano por la falta de claridad en las funciones de cada área, que se percibía como un solapamiento de tareas. En esa instancia, existían en el organismo políticas de seguridad de la información, aunque no eran utilizadas con fines prácticos, sino que más bien para cumplir con requerimientos normativos de la Administración Pública Nacional (APN).

La organización creció y demandó más y mejores servicios de TI al mismo tiempo que se incrementaban los conflictos y se hacían visibles falencias en las operaciones de seguridad. Las autoridades decidieron entonces iniciar un proceso de ordenamiento de las operaciones a través de la implementación de procesos. En primer lugar, se confeccionó un proceso de monitoreo de seguridad informática, que delimitaba el alcance del servicio de seguridad, ordenaba las actividades del área encargada de seguridad informática y la interacción con las demás áreas. Tecnológicamente, el monitoreo de registros de auditoría estaba limitado a ciertos repositorios que eran consultados sólo ante la necesidad de responder a incidentes y el monitoreo de vulnerabilidades se realizaba de forma manual utilizando principalmente aplicativos ofimáticos tales como Microsoft Excel o Word.

Este proceso de monitoreo marcó el rumbo y orientó los esfuerzos del área satisfactoriamente. Con el tiempo evolucionó y, gracias a la intervención de consultores especializados, devino en dos procesos independientes pero interrelacionados entre sí, a saber,

el proceso de gestión de vulnerabilidades y el proceso de gestión de respuesta a incidentes de seguridad. De esta forma, el área de seguridad asumió las funciones principales de operación de seguridad compatibles con un COS de tercera generación, que antes se encontraban delegadas en otras áreas.

El maestrando identifica la importancia de disponer no sólo de procesos consensuados entre las áreas, sino que también la importancia de que la organización contara con un marco de gestión de la calidad, que establecía la cadena de valor normativa. Así, de las políticas se desprenden reglas de gestión que son implementadas por procesos, procedimientos e instructivos técnicos. Cada instrumento requiere determinado nivel de aprobación, lo que permite ejercer autoridad ante la resistencia al cambio, situación que toma especial relevancia en la APN.

Fruto de la necesidad de contar con soluciones robustas que soporten la ejecución de los procesos y teniendo en cuenta el volumen de datos administrados, se hizo necesaria la incorporación de tecnología específica. Para la gestión de vulnerabilidades, el propio personal del área de seguridad informática desarrolló un sistema informático que le permitiera dar seguimiento a las vulnerabilidades descubiertas en la organización, en función de la ejecución de los procedimientos planificados en un cronograma anual. Por otro lado, la organización logró adquirir y desplegar un sistema de gestión de eventos e información de seguridad (SIEM), junto con la inclusión de servicios de reputación que permiten disponer de información de inteligencia de seguridad.

Es importante destacar que, en esta organización, el área de seguridad informática no administra ni configura mecanismos de seguridad, sino que realiza tareas de monitoreo mediante la lectura de configuraciones, la inspección del tráfico y la interpretación y análisis de los registros de auditoría, para luego producir reportes de incidentes o de vulnerabilidades. Este enfoque de limitar las funciones del COS a la lectura, simulando una auditoría en tiempo real, fue el adecuado para esta organización en determinado contexto. Si bien ha permitido alcanzar logros destacables, muestra por otro lado falencias que yacen en la falta de división de ciertas tareas y funciones entre las áreas administradoras de TI y el área de seguridad informática.

La gestión por procesos y la inclusión de tecnología para sustentar los procesos, permitieron alcanzar un COS de cuarta generación y fueron posibles porque las autoridades tomaron conciencia de la importancia de incluir la seguridad como aspecto de la calidad y, también, porque asumieron el desafío de impulsar un cambio organizacional en lo que refiere a las operaciones de seguridad. Esto habilitó que se implementen cambios en la estructura

orgánica y que se asigne presupuesto para hacer frente a la incorporación de tecnología, contratación de personas y capacitación del personal. Los recursos se orientaron a la construcción de un COS interno, pero contemplando el acompañamiento por parte de proveedores y consultores de forma tal que se logren desarrollar las capacidades propias y que en el tiempo se pudieran prescindir de servicios de terceros, para evitar la dependencia de agentes externos en estas tareas.

En cuanto a tecnología, la implementación de un SIEM (sistema de gestión de eventos e información de seguridad) fue un punto de inflexión que otorgó visibilidad al COS sobre la red de datos del organismo, los sistemas y los usuarios, y permitió ofrecer servicios de seguridad de alto valor para la organización. Al mismo tiempo se incorporó tecnología para automatizar el descubrimiento y gestión de vulnerabilidades en el código fuente de aplicaciones y también, tecnología para dar seguimiento a todas las vulnerabilidades, sean estas de código fuente, de dispositivos de red, de sistemas operativos o vulnerabilidades técnicas o administrativas.

El equipo humano se mantuvo estable y reducido por cuestiones particulares del tipo de organización lo que constituye un factor restrictivo para continuar con el desarrollo en calidad y cantidad de los servicios del COS. Esta limitante debió ser morigerada reduciendo los servicios prestados, priorizando los requerimientos, aumentando la lista de pendientes y reforzando la automatización de procesos y procedimientos como una alternativa para continuar dando servicios.

Como reflexión del maestrando, su experiencia en retrospectiva de ocho años de labor profesional, valida la importancia de contar con el apoyo de las autoridades para implementar cambios y utilizar la gestión por procesos como un instrumento para ordenar y dar calidad a la entrega de servicios, manteniendo alineadas las actividades del área con los objetivos de la organización. Asimismo, para evolucionar en generaciones de los COS, resultó imprescindible articular los procesos, las personas y la tecnología manteniendo el equilibrio entre los tres elementos, por lo que es esencial contar con una visión estratégica de la gestión de los recursos.

7. Bibliografía

Cisco Systems. (2015). *Security Operations Center. Building, Operating, and Mantaining Your SOC.* Indianapolis, Indiana, Estados Unidos: Cisco Press.

Comisión Europea. (5 de Julio de 2016). *The Directive on security of network and information systems*. Recuperado el Julio 18 de 2017, de ec.europa.eu: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

El Cronista. (28 de Junio de 2017). *Ciberataque afecta al negocio inmobiliario del BNP Paribas*. Recuperado el 5 de Julio de 2017, de cronista.com: https://www.cronista.com/finanzasmercados/Ciberataque-afecta-al-negocio-inmobiliario-del-BNP-Paribas-20170628-0074.html

El País. (28 de Junio de 2017). *Ransomware: Algunas empresas ceden y pagan a los 'hackers' para liberarse del ciberataque*. Recuperado el 5 de Julio de 2017, de elpais.com: https://internacional.elpais.com/internacional/2017/06/28/actualidad/1498649539_960151.html

Electric Power Research Institute. (2013). *Guidelines for Planning an Integrated Security Operations Center.* Recuperado el 1 de Septiembre de 2016, de Metering.com: https://www.metering.com/wp-content/uploads/2014/02/EPRI-Planning-ISOC-report.pdf

EY. (Octubre de 2014). *Security Operations Centers - helping you get ahead of cybercrime*. Obtenido de Security Operations Centers - helping you get ahead of cybercrime: http://www.ey.com/Publication/vwLUAssets/EY-security-operations-centers-helping-you-get-ahead-of-cybercrime/$FILE/EY-security-operations-centers-helping-you-get-ahead-of-cybercrime.pdf

HP Enterprise. (Noviembre de 2015). *Growing the security analyst. Hiring, training, and retention.* Recuperado el 1 de Septiembre de 2016, de HP.com: https://www.hpe.com/h20195/v2/getpdf.aspx/4AA5-3982ENN.pdf?ver=1.0

IBM Corporation. (Diciembre de 2013). *Strategy considerations for building a security operations center.* Obtenido de IBM Global Technology Services: https://www-356.ibm.com/partnerworld/wps/servlet/download/DownloadServlet?id=OULVYbVhue7iPCA$cnt&attachmentName=SEW03033USEN_02.pdf&token=MTUxMzEwMzA2NjQwMg==&locale=en_ALL_ZZ

International Organization for Standardization. (2012). *ISO/IEC 27032:2012 - Guidelines for cybersecurity.* Geneva: International Organization for Standardization.

International Organization for Standardization. (2013). *ISO/IEC 27002:2013 Code of practice for information security controls.* Ginebra, Suiza: ISO.

ISAO SO. (s.f.). *Info Sharing Groups*. Recuperado el 18 de Julio de 2017, de ISAO.org: https://www.isao.org/information-sharing-groups/

McAfee. (2013). *Creating and Mantaining a SOC. The details behind successful security operations centers.* Obtenido de McAfee.com: http://www.mcafee.com/de/resources/white-papers/foundstone/wp-creating-maintaining-soc.pdf

McKinsey. (Junio de 2011). *Meeting the cybersecurity challenge*. Obtenido de Digital McKinsey: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/meeting-the-cybersecurity-challenge

Microsoft. (28 de Marzo de 2003). *What is SNMP?* Recuperado el 27 de Agosto de 2017, de TechNet: https://technet.microsoft.com/en-us/library/cc776379(v=ws.10).aspx

Microsoft. (12 de Mayo de 2017). *Customer Guidance for WannaCrypt attacks*. Recuperado el 9 de Julio de 2017, de Microsoft TechNet: https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

MITRE Corporation. (2014). *Ten strategies of a world-class Cybersecurity Operations Center.* Estados Unidos: MITRE Corporate.

National Institute of Standards and Technology. (1 de Mayo de 2013). *Glossary of Key Information Security Terms.* Recuperado el 9 de Julio de 2017, de NIST.GOV: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

National Institute of Standards and Technology. (Julio de 2013). *Guide to Enterprise Patch Management Technologies.* Recuperado el 28 de Agosto de 2017, de NIST Special Publication: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

Oficina Nacional de Tecnologías de la Información. (8 de Agosto de 2013). *Disposición 2/2013: ICIC - CERT*. Recuperado el 18 de Julio de 2017, de InfoLEG: http://servicios.infoleg.gob.ar/infolegInternet/anexos/215000-219999/219212/norma.htm

Oficina Nacional de Tecnologías de la Información. (19 de Febrero de 2015). *Disposición 1/2015: Política de Seguridad de la Información Modelo*. Recuperado el 1 de Septiembre de 2016, de InfoLEG:

http://servicios.infoleg.gob.ar/infolegInternet/anexos/240000-244999/242859/norma.htm

Poder Ejecutivo Nacional. (27 de Abril de 2005). *Plan Nacional de Gobierno Electrónico y Planes Sectoriales de Gobierno Electrónico*. Recuperado el 1 de Septiembre de 2016, de InfoLEG: http://servicios.infoleg.gob.ar/infolegInternet/anexos/105000-109999/105829/norma.htm

PwC. (2017). *Key findings from the Global State of Information Security® Survey 2017*. Recuperado el 9 de Julio de 2017, de PwC.com: https://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

SANS Institute. (Mayo de 2015). *Building a World-Class Security Operations Center: A Roadmap.* Recuperado el 1 de Septiembre de 2016, de SANS Institute Reading Room: https://www.sans.org/reading-room/whitepapers/analyst/building-world-class-security-operations-center-roadmap-35907

Segu-Info. (27 de Junio de 2017). *Ransomware PetrWrap/Petya paraliza decenas de empresas (Actualizado)*. Recuperado el 5 de Julio de 2017, de Segu-Info: http://blog.segu-info.com.ar/2017/06/ransomware-petrwrappetya-paraliza.html

Tenable. (2017). *2017 Global Cybersecurity Assurance Report Card.* Recuperado el 9 de Julio de 2017, de Tenable.com: https://www.tenable.com/lp/2017-global-cybersecurity-assurance-report-card/

The New York Times. (29 de Mayo de 2009). *Text: Obama's Remarks on Cyber-Security*. Obtenido de NYTimes.com: http://www.nytimes.com/2009/05/29/us/politics/29obama.text.html?mcubz=2

The White House. (13 de Febrero de 2015). *Executive Order -- Promoting Private Sector Cybersecurity Information Sharing.* (O. o. Secretary, Ed.) Recuperado el 18 de Julio de 2017, de The White House - President Barack Obama: https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

Wikipedia. (3 de Enero de 2006). *ILOVEYOU*. Recuperado el 9 de Julio de 2017, de Wikipedia.org: https://en.wikipedia.org/wiki/ILOVEYOU

Wikipedia. (29 de Junio de 2006). *Syslog*. Recuperado el 27 de Agosto de 2017, de Wikipedia: https://en.wikipedia.org/wiki/Syslog

Wikipedia. (18 de Abril de 2011). *Big Data*. Recuperado el 29 de Agosto de 2017, de Wikipedia.org: https://en.wikipedia.org/wiki/Big_data

Wikipedia. (12 de Mayo de 2017). *WannaCry ransomware attack*. Recuperado el 5 de Julio de 2017, de Wikipedia.org: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack