UNIVERSIDAD IBEROAMERICANA

Estudios con Reconocimiento de Validez Oficial por Decreto Presidencial del 3 de abril de 1981

Diseño de modelos de priorización y clasificación de incidentes de seguridad para el SOC de Sm4rt.

ESTUDIO DE CASO

Que para obtener el grado de

MAESTRO EN GESTIÓN DE LA INNOVACIÓN TECNOLÓGICA

Presenta

Oscar Alexandre García Fonseca

Director: Dr. Gerardo R. Herrera Villanueva
Lectores: Dra. Alejandra Herrera Mendoza
Mtro. Edgar Ortiz Loyola Rivera Melo

Ciudad de México 2019

Dedicatorias.

A mi padre y a mi madre.
Por estar en el camino por ser el impulso a la perseverancia y enseñarme que todos se puede.

A mis amigos.
Alejandro, Ing. Mingram (+), Eder, Gustavo, Martha, Darío y Mariana.
La amistad a la larga se hace presentes en los frutos.
Gracias totales por los ejemplos, por crecer juntos, siempre presentes.

A Valeria y Ximena.
A ustedes que las amo con mi corazón que son la motivación de cada día, sus gritos, sus risas, su amor me mantiene vivo... gracias niñas.

Gracias a todos por las risas de los buenos momentos, por los abrazos de los momentos no tan buenos... en los que siempre me han acompañado.

Con cariño... Oscar Alexandre !!!

Índice

Resumen

Con el crecimiento acelerado de los servicios de seguridad de la información del SOC de Sm4rt Security Services (Sm4rt), los modelos de operación altamente contextualizados y personalizados establecen limitaciones y problemáticas que evitan la optimización de tiempos y personal. Este proyecto tiene el objetivo de diseñar un modelo de priorización y clasificación de incidentes que permita reducir tiempos y aumentar la capacidad operativa del personal.

Para diseñar estos modelos se realizó una investigación acerca de los modelos propuestos por distintas organizaciones reconocidas globalmente en la materia y sobre el estado actual de la seguridad de la información tanto en México como en el mundo. Para la elección del modelo más apropiado se efectuó una evaluación cuantitativa de cada modelo basada en 4 aspectos generales: utilidad del uso del modelo, optimización de los procesos actuales de análisis y notificación, factibilidad de adaptación y adopción del modelo y el grado de diferenciación competitiva que su implementación aporta al servicio. Para cada uno de los modelos identificados se definieron y ponderaron aspectos específicos que al ser evaluados permitieron comparar y seleccionar un modelo tanto para la priorización como para la clasificación de incidentes de seguridad. Los modelos seccionados luego fueron adaptados al contexto de México y la operación de Sm4rt con base en la investigación y experiencia operativa del SOC de Sm4rt.

Al finalizar el proyecto se diseñaron 2 modelos basados en las propuestas de organizaciones reconocidas a nivel mundial que se complementan entre si y que permiten optimizar el tiempo de análisis y notificación de incidentes de seguridad de la información en el SOC, al mismo tiempo que se reduce la cantidad de contexto de la operación del cliente que debe de tener el personal del SOC para estas actividades. Adicionalmente, este proyecto también permitió identificar un grupo de prerrequisitos de recopilación de información y procesos complementarios con los que se puede garantizar una mayor probabilidad de éxito y un seguimiento continuo de los modelos.

Con este proyecto se concluyó también que esta innovación en el proceso de análisis y notificación del SOC brinda beneficios potenciales al uso de economías de escala que permitan dar servicio a más clientes sin requerir seguir aumentado significativamente la cantidad de personal a través de la optimización de sus procesos y criterios de priorización y clasificación.

Capítulo 1. Introducción

Sm4rt es una empresa mexicana altamente especializada en servicios de Seguridad Informática con 12 años de experiencia en el mercado, dedicada a servicios de diagnóstico, consultoría de seguridad informática y protección de ciberseguridad. Los servicios de ciberseguridad de Sm4rt son provistos principalmente por el Centro de Operaciones de Seguridad (SOC "Security Operations Center" por sus siglas en inglés).

El SOC de Sm4rt funciona como un Proveedor de Servicios de Seguridad Administrada (MSSP "Managed Security Services Provider") lo cual implica que los servicios de Monitoreo de Seguridad y Gestión de Infraestructura son provistos por un grupo de especialistas de seguridad informática que de forma compartida dan servicio a varios clientes.

El servicio de Monitoreo de Seguridad puede definirse como la tarea ininterrumpida de analizar los eventos de seguridad, potencialmente maliciosos, que son identificados de forma automática por las tecnologías de seguridad implementadas en la infraestructura de un cliente. Estas tecnologías pueden ser tan variadas como: Firewalls, Sistemas de Prevención de Intrusos (IPS "intrusion Prevention System"), Antivirus, Anti Spam, Filtrado de Contenido Web ("WebFilters"), Sistemas de Correlación de Eventos (SIEM "Security Information and Event Management"), Sistemas de Prevención de Fuga de Información (DLP "Data Loss Prevention"), etc.

Dichas tecnologías, dependiendo de cada cliente, pueden estar presentes múltiples veces en la arquitectura y ser provistas por hasta 15 fabricantes diferentes, lo cual implica que los analistas de monitoreo deben de tener conocimientos suficientes para operar entre 20 y 30 tecnologías diferentes para dar servicio a los clientes a los cuales están asignados. Adicionalmente a esta complejidad se agrega que cada arquitectura de red de cada cliente puede ser completamente distinta y dependiendo de la posición dentro de la red donde la tecnología de seguridad esté implementada, entonces los eventos de seguridad potencialmente maliciosos que pueden ser identificados automáticamente pueden tener diferente interpretación, criticidad e impactos para la seguridad de la información del cliente.

A partir de la adquisición de sm4rt por parte de Grupo KIO a finales de 2013, y hasta finales de 2015 el crecimiento de la compañía ha sido exponencial, las ventas netas anuales en tan solo 3 años crecieron en 1000%, la cantidad de clientes se incrementó en más del 1500%, el número total de colaboradores de la empresa creció 500% y solo en el área del SOC el incremento de personal ha sido de alrededor del 800%.[1]

1.1 Problemática

Los modelos de operación, de procesos y la metodología diseñados en un inicio para entregar los servicios del SOC están basados en 2 premisas: atención al detalle y una contextualización profunda de los clientes, esto con el objetivo de personalizar los servicios y entregar el mayor valor posible a la seguridad del cliente. Sin embargo, este modelo resulta poco escalable cuando se aumenta la cantidad de clientes asignados a un analista pues siguiendo este proceso puede llegar a tomarle entre 30 y 120 minutos el realizar al análisis necesario para identificar si un evento es realmente un incidente de seguridad, clasificarlo y notificarlo al cliente.

[1] Documentación interna de Sm4rt Security Services.

Esta demora en la capacidad de análisis en ocasiones deriva en la infracción de los niveles de servicio pactados con el cliente para la notificación de incidentes de seguridad, y eso repercute directamente en la facturación de la empresa pues implica la aplicación de deductivas económicas en el contrato de servicio, por lo que este proyecto directamente beneficia al negocio de la empresa disminuyendo la probabilidad de incumplimientos que deriven en deductivas económicas.

Dado el ritmo de crecimiento de la operación, en cuanto al número de clientes a los que el SOC da servicio en la actualidad, el reducir el tiempo de análisis y la dependencia de una contextualización profunda se vuelven asuntos clave en la eficiencia operativa. Mientras un analista pueda analizar un evento siguiendo un conjunto de criterios estandarizados, repetibles y basados menos en contexto para lograr identificar más rápidamente un incidente de seguridad, y posterior a esto pueda categorizar e identificar la prioridad o criticidad del incidente para que tanto el cliente como el mismo equipo SOC puedan priorizar la atención de dicho incidente de forma adecuada.

En la primera mitad del año 2015 fue aprobado por la Dirección General un presupuesto de más de $200,000 dólares para un proyecto[2] de implementación de una solución de software Sistema de Gobierno, Gestión de Riesgos y Cumplimiento (GRC "Governance Risk Management and Compliance System" por sus siglas en inglés) en el SOC. Este software habilitaría automáticamente una capa de contextualización para identificar la gravedad de un incidente de seguridad con base en los activos de TI afectados de cada cliente. El objetivo de este software era reducir la dependencia de contexto de los analistas durante el análisis de un evento de seguridad. Para la implementación de este software se contrataron horas de consultoría de una empresa especializada de nombre internacional para la definición de procedimientos y de todos los insumos de información necesarios para que este software fuera funcional para la operación del SOC. 4 meses después del inicio de este proyecto se completó la instalación del mismo, sin embargo, los insumos de información que se requerían por cada cliente eran extensos y no se contaba con información detallada de los clientes que permitiera configuración de solución de forma adecuada para entregar resultados de utilidad a la operación. Se identificó además que se requeriría de un grupo de personas dedicadas a mantener al día las configuraciones de las herramientas pues no todos los clientes de forma periódica nos comunican los cambios que hacen en sus arquitecturas o los ingresos y egresos de equipos, sistemas, aplicaciones, bases de datos, aplicaciones, etc. Por lo que esta tarea tendría que ser realizada de forma un tanto artesanal y dependía de la retroalimentación que los clientes estuvieran dispuestos a comunicarnos. Debido a lo anterior el proyecto fue postergado

Debido a la relevancia de los clientes que actualmente tiene servicios contratados con el SOC, se hace indispensable que la metodología esté basada y referenciada a alguna norma internacional o mejores prácticas globales, por lo que esta metodología y procesos deberán estar alineados a estándares, sin embargo, se deberá realizar una tarea de personalización al contexto mexicano y del tipo y sectores de la industria de los clientes de Sm4rt.

El tener un proceso y criterios estandarizados para estas actividades del SOC permiten también realizar mediciones de la eficiencia operativa desde diferentes perspectivas que habiliten la toma de decisiones por parte de la gerencia y dirección. Estas mediciones pueden estar ligadas a los tiempos de análisis y notificación por cliente, por analista, etc. que permitan continuamente hacer

[2] Documentación interna de Sm4rt Security Services.

más eficiente el proceso y poder obtener gradualmente una capacidad operativa mayor sin incrementar sustancialmente la plantilla de analistas en el SOC.

1.2 Objetivos

- Diseñar un modelo para la priorización (“triage”) y clasificación de incidentes de seguridad que permita la disminución de los tiempos de notificación y análisis. Este modelo debe de estar basado en estándares internacionales y su implementación debe habilitar la generación de estadísticos útiles tanto para el cliente como para el Sm4rt.

1.3 Antecedentes de la compañía[3]

1.3.1 Origen de la compañía

Sm4rt Security Services fue fundada en 2003 por un grupo de expertos en tecnología como respuesta a la necesidad de garantizar la seguridad de la información y retomar la gestión de riesgos de los clientes de los socios fundadores.

El fundador de la sm4rt, a finales de 2003 con deseo de emprender y obtener éxito no alcanzado en sus emprendimientos anteriores, reunió a un pequeño grupo de amigos quienes contaban con amplios conocimientos y experiencia en tecnologías de la información (principalmente en temas de seguridad de la información); y fue de esa manera que Sm4rt inició operaciones con el servicio de pruebas de penetración (también conocido como “hackeo” ético o “PenTest”)

En sus inicios Sm4rt estuvo enfocada a empresas de tamaño grande, manteniendo una cartera reducida de clientes debido a la complejidad de los proyectos y al poco número de expertos en la materia disponibles para ejecutarlos.

Como muchas de las empresas de servicios de tecnologías nacientes, su creación y desarrollo fue impulsado por un grupo pequeño de proyectos que poco a poco fueron creciendo y requiriendo de mayor formalidad y recursos responsables de la entrega de los mismos.

El ritmo de crecimiento en la demanda de servicios Sm4rt y sus resultados con los clientes poco a poco la fueron posicionando como una de las principales empresas de servicios de seguridad de la información en el mercado mexicano, reconocida por ofrecer servicios innovadores.

1.3.2 El entorno de Sm4rt

Entre los años 2003 y 2006 la demanda de los servicios de seguridad de la información era limitada, durante este tiempo el fundador de Sm4rt aprovechó los primeros años de la empresa para crear una cultura de seguridad de la información entre las empresas del mercado objetivo de Sm4rt, para esto participó en diferentes foros, dando platicas acerca de seguridad informática y los impactos que causaban en las empresas no tenerla, debido a la exponenciación del uso y la importancia de las tecnologías de la información.

Las reacciones del mercado hacia la seguridad informática eran positivas y existía un gran interés por saber más acerca de este tema tan novedoso; con base en lo anterior, en 2006,

[3] Documentación interna de Sm4rt Security Services

Sm4rt organizó el evento denominado “WebSec”, uno de los primeros que dedicaban un día para hablar temas de seguridad de la información en México. En este evento, Sm4rt hizo participes tanto expertos de diferentes partes del mundo, como a jóvenes universitarios interesados en el tema y que ayudaron con la organización del evento.

Posterior a estos esfuerzos la empresa comenzó a crecer rápidamente, por lo que en 2006 y 2007 el fundador definió una estructura organizacional más compleja, estableciendo dos áreas principales, la primera comercial (ventas) y la segunda consultoría y fue el periodo en el que se incorporaron 3 socios más.

1.3.3 Los servicios

Sm4rt, desde un inicio, ha sido una empresa dinámica, y adaptable a las necesidades de los clientes, por lo que siempre ha tenido una amplia oferta servicios que pueden ser enmarcadas en las siguientes categorías.

Servicios de diagnóstico y cumplimiento

- Pruebas de Penetración. También conocidas con “PenTest” o “Hackeo” ético (“Ethical hacking”), la cual consiste en emular las actividades realizadas por un grupo de atacantes o “hackers”, cuyo objetivo es vulnerar la seguridad de los clientes para obtener control o acceso a información privilegiada o a activos críticos en su organización. Este servicio fue el servicio principal en los primeros años de Sm4rt, ya que era atractivo para los clientes. A pesar de esto, este servicio por si solo representaba ciertos inconvenientes para los clientes pues solo identificaba las deficiencias en la seguridad, pero sin las acciones necesarias para remediarlas, cosa que debían de realizar el cliente mismo. Por otro lado, muchas de estas acciones no eran realizadas debido a que el personal del cliente desconocía las técnicas y metodologías necesarias, o incluso no había un responsable que se hiciera cargo de la gestión de las vulnerabilidades identificadas.
- Cumplimiento de Seguridad de la Información. Estos servicios tienen la finalidad de definir o implementar los controles de seguridad requeridos por los clientes para su cumplimiento con estándares o normativas nacionales o internacionales. Estos servicios surgieron como respuesta a las deficiencias de las pruebas de penetración, ya que en estos servicios si se tiene como alcance el acompañamiento a los clientes para identificar riesgos y habilitar en el cliente lo necesario para minimizarlos.
- Consultoría especializada. En esta categoría entra cualquier servicio con alcance específico definido por el cliente, que pueden ir desde la definición de políticas hasta la gestión completa de sus riesgos, la definición técnica de controles de seguridad compensatorios, el diseño de herramientas de gestión, adaptaciones metodológicas, etc. Con el fin de solventar las necesidades específicas de los clientes principalmente en personal capacitado o experiencia en la materia.

Gestión de riesgos. Estos servicios surgen por la necesidad de los clientes de tener más ayuda en la identificación de riesgos y en la implementación de controles que pudieran adaptarse específicamente a sus requerimientos.

- Oficial de Seguridad o Gestor de Seguridad de la Cuenta (SAM). El objetivo de este servicio es proveer de personal especialista en seguridad de la información en las instalaciones de los clientes, con el fin de incorporar mejores prácticas y proyectos internos estratégicos orientados al elevar el nivel de seguridad de la organización no solo en términos de activos informáticos sino también de cultura organizacional y soporte a usuarios internos. Esta figura permite a los clientes traducir los hallazgos de otros servicios de diagnóstico a el contexto específico de la organización, además de identificar la manera más apropiada para la organización de definir sus planes de cumplimiento, regulaciones, y de cómo empatar todo esto con la estrategia organizacional.

Servicios administrados de protección de ciberseguridad. Para atender las necesidades cada vez más complejas de los clientes en cuestión de seguridad de la información, se requirió de la incorporación de tecnologías altamente sofisticadas en la identificación y análisis de vulnerabilidades y amenazas informáticas.

- Administración de vulnerabilidades. Este servicio consiste en la implementación de tecnología que de forma programada y periódica ejecuta escaneos de vulnerabilidades para identificar brechas de seguridad que afecten a los principales activos de tecnología de los clientes. Con este servicio de forma sistemática se tiene un seguimiento a la aparición y mitigación de vulnerabilidades en las organizaciones.

- Administración de tecnologías de información. Este servicio aporta el conocimiento técnico especialista de los ingenieros de SOC (Centro de Operaciones de Seguridad) para la gestión de los cambios en los dispositivos de seguridad implementados en la infraestructura del cliente. Esto permite a los clientes tener a su disposición personal 7x24 para la administración de sus dispositivos y la gestión de incidentes o fallas de su operación. Con lo cual los clientes pueden tener capas de protección de una forma sencilla sin la necesidad de contratar o formar técnicos especialistas.

- Monitoreo de seguridad. Este servicio surge por la necesidad de identificar oportunamente los ciberataques que continuamente son lanzados a los clientes por parte de grupos criminales alrededor del mundo. Este servicio permite a los clientes tener personal 7x24x365 especialistas en la detección y análisis de incidentes de seguridad para ejecutar las medidas de contención necesarias para bloquear o minimizar la afectación a la integridad, confidencialidad o disponibilidad de los activos de información de los clientes.

Tecnologías de Seguridad. Estos servicios están enfocados a la venta, arrendamiento o licenciamiento de tecnología de seguridad de la información para su implementación en la infraestructura del cliente.

- Venta o arrendamiento. Este servicio pone a disposición de los clientes una gran variedad de tecnologías de protección e identificación de amenazas a la información de los clientes, pudiéndose dividir en 3 áreas principales: perimetral, enfocada a la protección de los sistemas informáticos de los clientes expuestos a internet; usuarios, haciendo referencia a la detección y prevención de fugas de información; y sistemas

centrales, dedicados principalmente a la protección de bases de datos y los sistemas de información o aplicaciones de software de los clientes.

- Implementación: Este servicio consiste en la instalación y puesta a punto de los dispositivos de seguridad en la infraestructura de los clientes, permitiendo incorporar capas de protección a los sistemas de información de clientes y sus usuarios.

1.3.4 Las ventas

Uno de los principales retos desde un inicio para Sm4rt fue el tener una facturación constante que permitiera cubrir los costos base de una empresa, razón por la cual el grupo de socios fue reacios a la consolidación de una sociedad mercantil en los comienzos de la empresa.

La complejidad de la venta estuvo basada en los siguientes factores, los cuales no favorecían a tener un flujo de efectivo que mes con mes permitiera cubrir los costos base de la operación de la empresa, principalmente la nómina:

1. La estacionalidad de los proyectos. La mayor parte de los clientes de los servicios iniciales de Sm4rt referentes a diagnóstico y cumplimiento de seguridad, no tenían necesidad de servicios de forma continua, estos eran solicitados periódicamente de forma anual o bianual. Esto debido a que los clientes con presupuesto para seguridad de la información, ejercían sus presupuestos de forma regular alrededor del tercer y cuarto trimestre del año calendario, por lo que el primer trimestre del año era complicado pues no existían una demanda constante de servicios.
2. Cada venta es un esfuerzo individual y personalizado. Debido a la poca conciencia de seguridad de la mayoría de las empresas en México, cada venta requería de un acompañamiento consultivo para ayudar a los clientes potenciales a identificar sus riesgos globales y las consecuencias de no implementar controles de seguridad en sus sistemas.
3. Ciclos de venta extensos. frecuentemente las propuestas de servicios a los clientes eran revisadas en más de 2 ocasiones por los clientes, pues siempre se requerían hacer ajustes de alcance. Como muchas empresas no tenían un presupuesto especializado en seguridad de la información, muchas de las propuestas le servían al cliente para justificar sus presupuestos de años posteriores por lo que en ocasiones una venta podía durar para cerrar hasta 18 meses.

Con la adición de servicios administrados de ciberseguridad en 2011, las ventas en Sm4rt tomaron un rumbo diferente, ya no eran proyectos finitos de corta duración, se empezaron a obtener contratos multianuales que permitieron facturar y tener un flujo de caja constante a lo largo de toda la duración del contrato, brindando una base económica a la empresa para garantizar los gastos operativos.

En los 6 primeros años de existencia de Sm4rt, se observó un crecimiento estable de la facturación de la empresa, habiendo años con incrementos entre el 40% y 70% anual, sin embargo, es a partir del 2011 cuando se observó una desaceleración en el crecimiento, llegando a ser negativo en 2013. Fue hasta 2014 cuando las ventas volvieron a tener

crecimiento por encima del 50% y para finales de 2015 el presupuesto de ventas había rebasado alrededor del 200% de ventas en comparación con 2014. En 11 años de existencia, Sm4rt había pasado de facturar $4MDP a $261MDP lo que representa un crecimiento de 50 veces. Para finales de 2016 se proyecta tener ventas netas que ronden los $400MDP. (ver Fig. 1)

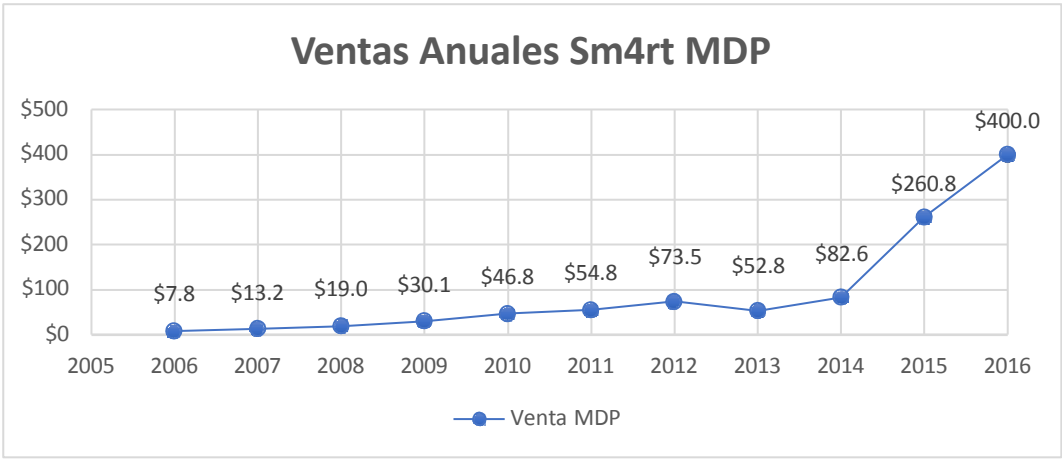


Fig. 1 Ventas netas de 2006 a 2015 y prospección de ventas 2016 al 2Q

1.3.5 El perfil de clientes

La filosofía de Sm4rt en sus primeros 8 años de existencia estuvo relacionada al agnosticismo tecnológico, es decir, nunca se estuvo comprometido con alguna marca o fabricante de software o hardware, Sm4rt simplemente no vendía dispositivos de seguridad a pesar de que los clientes lo solicitaban expresamente.

Así mismo la práctica común era evitar las ventas a dependencias gubernamentales pues era difícil soportar para el tamaño de la empresa la gran cantidad de servicios solicitados en licitaciones públicas además de que el financiamiento requerido para costear el capital de trabajo durante el tiempo que durara el ciclo de pago estaba fuera de la capacidad de la empresa. Por lo anterior, los principales clientes de Sm4rt hasta 2012 fueron empresas privadas de los ramos telecomunicaciones, financieros y de servicios.

Fue hasta 2013 cuando esta tendencia cambió y con el crecimiento de la empresa y la integración a Grupo KIO se empezó a contar con la cantidad de personal y soporte necesarios para entregar servicios de mayores magnitudes y exigencias a entidades gubernamentales mexicanas, convirtiéndose así el sector gobierno en la mayor fuente de ingresos para la compañía.

Uno de los principales cambios en la cultura de Sm4rt posterior a la integración con Grupo KIO fue la formalización del conocimiento del personal de Sm4rt. Se comenzó con un programa de capacitación y certificación intensivo el cuál dotó al persona de las credenciales internacionales que Sm4rt requería para poder concursar y ser un candidato serio en licitaciones públicas y privadas. Esto le abrió las puertas para poder trabajar con dependencias gubernamentales y corporativos nacionales e internacionales de gran tamaño con requerimientos especializados y/o a gran escala.

Para el año 2015 las ventas de Sm4rt estaban conformadas por los siguientes sectores:

- Gobierno: ~50% a dependencias gubernamentales a niveles federal y estatal.
- Telecomunicaciones: ~15% a sector privado de telecomunicaciones.
- Financiero: ~10% a banca y sector financiero a fin.
- Manufactura: ~5%.
- Salud privado: <5% en México.
- Comercializadores: <5% principalmente comercio al menudeo.
- Otros: <10%.

A través de los años, la cantidad de clientes ha crecido de forma constante, con una aceleración en los últimos 3 años referente a la consolidación de los servicios administradores de seguridad y la incorporación a grupo KIO. Esto se refleja en la siguiente gráfica que muestra la cantidad de clientes que Sm4rt ha tenido desde 2006 hasta la fecha en cifras aproximadas como puede verse en la Fig. 2.

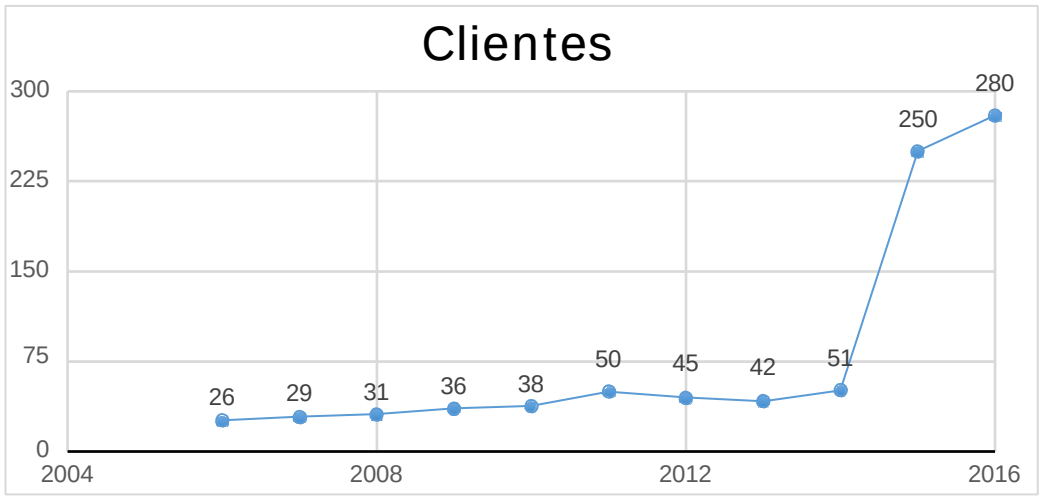


Fig. 2 Número de Clientes de Sm4rt entre 2005 y 2016

El crecimiento en cantidad de clientes entre 2014 y 2015 se debe principalmente a la incorporación de la cartera de clientes de servicios administrados de seguridad de KIO Networks y RedIT, esta última fue adquisición de grupo KIO en 2014.

1.3.6 Los competidores

Es hasta finales de los años 90's cuando la cultura de seguridad de la información comenzó a tener un foro público, principalmente en Estados Unidos. Conferencias y convenciones especializadas en seguridad de la información y "hacking" empezaron a ser un tema recurrente cada año, como las conferencias "Black Hat" y "DEFCON" realizadas regularmente en Las Vegas. Sin embargo, no es hasta comienzos de los años 2000 cuando empieza a haber regulaciones o estándares en Estados Unidos que incluyen aspectos relacionados a seguridad de la información.

Es en el año 2002 cuando el "Sarbanes-Oxley Act" (mejor conocida como SOx) establece controles de auditoría a nivel sistemas de información a las empresas públicas cotizantes en la bolsa de valores de Estados Unidos. Con esta normativa comienza a existir una demanda

real de servicios de consultoría y ciberseguridad de parte de las empresas pues se requieren implementar sistemas de control. Estos controles a nivel informático requirieron de la integración de tecnología y servicios de seguridad de la información para poder cumplir con la regulación y mantener su operación

Posteriormente en 2005 se libera el estándar ISO/IEC 27000 que describe el propósito y tipo de controles que deben de ser implementados en un Sistema de Gestión de Seguridad de la Información. Con lo que existe por primera vez una norma internacional únicamente enfocada a controles de seguridad de la información, la cual fue tomada como base para la elaboración de normativas locales o específicas de ciertas industrias.

Posteriormente los mayores impulsos en México para en los servicios de seguridad de la información se dieron en 2010 y en 2012, con la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP) y el Manual Administrativo de Aplicación General en materia de Tecnologías de la Información y Comunicación de Seguridad de la Información (MAAGTICSI) respectivamente.

Con la liberación o promulgación en México de estas diferentes normas, la demanda de servicios incrementó sustancialmente, pues ya no se trataban de requerimientos proactivos de los clientes para proteger su infraestructura, si no que ahora tenían como obligación regulatoria para su operación el tener algún tipo de sistema de monitoreo, auditoría y protección de ciberseguridad.

Algunas de las empresas que brindan servicios de ciberseguridad a nivel internacional y que han dado o prestan actualmente servicios para clientes México se encuentran en la Tabla 1.

Empresa	Inicio MSSP	Localización	Cantidad de SOC worldwide	Ingresos Anuales
Dell SecureWorks	1996	Atlanta, EUA	6 (3xEUA, Reino Unido, Japón y Rumania)	~ 339 MDD
IBM Security	2002	Atlanta, EUA	6 (2xEUA, Costa Rica, Brasil, Japón y Polonia	~ 2,000 MDD
Symantec	2002	California, EUA	6 (EUA, Reino Unido, Japón y 3xAsia)	~480 MDD

Tabla 1 Empresas internacionales de ciberseguridad que ofrecen servicios en México.

En México existen diferentes empresas como puede verse en la Tabla 2, la mayoría de inversión mexicana, las cuales ofrecen servicios de seguridad administrada (SOC) como Sm4rt Security Services.

Empresa	Inicio	Localización	Tipo principal de clientes	SOC en México	Ingresos Anuales
Scitum - Telmex	2005 (como MSSP)	CDMX	Gobierno / Corporativo	1	~ 60 MDD
Sm4rt	2011 (como MSSP)	CDMX y EDOMEX	Gobierno	3	~ 17 MDD
Insys	2010 (como MSSP)	CDMX	Corporativo	1	~ 9 MDD
IQSec	2007	CDMX	Corporativo	1	~ 7 MDD
CoreOne	2006	CDMX	Corporativo	1	~ 6 MDD
Mexis	2003	CDMX	Corporativo	1	~ 6 MDD
Onlinet	1997	CDMX	Corporativo	1	~ 5 MDD
Dicofra	1999	CDMX	Corporativo	1	~ 3 MDD

Tabla 2 Empresas mexicanas de ciberseguridad que ofrecen servicios en México.

Capítulo 2. Marco teórico

En esta sección se referencian los temas que son relevantes para la elaboración de este documento, sirviendo para dar contexto y sustento al desarrollo de la propuesta el para el cumplimiento de los objetivos.

2.1 Entorno general

El término Gestión de Incidentes se refiere a las actividades, procedimientos y lineamientos usados por las organizaciones para dar tratamiento a sus incidentes de seguridad. Esta práctica se ha vuelto de mayor relevancia en las organizaciones públicas como privadas en el mundo, debido a la dependencia tecnológica ocasionada por el uso de sistemas de información para la operación y soporte de las actividades críticas económicas, políticas y sociales.

De forma general los diferentes estándares y mejores prácticas relacionadas a la gestión de incidentes están compuestas de los siguientes grupos de actividades: Preparación, Detección, Análisis y Respuesta. Dentro del grupo de Análisis se contemplan las actividades de "triage" o Priorización y Clasificación, las cuales son el foco principal de este trabajo.

El término "triage", que en este trabajo es sinónimo de priorización, es un término usado actualmente en el campo de la ciberseguridad para referirse a la priorización de un evento, que potencialmente puede tratarse de un incidente de seguridad, para su análisis y tratamiento. La palabra "triage" proviene del francés "trier" que principalmente fue aplicado para referirse a un proceso de ordenamiento. Con base en el diccionario de Cambridge[4] se trata de "el proceso de examinación rápida de pacientes que fueron llevados al hospital para decidir cuáles son los enfermos más graves y que deben de ser tratados primero" y al diccionario Médico "Triage es el proceso de ordenamiento de personas basado en su necesidad de tratamiento médico inmediato en comparación con su oportunidad de beneficio de dicho tratamiento. El triage es hecho en salas de urgencias, desastres, y guerras, cuando los recursos médicos son limitados y deben de ser usados para maximizar el número de sobrevivientes. El triage en esta última forma se originó en la Primera Guerra Mundial, donde los soldados heridos eran clasificados dentro de 3 grupos: los que se podía esperar que sobrevivieran sin tratamiento médico, los que posiblemente morirían aun con tratamiento, y aquellos que podrían sobrevivir con tratamiento médico."[5] Desde otro punto de vista médico "Las salas de urgencias alrededor del globo siguen un sistema de triage para hacer frente a la sobre saturación. La intención detrás del triage es mejorar la atención de urgencias y priorizar los casos en términos de urgencia clínica."[6]

Conforme se realizan las actividades necesarias para priorizar un incidente, también es necesario poder tipificarlos dentro de una clasificación dependiendo de diferentes características intrínsecas

---

[4] Definition of "triage" - English Dictionary. (s.f.). Recuperado 26 de mayo, 2017, de http://dictionary.cambridge.org/us/dictionary/english/triage

[5] Medical Definition of Triage. (2016). Recuperado 4 de junio, 2017, de http://www.medicinenet.com/script/main/art.asp?articlekey=16736

[6] Ramesh P Aacharya, Chris Gastmans and Yvonne Denier. (2011). Emergency department triage: an ethical analysis. Recuperado 22 de octubre, 2016, de BMC Emergency Medicine 2011 Sitio web: http://bmcemergmed.biomedcentral.com/articles/10.1186/1471-227X-11-16

al incidente. Esta tipificación es también conocida como “Taxonomía”. El beneficio de tener una taxonomía para la clasificación y nombrado de un incidente permite, al tener un registro del incidente, obtener métricas para dar seguimiento a los incidentes más importantes y retroalimentar los análisis de riesgos de la organización y con ello las prácticas de gestión de incidentes. Adicionalmente esto también permite la interacción con otras organizaciones para el intercambio de inteligencia. A esta estructura estandarizada se le conoce como Taxonomía. De acuerdo con el origen griego de la palabra taxonomía se deriva de los vocablos “taxis” que significa arreglo u ordenamiento y “nomos” que significa norma o regla, por lo que en conjunto implican un “norma de arreglo”. Comúnmente el término Taxonomía es usado en la biología para la clasificación y nombrado de las especies animales y vegetales.

2.2 Estado actual de la ciberseguridad

La ciberseguridad en el mundo, es un tema que año con año se ha vuelto más relevante desde finales de años 90s. Esta relevancia no es necesariamente porque constantemente se conocen más grupos criminales, sino porque las organizaciones tanto públicas como privadas de todo el mundo se han vuelto más conscientes de la necesidad de contar con controles informáticos y no informáticos que minimicen la superficie de ataque, detecten una parte de las actividades sospechosas, que les permitan contrarrestar los ataques y tener una mayor visibilidad de los incidentes para poder contenerlos de forma eficiente y efectiva.

Continuamente las amenazas informáticas evolucionan, como si se tratasen de organismos vivos, algunas se extinguen y otras se hacen más dominantes sobre otras, permitiendo a la industria de fabricantes de tecnologías de la seguridad desarrollar nuevas soluciones de ciberseguridad que mitiguen la efectividad de las amenazas. Sin embargo, la carrera por la mitigación de vulnerabilidades es una guerra que solo puede ser contenida pero no detenida pues la velocidad de crecimiento de nuevas tecnologías de la información, como el “IoT” (Internet de las Cosas), los dispositivos móviles (teléfonos inteligentes, tabletas digitales y equipos de cómputo laptops), la digitalización de casi todas nuestras actividades y la omnipresencia del acceso a internet, son un fuente inagotable de recursos y víctimas potenciales de los grupos criminales. De acuerdo con las siguientes fuentes “Internet World Stats”[7] y la “Internet Live Stats”[8] calculan que el crecimiento de los usuarios de internet del año 2000 hasta la primera mitad del 2016 ha sido de entre 825% y el 905%, pasando de aproximadamente 400 millones de usuarios de internet a 3.5 miles de millones.

En la publicación anual de la empresa de telecomunicaciones “Verizon” conocida como “Reporte de Investigaciones de Brechas de Datos”[9] de 2016, la cual está basada en información de más de 60 organizaciones en 82 países, se muestra el incremento de incidentes de ciberseguridad que derivan en la fuga y compromiso de datos a través del tiempo (ver Fig. 3). También es posible identificar que a partir de 2005 se ha tenido un incremento de estos en los incidentes de por lo menos 10 veces.

---

[7] Miniwatts Marketing Group. (2016). TOP 20 COUNTRIES WITH THE HIGHEST NUMBER OF INTERNET USERS. Recuperado 22 de octubre, 2016, de: http://www.internetworldstats.com/top20.htm

[8] InternetLiveStats.com. (2016). InternetLiveStats.com. Recuperado 22 de octubre, 2016, de: http://www.internetlivestats.com/internet-users/

[9] Verizon. (2016). 2016 Data Breach Investigations Report. Recuperado 22 de octubre, 2016, de: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

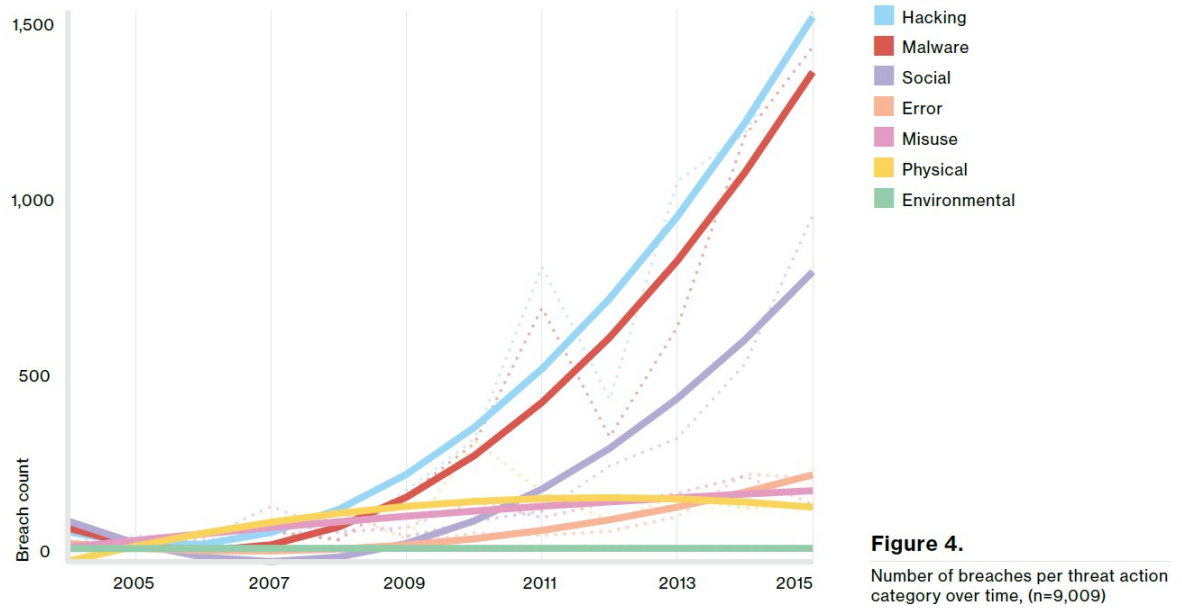


Fig. 3 Número de incidentes por categoría de acción de amenaza en el tiempo.

En la siguiente imagen (ver Fig. 4) se muestra como los diferentes tipos de amenazas han evolucionado en los últimos 7 años, algunas tomando más fuerza, otras dejando de ser efectivas, e incluso las líneas grises muestran ejemplos de tipos de amenazas que dejaron de ser de alto impacto.

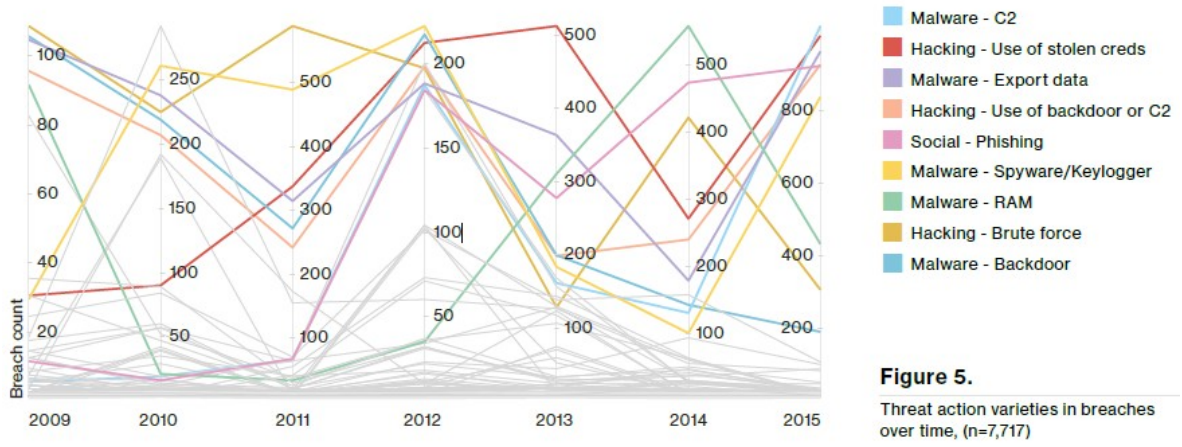


Fig. 4 Variación de la acción de amenaza en incidentes en el tiempo.

Una tendencia de los últimos años, derivada de la adopción del acceso a internet, y de que el nivel técnico promedio de los usuarios de internet disminuye rápidamente, es que los atacantes ya no tienen como primer objetivo de ataque servidores de grandes corporaciones, si no que cada vez más hacen uso de los dispositivos de los usuarios y se enfocan en explotar el desconocimiento humano más que las vulnerabilidades tecnológicas. Esto se puede observar en la Fig. 5.

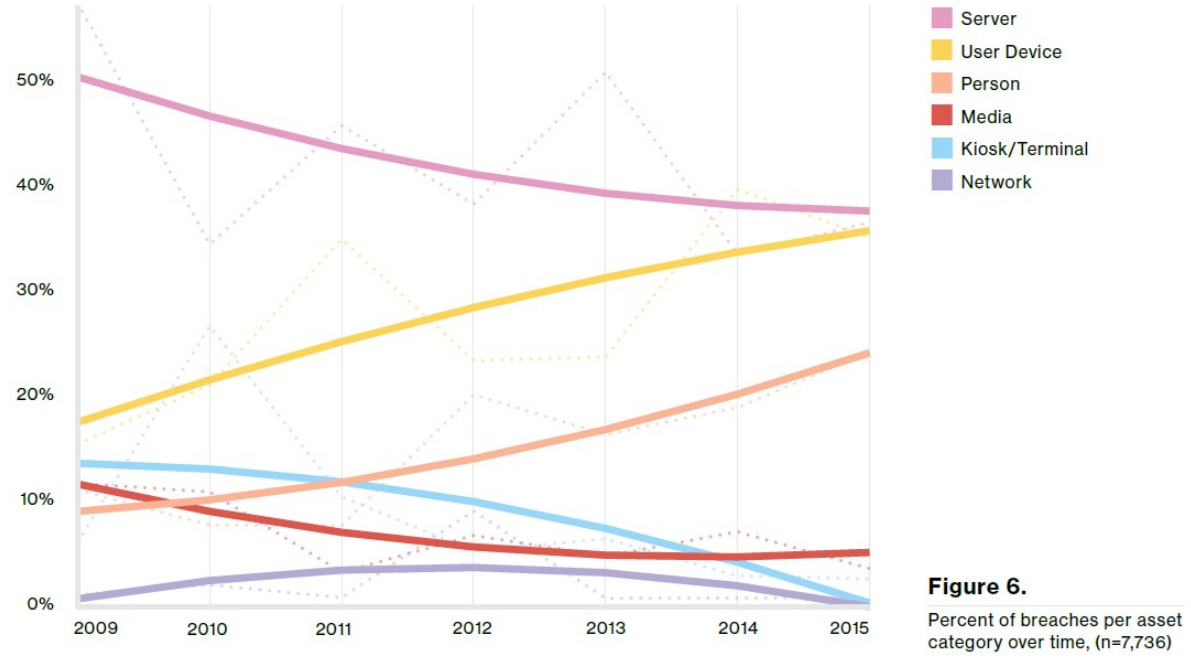


Fig. 5 Porcentaje de incidentes por categoría de activo en el tiempo.

Según la investigación realizada por "Kaspersky Labs", uno de los principales fabricantes y desarrolladores de tecnologías de protección de usuarios para protección de malware, en su reporte "Control de daños: el costo de las brechas de seguridad"[10] el costo de una brecha de seguridad de la información (ver Fig. 6) rebasa el medio millón de dólares americanos en el caso de Empresas grandes, mientras que para PyMEs (Pequeña y Medianas Empresas) es de alrededor de 40 mil dólares.

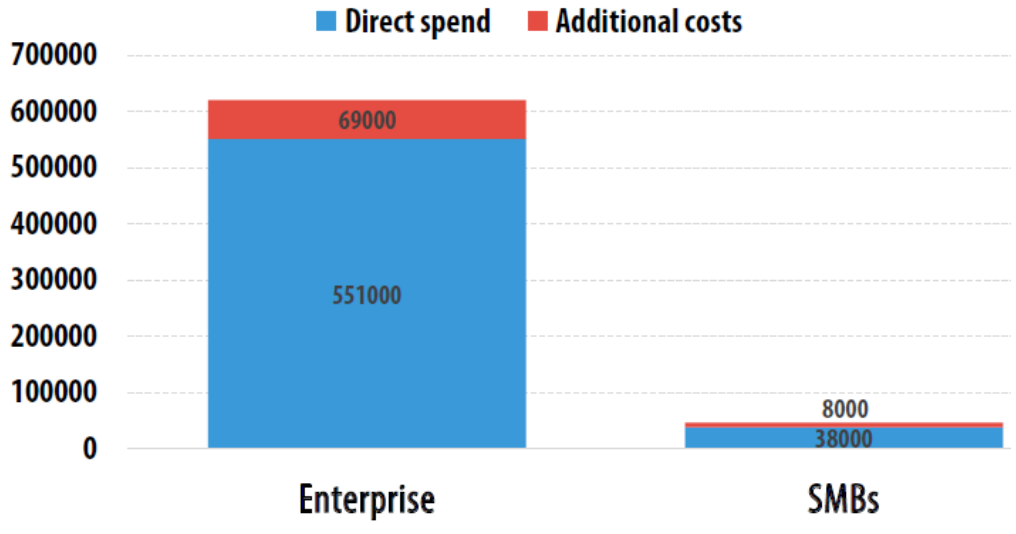


Fig. 6 Costo de un incidente de seguridad en dólares.

[10] Kaspersky Labs. (2016). Damage Control the Cost of Security Breaches - IT Security Risk Special Report Series. Recuperado 22 de octubre, 2016, de: https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf

Es por lo anterior que cada vez más empresas alrededor del mundo implementan o contratan servicios de ciberseguridad para la protección de su infraestructura crítica. Adicionalmente existen otros retos importantes a los cuales las organizaciones se enfrentan cuando implementan controles de ciberseguridad internamente en sus organizaciones. La ISACA (Asociación de Auditoría y Control de Sistemas de Información) a través de su estudio anual de 2016 conocido como "El estado de la ciberseguridad, Implicaciones para 2016"[11] identifica que uno de los principales problemas para tener un programa de ciberseguridad eficientemente dentro de una organización radica es la escasez de profesionales calificados en ciberseguridad como puede observarse en la Fig. 7, y correlaciona la capacidad técnica con la inhabilidad para entender al negocio con su capacidad de comunicarse efectivamente.

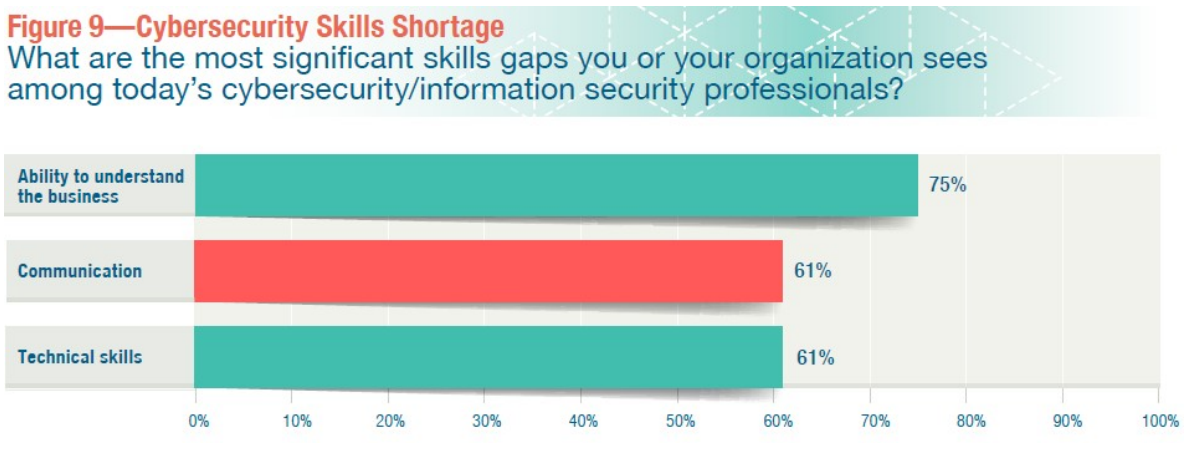


Fig. 7 Falta de habilidades de ciberseguridad.

2.3 Estado actual de la ciberseguridad en México

A pesar de que puede pensarse que México no es país atractivo para las organizaciones de crimen informático, el paisaje informático a diferencia del paisaje físico es más homogéneo en el mundo. Los grupos de crimen informático usan principalmente técnicas oportunistas para comprometer infraestructura en el mundo, y emplean los recursos informáticos comprometidos para obtener un beneficio económico que puede ir desde el robo de información sensible, como tarjetas de crédito, hasta tomar control del dispositivo para el procesamiento de ataques de negación distribuida de servicio (DDoS) para luego solicitar un rescate, etc.

Con base en la investigación realizada por "CyberEdge Group" en su Reporte de Defensa de Ciber Amenazas 2016 (2016 Cyberthreat Defense Report[12], el cual concentra la retroalimentación de 1000 tomadores de decisiones de 10 países en Norte América, Europa, Asia Pacífico y Latino América, las organizaciones en México tienen la percepción de haber sido comprometidas casi en el mismo porcentaje que organizaciones en países desarrollados como Estados Unidos, Japón y Reino Unido, como puede verse en la Fig. 8.

---

[11] ISACA. (2016). State of Cybersecurity - Implications for 2016. Recuperado 22 de octubre, 2016, de: http://www.isaca.org/cyber/pages/state-of-cybersecurity-implications-for-2016.aspx

[12] CyberEdge Group. (2016). 2016 Cyberthreat Defense Report. Recuperado 22 de octubre, 2016, de: https://cyber-edge.com/2016-cdr/

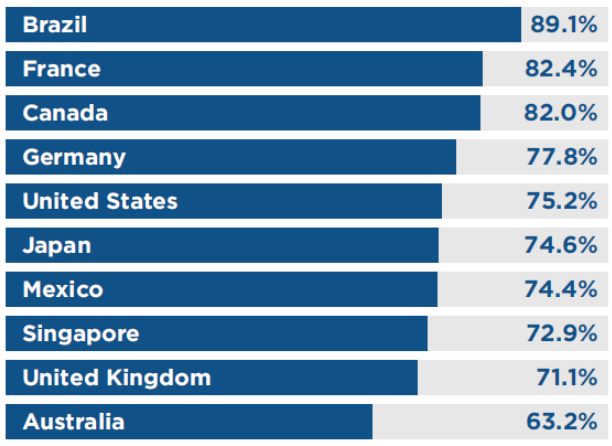


Fig. 8 Porcentaje de empresas comprometidas por lo menos a 1 ataque en los últimos 12 meses.

A pesar de que el escenario se vea similar al del resto del mundo, y debido a la cultura y la legislación de los países en vías de desarrollo como México, las empresas públicas y privadas no tienen la obligación de informar a un órgano centralizado de sus incidentes de seguridad, por lo que no existen estadísticas precisas al respecto. La mayoría de las empresas en México prefieren no reportar sus incidentes de seguridad para evitar ser auditados o que dichos incidentes tengan un fuerte impacto reputacional, mientras que otras no tienen los controles de ciber seguridad implementados que les permita identificar que son víctima de un ataque.

Los principales sectores en México que son objetivo de grupos de crimen informático son el Sector Financiero y las Asociaciones Gubernamentales (reguladoras y judiciales), esto con base en el análisis de "Amenazas Cibernéticas al Sector Financiero Mexicano"[13] (ver Fig. 9) de "Control Risks Group". En este artículo se analizan las principales causas de estas amenazas y se observa que México es un país atractivo al crimen informático por 3 razones: el crecimiento económico, el activismo político/social y la cercanía con Estados Unidos, a partir de lo cual se identifica que los 3 principales tipos de grupos que atacan a las organizaciones en nuestro país: 1) espionaje estratégico de estados-nación, 2) grupos criminales y 3) activistas. Por otro lado se hace un excelente análisis, desde el punto de vista económico de los grupos que atacan a las organizaciones, los tipos de ataques informáticos usados y el impacto económico que ocasionan al realizar estos tipos de ataques.

[13] Control Risks Group Limited. (2015). Amenazas Cibernéticas al Sector Financiero Mexicano. Recuperado 22 de octubre, 2016, de: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/mexican-financial-sector-cybersecurity-healthcheck

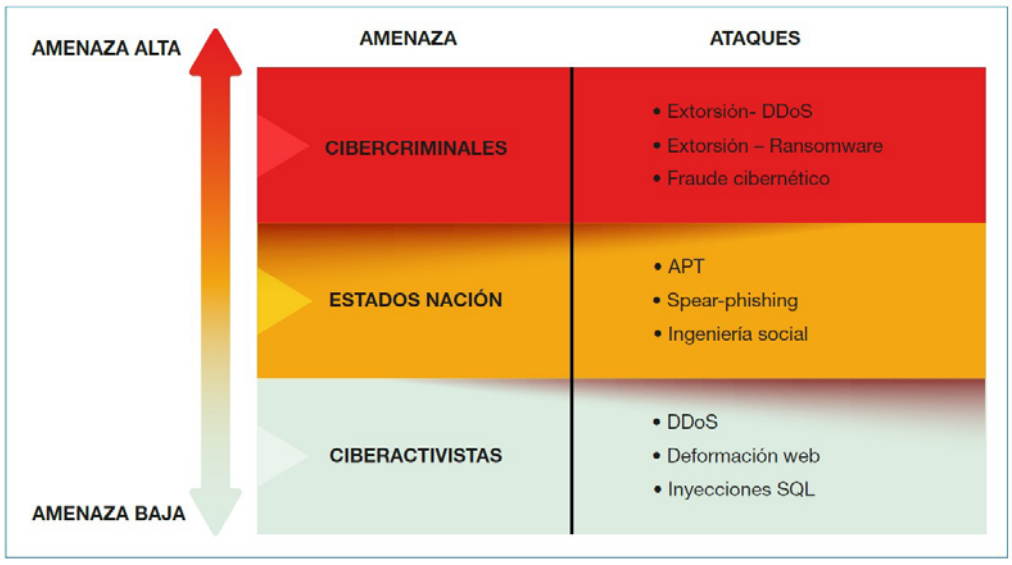


Fig. 9 Amenazas a las que se enfrenta el sector financiero mexicano.

De acuerdo con un informe publicado por PWC "Ciberseguridad en México"[14] y el CERT-MX de la Comisión Nacional de Seguridad de México en su informe "Impacto y gravedad de los ciber-delitos"[15], México es el segundo país de Latinoamérica más afectado por el crimen informático. Según este mismo informe la Policía Federal de México registró 23,549 casos de ciber-crimen en 2013, de los cuales alrededor del 50% corresponde a infecciones de virus de tipo "ransomware" como puede verse en la Fig. 10.

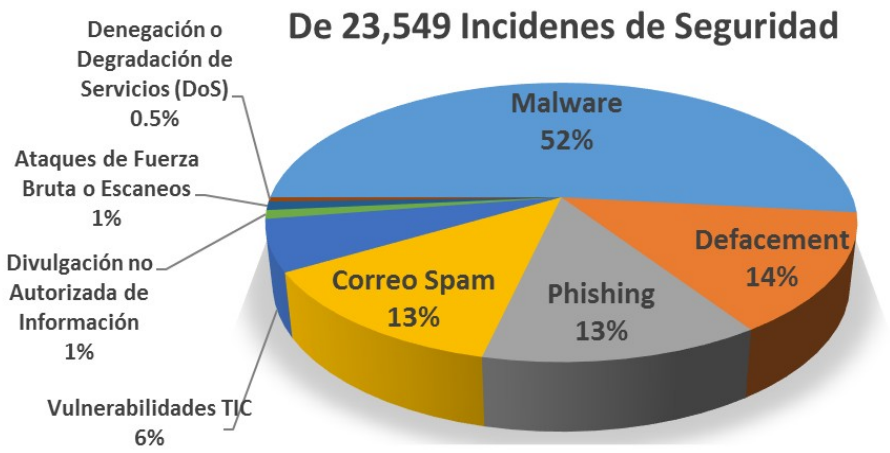


Fig. 10 Incidentes de seguridad por tipo de amenaza según la Comisión Nacional de Seguridad

En el mismo informe se hacen mención por parte de la Policía Federal y el CERT-MX de los cambios en las tendencias con base en los sectores financieros y gubernamentales a nivel federal, municipal

[14] PWC México. (2015). Cybersecurity in Mexico. Recuperado 22 de octubre, 2016, de: https://www.pwc.com/mx/es/knowledge-center/archivo/20150917-kc-cybersecurity.pdf
[15] Comisión Nacional de Seguridad. (2014). Impacto y gravedad de los ciberdelitos. Recuperado 22 de octubre, 2016, de: http://seguridad2012.politicadigital.com.mx/pdf/03.pdf

y estatal. En el cuál se puede observar claramente los tipos de técnicas o tipos de ataque más usadas para comprometer cada sector (ver Fig. 13, Fig. 12 y Fig. 13). Con base en estos análisis se puede correlacionar el hecho de que México, como el resto del mundo, es un blanco deseable para los grupos de crimen informático en el mundo pues de hecho es posible para estos grupos criminales obtener un beneficio económico, reputacional significativo en el mundo e incluso obtener acceso a infraestructura crítica no solo de México sino de Estados Unidos.

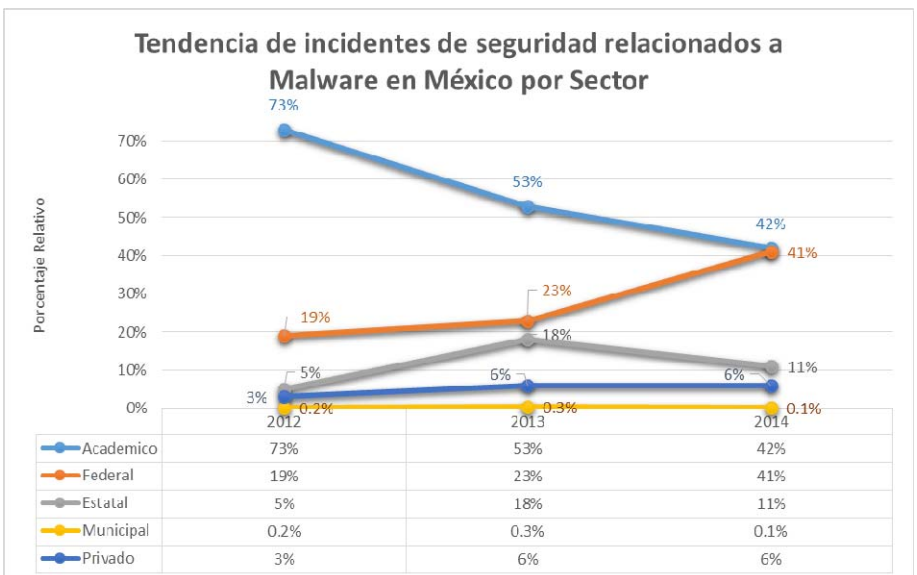


Fig. 11 Tendencia de incidentes de seguridad detallada por tipo de amenaza y sector. Fuente Comisión Nacional de Seguridad

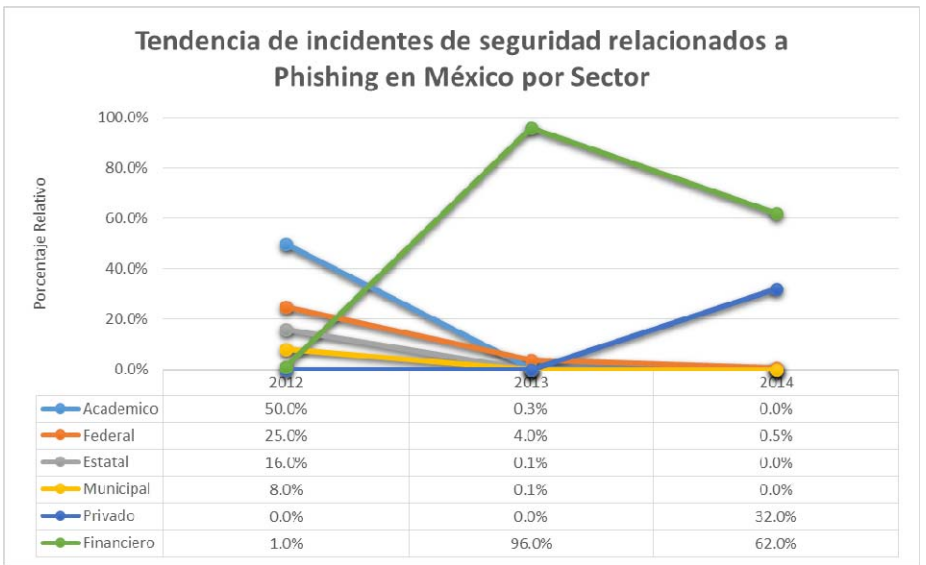


Fig. 12 Tendencia de incidentes de seguridad detallada por tipo de amenaza y sector. Fuente Comisión Nacional de Seguridad

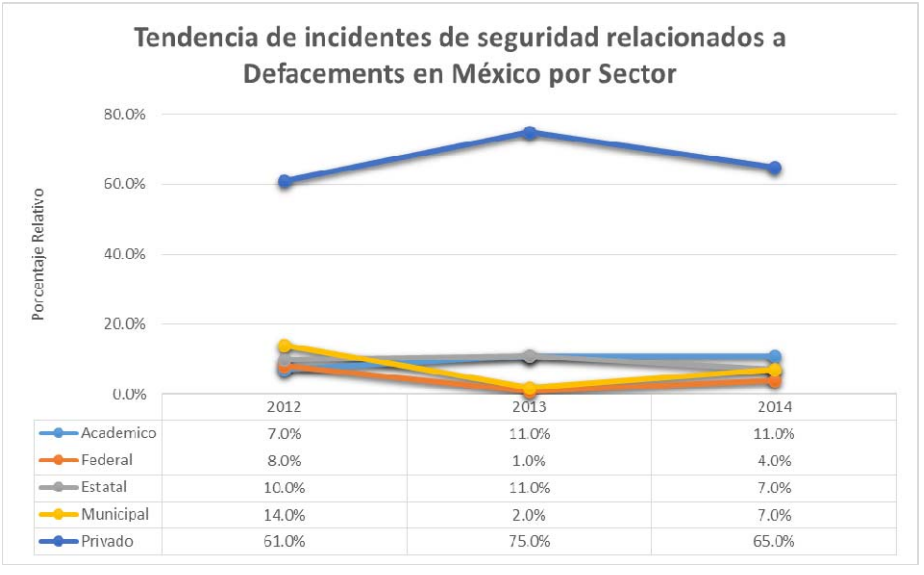


Fig. 13 Tendencia de incidentes de seguridad detallada por tipo de amenaza y sector. Fuente Comisión Nacional de Seguridad

2.4 Gestión de incidentes

Diferentes organizaciones alrededor del mundo, principalmente en los países desarrollados, han creado marcos de trabajo, estándares, lineamientos y emitido buenas prácticas que de forma directa o indirecta están relacionadas con la gestión de incidentes. Las principales organizaciones son: NIST (Instituto Nacional de Estándares y Tecnología), ISO/EIC (Organización Internacional de Estandarización / Comisión Internacional Electrotécnica), ENISA (Agencia de la Unión Europea para la Seguridad en Redes y de la Información) e ITIL (Biblioteca de Infraestructura y Tecnologías de Información)[16].

La gestión de incidentes en las organizaciones es una práctica ampliamente usada por instituciones financieras desde los años 90's, mientras que para otros sectores de la industria estas actividades son ejercidas por motivaciones externas, entre las cuales el más importante son los requerimientos normativos implementado por las autoridades locales de cada sector industrial y por otro lado la experiencia de haber sido víctima de una brecha de seguridad en la confidencialidad de su información, la integridad de su información o la disponibilidad de sus servicios.

Una de las maneras más rápidas de implementar controles de ciberseguridad de la información que permitan tener una gestión de incidentes es a través de la integración de un Proveedor de Servicios Administrados de Seguridad (MSSP "Managed Security Service Provider") el cuál integre y opere en la arquitectura de la organización un conjunto de soluciones de tecnologías de ciberseguridad.

[16] Alfredo Ramiro Reyes Zuniga. (2015). Outsourced incident management services. Recuperado 22 de octubre, 2016, NTNU - Trondheim Norwegian University of Science and Technology de: https://brage.bibsys.no/xmlui/bitstream/handle/11250/2352751/13819_FULLTEXT.pdf?sequence=1&isAllowed=y

Adicional a esto algunos MSSPs ofrecen servicios también de detección y respuesta a incidentes de seguridad. Con base en Investigación de Allen, Gabbard y May[17]:

"Tercerizar servicios de seguridad asociándose con un Proveedor de Servicios Administrados de Seguridad (MSSP) es comúnmente una buena solución para transferir la responsabilidad y operaciones de seguridad de la información. Aunque la organización aun es dueña de sus riesgos de seguridad de la información y de negocio, contratar un MSSP le permite compartir la gestión de riesgos y enfoques de mitigación."

Allen, Gabbard y May[17] también mencionan los beneficios de incorporar el uso de los servicios de un MSSP en las organizaciones ver Fig. 14:

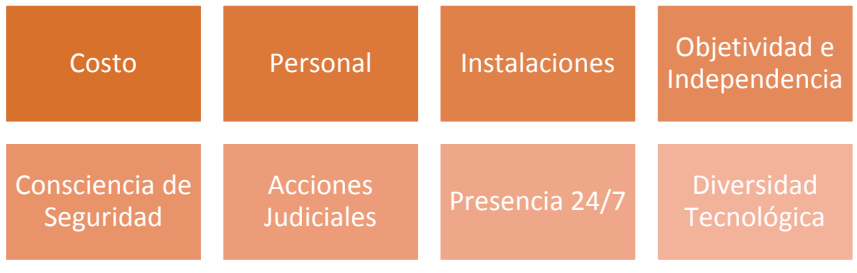


Fig. 14 Beneficios del uso de servicios MSSP en las organizaciones según Allen, Gabbard y May.

Según la publicación de Bussa, Lawson y KAvanag en la nota de investigación de Gartner[18]: "Nuevos proveedores de servicios han emergido para dar soporte a las organizaciones que buscan mejorar su detección de amenazas y capacidad de respuesta a Incidentes." Debido a que el alcance de los servicios de los diferentes MSSPs en el mundo son heterogéneos, algunos se limitan a la gestión de cambios y soporte a fallas de las tecnologías de ciberseguridad mientras que otros realizan también tareas de análisis y notificación de eventos de ciberseguridad, sin embargo no realizan funciones de respuesta y coordinación de incidentes.

Los servicios relacionados a respuesta a incidentes surgen como respuesta a la necesidad de las organizaciones en el mundo por tener servicios administrados de seguridad mucho más especializados y que agreguen mayor valor a sus procesos de gestión de riesgos. La misma publicación de Gartner señala lo siguiente "Estos servicios se enfocan en remover la carga para los clientes de tener que identificar el método o dispositivo a ser usado para el monitoreo de seguridad y capacidad de respuesta".

Estándares y lineamientos

Las siguientes son los principales lineamientos, marcos de trabajo o estándares internacionales publicados o recomendados por las instituciones más relevantes en términos de Gestión de Incidentes y Riesgos a nivel mundial. Todas ellas tienen similitudes, sin embargo, como podrá

---

[17] Julia H. Allen, Derek Gabbard y Christopher J. May. (2003). Outsourcing Managed Security Services. Recuperado 22 de octubre, 2016, de Software Engineering Institute, Carnegie Mellon University Sitio web: http://repository.cmu.edu/cgi/viewcontent.cgi?article=1578&context=sei

[18] Alfredo Ramiro Reyes Zuniga. (2015). Outsourced incident management services. Recuperado 22 de octubre, 2016, de NTNU - Trondheim Norwegian University of Science and Technology Sitio web: https://brage.bibsys.no/xmlui/bitstream/handle/11250/2352751/13819_FULLTEXT.pdf?sequence=1&isAllowed=y

observarse, cada una tiene un enfoque diferente el cual puede ser complementado o adaptado para servir mejor al negocio donde se implementen o a un sector industrial específico. El objeto de enumerarlas es el de observar algunas de las recomendaciones que serán usadas para la adaptación o complemento de las clasificación propuesta de incidentes de ciberseguridad.

2.4.1 Marco de trabajo de ITIL

De acuerdo al análisis de Agutter, ITIL[19] son el conjunto de mejores prácticas para actividades o procesos probados que se han usado con éxito en múltiples organizaciones. Estas buenas prácticas incluyen, dentro de los procesos de operación, la Gestión de Incidentes cuyo propósito y objetivo enuncian según el autor: "Para restaurar el servicio tan pronto posible para minimizar el tiempo de caída y el impacto al negocio." En el contexto de ITIL un incidente no necesariamente está relacionado con la seguridad de la información o ataque informático, por definición un incidente se trata de "Una interrupción no planeada de un Servicio de TI – o una reducción de la calidad de un Servicio de TI. La falla de un Objeto de Configuración que no ha tenido aún un efecto en el servicio también es un incidente".

En el proceso del manejo de un incidente en ITIL se identifican las siguientes actividades principales: Identificación, Análisis, Escalación, Respuesta y Cierre. Estas actividades son fácilmente aplicables a un contexto de ciberseguridad pues una de las funcionalidades principales de cualquier tecnología de ciberseguridad es la de la notificación de eventos que potencialmente pueden convertirse en un incidente para la confidencialidad, integridad o disponibilidad de un servicio o usuario de TI. Para ITIL los eventos pueden ser notificados por cualquier proceso o actividad operativa de la organización y puede ser reportado por cualquier medio a través de una mesa de servicio o directamente o al personal responsable de la gestión de incidentes.

[19] Agutter, C. (2012). ITIL Foundation Essentials: The Exam Facts You Need. Ely, Cambridgeshire, U.K.: IT Governance Publishing.

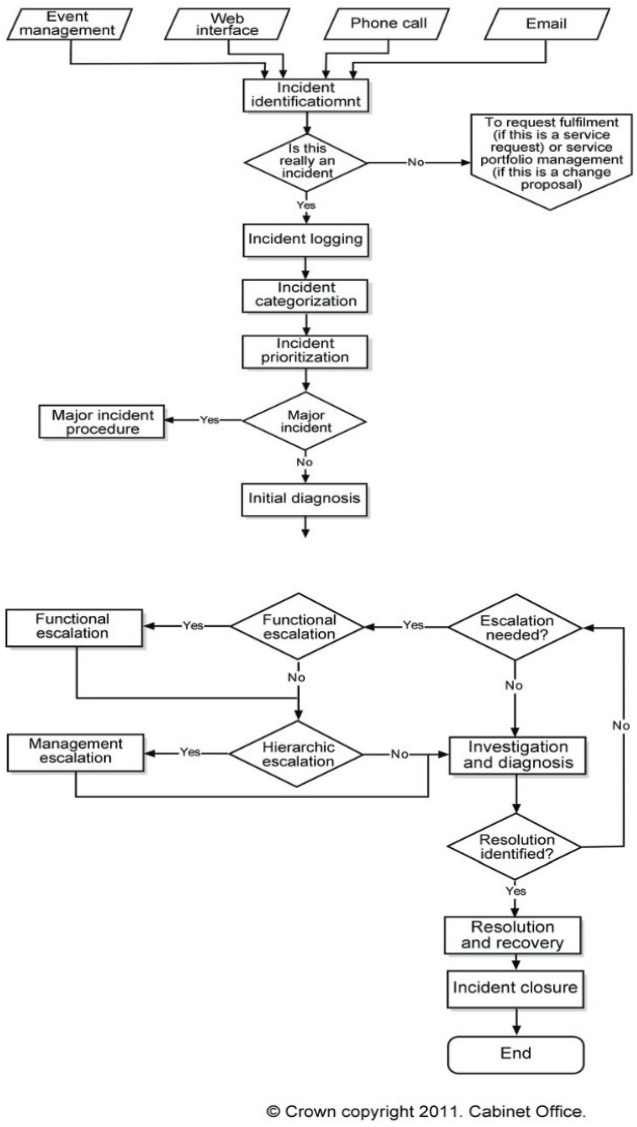


Fig. 15 Proceso de Gestión de Incidentes de ITIL

Como puede observarse en la Fig. 15 del proceso de gestión de Incidentes de ITIL[20], puede aplicarse a cualquier servicio de TI, sin importar el área responsable o la parte del negocio afectada. Es importante notar que parte central de este proceso corresponde a actividades de Análisis, la cuales vienen descritas en el proceso como Clasificación del Incidente, Priorización del Incidente y Diagnóstico. Estas actividades son realizadas por los MSSPs durante la investigación de un evento de seguridad de la información, el cuál debe determinarse si se trata de un incidente real o de un falso positivo.

[20] Agutter, C. (2012). ITIL Foundation Essentials: The Exam Facts You Need. Ely, Cambridgeshire, U.K.: IT Governance Publishing.

2.4.2 Publicación especial NIST 800-61

La publicación especial 800-61 [21] del NIST (Instituto Nacional de Estándares y Tecnología del Departamento de Comercio de los Estados Unidos de América, por sus siglas en inglés) menciona que "un CSIRT (Computer Security Incident Response Team) se ha convertido en un componente importante de las Tecnologías de Información. […] La capacidad de respuesta a incidentes es necesaria para la detección rápida de incidentes, minimización de las perdidas y la destrucción, mitigando las debilidades que fueron explotadas y la recuperación del servicio de TI.".

Según esta publicación, Las organizaciones deben crear, provisionar y operar la capacidad formal de respuesta a incidentes. La ley Federal requiere que las agencias Federales reporten los incidentes a la oficina del US-CERT ("United States Computer Emergency Readiness Team" dentro del Departamento de Seguridad de la Patria (DHS "Department of Homeland Security").

Para el NIST existen 2 conceptos directamente relacionados: Eventos e Incidentes. "Un evento es una ocurrencia observable de un sistema o red.[…] Los Eventos Adversos son eventos con una consecuencia negativa […]. Un Incidente de seguridad en cómputo es una violación o amenaza inminente de violación de las políticas de seguridad en cómputo, políticas de uso aceptable, o prácticas estándares de seguridad."

El NIST hizo un grupo de recomendaciones que los MSSPs deben de mantener en mente para labores de respuesta a incidentes, los más importantes desde el punto de vista del MSSP son:

- Información sensible entregada al proveedor. Las organizaciones deben de poder identificar la información que es indispensable compartir con el proveedor del servicio, mientras esto le permita realizar sus tareas sin sobre exponer o comprometer la información de la organización. Estos acuerdos se realizan a través de Acuerdos de No Revelado de Información (NDA "Non Disclosure Agreement")
- Falta de conocimiento específico de la organización. En análisis preciso y priorización de incidentes depende del conocimiento específico del entorno de la organización. La organización debe de proveer regularmente al proveedor de documentos de actualización que definan cuales son los incidentes más relevantes, cuales son los recursos críticos y cuál es el nivel de respuesta adecuado bajo un conjunto de circunstancias. La organización deberá reportar todos los cambios y actualizaciones hechas a su infraestructura de TI, configuraciones de red, y sistemas. De otra forma el proveedor tendrá que hacer su mejor suposición de cómo cada incidente debe de ser manejado, inevitablemente llevan do a incidentes mal atendidos, y frustración en ambos lados.
- Falta de correlación. Cuando el proveedor no tiene acceso a todos los dispositivos que le puedan ayudar a investigar un posible incidente entonces el proveedor no podrá obtener evidencia que le permita confirmar o descartar un incidente.

---

[21] Paul Cichonski, Tom Millar, Tim Grance y Karen Scarfone. (2012). Computer Security Incident Handling Guide - Recommendations of the NIST. Recuperado 22 de octubre, 2016, de National Institute of Standards and Technology - US Department of Commerce. Sitio web: http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

De esta forma, el NIST 800-61 pretende proveer de lineamientos para el desarrollo de la capacidad de gestión de incidentes y para la interacción con partes externas, como son fabricantes o CSIRT. Esta organización propone el siguiente modelo para la Respuesta a Incidentes (ver Fig. 16):

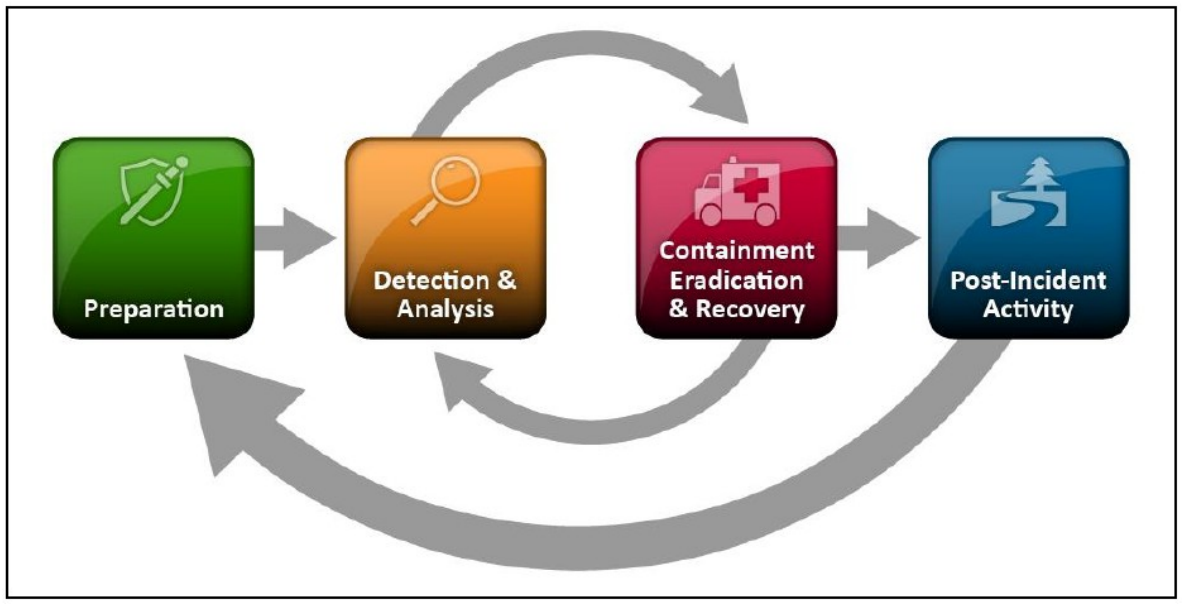


Fig. 16 Ciclo de Vida de la Respuesta a Incidentes según NIST.

Los elementos se retroalimentan entre sí, no son propiamente fases en un proceso, sino un ciclo continuo donde se realizan actividades contantes para incrementar el nivel de preparación, capacidad de detección y respuesta a incidentes de seguridad. Este modelo se describe como sigue:

- Preparación. No solo se refiere a la preparación para responder a un incidente, sino también para prevenir incidentes al asegurarse que los sistemas, redes, y aplicaciones están suficiente asegurados.
- Detección y Análisis. Son todas las actividades relacionadas al monitoreo de eventos, identificación de incidentes, priorización, clasificación y documentación del incidente.
- Contención, Erradicación y Recuperación. Estas son las actividades relacionadas con la elección del curso de respuesta, la documentación de evidencia, identificación del atacante, la erradicación de la amenaza y las acciones de recuperación o continuidad del servicio.
- Actividades Posteriores al Incidente. Son las actividades de documentación de lecciones aprendidas, revisar y retroalimentar el proceso, efectuar mediciones y cálculo de indicadores

2.4.3 ENISA – Guía de buenas prácticas para la gestión de incidentes

La Agencia de Redes y Seguridad de la Información Europea liberó en 2010 la Guía de Buenas Prácticas para la Gestión de Incidentes[22] con el objetivo de proveer una descripción de buenas prácticas para la gestión de incidentes de seguridad. El principal alcance de la gestión de incidentes

[22] Miroslaw Maj MSc, Roeland Reijers y Don Stikvoort MSc. (2010). Good Practice Guide for Incident Management. Recuperado 22 de octubre, 2016, de ENISA Sitio web: https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

es TI y los incidentes de seguridad de la información, como incidentes que están limitados a computadoras, dispositivos de red, redes y la información en es aquí o en tránsito.

El modelo de gestión de incidentes de la ENISA muestra una orientación reactiva como puede verse en la Fig. 17, pues no contempla las fases de planeación y a retroalimentación constante de las lecciones aprendidas al respecto de los incidentes de seguridad. El modelo para la gestión de incidentes está basado las 4 actividades siguientes:

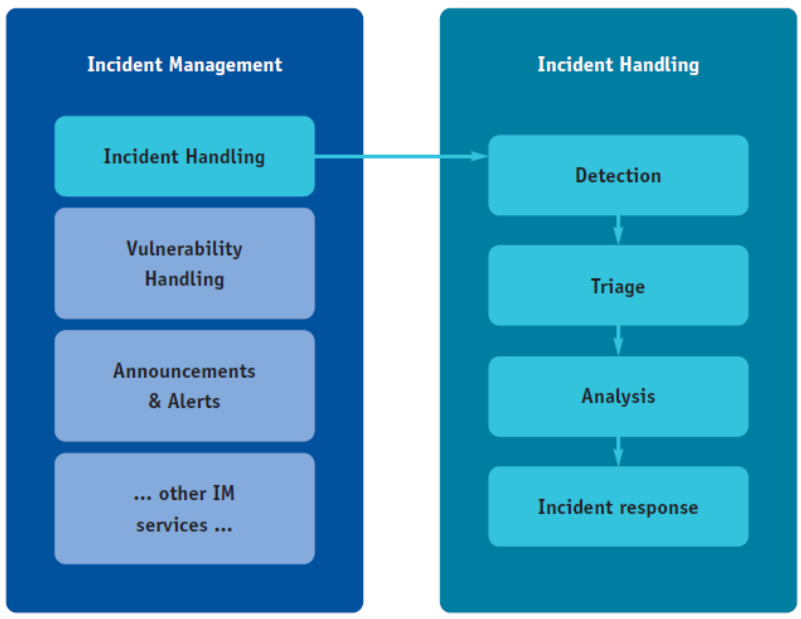


Fig. 17 Actividades de la Gestión de Incidentes y Manejo de Incidentes de acuerdo con el ENISA

Dentro de las actividades del manejo de incidentes se observa el conjunto llamado Triage el cuál hace referencia a aquellas actividades para dar clasificación y prioridad de atención a los incidentes.

2.4.4 Estándar ISO/IEC 27035

Conforme al estándar publicado por la BSI[23] en 2011 para la gestión de incidentes y con base en los explicado por Reyez Zuniga en "Outsourced Incident Management Services"[24] este estándar de la familia del ISO 27000 el cual establece los lineamientos para la definición, implementación y seguimiento de un Sistema de Gestión de la Seguridad de la Información. Conforme a Zuniga: "El estándar ISO 27035 provee una guía para la gestión de incidentes. Ofrece un enfoque estructurado para tratar con los incidentes incluyendo Planeación, Detección, Respuesta y a partir de ello generar Lecciones Aprendidas". El modelo de gestión de incidentes de ISO/IEC 2735 se muestra en la Fig. 18 a continuación:

---

[23] ISO/IEC. ISO 27035-2 (2nd Working Draft), Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management

[24] Alfredo Ramiro Reyes Zuniga. (2015). Outsourced incident management services. Recuperado 22 de octubre, 2016, de NTNU - Trondheim Norwegian University of Science and Technology Sitio web: https://brage.bibsys.no/xmlui/bitstream/handle/11250/2352751/13819_FULLTEXT.pdf?sequence=1&isAllowed=y

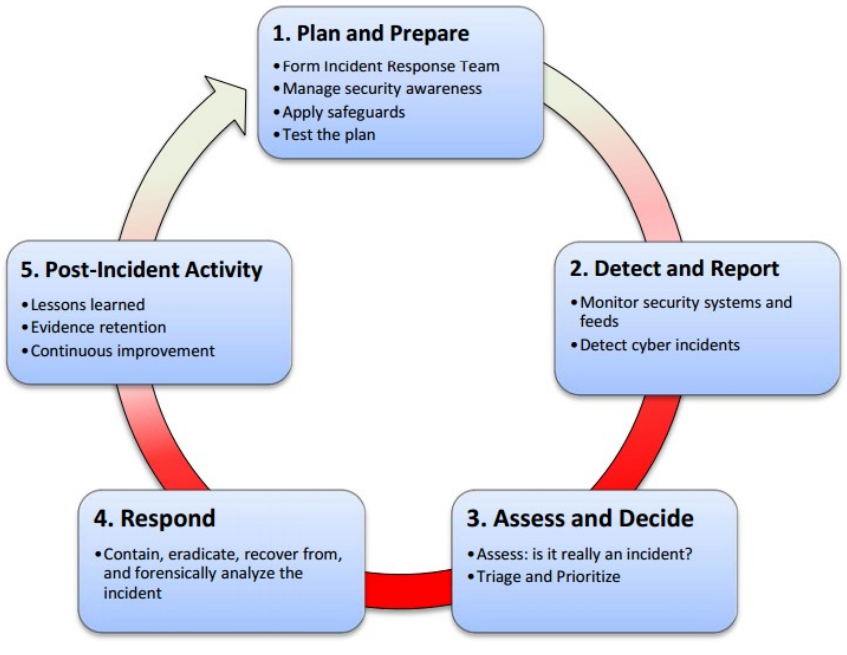


Fig. 18 Elementos claves de la Gestión de Incidentes de Ciberseguridad según ISO/IEC 27035[25]

Zuniga también expone que "El estándar ISO/IEC 27035:2011 busca ayudar a las organizaciones a satisfacer los requerimientos de establecer, implementar, mantener y mejorar continuamente el ISMS especificado en el ISO/IEC 27001:2013".

2.5 Priorización y clasificación de incidentes de seguridad de la información

A continuación se muestra cuáles son las clasificaciones existentes, y taxonomías usadas para el nombrado, de incidentes de seguridad. Estas son recomendaciones emitidas por las mismas organizaciones internacionales de la sección anterior o por terceros avalados. El objetivo de esto es mostrar una línea base la cuál es adecuada en el desarrollo de este proyecto.

2.5.1 NIST

De acuerdo al NIST SP 800-61[26] la Priorizar el manejo de un incidente es quizá la decisión más crítica en el proceso de manejo. Los incidentes no deben de ser manejados en forma "primero en entrar, primero en salir" debido a la limitación de los recursos. La priorización de acuerdo al NIS debe de tomar en cuenta los siguientes factores (ver las siguientes tablas: Tabla 3, Tabla 4, Tabla 5 y Tabla 6):

[25] Juno Risk Solutions. (2015). Cyber Incident Management Planning Guide for IIROC Dealer Members. Recuperado 22 de octubre, 2016, de Investment Industry Regulatory Organizacion of Canada Sitio web: http://www.iiroc.ca/industry/Documents/CyberIncidentManagementPlanningGuide_en.pdf

[26] Paul Cichonski, Tom Millar, Tim Grance y Karen Scarfone. (2012). Computer Security Incident Handling Guide - Recommendations of the NIST. Recuperado 30 de octubre, 2016, de National Institute of Standards and Technology - US Department of Commerce. Sitio web: http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

Tipo de Impacto	Descripción	
Funcional	Se debe de considerar como el incidente impactará actual y futuramente la funcionalidad del sistema afectado.	Estos combinados determinan el Impacto a Negocio del Incidente.
A la Información	Se debe de considerar afectación a la integridad, confidencialidad o disponibilidad de la información del sistema. Se debe evaluar si la afectación impacta la misión de la organización.	
A la Capacidad de Recuperación	El tamaño del incidente y el tipo de recursos afectados determina el tiempo y recursos que deberán ser usados para recuperarse del incidente.	Estos determinan las posibles respuestas.

Tabla 3 Tipos de impacto de un incidente al negocio según la NIST.

Dependiendo de la combinación de estos tipos de impactos, y la capacidad de recuperación de un incidente, cada organización puede priorizar la atención de sus incidentes con base en sus propios criterios.

Niveles de Impacto Funcional	Definición
Ninguna	No afecta la habilidad de la organización para proveer servicios a todos los usuarios.
Bajo	Impacto mínimo, la organización aún puede proveer servicios críticos a los usuarios afectados.
Medio	La organización ha perdido la habilidad para proveer servicios críticos.
Alto	La organización no puede proveer de los servicios críticos a ningún usuario.

Tabla 4 Niveles de impacto funcional de un incidente según la NIST.

Niveles de Impacto a la Información	Definición
Ninguna	Ningún dato fue extraído, modificado, borrado o comprometido.
Violación a la privacidad	Datos sensibles de información de identificación, pagos de impuesto, empleadores, beneficiarios fueron accedidos o extraídos.
Violación a la propiedad	Acceso o extracción de información propietaria.
Perdida de integridad	Modificación o borrado de información sensible o propietaria.

Tabla 5 Niveles de impacto inherente a la información de un incidente según la NIST.

Niveles de Impacto a la Capacidad de Recuperación	Definición
Regular	Tiempo de recuperación es predecible con los recursos existentes.
Suplementada	Tiempo de recuperación es predecible con recursos adicionales.
Extendida	Tiempo de recuperación es impredecible, recursos adicionales y ayuda externa necesaria.
No Recuperable	La recuperación del incidente no es posible.

Tabla 6 Niveles de impacto a la capacidad de recuperación de un incidente según la NIST.

2.5.2 ENISA

La Agencia de Redes y Seguridad de la Información Europea (ENISA) en su Guía de Buenas Prácticas para la Gestión de Incidentes[27] durante las actividades denominadas "Triage" explica que se deben llevar a cabo 3 acciones: verificación (validar si es o no un incidente), clasificación inicial y asignación.

La priorización, con base en las recomendaciones de la ENISA es: "Es probable que no sea posible gestionar todos los incidentes, incluso en el máximo de efectividad operativa. Esto obliga a diferenciar los niveles de servicio. Es necesario dividir los tipos de incidentes por una priorización. […] Si se trata de un CERT privado (o un MSSP) con contratos comerciales para servicios de manejo de incidentes, el objetivo será entregar el mejor servicio para los clientes que pagan por el servicio. […] Otro factor que debe tomarse en cuenta en la priorización es a severidad inherente de un incidente. […] Este mecanismo debe de ser lo más simple posible."

ENISA recomiendan crear una matriz como se muestra en la Tabla 7 basado en la severidad del ataque:

[27] Miroslaw Maj MSc, Roeland Reijers y Don Stikvoort MSc. (2010). Good Practice Guide for Incident Management. Recuperado 22 de octubre, 2016, de ENISA Sitio web: https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management

Group	Severity	Examples
RED	Very High	DDoS, phishing site
YELLOW	High	Trojan distribution, unauthorised modification of information
ORANGE	Normal	Spam, copyright issue

Tabla 7 Priorización básica de incidentes por la severidad del ataque según la ENISA.

Y otra solución para la priorización es una matriz que combine la importancia del cliente y la severidad del ataque, como se muestra en la Tabla 7:

PRIORITY	.GOV ORGANISATION	SLA CUSTOMER	OTHERS
RED	1	1	2
YELLOW	2	1	3
ORANGE	3	2	3

Tabla 8 Priorización básica de incidentes por el tipo de miembro del constituyente (cliente).

- Latvia CERT NIC-LV[28]. Esta taxonomía consiste en 11 tipos de ataques a la seguridad en internet, y fue creado a partir de la experiencia de esta organización:
    1. Ataque a infraestructura crítica
    2. Ataques a la infraestructura de internet
    3. Ataques persistentes deliberados a recursos específicos
    4. Ataques automatizados generalizados contra sitios de internet
    5. Amenazas, acoso y otras ofensas criminales donde se involucran cuentas individuales
    6. Nuevos tipos de ataques o vulnerabilidades
    7. "Botnets"
    8. Negación de servicio hacia cuentas de usuarios individuales
    9. Falsificaciones y violaciones a reglas locales
    10. Compromiso de equipos individuales
    11. Violaciones de derechos de autor
- CERT-Hungary. Basada en el origen del reporte de incidente, y consiste de 4 categorías:
    1. CIIP Nacional (institución)
    2. CIIP socio con Niveles de Servicio (SLA)
    3. Reporte realizado por socio internacional
    4. Amenazas e incidentes reportados por organizaciones cooperativas.
- Common Language[29]. Este es un modelo abierto desarrollado por la Sandia National Laboratories. Esta taxonomía está compuesta por 3 términos principales (ver Fig. 19):
    a. Evento
    b. Ataque

[28] CERT NIC.LV team, (s.f), Recuperado 10 de octubre, 2016, de Sitio web: http://cert.nic.lv/
[29] John D. Howard, Thomas A. Longstaff. (1998). A Common Language for Computer Security Incidents. Recuperado 22 de octubre, 2016, de Sandia National Laboratories Sitio web: http://prod.sandia.gov/techlib/access-control.cgi/1998/988667.pdf

c. Incidente

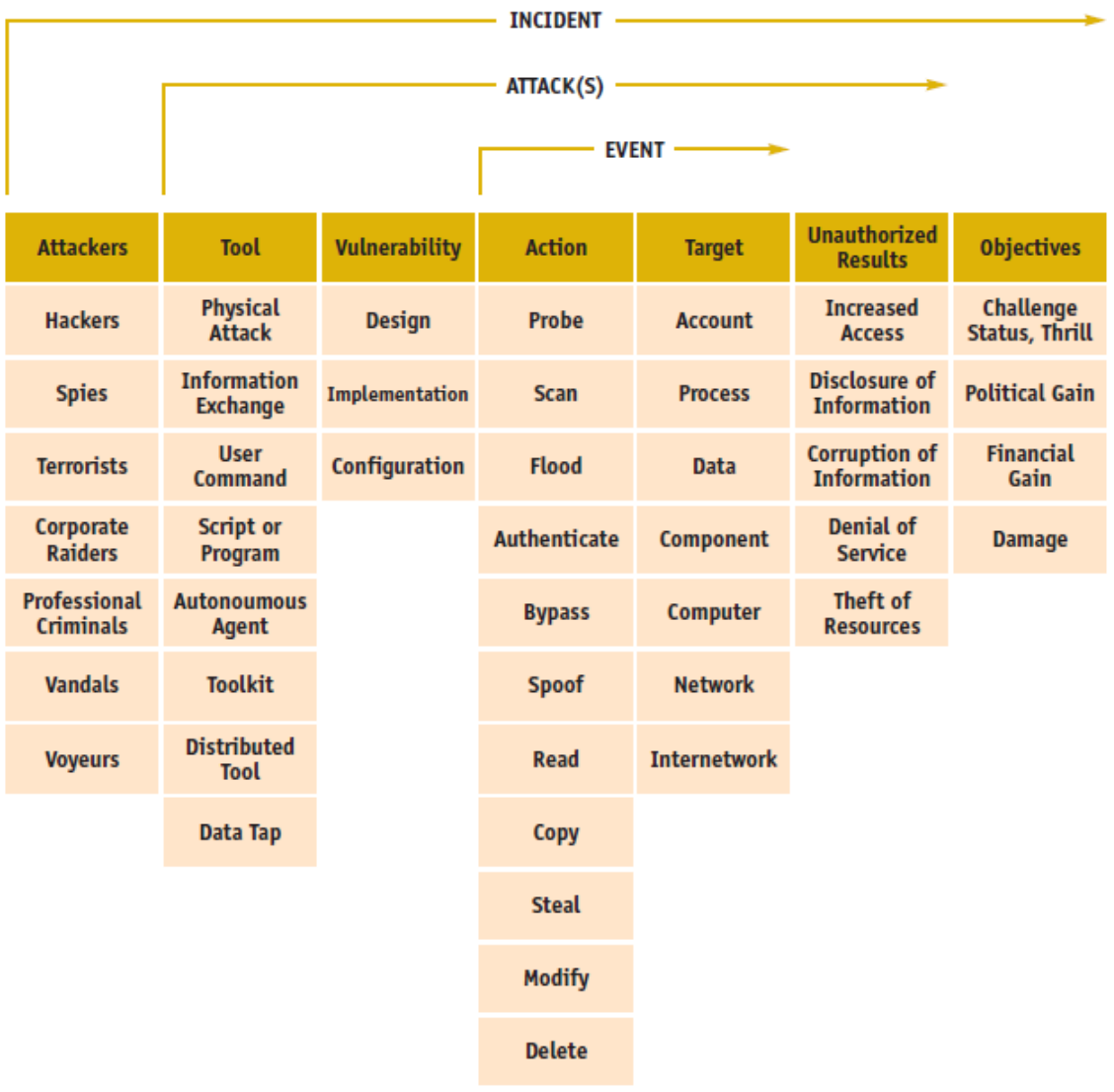


Fig. 19 Taxonomía de un incidente de seguridad según el Common Language.

- "CSIRT Network Project" eCSIRT[30].net esta taxonomía está basada en la taxonomía del CERT Sueco TS-CERT. Tiene 8 categorías o clases y 25 subcategorías o tipos
    a. Contenido Abusivo
    b. Código Malicioso
    c. Obtención de Información
    d. Intento de Intrusión
    e. Intrusión
    f. Disponibilidad
    g. Seguridad de la Información
    h. Fraude

[30] CSIRT Network Project, (s.f), Recuperado 10 de octubre, 2016, de Sitio web: http://www.ecsirt.net/

i. Otro

2.5.3 FIRST (Foro de Respuesta a Incidentes y Equipos de Seguridad)

Con base en la publicación denominada "CSIRT Case Classification (Example for Enterprise CSIRT)"[31] se establece la necesidad de que las organizaciones cuenten con un ITS (Sistema de Seguimiento a Incidentes) el cuál en muchas organizaciones es conocido como "herramienta de tickets" la cual permite crear un "caso" para darle seguimiento tanto a incidentes como a requerimientos, fallas, actividades programadas, etc.

Este documento establece que cualquier incidente gestionado por un CSIRT debe de ser clasificado en uno de las categorías listadas en la Tabla 9:

Categoría del Incidente	Sensibilidad
Negación de Servicio	S3
Forensia	S1
Información Comprometida	S1
Activo Comprometido	S1, S2
Actividad Ilegal	S1
"Hacking" Interno	S1, S2, S3
"Hacking" Externo	S1, S2, S3
"Malware"	S3
Correo electrónico	S3
Consultoría	S1, S2, S3
Violación de políticas	S1, S2, S3

Tabla 9 Categorías de incidente y su nivel de sensibilidad según la FIRST.

La Sensibilidad se refiere a una matriz que ayuda a definir la "necesidad de saber" (principio de la seguridad de la información que hace referencia a que solo las personas autorizadas o que necesiten saber de un asunto, sean los únicos informados dependiendo de su jerarquía o rol específico dentro de una organización) al clasificar los casos dependiendo de su nivel de sensibilidad como se muestra en la Tabla 10.

[31] Gavin Reid, Dustin Schieber y Ivo Peixinho. (2004). CSIRT Case Classification (Example for Enterprise CSIRT). Recuperado 10 de octubre, 2016, de FIRST.ORG Sitio web: https://www.first.org/_assets/resources/guides/csirt_case_classification.html

Nivel de Sensibilidad	Definición de nivel de Sensibilidad	Categoría Típica de Incidentes	Necesidad de Saber
1	Extremadamente Sensible	• Investigación Global Iniciada • Solicitud de Forensia • Destrucción de Propiedad • Activos Comprometidos • Información Comprometida • Actividades Ilegales • Uso Inapropiado de Propiedad • Violación de Políticas	Grupo 1 Individuo 1 Organización 1
2	Sensible	• "Hacking" Externo • "Hacking" Interno • Acceso No Autorizado	Grupo 2 Individuo 2 Organización 2
3	No Sensible	• Negación de Servicio • Virus/Gusanos • Correo Electrónico	Grupo 3 Individuo 3 Organización 3

Tabla 10 Definición de los niveles de sensibilidad de incidente según la FIRST.

En este caso se observa como esta matriz puede ser interpretada también como una matriz de contactos en caso de cierta tipificación de incidentes.

Por último, la FIRST propone la existencia de 3 niveles de clasificación de criticidad de un incidente y con base en ello la definición de tiempos de respuesta inicial aceptables, y los requerimientos de comunicación de cada nivel como se muestra en la Tabla 11.

Nivel de Criticidad	Definición	Tiempo de Respuesta Inicial	Tipo de respuesta
1	Afectación a sistemas críticos o con impacto a ingresos.	60 minutos	24/7
2	Afectación a sistemas no-críticos o ingresos. Investigaciones de personal.	4 horas	24/7
3	Posible incidente a sistemas no-críticos. Investigaciones a largo plazo	48 horas	ASAP

Tabla 11 Definición de niveles de criticidad de un incidente y tiempos de respuesta inicial según la FIRST.

2.5.4 US-CERT Lineamientos para la notificación de incidentes federales

Esta organización en su publicación de 2014[32] establece la información que debe de ser enviada al US-CERT como parte de una notificación de incidente:

- Identificación del impacto funcional (basado en NIST)
- Identificación del impacto a la información (basado en NIST)
- Identificación del impacto a la capacidad de recuperación (basado en NIST)

[32] US-CERT. (2014). US-CERT Federal Incident Notification Guidelines. Recuperado 17 de octubre, 2016, de US-CERT Sitio web: https://www.us-cert.gov/incident-notification-guidelines

- Identificación del vector de amenaza (se mostrará a continuación)
- Proveer detalles de la mitigación
- Proveer información de contacto

En este caso el US-CERT establece la taxonomía del vector de amenaza que ellos usan para la gestión de incidentes y que es similar a las que hemos visto anteriormente, con diferentes en algunas de las categorías listadas como puede verse en la Tabla 12:

Vector de Amenaza	Descripción
Desconocido	Causa no identificada
Desgaste	Uso de métodos de fuerza bruta, degradación o destrucción
Web	Ataque hacia aplicaciones web
Correo Electrónico	Ejecución de ataques usando correos electrónicos y sus anexos
Medios Externos/Removibles	Ataques desde periféricos o dispositivos removibles
Suplantación de Identidad	Ataque que involucra el reemplazo de una identidad legítima
Uso Inapropiado	Violación de las políticas de uso aceptable
Pérdida o Robo de Equipo	Pérdida o robo de dispositivos
Otro	Cualquier que no caiga en las anteriores.

Tabla 12 Taxonomía de la clasificación de incidentes con base en su vector de amenaza según el US-CERT

2.6 Graficas de tipo radial

De acuerdo a la descripción de Microsoft[33] para las gráficas radiales: "El tipo de gráfico radial es un gráfico circular que se utiliza principalmente como herramienta de comparación de datos. A veces, se denomina también gráfico de araña o gráfico de estrella. El área de trazado también se puede mostrar como un polígono.".

Este tipo de gráficos permite una comparación visual basado en el área de cada objeto evaluado. Como se trata de áreas, es indispensable que los objetos sean evaluados en por lo menos 3 aspectos para poder generar un polígono con un área determinada. Normalmente para este tipo de gráficos es mas conveniente utilizar aspectos de evaluación con escalas en números enteros positivos y el cero, donde una evaluación mayor represente un mayor cumplimiento con el aspecto evaluado. Con base en lo anterior, el polígono de mayor área indica que el objeto evaluado tiene mejores ponderaciones en comparación con los demás objetivos.

En la siguiente ilustración de ejemplo se muestra un comparativo superpuesto de objetos evaluados en una gráfica radial, donde cada polígono de diferente color representa un objeto evaluado distinto y cada arista del polígono representa un aspecto evaluado diferente para cada objeto. (Ver Fig. 20)

[33] Microsoft Corporation. (s.f.). Gráfico radial. Recuperado 30 marzo, 2018, de https://msdn.microsoft.com/es-es/library/dd489241.aspx

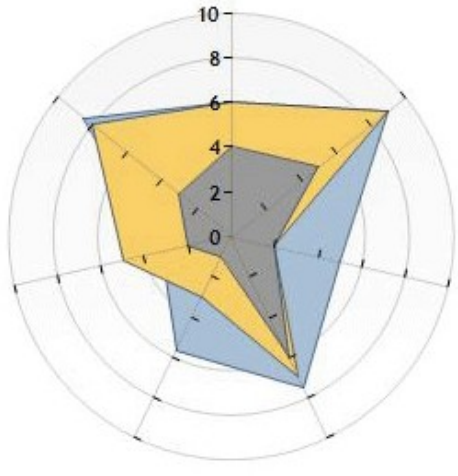


Fig. 20 Ejemplo de gráfico radial comparando 3 objetos en 7 aspectos diferentes..

Capítulo 3. Propuesta de implementación

En esta sección se revisará la metodología usada para la identificación de la solución propuesta, así como los criterios de selección, herramientas usadas y las consideraciones tomadas en cuenta para el diseño de una propuesta de solución general y otra localizada para el contexto de Sm4rt Security Services.

3.1 Metodología

En términos generales se realizaron las siguientes actividades que serán detalladas posteriormente.

1. Identificación de modelos candidatos a ser implementados para
    a. Priorización
    b. Clasificación de incidentes de seguridad
2. Marco de evaluación de los modelos
3. Evaluación Individual de los modelos
4. Selección de modelo
5. Adaptación del modelo al contexto de Sm4rt

3.2 Resultados

3.2.1 Identificación de modelos

La identificación de modelos candidatos fue realizado durante la elaboración del marco teórico de este documento, a partir del cual se identificaron 3 modelos para la parte de priorización de incidentes y 4 para la clasificación de incidentes.

1. Priorización:
    a. Modelo 1
        i. Organización: ENISA
        ii. Descripción: Priorización basada en severidad de los ataques y tipo de organización afectada.
    b. Modelo 2
        i. Organización: NIST
        ii. Descripción: Priorización de incidentes basada en definición de los posibles impactos a la organización.
    c. Modelo 3
        i. Organización: FIRST
        ii. Descripción: Priorización basada en la criticidad de los sistemas afectados o en la pérdida económica.
2. Clasificación:
    a. Modelo 1
        i. Organización: ENISA y la “Sandía National Laboratories”
        ii. Descripción: Clasificación basada en características intrínsecas del Evento, Ataque e Incidentes.
    b. Modelo 2
        i. Organización: ENISA y la “European CSIRT Network”
        ii. Descripción: Clasificación basada en tipo de ataque y tipo de amenaza
    c. Modelo 3
        i. Organización: FIRST

ii. Descripción: Modelo basado en la conjunción de tipo de incidente y criticidad de la información afectada.

d. Modelo 4
   i. Organización: US-CERT
   ii. Descripción: Modelo basado en niveles de atención, localización, Impacto y Vector de Ataque.

3.2.2 Marco de evaluación de los modelos.

La evaluación de los modelos candidatos, tanto para priorización como categorización, se realizó a través de 4 aspectos generales y 15 aspectos particulares. Para cada uno de los 4 aspectos generales se definió su peso con respecto al 100%, los cuales se muestra en la Tabla 13Tabla 13:

Aspectos General	Porcentaje	Descripción
Utilidad	40%	Son criterios relacionados al grado de utilidad que el uso del modelo tendría en la operación del SOC.
Optimización	30%	Son criterios relacionados a los beneficios de optimización, principalmente de tiempos que el uso del modelo tendría en la operación del SOC.
Diferenciadores	20%	Son criterios relacionados con las ventajas competitivas, con respecto a los competidores locales, que el uso del modelo tendría en el servicio del SOC.
Factibilidad	10%	Son criterios relacionados con las facilidades que el modelo tienen para ser adaptado o usado por el personal del SOC y de Sm4rt.
	100%	

Tabla 13 Aspectos generales para la evaluación de los modelos

Cada uno de los aspectos generales fue desglosado en varios aspectos particulares los cuales tienen diferentes rangos de ponderación, principalmente en una escala del 1 al 5 con base en el grado de cumplimiento con el criterio. Cada uno de los modelos candidatos identificados en la etapa anterior fueron evaluados en cada uno de los 15 criterios específicos.

La lista de aspectos particulares se describe a continuación en la Tabla 14

Id	Aspecto	Criterio	Descripción	Rango de Evaluación
1	Optimización	¿Permite disminuir el tiempo de priorización o categorización de incidentes?	Se refiere a si la propuesta habilita la reducción de tiempos para la priorización o categorización de incidentes de seguridad.	Escala del 1 al 5
2	Optimización	¿Permite disminuir los tiempos de notificación al cliente?	Se refiere a si la propuesta habilita la reducción de tiempos para la notificación de incidentes de seguridad al cliente.	Escala del 1 al 5
3	Optimización	¿Permite disminuir los tiempos de análisis?	Se refiere a si la propuesta habilita la reducción de tiempos de análisis para la notificación de incidentes de seguridad al cliente.	Escala del 1 al 5
4	Utilidad	Facilidad de adaptación	Se refiere a la facilidad para hacer modificaciones al marco inicial propuesto, esto principalmente para agregar o quitar criterios, categorías, etc.	Escala del 1 al 5
5	Utilidad	¿Habilita la generación de estadísticas internas útiles?	Se refiere a que la utilización de la propuesta permite la obtención de estadísticas que habilitan la mejora continua de los servicios del SOC.	Escala del 1 al 5
6	Utilidad	¿Facilita la evaluación comparativa (“bechmark” en idioma inglés) de los servicios a nivel internacional?	Se refiere a que la utilización de la propuesta permite comparar las estadísticas de organizaciones internacionales con las estadísticas internas o de clientes.	Escala del 1 al 5
7	Utilidad	¿Habilita la generación de estadísticas útiles para los clientes?	Se refiere a que la utilización de la propuesta permite la generación de estadísticas que sean presentadas al cliente.	Escala del 1 al 5
8	Diferenciadores	Conveniencia de uso	Se refiere a que el uso de la propuesta permite alinearse con alguna regulación o marco de trabajo conveniente para Sm4rt o para sus clientes	Escala del 1 al 5
9	Diferenciadores	¿Habilita el intercambio de información con organizaciones en México?	Se refiere a que el uso de la propuesta habilita el intercambio de información acerca del estado de la seguridad de la información de las empresas tanto públicas como privadas en México	Escala del 1 al 5
10	Diferenciadores	¿Habilita el intercambio de información con organizaciones internacionales?	Se refiere a que el uso de la propuesta habilita el intercambio de información acerca del estado de la seguridad de la información de las empresas tanto públicas como privadas en el mundo.	Escala del 1 al 5
11	Factibilidad	¿Experiencia del equipo gerencial del SOC en el enfoque?	Se refiere al nivel de conocimiento previo que tiene el personal desde Gerencia hasta Dirección del SOC acerca del enfoque que usa	Escala del 1 al 5

Id	Aspecto	Criterio	Descripción	Rango de Evaluación
			la propuesta. Esto derivado de conocimiento formal y empírico en el ámbito de la seguridad de la información	
12	Factibilidad	¿Facilidad para capacitar al personal operativo del SOC?	Se refiere a si la propuesta es fácil de entender o intuitiva que permita al personal del SOC aprender fácilmente su uso.	Escala del 1 al 5
13	Factibilidad	¿Experiencia de la organización en el enfoque?	Se refiere al nivel de conocimiento previo que tiene el personal de Sm4rt Security Services acerca del enfoque que usa la propuesta. Esto derivado de conocimiento formal o empírico en el ámbito de la seguridad de la información.	Escala del 1 al 5
14	Factibilidad	¿Se requiere de una inversión económica para la implementación?	Se refiere a si la implementación de la propuesta tiene alguna implicación de tipo económica, ya sea para capacitaciones, licenciamientos, tecnología, etc.	Escala de 0 o 1
15	Factibilidad	Facilidad de preparación	Se refiere a que la propuesta tiene prerrequisitos que deben ser preparados previo a la implementación.	Escala del 1 al 5.

Tabla 14 Aspectos particulares para la evaluación de los modelos.

3.2.3 Evaluación Individual de los modelos

A continuación se muestra la evaluación de cada uno de los criterios para los modelos identificados como candidatos.

1. Priorización:

1.1. Modelo 1

1.1.1. Organización: ENISA

1.1.2. Descripción: Priorización basada en severidad de los ataques y tipo de organización afectada. Ver en la Tabla 15 la evaluación del modelo y en la Tabla 16 los resultados de la misma, así como la representación gráfica en la Fig. 21.

1.1.3. Prerrequisitos: Tener documentados los SLAs de todos los clientes de forma centralizada y una lista de Ataques base.

Id	Tipo	Criterio	Evaluación
1	Optimización	¿Permite disminuir el tiempo de priorización o categorización de incidentes?	4
2	Optimización	¿Permite disminuir los tiempos de notificación al cliente?	4
3	Optimización	¿Permite disminuir los tiempos de análisis?	4
4	Utilidad	Facilidad de adaptación	5
5	Utilidad	¿Habilita la generación de estadísticas internas útiles?	4
6	Utilidad	¿Facilita la evaluación comparativa (“bechmark” en idioma inglés) de los servicios a nivel internacional?	3
7	Utilidad	¿Habilita la generación de estadísticas útiles para los clientes?	5
8	Diferenciadores	Conveniencia de uso	3
9	Diferenciadores	¿Habilita el intercambio de información con organizaciones en México?	2
10	Diferenciadores	¿Habilita el intercambio de información con organizaciones internacionales?	3
11	Factibilidad	¿Experiencia del equipo gerencial del SOC en el enfoque?	4
12	Factibilidad	¿Facilidad para capacitar al personal operativo del SOC?	4
13	Factibilidad	¿Experiencia de la organización en el enfoque?	5
14	Factibilidad	¿Se requiere de una inversión económica para la implementación?	0
15	Factibilidad	Facilidad de preparación	4

Tabla 15 Evaluación del modelo basado en ENISA para la priorización de incidentes

Criterio	Sumatoria	Máximo	Ponderado
Optimización	12	15	24%
Utilidad	17	20	34%
Diferenciadores	8	15	5%
Factibilidad	17	21	16%
Total			80%

Tabla 16 Resultados de la evaluación del modelo basado en ENISA para la priorización de incidentes

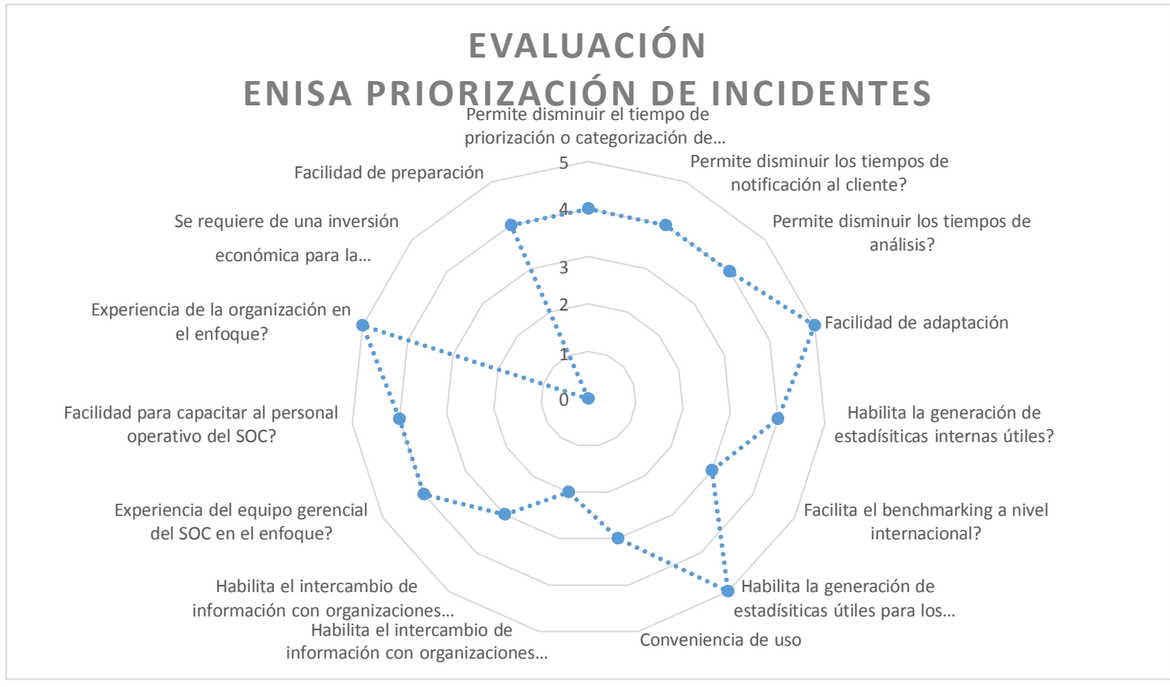


Fig. 21 Representación gráfica de los resultados de la evaluación del modelo basado en ENISA

1.2. Modelo 2

1.2.1. Organización: NIST

1.2.2. Descripción: Priorización de incidentes basada en definición de los posibles impactos a la organización. Ver en la Tabla 17 la evaluación del modelo y en la Tabla 18 los resultados de la misma, así como la representación gráfica en la Fig. 22.

1.2.3. Prerrequisitos: Matriz de criticidad de activos y/o aplicaciones de los clientes.

Id	Tipo	Criterio	Evaluación
1	Optimización	¿Permite disminuir el tiempo de priorización o categorización de incidentes?	3
2	Optimización	¿Permite disminuir los tiempos de notificación al cliente?	2
3	Optimización	¿Permite disminuir los tiempos de análisis?	2
4	Utilidad	Facilidad de adaptación	3
5	Utilidad	¿Habilita la generación de estadísticas internas útiles?	2
6	Utilidad	¿Facilita la evaluación comparativa (“bechmark” en idioma inglés) de los servicios a nivel internacional?	3
7	Utilidad	¿Habilita la generación de estadísticas útiles para los clientes?	4
8	Diferenciadores	Conveniencia de uso	4
9	Diferenciadores	¿Habilita el intercambio de información con organizaciones en México?	2
10	Diferenciadores	¿Habilita el intercambio de información con organizaciones internacionales?	3
11	Factibilidad	¿Experiencia del equipo gerencial del SOC en el enfoque?	3
12	Factibilidad	¿Facilidad para capacitar al personal operativo del SOC?	3
13	Factibilidad	¿Experiencia de la organización en el enfoque?	4
14	Factibilidad	¿Se requiere de una inversión económica para la implementación?	0
15	Factibilidad	Facilidad de preparación	2

Tabla 17 Evaluación del modelo basado en NIST para la priorización de incidentes

Criterio	Sumatoria	Máximo	Ponderado
Optimización	7	15	14%
Utilidad	12	20	24%
Diferenciadores	9	15	6%
Factibilidad	12	21	11%
Total			55%

Tabla 18 Resultados de la evaluación del modelo basado en NIST para la priorización de incidentes

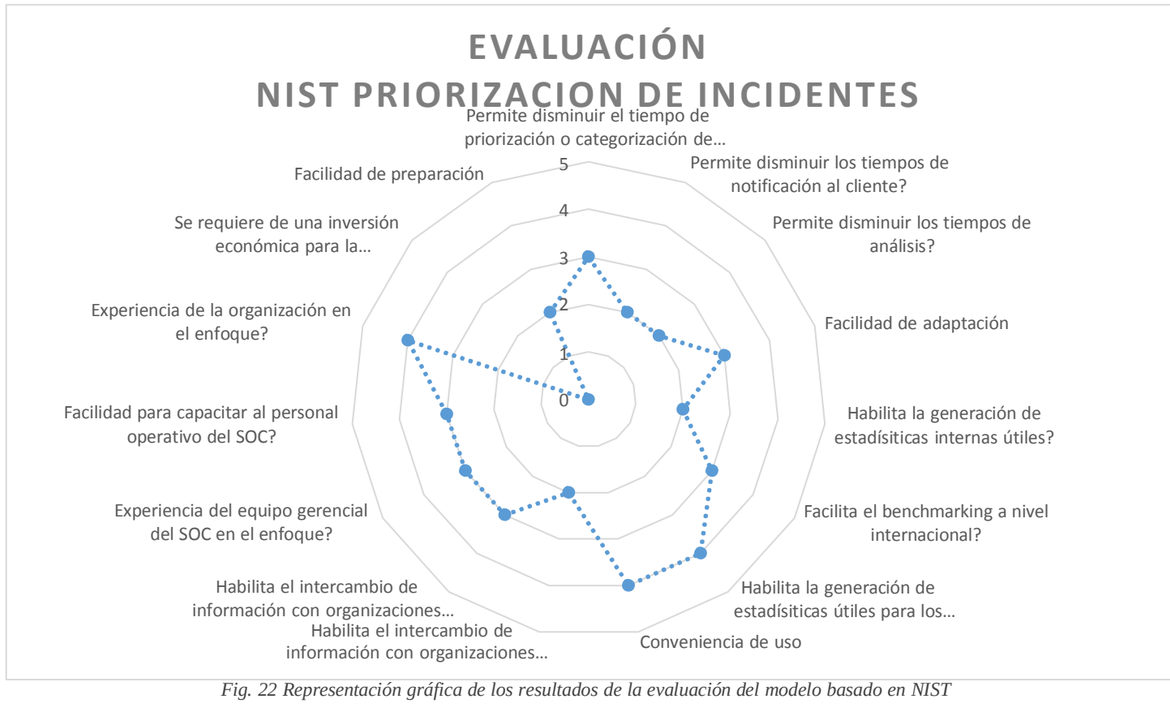


Fig. 22 Representación gráfica de los resultados de la evaluación del modelo basado en NIST

1.3. Modelo 3

1.3.1. Organización: FIRST

1.3.2. Descripción: Priorización basada en la criticidad de los sistemas afectados o en la pérdida económica. Ver en la Tabla 19 la evaluación del modelo y en la Tabla 20 los resultados de la misma, así como la representación gráfica en la Fig. 23.

1.3.3. Prerrequisitos: Matriz de criticidad de activos. Matriz de riesgos de cada cliente. Estimaciones económicas de riesgos.

Id	Tipo	Criterio	Evaluación
1	Optimización	¿Permite disminuir el tiempo de priorización o categorización de incidentes?	2
2	Optimización	¿Permite disminuir los tiempos de notificación al cliente?	4
3	Optimización	¿Permite disminuir los tiempos de análisis?	4
4	Utilidad	Facilidad de adaptación	2
5	Utilidad	¿Habilita la generación de estadísticas internas útiles?	2
6	Utilidad	¿Facilita la evaluación comparativa (“bechmark” en idioma inglés) de los servicios a nivel internacional?	1
7	Utilidad	¿Habilita la generación de estadísticas útiles para los clientes?	5
8	Diferenciadores	Conveniencia de uso	3
9	Diferenciadores	¿Habilita el intercambio de información con organizaciones en México?	2
10	Diferenciadores	¿Habilita el intercambio de información con organizaciones internacionales?	2
11	Factibilidad	¿Experiencia del equipo gerencial del SOC en el enfoque?	3
12	Factibilidad	¿Facilidad para capacitar al personal operativo del SOC?	3
13	Factibilidad	¿Experiencia de la organización en el enfoque?	3
14	Factibilidad	¿Se requiere de una inversión económica para la implementación?	0
15	Factibilidad	Facilidad de preparación	1

Tabla 19 Evaluación del modelo basado en FIRST para la priorización de incidentes

Criterio	Sumatoria		Máximo	Ponderado
Optimización	10		15	20%
Utilidad	10		20	20%
Diferenciadores	7		15	5%
Factibilidad	10		21	10%
Total				54%

Tabla 20 Resultados de la evaluación del modelo basado en FIRST para la priorización de incidentes

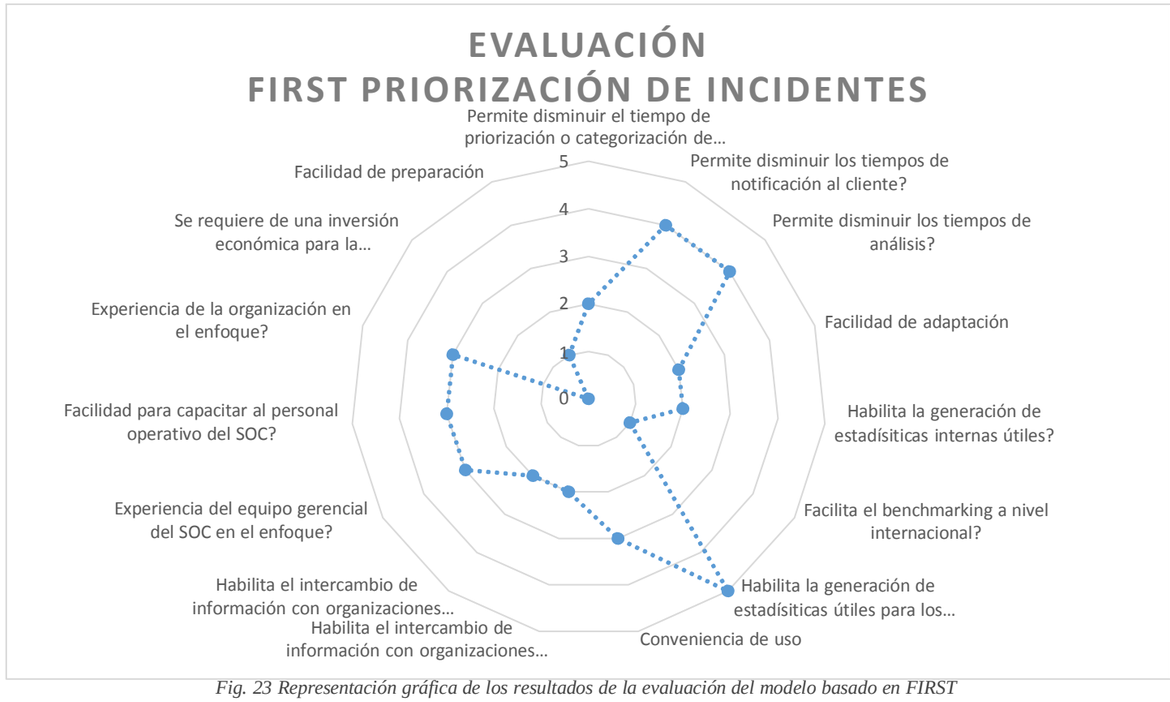


Fig. 23 Representación gráfica de los resultados de la evaluación del modelo basado en FIRST

2. Clasificación:

2.1. Modelo 1

2.1.1. Organización: ENISA y la “Sandía National Laboratories” – “Common Language Security Incident Taxonomy”

2.1.2. Descripción: Clasificación basada en características intrínsecas del Evento, Ataque e Incidentes. Ver en la Tabla 21 la evaluación del modelo y en la Tabla 22 los resultados de la misma, así como la representación gráfica en la Fig. 24.

2.1.3. Prerrequisitos: Preclasificación de Atacantes, Alta retroalimentación del cliente, Inventarios tecnológicos.

Id	Tipo	Criterio	Evaluación
1	Optimización	¿Permite disminuir el tiempo de priorización o categorización de incidentes?	2
2	Optimización	¿Permite disminuir los tiempos de notificación al cliente?	3
3	Optimización	¿Permite disminuir los tiempos de análisis?	1
4	Utilidad	Facilidad de adaptación	4
5	Utilidad	¿Habilita la generación de estadísticas internas útiles?	5
6	Utilidad	¿Facilita la evaluación comparativa (“bechmark” en idioma inglés) de los servicios a nivel internacional?	4
7	Utilidad	¿Habilita la generación de estadísticas útiles para los clientes?	2
8	Diferenciadores	Conveniencia de uso	2
9	Diferenciadores	¿Habilita el intercambio de información con organizaciones en México?	2
10	Diferenciadores	¿Habilita el intercambio de información con organizaciones internacionales?	3
11	Factibilidad	¿Experiencia del equipo gerencial del SOC en el enfoque?	4
12	Factibilidad	¿Facilidad para capacitar al personal operativo del SOC?	2
13	Factibilidad	¿Experiencia de la organización en el enfoque?	4
14	Factibilidad	¿Se requiere de una inversión económica para la implementación?	0
15	Factibilidad	Facilidad de preparación	2

Tabla 21 Evaluación del modelo basado en ENISA-Sandia para la clasificación de incidentes

Criterio	Sumatoria	Máximo	Ponderado
Optimización	6	15	12%
Utilidad	15	20	30%
Diferenciadores	7	15	5%
Factibilidad	12	21	11%
Total			58%

Tabla 22 Resultados de la evaluación del modelo basado en ENISA-Sandia para la clasificación de incidentes

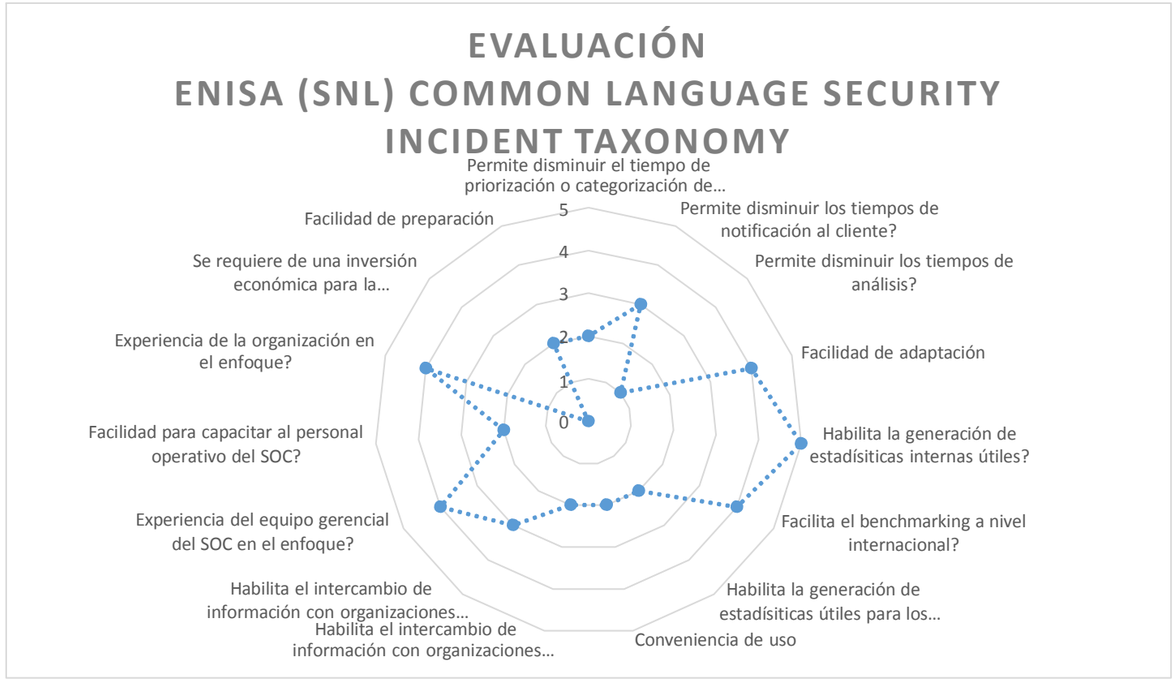


Fig. 24 Representación gráfica de los resultados de la evaluación del modelo basado en ENISA-Sandia

2.2. Modelo 2

2.2.1. Organización: ENISA y la European CSIRT Network

2.2.2. Descripción: Clasificación basada en tipo de ataque y tipo de amenaza. Ver en la Tabla 23 la evaluación del modelo y en la Tabla 24 los resultados de la misma, así como la representación gráfica en la Fig. 25.

2.2.3. Prerrequisitos: Sólida definición de cada clase y amenaza. Capacitación técnica

Id	Tipo	Criterio	Evaluación
1	Optimización	¿Permite disminuir el tiempo de priorización o categorización de incidentes?	4
2	Optimización	¿Permite disminuir los tiempos de notificación al cliente?	3
3	Optimización	¿Permite disminuir los tiempos de análisis?	3
4	Utilidad	Facilidad de adaptación	5
5	Utilidad	¿Habilita la generación de estadísticas internas útiles?	5
6	Utilidad	¿Facilita la evaluación comparativa (“bechmark” en idioma inglés) de los servicios a nivel internacional?	4
7	Utilidad	¿Habilita la generación de estadísticas útiles para los clientes?	3
8	Diferenciadores	Conveniencia de uso	3
9	Diferenciadores	¿Habilita el intercambio de información con organizaciones en México?	3
10	Diferenciadores	¿Habilita el intercambio de información con organizaciones internacionales?	3
11	Factibilidad	¿Experiencia del equipo gerencial del SOC en el enfoque?	4
12	Factibilidad	¿Facilidad para capacitar al personal operativo del SOC?	2
13	Factibilidad	¿Experiencia de la organización en el enfoque?	5
14	Factibilidad	¿Se requiere de una inversión económica para la implementación?	0
15	Factibilidad	Facilidad de preparación	3

Tabla 23 Evaluación del modelo basado en ENISA-eCIRT para la clasificación de incidentes

Criterio	Sumatoria	Máximo	Ponderado
Optimización	10	15	20%
Utilidad	17	20	34%
Diferenciadores	9	15	6%
Factibilidad	14	21	13%
Total			73%

Tabla 24 Resultados de la evaluación del modelo basado en ENISA-eCIRT para la clasificación de incidentes

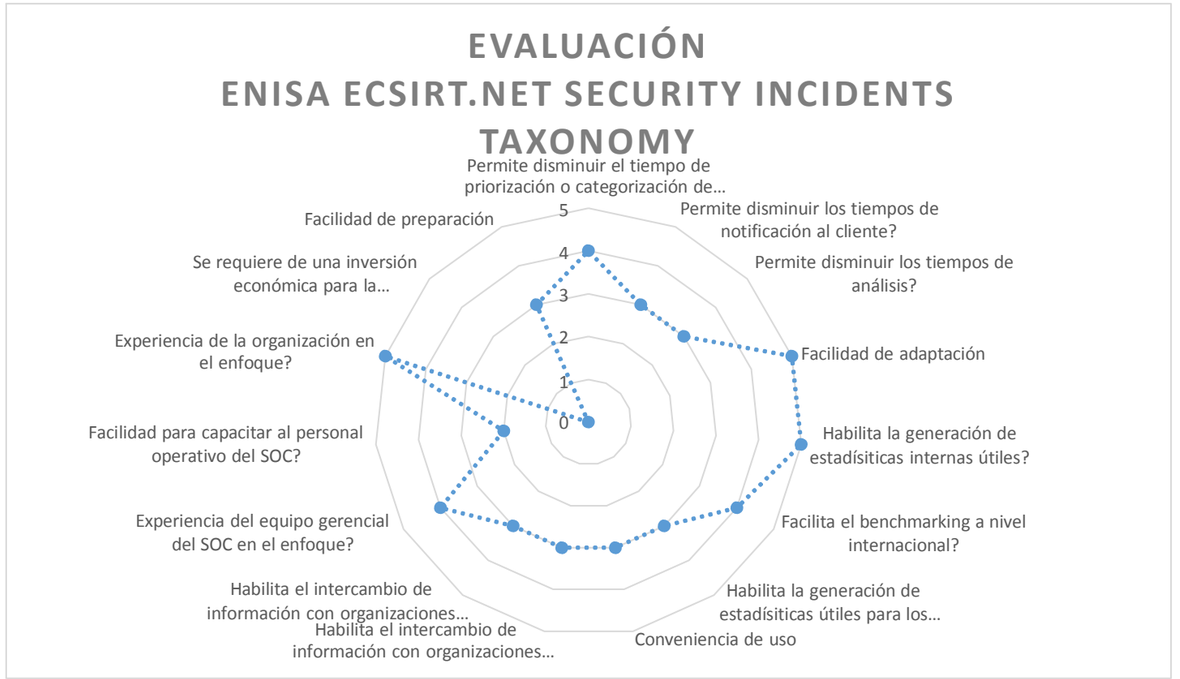


Fig. 25 Representación gráfica de los resultados de la evaluación del modelo basado en ENISA-eCIRT

2.3. Modelo 3

2.3.1. Organización: FIRST

2.3.2. Descripción: Modelo basado en la conjunción de tipo de incidente y criticidad de la información afectada. Ver en la Tabla 25 la evaluación del modelo y en la Tabla 26 los resultados de la misma, así como la representación gráfica en la Fig. 26.

2.3.3. Prerrequisitos: Inventario de datos y sistemas críticos.

Id	Tipo	Criterio	Evaluación
1	Optimización	¿Permite disminuir el tiempo de priorización o categorización de incidentes?	2
2	Optimización	¿Permite disminuir los tiempos de notificación al cliente?	3
3	Optimización	¿Permite disminuir los tiempos de análisis?	2
4	Utilidad	Facilidad de adaptación	3
5	Utilidad	¿Habilita la generación de estadísticas internas útiles?	2
6	Utilidad	¿Facilita la evaluación comparativa (“bechmark” en idioma inglés) de los servicios a nivel internacional?	2
7	Utilidad	¿Habilita la generación de estadísticas útiles para los clientes?	3
8	Diferenciadores	Conveniencia de uso	2
9	Diferenciadores	¿Habilita el intercambio de información con organizaciones en México?	1
10	Diferenciadores	¿Habilita el intercambio de información con organizaciones internacionales?	2
11	Factibilidad	¿Experiencia del equipo gerencial del SOC en el enfoque?	4
12	Factibilidad	¿Facilidad para capacitar al personal operativo del SOC?	3
13	Factibilidad	¿Experiencia de la organización en el enfoque?	4
14	Factibilidad	¿Se requiere de una inversión económica para la implementación?	0
15	Factibilidad	Facilidad de preparación	3

Tabla 25 Evaluación del modelo basado en FIRST para la clasificación de incidentes

Criterio	Sumatoria	Máximo	Ponderado
Optimización	7	15	14%
Utilidad	10	20	20%
Diferenciadores	5	15	3%
Factibilidad	14	21	13%
Total			51%

Tabla 26 Resultados de la evaluación del modelo basado en FIRT para la clasificación de incidentes

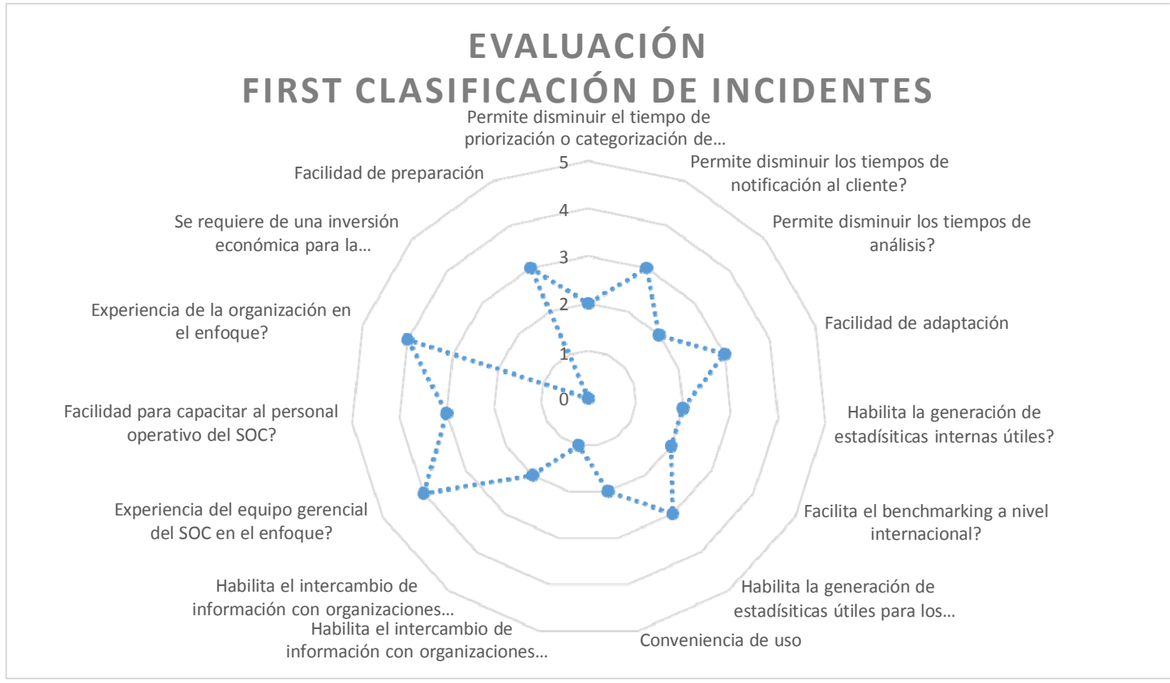


Fig. 26 Representación gráfica de los resultados de la evaluación del modelo basado en FIRST

2.4. Modelo 4

2.4.1. Organización: US-CERT

2.4.2. Descripción: Modelo basado en niveles de atención, localización, Impacto y Vector de Ataque. Ver en la Tabla 27 la evaluación del modelo y en la Tabla 28 los resultados de la misma, así como la representación gráfica en la Fig. 27.

2.4.3. Prerrequisitos: Inventario perimetral, de datos y de activos principales del cliente.

Id	Tipo	Criterio	Evaluación
1	Optimización	¿Permite disminuir el tiempo de priorización o categorización de incidentes?	4
2	Optimización	¿Permite disminuir los tiempos de notificación al cliente?	4
3	Optimización	¿Permite disminuir los tiempos de análisis?	3
4	Utilidad	Facilidad de adaptación	5
5	Utilidad	¿Habilita la generación de estadísticas internas útiles?	5
6	Utilidad	¿Facilita la evaluación comparativa (“bechmark” en idioma inglés) de los servicios a nivel internacional?	4
7	Utilidad	¿Habilita la generación de estadísticas útiles para los clientes?	4
8	Diferenciadores	Conveniencia de uso	5
9	Diferenciadores	¿Habilita el intercambio de información con organizaciones en México?	4
10	Diferenciadores	¿Habilita el intercambio de información con organizaciones internacionales?	5
11	Factibilidad	¿Experiencia del equipo gerencial del SOC en el enfoque?	4
12	Factibilidad	¿Facilidad para capacitar al personal operativo del SOC?	3
13	Factibilidad	¿Experiencia de la organización en el enfoque?	4
14	Factibilidad	¿Se requiere de una inversión económica para la implementación?	0
15	Factibilidad	Facilidad de preparación	4

Tabla 27 Evaluación del modelo basado en US-CERT para la clasificación de incidentes

Criterio	Sumatoria	Máximo	Ponderado
Optimización	11	15	22%
Utilidad	18	20	36%
Diferenciadores	14	15	9%
Factibilidad	15	21	14%
Total			82%

Tabla 28 Resultados de la evaluación del modelo basado en US-CERT para la clasificación de incidentes

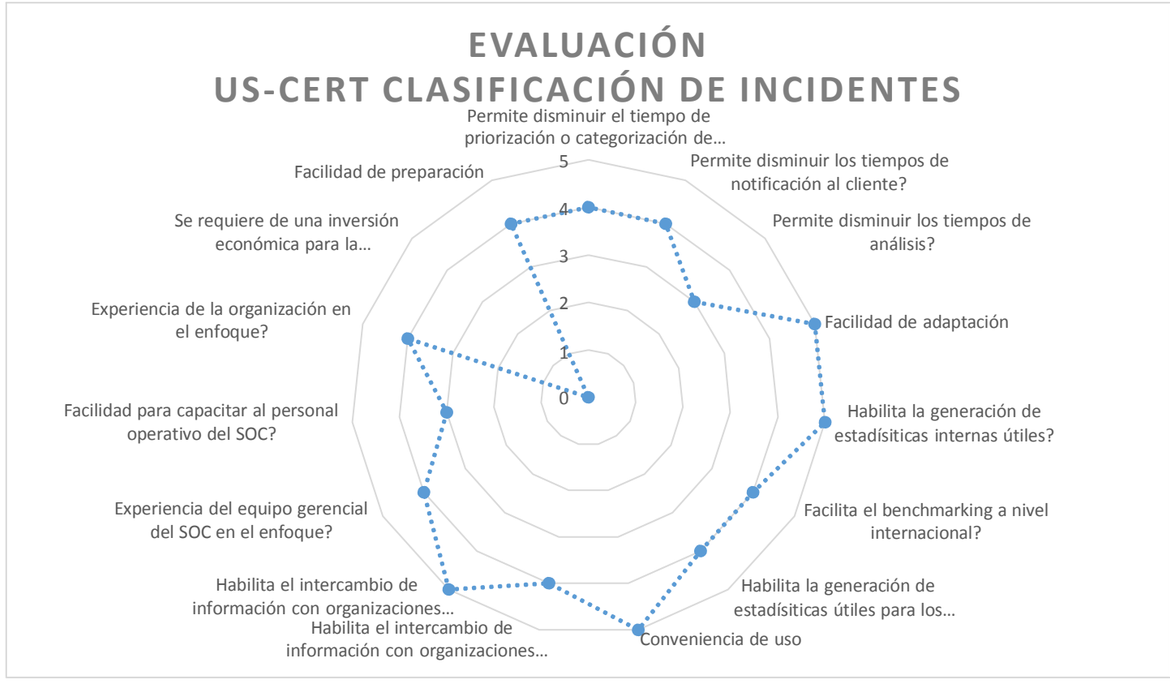


Fig. 27 Representación gráfica de los resultados de la evaluación del modelo basado en US-CERT

3.2.4 Selección de modelos

Para elegir el modelo a ser usado para la priorización y clasificación de incidentes se tomó en cuenta la sumatoria de los resultados ponderados de cada evaluación de los modelos candidatos evaluados en una escala de 100%. Adicional a esto se hizo una comparativa con base en las áreas de las gráficas de evaluación radial. Esta representación radial permite visualizar cuál de los modelos fue evaluado de mejor forma con base en los criterios definidos.

1. Evaluación para comparar modelos de priorización. En la Tabla 29 y la Fig. 28 se muestran los resultados en comparativa radial sobrepuesta y el grado de cumplimiento de cada Aspecto General evaluado con base en los criterios específicos para los modelos de priorización.

Id	Tipo	Criterio	P1 ENISA	P2 NIST	P3 FIRST
1	Optimización	¿Permite disminuir el tiempo de priorización o categorización de incidentes?	4	3	2
2	Optimización	¿Permite disminuir los tiempos de notificación al cliente?	4	2	4
3	Optimización	¿Permite disminuir los tiempos de análisis?	4	2	4
4	Utilidad	Facilidad de adaptación	5	3	2
5	Utilidad	¿Habilita la generación de estadísticas internas útiles?	4	2	2
6	Utilidad	¿Facilita la evaluación comparativa (“bechmark” en idioma inglés) de los servicios a nivel internacional?	3	3	1
7	Utilidad	¿Habilita la generación de estadísticas útiles para los clientes?	5	4	5
8	Diferenciadores	Conveniencia de uso	3	4	3
9	Diferenciadores	¿Habilita el intercambio de información con organizaciones en México?	2	2	2
10	Diferenciadores	¿Habilita el intercambio de información con organizaciones internacionales?	3	3	2
11	Factibilidad	¿Experiencia del equipo gerencial del SOC en el enfoque?	4	3	3
12	Factibilidad	¿Facilidad para capacitar al personal operativo del SOC?	4	3	3
13	Factibilidad	¿Experiencia de la organización en el enfoque?	5	4	3
14	Factibilidad	¿Se requiere de una inversión económica para la implementación?	0	0	0
15	Factibilidad	Facilidad de preparación	4	2	1

Tabla 29 Integración comparativa de las evaluaciones de los 3 modelos de priorización de incidentes.

A continuación se muestra la gráfica radial comparativa

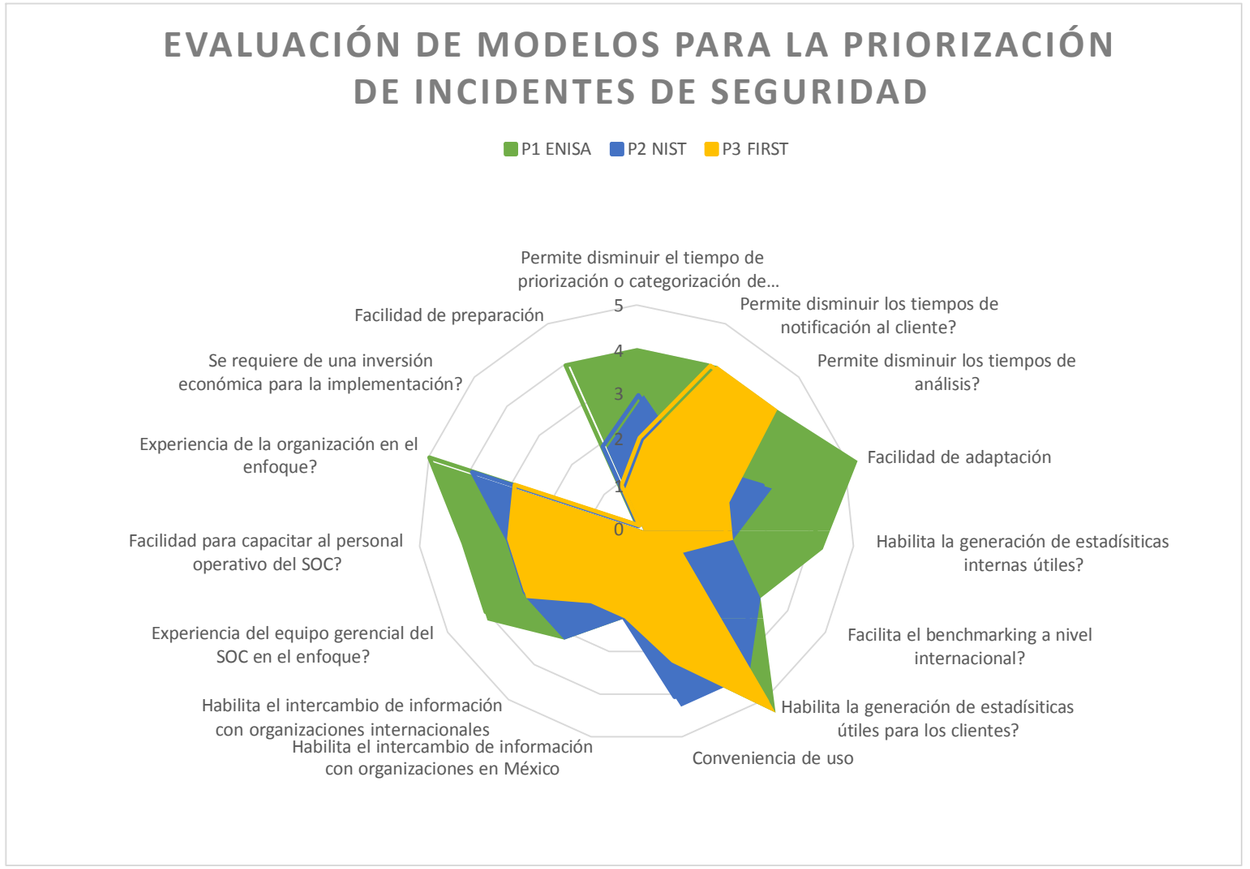


Fig. 28 Representación gráfica de la comparativa de las evaluaciones de los modelos de priorización de incidentes

En la Tabla 30 se muestra la comparativa de cada aspecto general evaluado en los modelos. Por otro lado, también se muestran en la Fig. 29 las representaciones gráficas de la evaluación general y la evaluación total de cada modelo

Criterio	Máximo	P1 ENISA	P2 NIST	P3 FIRST
Optimización	30%	24%	14%	20%
Utilidad	40%	34%	24%	20%
Diferenciadores	10%	5%	6%	5%
Factibilidad	20%	16%	11%	10%
Total	**100%**	**80%**	**55%**	**54%**

Tabla 30 Integración comparativa de las evaluaciones generales de los modelos de priorización de incidentes

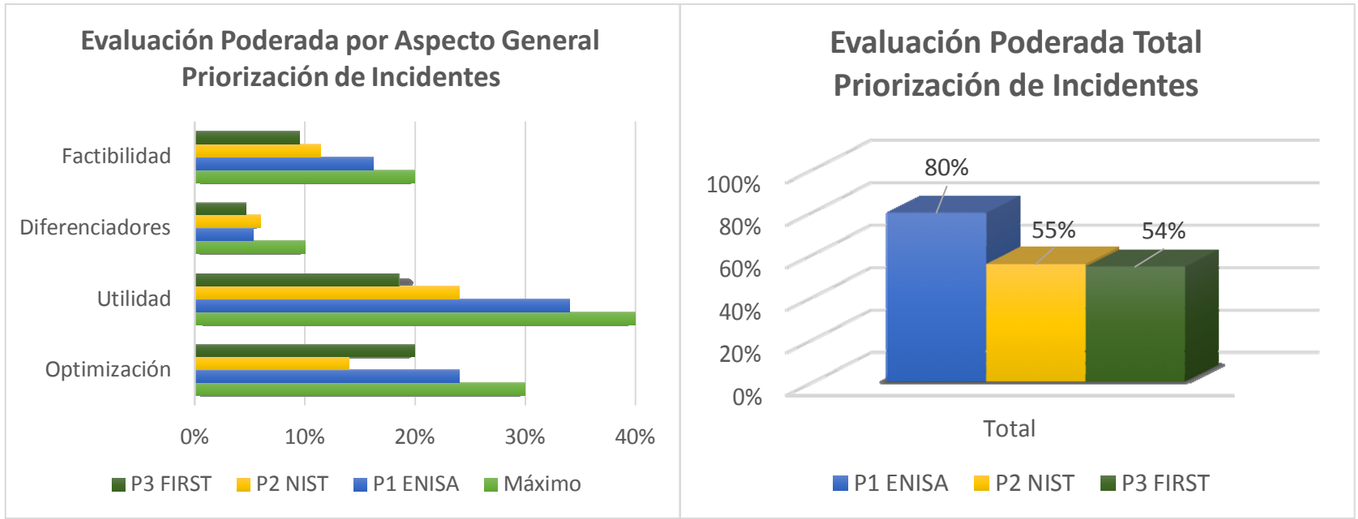


Fig. 29 Representaciones gráficas de las evaluaciones generales y totales de los modelos de priorización de incidentes

Con base en los resultados anteriores se puede observar que el modelo de priorización de incidentes de la ENISA es la que mejor cumple con los aspectos definidos para su evaluación por lo que será el Modelo que será adaptado al contexto de México y Sm4rt.

2. Evaluación compara de modelos de Clasificación: En la Tabla 31Tabla 29 y la Fig. 30 se muestran los resultados en comparativa radial sobrepuesta y el grado de cumplimiento de cada Aspecto General evaluado con base en los criterios específicos para los modelos de clasificación.

Id	Tipo	Criterio	C1 ENISA (SNL)	C2 ENISA (ECSIRT.NET)	C3 FIRST	C4 US-CERT
1	Optimización	¿Permite disminuir el tiempo de priorización o categorización de incidentes?	2	4	2	4
2	Optimización	¿Permite disminuir los tiempos de notificación al cliente?	3	3	3	4
3	Optimización	¿Permite disminuir los tiempos de análisis?	1	3	2	3
4	Utilidad	Facilidad de adaptación	4	5	3	5
5	Utilidad	¿Habilita la generación de estadísticas internas útiles?	5	5	2	5
6	Utilidad	¿Facilita la evaluación comparativa (“bechmark” en idioma inglés) de los servicios a nivel internacional?	4	4	2	4
7	Utilidad	¿Habilita la generación de estadísticas útiles para los clientes?	2	3	3	4
8	Diferenciadores	Conveniencia de uso	2	3	2	5
9	Diferenciadores	¿Habilita el intercambio de información con organizaciones en México?	2	3	1	4
10	Diferenciadores	¿Habilita el intercambio de información con organizaciones internacionales?	3	3	2	5
11	Factibilidad	¿Experiencia del equipo gerencial del SOC en el enfoque?	4	4	4	4
12	Factibilidad	¿Facilidad para capacitar al personal operativo del SOC?	2	2	3	3
13	Factibilidad	¿Experiencia de la organización en el enfoque?	4	5	4	4
14	Factibilidad	¿Se requiere de una inversión económica para la implementación?	0	0	0	0
15	Factibilidad	Facilidad de preparación	2	3	3	4

Tabla 31 Integración comparativa de las evaluaciones de los 4 modelos de clasificación de incidentes.

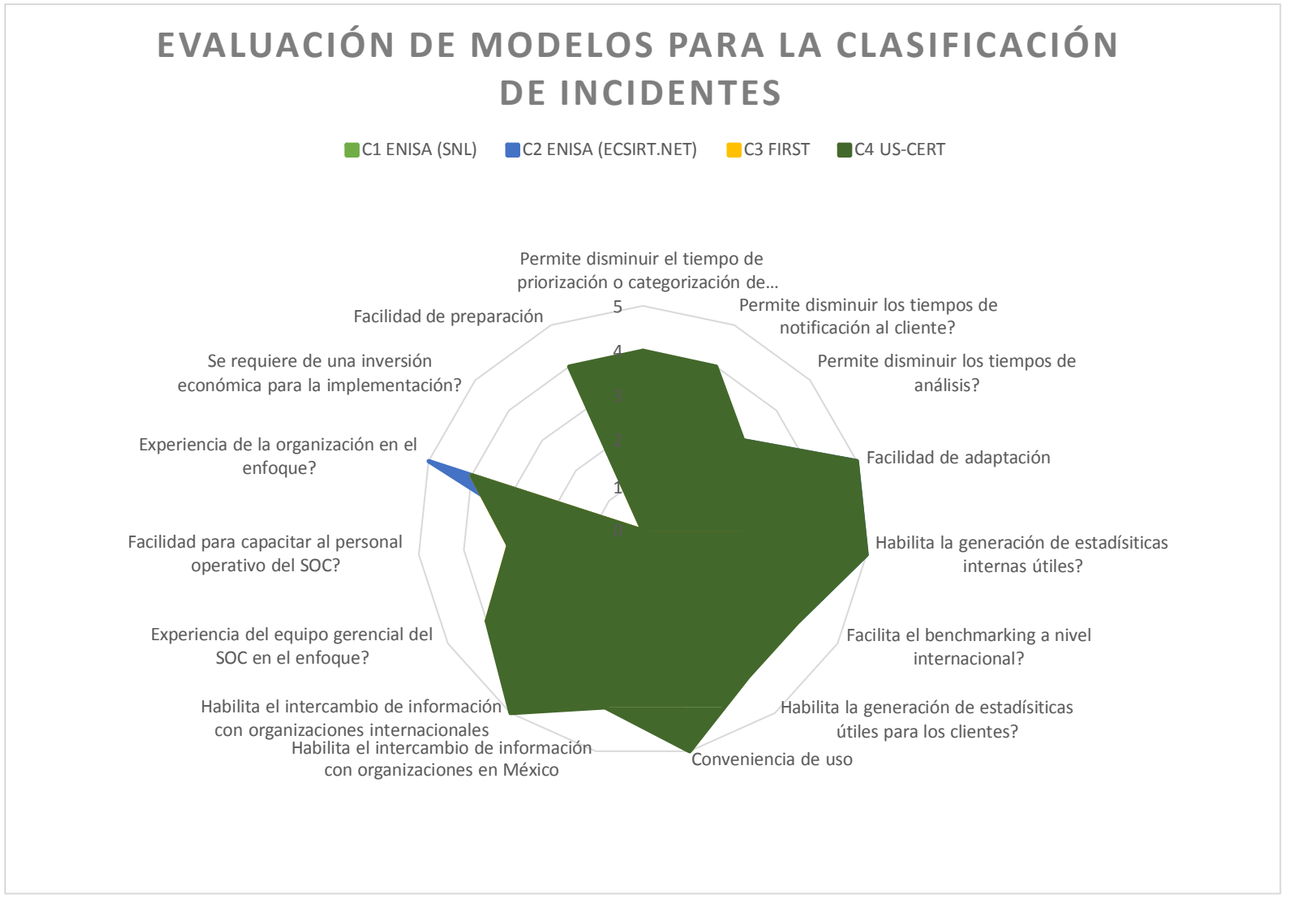


Fig. 30 Representación gráfica de la comparativa de las evaluaciones de los modelos de clasificación de incidentes

En la Tabla 32 se muestra la comparativa de cada aspecto general evaluado en los modelos. Por otro lado también se muestran en la Fig. 31 las representaciones gráficas de la evaluación general y la evaluación total de cada modelo

Criterio	Máximo	C1 ENISA (SNL)	C2 ENISA (ECSIRT.NET)	C3 FIRST	C4 US-CERT
Optimización	30%	12%	20%	14%	22%
Utilidad	40%	30%	34%	20%	36%
Diferenciadores	10%	5%	6%	3%	9%
Factibilidad	20%	11%	13%	13%	14%
Total	**100%**	**58%**	**73%**	**51%**	**82%**

Tabla 32 Integración comparativa de las evaluaciones generales de los modelos de clasificación de incidentes

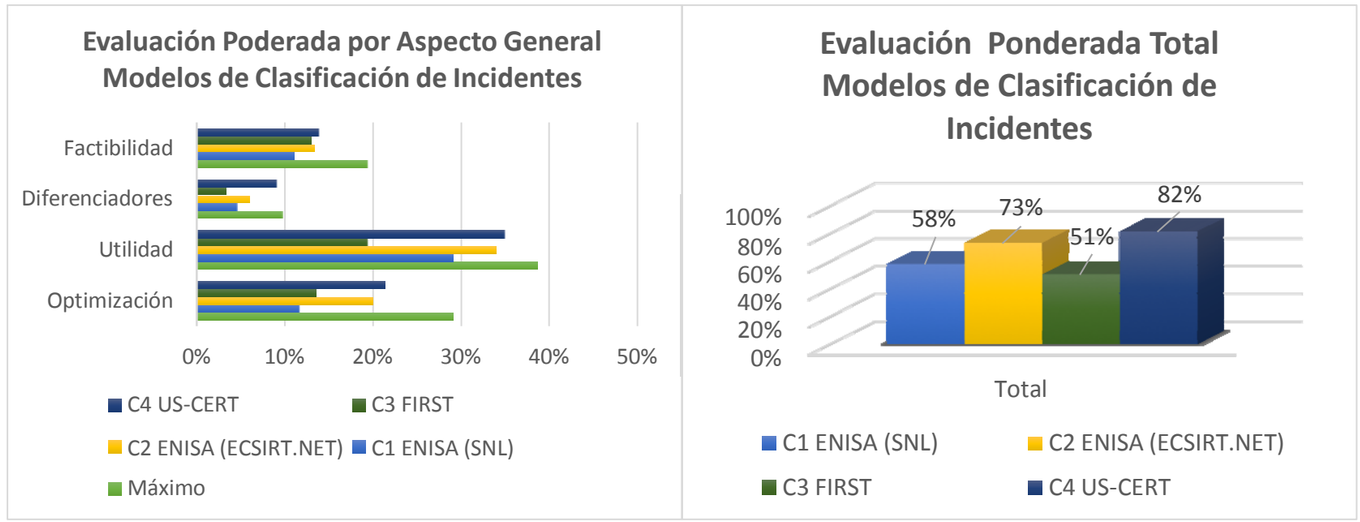


Fig. 31 Representaciones gráficas de las evaluaciones generales y totales de los modelos de clasificación de incidentes

Con base en los resultados anteriores se puede observar que el modelo de clasificación de incidentes del US-CERT es la que mejor cumple con los aspectos definidos para su evaluación por lo que será el modelo que será adaptado al contexto de México y Sm4rt.

3.2.5 Adaptación del modelo al contexto de Sm4rt

Los modelos seleccionados en las etapas anteriores, tanto para la priorización y clasificación de incidentes de seguridad, son por definición generales para poder ser aplicados a la mayoría de las industrias y organizaciones alrededor del mundo o país para el cuál fue diseñado.

En el caso de México no existe un modelo adaptado al contexto específico del país ni tampoco existe una organización pública o privada que establezca un lineamiento base para el uso de un modelo de priorización o clasificación de incidentes.

Con base en lo anterior tomaremos los modelos seleccionados y basados también en la experiencia y en los datos generados en Sm4rt Security Services al respecto de incidentes de seguridad, los tipos de clientes, tecnologías principales y el contexto del país se adaptarán estos modelos para ser propuestos como una innovación a la organización.

- Modelo de priorización de incidentes Sm4rt basado en lo propuesto por la ENISA por la combinación de tipos de ataques informáticos y el tipo de organización o niveles de SLA afectada.

Con base en este modelo se establece el uso de un enfoque de Cola Priorizada de Atención de Incidentes. El uso de una cola de incidentes implica que el primer incidente en entrar es el primero en ser atendido, mientras que en una cola priorizada se atienden primero los incidentes dependiendo de su priorización. En una cola priorizada cuando existen 2 incidentes de la misma prioridad, el primero en entrar a la cola es el primero en ser atendido. Con este acercamiento se pretende hacer un uso optimizado de los recursos limitados con los que cuenta el SOC para la atención de incidentes de seguridad.

Una representación gráfica de una cola priorizada de los incidentes se observa en la Fig. 32, donde se observan varios incidentes de diferentes prioridades que llegaron en diferentes momentos en el tiempo:

- Incidente #5
  - Hora de llegada: 12:20
- Incidente #2
  - Hora de llegada: 12:05
- Incidente #6
  - Hora de llegada: 12:25
- Incidente #1
  - Hora de llegada 12:00
- Incidente #4
  - hora de llegada 12:15
- Incidente #3
  - Hora de llegada 12:10

En este ejemplo se observan 6 incidentes que son identificados o reportados al SOC en un lapso de 30 minutos.

Asumiendo que solo hay 1 ingeniero analista del SOC para la atención de todos los incidentes y que no hay otros incidentes previos a la llegada del primer incidente: el incidente #1 de prioridad 2 es atendido inmediatamente a las 12:00 que es recibido. El siguiente incidente #2 de prioridad 3 recibido a las 12:05 es colocado en cola priorizada y será atendido una vez atendidos los incidentes de mayor prioridad. Sin embargo, a las 12:10 cuando se recibe el incidente #3 de prioridad 1, el analista coloca de nuevo al incidente #1 en la cola (antes que el incidente #2) para darle atención al incidente 3 que es de mayor prioridad de atención.

Fig. 32 Ejemplo de cola priorizada de incidentes

El incidente #4 de prioridad 1 es colocado justo después de atender al incidente #3. El incidente #5 de prioridad 3 es colocado posteriormente al incidente #2. El incidente #6 es colocado posteriormente al incidente #1 y antes del incidente #2 y del incidente #5.

Con base en lo anterior se establece la siguiente Tabla 33 que permite identificar el código de prioridad de un incidente con base en el tipo de identificado:

Clasificación Inicial del Incidente		
Código Prioridad	**Severidad**	**Tipo de Incidente**
Negro	Critica	Modificación no autorizada de información Negación de Servicio Deformación de Interfaces
Rojo	Alta	"Ransomware" Ejecución de Exploits o Zero-day Acceso no autorizado a información
Naranja	Media	Ataques de inyección "Spear Phishing" "Malware" Ataques web Abuso de configuraciones inseguras Suplantación de identidad
Amarillo	Normal	Escaneo de puertos o servicios Ataques a correo electrónico Ingeniería social

Tabla 33 Ejemplo de clasificación inicial de incidentes

En términos generales el código de prioridad se puede explicar de la siguiente forma:

- Negro. Son incidentes que afectan la integridad de la información o limitan la capacidad de operación de la infraestructura afectada o la reputación del cliente.
- Rojo. Son incidentes que afectan la confidencialidad de la información o de los cuales los controles de seguridad tecnológicos fue insuficiente.
- Naranja. Son incidentes que aprovechan controles de seguridad en infraestructura o del capital humano deficientes.
- Amarillo. Son incidentes que principalmente tienen el objetivo de obtener mayor información para efectuar un ataque posterior.

Con base al código de colores anteriormente descrito y relacionándolo con los diferentes tipos de cliente dependiendo de sus niveles de servicio o prioridad de atención se crea la siguiente Tabla 34 que muestra la prioridad de en la cola priorizada de atención de incidentes:

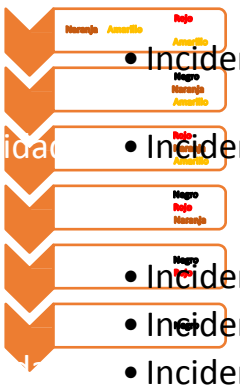
Posición de ingreso en Cola de Incidentes Priorizada				
Código	Grupo A (SLAs Especiales o Atención Especial)	Grupo B (SLAs Estándar)	Grupo C (Sin SLA)	Grupo D (Otros)
Negro	1	2	3	5
Rojo	2	3	4	6
Naranja	3	4	5	6
Amarillo	4	5	6	6

Tabla 34 Ejemplo de posición de ingreso en la cola de incidentes

La clasificación de clientes obedece a los siguientes criterios:

- Grupo A (SLAs especiales). Sin aquellos clientes que tienen contratos con niveles de servicio (SLA Service Level Agreement) que requieren de cumplimiento muy estricto o que requieren tiempos de atención muy cortos.
- Grupo A (Atención Especial). Son aquellos clientes que por cualquier razón, ya sea de tipo comercial o estratégico, son considerados que deben tener atención especial y ser atendidos con la mayor prioridad posible.
- Grupo B (SLAs Estándar). Son aquellos clientes que tienen contratos con niveles de servicio estándar y que por consiguientes no tienen niveles de cumplimiento muy exigentes o que tienen tiempos de atención genéricos.
- Grupo C (Sin SLA). Son aquellos clientes que tienen contratos los cuales no especifican un nivel de servicio. Los cuales se atienden en un esquema de “mejor esfuerzo posible”
- Grupo D (Otros). Son aquellos incidentes a cualquier otra entidad que no son clientes de la empresa, pero que si pueden ser clientes del alguna otra empresa del grupo y que requieren de apoyo en la atención de un incidente.

Un ejemplo visual de la cola priorizada de atención de incidentes con base el modelo propuesto anteriormente basado en la ENISA es la Fig. 33:



- Incidente **Grupo D** Código , o Incidente **Grupo C** Código
- Incidente **Grupo D** Código
- Incidente **Grupo C** código
- Incidente **Grupo B** Código
- Incidente **Grupo C** Código
- Incidente **Grupo B** Código
- Incidente **Grupo A** Código
- Incidente **Grupo C** Código
- Incidente **Grupo B** Código
- Incidente **Grupo A** Código
- Incidente **Grupo B** Código
- Incidente **Grupo A** Código
- Incidente **Grupo A** Código

Fig. 33 Ejemplo de cola priorizada de incidentes basado en el modelo ENISA con 6 niveles de prioridad

El modelo propuesto está basado en la optimización del personal disponible (analistas del SOC) para la atención, investigación, seguimiento y clasificación de los incidentes. De esta manera se pueden gestionar los incidentes de los clientes de la organización que son más prioritarios primero, sin esto significar que los incidentes de clientes menos prioritarios sean olvidados o no atendidos. En un escenario donde no existen incidentes de clientes de grupos de alta prioridad, el incidente de alta severidad de un cliente de baja prioridad es atendido primero, sin embargo, en la ocurrencia de un incidente donde la combinación de severidad del incidente y prioridad del cliente derive en una posición más prioritaria dentro de la cola priorizada de incidentes implicará la atención anticipada de este incidente y la puesta en espera del incidente previamente atendido.

- Modelo de clasificación de incidentes de seguridad Sm4rt basado en lo propuesto por el US-CERT usando escala de impactos y vectores de ataque

El modelo de clasificación de incidentes del US-CERT tiene el objeto de documentar y reportar los incidentes mayores relacionados con la infraestructura crítica de los Estados Unidos de América tanto de agencias de gobierno como del sector privado que tengan un impacto en la economía del país.

Tomando en cuenta lo anterior, el modelo de clasificación del US-CERT es revisado y adaptado constantemente a las amenazas persistentes, a partir de eso se ha desarrollado para Sm4rt un modelo de clasificación basado en el US-CERT con un mapeo de 1 a 1 y 1 a muchos en diferentes casos adaptados al contexto de México, la experiencia de Sm4rt y los tipos de tecnologías administradas. Este modelo habilita a Sm4rt para comparar estadísticas con aquellas publicadas a nivel internacional para valorar el nivel de exposición y de riesgo de seguridad de la información de sus clientes.

El siguiente modelo, como se muestra en la Tabla 35, deberá ser usado durante la actividad de análisis del incidente una vez haya sido priorizado usando el Modelo de Priorización de Incidentes de Seguridad Sm4rt anteriormente definido. En la Tabla 35 del lado izquierdo se muestra el nombre en inglés del Vector de Ataque debido a que es el idioma original del modelo y es la forma estandarizada para el nombramiento de los Vectores de Ataque por lo cual no fueron traducidos al español.

Vector de Ataque US-CERT	Descripción US CERT	Vector de Ataque Sm4rt	Vector Específico Sm4rt	Descripción Sm4rt
“Unknown”	La causa del ataque no está identificada.	Desconocido	Desconocido	La causa del ataque no está identificada.
“Attrition”	Ataques basados en fuerza bruta con objetivo de comprometer, degradar o hacer no disponibles sistemas, redes o servicios.	Desgaste	Fuerza bruta/ Diccionario	Cualquier ataque relacionado a fuerza bruta o de diccionario a sistemas, mecanismos de autenticación, que derive en el bloqueo de cuentas legítimas de usuarios o degradación del servicio.
			Negación de Servicio	Ataques con el objetivo de hacer indisponible un servicio, sistema o información para la operación normal. Este puede ser derivado de inundación de paquetes, amplificación de peticiones, o explotación de vulnerabilidades que corrompan procesos.

Vector de Ataque US-CERT	Descripción US CERT	Vector de Ataque Sm4rt	Vector Específico Sm4rt	Descripción Sm4rt
			Reconocimiento	Cualquier tipo de escaneo de puertos, servicios, direcciones co3n el objeto de hacer una tarea de reconocimiento para realizar ataques a futuro.
			Hacktivismo	Actividades o ataques realizadas de manera organizada con el objeto de promover una causa hacktivista contra organizaciones gubernamentales o privadas.
Web	Un ataque ejecutado desde un sitio web o una aplicación basada en web.	Web	SQL Injection	Ataques orientados a afectar las bases de datos de aplicativos internos o externos.
			XSS/CSRF/XPath	Ataques orientados a inyectar comandos para modificar la ejecución normal de un portal web para obtener ventaja de su funcionalidad y/o usuarios
			Otros ataques web	Cualquier otro tipo de ataque realizado desde o a través de un portal web.
“Email”/ “Phishing”	Un ataque ejecutado a través de un correo electrónico o un archivo adjunto.	Correo/ Phishing	Phishing	Ataques recibidos a través de correo electrónico que tengan el fin de engañar al usuario para proporcionar información personal o de la organización.
			Ingeniería Social	Ataques recibidos a través de algún medio electrónico con el fin de engañar al usuario para proporcionar información personal o de la organización.
“External”/ “Removable Media”	Un ataque ejecutado desde un medio removible o un dispositivo periférico.	Medios Removibles o Externos	Medios Removibles o Externos	Un ataque ejecutado desde un medio removible o un dispositivo periférico.

Vector de Ataque US-CERT	Descripción US CERT	Vector de Ataque Sm4rt	Vector Específico Sm4rt	Descripción Sm4rt
"Impersonation"/"Spoofing"	Un ataque que involucra la sustitución de contenido o servicios legítimos con un fin malicioso.	Suplantación de Identidad/ Spoofing	Deformación de Interfaces (Defacements)	Son los ataques que tienen como objetivo modificar maliciosamente la apariencia de un sistema.
			Intercepción o Falsificación de Información (Spoofing)	Ataques que involucren la intercepción de comunicaciones por cualquier medio físico o electrónico, estos pueden ser a través de escucha de un canal o la suplantación de identidad de un activo legítimo de la infraestructura.
"Improper usage"	Cualquier incidente resultado de una violación a la política de uso aceptable de la organización por un usuario autorizado, excluyendo las categorías anteriores.	Malware	Ransomware	Incidentes relacionados a malware principalmente del tipo Ransomware
			Backdoors	Incidentes relacionados a malware principalmente del tipo Backdoor, Spyware o Callback.
			Malware	Incidentes relacionados a otros tipos de malware.
		Fuga de Información	Complicidad interna	Cualquier incidente donde se observe o presuma complicidad interna de un usuario legítimo. Como la extracción o destrucción de información de la organización.
		Uso inapropiado	Uso inapropiado	Cualquier incidente resultado de una violación a la política de uso aceptable de la organización por un usuario autorizado, excluyendo las categorías anteriores.
"Loss or Theft of Equipment"	La pérdida o robo de un dispositivo de cómputo o medio de almacenamiento usado por la organización.	Pérdida o robo de equipos	Pérdida o robo de equipos	La pérdida o robo de un dispositivo de cómputo o medio de almacenamiento usado por la organización.

Vector de Ataque US-CERT	Descripción US CERT	Vector de Ataque Sm4rt	Vector Específico Sm4rt	Descripción Sm4rt
“Other”	Métodos de ataque que no encajan en ningún otro vector	Otros	Configuraciones inseguras	Incidentes relacionados al abuso de usuarios legítimos o ilegítimos de malas prácticas de configuración o falta de hardening.
			Otros	Métodos de ataque que no encajan en ningún otro vector

Tabla 35 Matriz comparativa de vectores de ataques del modelo de clasificación de incidentes basado en el US-CERT original y vectores de ataque en el modelo de clasificación de incidentes basado en el US-CERT adaptado a Sm4rt.

De acuerdo con el modelo del US-CERT se requiere identificar el impacto a la organización derivado del incidente de seguridad. Este impacto está basado en 3 aspectos principales: funcional, afectación a la información y la recuperación del negocio. En México, adicional a los impactos propuestos por el US-CERT y debido a los sectores industriales a los que pertenecen los clientes de Sm4rt se deberán de considerar otros tipos de impacto que agregan valor a la notificación y seguimiento de un incidente de seguridad de un cliente operado por el SOC de Sm4rt. Estas categorías de Impactos son Impacto Político, Impacto Reputacional e Impacto Regulatorio y observan en la Tabla 36 donde complementan las categorías usadas por el US-CERT para adaptarse al alcance de los servicios del SOC de Sm4rt:

Impact Category US-CERT	Catálogo de Niveles de Severidad	Categoría de Impacto Sm4rt	Catálogo de Niveles de Severidad
Impacto Funcional	Sin Impacto Sin impacto a servicios Mínimo impacto a servicios no críticos Mínimo impacto a servicios críticos Significativo impacto a servicios no críticos Negación de sistemas no críticos Significativo impacto a servicios críticos Negación o pérdida de control de servicios críticos	**Impacto Funcional.** Es el impacto a la funcionalidad del negocio o la habilidad para la entrega de su servicio.	Sin impacto Mínimo Significativo Negación o pérdida de control
Impacto a la Información	Sin impacto Sospechado pero no Identificado Fuga de datos de privacidad Fuga de datos propietarios Destrucción de servicios no críticos Fuga de datos de sistemas críticos Fuga de credenciales clave Destrucción de servicios críticos	**Impacto a la información.** Es el tipo de información perdida, comprometida o corrupta	Sin impacto No confirmado Fuga de datos internos Fuga de datos privados Destrucción de información Fuga de datos restringidos Fuga de credenciales clave Destrucción de servicios
Impacto a la capacidad de recuperación	Regular Requiere suplementarse Extendido No recuperable No aplicable	**Impacto a la capacidad de recuperación.** Identifica el alcance de los recursos necesarios para	Sin impacto Regular Extendido No recuperable No aplica

Impact Category US-CERT	Catálogo de Niveles de Severidad	Categoría de Impacto Sm4rt	Catálogo de Niveles de Severidad
		recuperarse del incidente.	
No Aplica	No Aplica	**Impacto Político.** Es el nivel de afectación política que podría tener el cliente.	Sin impacto Moderado Alto
No Aplica	No Aplica	**Impacto Reputacional.** Es el impacto a la confianza en la organización.	Sin impacto Moderado Alto
No Aplica	No Aplica	**Impacto Regulatorio.** Es la posible consecuencia regulatoria para el cliente derivada del incidente.	Sin impacto Sanción administrativa Multa Revocación de concesión

Tabla 36 Matriz comparativa de categorías de impacto del modelo de clasificación de incidentes basado en el US-CERT original y categorías de impacto del modelo de clasificación de incidentes basado en el US-CERT adaptado a Sm4rt.

En la Fig. 34 se observa un ejemplo de reporte de clasificación de incidentes con base en el modelo basado en el modelo el US-CERT:

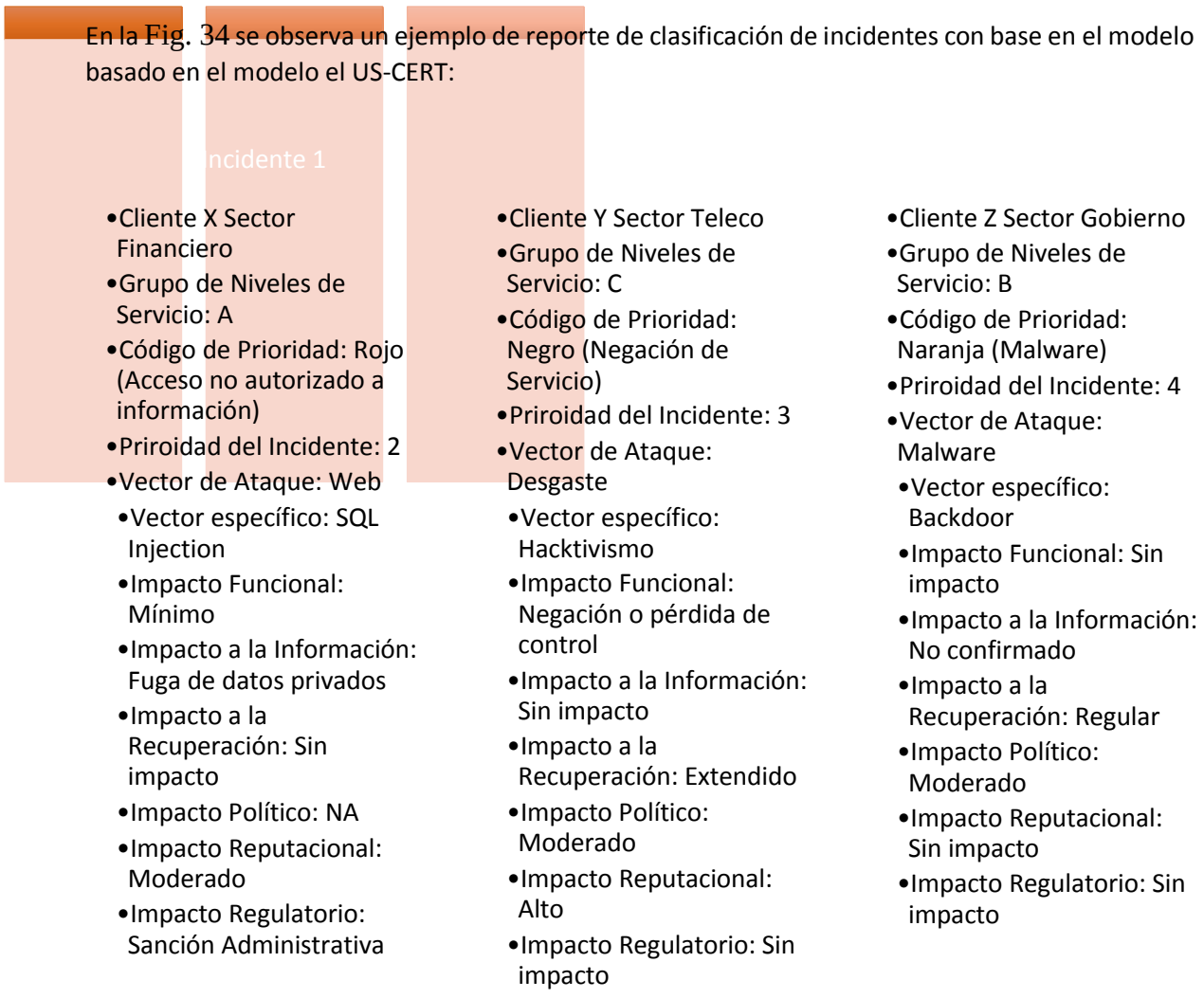


Fig. 34 Ejemplo de reporte de clasificación de incidentes empleado el modelo basado en US-CERT adaptado a Sm4rt

Por último, la documentación de un incidente de seguridad debe de contener la siguiente información básica intrínseca del evento, de la organización afectada y del proceso de gestión de incidentes. La información que debe ser recolectada con base en las mejores prácticas de la NIST es:

1. **Elementos básicos de información:**
   1.1. Información del Analista/Manejador del Incidente
      - Nombre
      - Puesto
      - Número telefónico y/o extensión
      - Correo electrónico
      - El incidente fue identificado por el SOC?

   1.2. Información de contacto de quien notifica el incidente (en el caso de que el incidente haya sido reportado al SOC por parte de un tercer)
      - Nombre
      - Rol o Puesto
      - Organización y unidad
      - Correo electrónico
      - Número telefónico y/o extensión
      - Localización

   1.3. Detalles del Incidente:
      - Cambios en el estatus del incidente (por fecha o estampa de tiempo) inicio, descubrimiento/detección, reporte, resolución, término.
      - Localización física del incidente
      - Estatus actual del incidente
      - Fuente o causa del incidente (si es sabida) incluyendo “hostnames” o direcciones IP
      - Descripción del incidente
      - Descripción de los recursos afectados, incluyendo sistemas, “hostnames”, direcciones IP y función
      - Categoría del incidente, vector de ataque, e indicadores relacionados al incidente (patrones de tráfico, registros, etc)
      - Factores de priorización
      - Factores de mitigación
      - Acciones de Respuesta realizadas
      - Lista de otras organizaciones contactadas

   1.4. Comentarios Generales

2. **Elementos para el Manejador del Incidente**
   2.1. Estatus actual de la respuesta al incidente
   2.2. Resumen del incidente
   2.3. Acciones de Manejo del Incidente
      - Bitácoras de acciones realizadas por todos los manejadores
      - Información de contacto para todas las partes involucradas
      - Lista de evidencia obtenida

   2.4. Comentarios de los manejadores del incidente
   2.5. Causa del incidente
   2.6. Costo del incidente
   2.7. Impacto al negocio del incidente

Capítulo 4. Recomendaciones y conclusiones

En esta sección se listan tanto la recomendaciones y conclusiones que se derivan de la elaboración de este documento.

Recomendaciones

Durante la elaboración de los Modelos de Priorización de Incidentes Sm4rt y el Modelo de Clasificación de Incidentes de Seguridad Sm4rt se identificaron algunos prerrequisitos que facilitan y optimizan el uso de los modelos los cuales se listan en la Tabla 37.

Modelo	Prerrequisito	Descripción	Información que debe contener y como complementa el Modelo
Modelo de Priorización de Incidentes Sm4rt	Matriz de ataques base	Este documento contiene un listado detallado de los ataques informáticos que son posible identificar a través del uso de la tecnología de seguridad con la que cuentan los clientes de Sm4rt.	Debe de contener lo siguiente: 1. Nombre del ataque 2. Clasificación inicial y código de tipo de incidente en el Modelo de Priorización de Incidentes Sm4rt 3. Tecnologías de Seguridad donde puede ser identificado 4. Descripción conceptual del ataque 5. Descripción técnica del ataque 6. Ligas a ejemplos donde se observe el comportamiento del ataque
	Matriz de Niveles de Servicio de Cliente	Es un repositorio centralizado donde se ubican todos los clientes del SOC en conjunto con sus niveles de servicio contratados o estado de relevancia.	Debe de contener lo siguiente 1. Nombre del cliente 2. Giro o Sector 3. Grupo de priorización con base en el Modelo de Priorización de Incidentes Sm4rt 4. Nivel de servicio para atención de incidentes 5. Matriz de contactos internos 6. Matriz de contactos del cliente 7. Listado de Tecnologías de Seguridad en el alcance de la arquitectura de seguridad de la información administrada por Sm4rt.
	-	-	-
Modelo de Clasificación de Incidentes	Inventario de la infraestructura perimetral	Este documento contiene un inventario, lo más completo posible, de	Se debe de tener documentado y si es posible poseer diagramas que contengan lo siguiente:

Modelo	Prerrequisito	Descripción	Información que debe contener y como complementa el Modelo
de Seguridad Sm4rt		todos los componentes de la arquitectura de TI del cliente.	1. Diagrama lógico de la red perimetral del cliente 2. Diagrama físico de la red perimetral del cliente 3. Listado de dispositivos perimetrales 3.1. Hostname 3.2. Función 3.3. Relevancia para el negocio 3.4. Tecnología 3.5. Dirección IP 3.6. Información de contacto del responsable del dispositivo 4. Listado de subredes perimetrales 4.1. Dirección IP de la subred 4.2. Mascara de red 4.3. Función 4.4. Localización (DMZ perimetral, DMZ interna, producción, preproducción, red de administración, etc)
	Diccionario de datos	Este documento contiene una lista conceptual de la información más importante de la organización.	El diccionario de datos debe de contener lo siguiente: 1. Nombre del tipo de dato 2. Descripción conceptual 3. Descripción estructural del dato (como está formado) 4. Relevancia del dato para el negocio 5. Principales sistemas, equipos o procesos en los cuales es usado este dato. 6. Ejemplos del dato.
	Marco regulatorio	Este repositorio contiene una lista de clientes y las regulaciones locales o internacionales a las cuales está sujeto.	Debe de contener lo siguiente: 1. Nombre del cliente 2. Giro o Sector 3. Regulaciones locales a. Datos o procesos relacionados en el diccionario de datos relacionados

Modelo	Prerrequisito	Descripción	Información que debe contener y como complementa el Modelo
			4. Regulaciones internacionales a. Datos o procesos relacionados en el diccionario de datos relacionados 5. Sanciones, multas o situaciones anteriores relevantes.
Ambos	ITSM	Se debe de contar con un ITSM que posea en la documentación de incidentes la opción de documentar incidentes de Seguridad de la Información	Se debe configurar las plantillas de incidentes para poder contar con una de Incidentes de Seguridad alineada al Modelo de Priorización de Incidentes Sm4rt y el Modelo de Clasificación de Incidentes de Seguridad Sm4rt. Esto implica habilitar campos para seleccionar el Grupo de Priorización del Cliente, el Código de tipo de incidente y la Posición de ingreso a la cola de atención de incidentes, así como toda la información inherente al incidente y la cronología de atención del mismo, así como campos para la documentación del Modelo de Clasificación de Incidentes de Seguridad Sm4rt
	Proceso de Revisión Anual de los Modelos	Documentación de un procedimiento para la revisión técnica de forma anual del Modelo de Priorización de Incidentes Sm4rt y del Modelo de Clasificación de Incidentes de Seguridad Sm4rt. Su objetivo es tener actualizado constantemente los modelos para adaptarlo al entorno cambiante interno y externo a Sm4rt.	Es importante que en este proceso estén involucrados personal de las siguientes áreas del SOC: 1. Monitoreo SOC 2. Administración SOC 3. Líderes de Operación 4. Líderes de Servicio 5. Entrega de Servicio 6. Experto en la Materia (se recomienda que sea externo a la organización)

Tabla 37Matriz de prerrequisitos para la implementación de los modelos de priorización y clasificación de incidentes adaptados para el SOC de Sm4rt.

Conclusiones

La elaboración de este trabajo y el objetivo perseguido fueron motivados por la continua necesidad del negocio de la seguridad informática, y mas específicamente del centro de operaciones de seguridad o SOC donde yo me desempeño, de mantenerse a la vanguardia técnicamente al mismo tiempo que se buscar hacer más eficiente la operación y logro de compromisos con los clientes.

Como puede observarse en el desarrollo de este trabajo, es basta la información existente a nivel internacional referente a seguridad informática, gestión de tecnologías de la información y gestión de riesgos o incidentes, sin embargo, las diferentes organizaciones alrededor del mundo basan sus modelos o metodologías en el contexto específico de donde fueron creadas. Debido a lo anterior, los modelos seleccionados fueron adaptados con base en la propia experiencia al contexto de la operación del SOC donde podrían ser implementados.

Se evaluaron 3 modelos de priorización y 4 modelos de clasificación de incidentes de seguridad, a través de 15 aspectos en 4 categorías: impacto positivo a la optimización, utilidad del modelo, diferenciadores que implica su uso y factibilidad del modelo para ser usado. La definición de los aspectos a ser evaluados y la ponderación para cada uno de ellos fue una tarea de introspección y conocimiento de la compañía derivados de 8 años de experiencia en la misma. Los valores y comportamientos de la empresa también fueron considerados para determinar el grado de importancia de cada aspecto.

De los modelos mencionados en el marco teórico se seleccionó, para ser adaptado, el que mejor puntuación general obtuvo, que para el caso de priorización se eligió adaptar un modelo basado en la propuesta de ENISA y para el caso de clasificación se eligió adaptar un modelo basado en la propuesta del US-CERT.

Aunque podría ser compleja la implementación de estos modelos a los servicios o clientes ya existentes en el SOC de Sm4rt, es muy posible que su adopción sea principalmente en servicios o clientes nuevos donde se presente como propuesta inicial de operación y como valor agregado al cliente. En el resto de la base instalada de clientes del SOC, estos modelos pueden ser presentados como propuesta de mejora, sin embargo, en los clientes mas importantes tendría que ser aceptado por el cliente antes de poderlo implementar formalmente.

Como parte del aprendizaje derivado de la elaboración de este trabajo, considero que incluso es factible la creación de un servicio de tipo respuesta a incidentes de seguridad informática o equipo de respuesta a emergencias computacionales (CERT – “Computer Emergency Response Team” por sus siglas en inglés) o equipo de respuesta a incidentes de seguridad (CSIRT – “Computer Security Incident Response Team”), aunque el diseño, implementación o puesta en operación de un servicio de esta índole sale fuera del alance de este trabajo e incluso del área de operaciones a la cuál me encuentro adscrito.

Continuidad del trabajo

Como se muestra en las recomendaciones, se debe de dar mantenimiento a los modelos, por lo menos de forma anual y es indispensable integrar estos modelos a una metodología de gestión de incidentes que permita visualizar desde el punto de vista de Sm4rt como MSSP todo el ciclo de vida de un incidente de seguridad con sus clientes. Esto puede abrir la puerta a Sm4rt a ofrecer nuevos

servicios que involucren este ciclo de vida del incidente de forma más integral a través de servicios de OIMS (“Outsourced Incident Management Services”).

La transición a implementación y operación de los modelos aquí definidos requerirá de esfuerzos conjuntos con las áreas de documentación de procesos de Sm4rt, de sesiones de capacitación y entrenamiento de los analistas del SOC de tal manera que se genere la habilitada necesaria para lograr parte del objetivo de este proyecto que es incrementar la capacidad operativa del personal.

De forma paralela se deberá buscar el apoyo de las áreas correspondientes para la creación o adaptación de los documentos o recursos mencionados en las recomendaciones en la sección anterior. Estos documentos o recursos no son indispensables para echar a andar los Modelos, sin embargo, incrementaran la efectividad de los esfuerzos necesarios para poner a punto su implementación.

Anexos

Glosario

Término	Significado