Universidad de Buenos Aires. Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería.

Carrera de Maestría en Seguridad Informática.

Tesis de Maestría.

Tema:

“Proyecto de aplicación profesional”

Título:

“Implementación profesional de un proyecto de desarrollo de métricas de Seguridad Informática para entidades financieras"

Autor: Esp. Abigail Kauf

Tutor: Mg. Diego Sebastián Escobar

Año: 2017

Declaración Jurada de Origen de los Contenidos

Por medio de la presente, manifiesto conocer y aceptar el Reglamento de Tesis vigente y me hago responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Abigail Kauf
DNI 34.646.428

Resumen

Este trabajo busca documentar un caso de aplicación profesional en la República Argentina sobre la confección de Indicadores de seguridad de la información en entidades bancarias.

Se brindará un marco teórico de referencia sobre la temática y luego se investigarán y analizarán detalles técnicos, teóricos y prácticos, sobre la confección de los mismos teniendo en cuenta la normativa vigente en el ámbito.

A su vez se justificará oportunamente la necesidad de la existencia de dicha metodología y se asesorará sobre formas eficientes de implementarla.

Introducción

Este trabajo pretende continuar con el proyecto de especialización realizado en el primer año de la maestría que consistió en un relevamiento profesional de los controles desarrollados por el área operativa de seguridad informática de la empresa “Identidad Privada”.

Basado en los conocimientos adquiridos, la experiencia profesional en el área de Seguridad Informática Operativa y la realizada en un banco argentino, considero que la tesis y el trabajo cotidiano pueden retroalimentarse incrementando la productividad y aportando al conocimiento que hoy en día existe en el área profesional.

El objetivo general del presente trabajo es que sea de aplicación profesional y pueda aportarse entidades bancarias de la República Argentina una metodología genérica para el desarrollo de métricas continuando con la línea de desarrollo de controles y en colaboración y cumplimientos con la normativa del Banco Central de la República Argentina (BCRA).

Se pretende diseñar un modelo de métricas específicas relacionado con la gestión de la Seguridad de la Información. El mismo aportará a la gerencia en la toma de decisiones y visibilidad del área. Se persigue también como objetivos particulares, elaborar un marco teórico, enumerar tareas y relevar la metodología para la elaboración de métricas generales, que aportan información adicional a la operatoria cotidiana. A su vez, que dichas métricas darán visibilidad para tomar decisiones, gestionar, proponer mejoras y/o monitorear el desarrollo normal de la operatoria.

Es así como en los primeros capítulos, se describe el marco conceptual vinculando teóricamente normas, procedimientos y buenas prácticas de seguridad de la información. El mismo sentará una base de conocimiento sólida sobre la cual se basará el trabajo para cotejar la realidad de las métricas vigentes hoy en día con lo sugerido por la teoría.

En una segunda etapa, se analizará en detalle las métricas citadas y se procederá al armado de las mismas. Considerando anotaciones y salvedades producto del ejercicio profesional tales como: desconocimiento del alcance que el área pretendía, mejoras en la matriz de controles o automatización de los mismos para ser más eficientes en el uso de los recursos. A su vez, cuando las métricas no arrojan ninguna información adicional para tomar decisiones, debe considerarse el hecho de dejar de ejecutarla dependiendo de cuál sea el esfuerzo que implique.

Por último, se arribará a conclusiones sobre el trabajo realizado hasta el momento reflexionando sobre alternativas superadoras y proponiendo un camino de mejora de cara al futuro y evolución del área.

Considerando que la Seguridad Informática posee un nivel de madurez entre tres y cuatro, basado en el Modelo de Capacidad del Instituto de Ingeniería de Software (SEI CMMI), en las diferentes áreas en las que están segregadas la dirección de seguridad informática, creemos que relevar los controles y todo lo relacionados a ellos permitirá a la organización gestionar eficazmente los recursos disponibles y maximizar sus beneficios.

Justificación del tema elegido

Esta tesis se desarrolla y toma como punto de partida un relevamiento teórico exhaustivo sobre controles del área de seguridad informática en una entidad bancaria; el cual contempló en análisis de metodologías, normativas, buenas prácticas y contrastandolas con la realidad operativa.

Si bien la normativa vigente en entidades financieras establece la necesidad de contar con indicadores para medir la gestión y la eficacia de los controles de seguridad, el nivel de desarrollo del mismo no cumple con las expectativas del organismo de control.

Habiendo cursado la maestría en Gestión de Seguridad Informática poseo los conocimientos técnicos necesarios para poder investigar e idear métricas que colaboren la tarea diaria de una entidad financiera o bancaria en la República Argentina. Creo que este trabajo puede aportar visibilidad acerca de la importancia de medir la operatoria y los beneficios que las mismas aportan a la hora de tomar decisiones gerenciales.

CAPITULO I: Identificación del Marco Teórico de las Métricas en Seguridad de la Información.

Introducción

Cada organización tiene objetivos de seguridad informática así como riesgos asociados a la gestión de la misma. Debido a esto, y entre otras cuestiones, se vuelve necesario el uso de las métricas relacionadas a la gestión estratégica de la seguridad de la información que colaboran a tener mayor visibilidad de los procesos que ocurren dentro de la compañía y sus resultados.

Algunos objetivos a tener en cuenta que son necesarios a la hora de idear métricas de seguridad son:

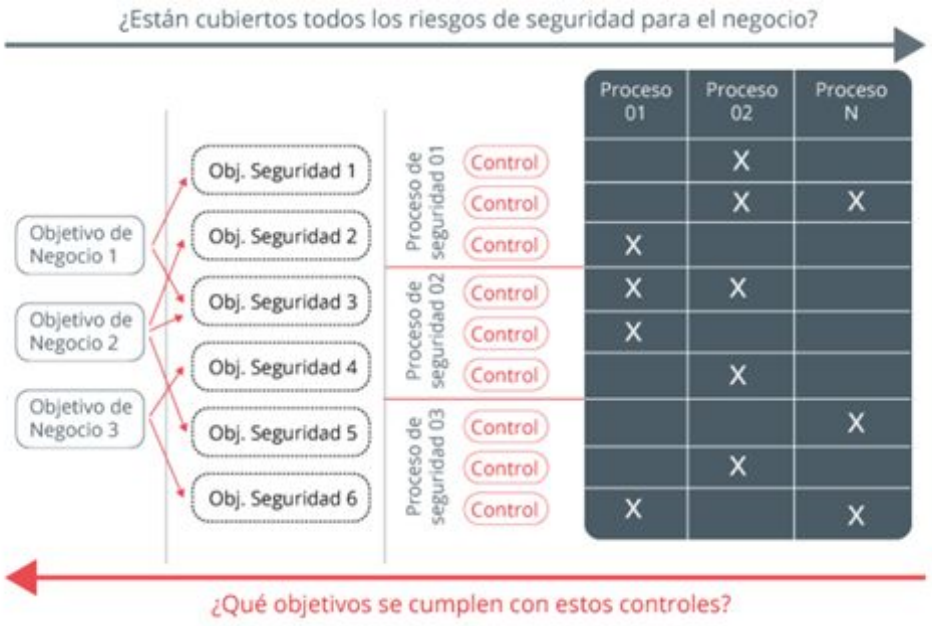
- Definir un Plan Estratégico de Seguridad de la Información considerando como referencia el análisis previo que se haya hecho sobre los riesgos en función de los activos de la información.
- Contar con una clasificación de la información ordenada y trasversal a toda la organización.
- Tener accesibles y claramente establecidas las políticas y procedimientos referentes a la seguridad de la información.
- Considerar cuál es la posición actual de la empresa respecto a los estándares de buenas prácticas.
- Incluir en la planificación anual del presupuesto las inversiones y costos necesarios para llevar adelante las medidas para alcanzar el nivel de seguridad de la información deseado.
- Incrementar la securización de la información al motivar una cultura organizacional alineada con los estándares de seguridad de la información a todos los niveles.

A continuación, se analizarán los modelos de gestión más relevantes de la seguridad informática en la actualidad:

Modelo del Instituto Nacional de Ciberseguridad de España (I.N.C.I.B.E)

Con respecto a los puntos detallados arriba el Instituto Nacional de Ciberseguridad de España (INCIBE) propone el siguiente diagrama:

Tabla 1



Analizando el esquema que propone I.N.C.I.B.E podríamos continuar detallando algunos procesos de seguridad que serían necesarios. En este contexto se recomienda entonces:

- Tener identificados a nivel organizacional cuales son los activos de la información considerados críticos en los procesos de negocio de la organización.

- Definir una metodología de riesgos y realizar un análisis bajo la misma detallando claramente cuáles son los riesgos y amenazas detectados en los activos de la información críticos según la clasificación antes sugerida.
- Proponer un camino de acción y/o tratamiento de los riesgos, ya sea asumiéndolos, mitigándolos, transfiriéndolos o evitándolos.
- Utilizar las métricas para medir el nivel de seguridad que predomina en los sistemas, aplicaciones, servicios, bases de datos, etc.
- Brindar de forma continua concientización a los empleados ya que se considera que son ellos la primera línea de defensa de la organización.

Cuando la decisión de la empresa es mitigar los riesgos es donde se establecen controles de seguridad de la información; (algunos de los cuales fueron estudiados y detallados en el Trabajo Final de Especialización). En esta tesis se pretende desarrollar métricas acordes con el plan Estratégico de la Gestión de la Seguridad de la Información.

Para poder prevenir los riesgos que puedan surgir y tener un alto grado de adaptabilidad a un entorno dinámico como es el de la seguridad de la información en la actualidad, se recomienda medir el rendimiento de los controles, los procesos y las acciones en general que se hayan llevado a cabo. Las métricas son una herramienta esencial para poder verificar si se está yendo por el camino correcto y si están dando resultados los planes, procesos y controles previamente diseñados y establecidos.

A su vez la distribución de recursos humanos y económicos puede basarse en lo que las métricas arrojen como resultados dedicando recursos en mayor medida a aquellos desvíos que arrojen las métricas. También se puede considerar una reasignación de los mismos en caso de que se considere que algún aspecto esté en los niveles previstos y otro no, compensando el esfuerzo hacia donde más se necesita.

Para dichas métricas I.N.C.I.B.E propone un modelo S.M.A.R.T por sus iniciales en inglés, que traducidas significan:

- Específica (S)

- Medibles (M)
- Alcanzables (A)
- Repetibles (R)
- Dependientes del tiempo (T)

Este instituto propone el siguiente listado de métricas entre los cuales se puede elegir una, varias o todas para adaptar a la empresa en estudio:

- Eficacia o efectividad que miden en qué grado se cumplen los objetivos, por ejemplo:
    - Porcentaje de disminución de contraseñas débiles tras las campañas de concienciación.
    - Porcentaje de disminución del número de incidentes.
- Un caso particular de las anteriores son las de progreso de la implementación, por ejemplo:
    - Porcentaje de implementación del plan de seguridad (o del plan de continuidad de negocio).
    - Porcentaje de planes de acción definidos o implantados.
    - Porcentaje de empleados que han recibido concienciación en seguridad.
    - Porcentaje de equipos en los que se ha instalado antivirus.
    - Porcentaje de sistemas en los que se han instalado parches o un sistema que automatice esta tarea.
- Eficiencia que muestran la proporcionalidad entre los objetivos y los resultados alcanzados como, por ejemplo:
    - Coste de los incidentes de seguridad informática respecto al presupuesto de seguridad informática.
    - Coste de la política de *backup* respecto al coste de inactividad en caso de incidente.
- Impacto como por ejemplo:
    - Coste de la recuperación ante un incidente (o ahorro si se ha evitado el incidente o alguna multa).
    - Coste del software de seguridad adquirido o los servicios contratados.

Es importante aclarar que cada empresa tiene sus propios objetivos de seguridad que son primordiales tener en cuenta a la hora de evaluar qué métrica se desea implementar ya que la misma llevará esfuerzo y se pretende que tal esfuerzo se vea reflejado en resultados productivos y aplicables a los procesos de la organización.

Asociación de Auditoría y Control de Sistemas de Información (I.S.A.C.A.)

De acuerdo con lo que plantea I.S.A.C.A. La Tecnología de la Información (T.I.) está envuelta por un proceso que consiste en evaluar, dirigir y monitorear (E.D.M). Las métricas contribuyen con esta última etapa del proceso y colaboran con el área gerencial en la medición de aquello que se ha establecido como meta tanto en el área del negocio como en el de TI.

El objetivo de la elaboración de métricas es el poder tomar decisiones, pero también el responder algunas preguntas que encuentra la organización en un paso intermedio a la toma de decisiones. Algunas de las cuales podemos enumerar son:

1. ¿Fue mejor al del año pasado el rendimiento de T.I?
2. De acuerdo con la inversión que la empresa hace en T.I, ¿que obtiene a cambio?
3. Basado en el desarrollo de las métricas, ¿es posible determinar un punto de referencia (Benchmark) acerca del rendimiento?

Representa un arduo trabajo el reflejar hechos cualitativos en mediciones cuantitativas. Es por ello que se recomienda utilizar indicadores para cada una de las preguntas. Vale aclarar que una sola pregunta puede estar asociada a más de un indicador, esto se debe a que un conjunto de indicadores puede aproximar al observador a una mejor idea de la realidad. Es así como al describir una calidad se vuelve preciso una base de medición donde, generalmente, dos variables se ven vinculadas.

Por ejemplo, podemos decir que el 15% de los incidentes que ha recibido el área han sido cerrados con resolución exitosa en menos de tres horas. Estas mediciones están tomando como referencia la actividad que ha tenido el área y la carga de trabajo o esfuerzo requerido para atender esa actividad medido en horas.

Con el ejemplo anterior, queda a la vista la utilidad de las métricas en cuanto a la evaluación del cumplimiento concorde al acuerdo de servicios que se haya pactado, y también es posible evidenciar la efectividad en los procesos. Con ambos resultados vinculados establecidos, podemos medir el éxito contra objetivos fijados previamente por la compañía.

Para poder desarrollar métricas asociadas al rendimiento, de acuerdo con esta normativa, se suele seguir el siguiente proceso:

1. Establecer cuáles son los procesos críticos de la entidad para cumplir con los requisitos de los clientes. En el caso de las entidades financieras que competen a este trabajo, será tan importante cumplir con las expectativas de los clientes, así como con la normativa emitida por el ente regulatorio de las mismas.
2. Distinguir cuales son los resultados específicos y cuantificables con las cuales se va a trabajar a partir de los procesos detectados en el punto anterior.
3. Asentar los objetivos que se van a considerar al momento de calificar los resultados.

De acuerdo con Bakshi (2016):

> El desarrollo de las métricas incluye la definición de un equilibrado conjunto de objetivos de rendimiento, métricas, objetivos y puntos de referencia. La métrica debe cubrir las actividades y resultados que se miden utilizando indicadores de avance y retroceso y un equilibrio adecuado de medidas financieras y no financieras. Las

métricas deberían ser revisadas y acordadas con TI, otras funciones de negocio y otras partes interesadas relevantes.[1](sec. Desarrollo de métricas de performance)

Continuando con esta propuesta, se sugiere tener en cuenta cuestiones como la normalización a un parámetro de atributo común de las métricas con el objetivo de entender tendencias de forma adecuada, la inclusión en las métricas de características que permitan compararlas de forma exacta y detallada. En teoría, se puede considerar una buena métrica a aquella que es: lineal, confiable, repetible, fácil de usar, consistente e independiente.

Además sugiere evitar las comparaciones con empresas del mismo rubros o similares, tratar de disminuir al mínimo las comparaciones vinculadas a los costos generales de la compañía apuntándolas, más bien, a medir los beneficios en el área de T.I. Por último, también es destacable el punto en donde se remarca que las métricas deben ser manejables en cuanto a los volúmenes de información. Dejando así en evidencia, que una gran cantidad de información reflejadas en cuantiosa cantidad de páginas es altamente probable que no le resulte beneficiosa ni útil a la gerencia.

Informe COSO II

El Informe COSO es un documento con gran aceptación, que se convirtió en un estándar de referencia, donde se pueden encontrar directivas para implementar, gestionar y monitorear un sistema de control. Es importante aclarar que el informe no está compuesto únicamente por normativas, políticas o procedimientos, sino que también involucra gente.

Fue pensado con el objetivo de ayudar a detectar los riesgos que podrían afectar a la organización y gestionar los riesgos, proporcionar un nivel razonable de seguridad para la administración y la junta directiva de la entidad, siempre orientado hacia el logro de los objetivos que hayan sido planteados por el negocio.

[1] Véase referencia bibliográfica N° [01].

Dentro del proceso que plantea el Informe COSO, el trabajo se basará en el componente de monitoreo, tal como se muestra en la figura debajo, sin perjuicio de que se deba dar contexto de los puntos anteriores de los procesos con el objetivo de contextualizar el tema que se esté desarrollando.

Tabla 2

El informe COSO II (2013) define al monitoreo como:

> Evaluaciones concurrentes o separadas, o una combinación de ambas es utilizada para determinar si cada uno de los componentes del Control Interno, incluidos los controles para efectivizar los principios dentro de cada componente, está presente y funcionando. Los hallazgos son evaluados y las deficiencias son comunicadas

oportunamente, las significativas son comunicadas a la alta gerencia y al directorio[2]. (sec. Monitoreo).

ISO/IEC 27.001

Esta normativa pertenece a la Organización Internacional de Normalización (I.S.O.) y se basa en la ISO/IEC 27.001 que versa sobre los sistemas de gestión de seguridad de la información. El objetivo que persigue esta norma es medir el resultado de la gestión propuesta en la normativa 27.001.

Entre otras cosas, la normativa que estamos tratando se explaya sobre cómo realizar el programa de medición y también describe los parámetros que se deben tener en cuenta a la hora de efectuar las mediciones. A su vez, aporta información valiosa en virtud de marcar un norte para la creación exitosa de objetivos de rendimiento y el establecimiento de los criterios de éxitos.

Este último es un tema no menor, ya que si los objetivos de rendimiento y los criterios de éxitos no son establecidos de forma correcta todo el trabajo de recopilación de información en el tiempo, el procesamiento de la misma y su posterior exposición puede ser totalmente inútil para la organización a la hora de tomar decisiones.

Según esta normativa, tener en consideración la medición en aspectos referentes a la seguridad de la información le permite a la organización proteger sus sistemas y estar preparado para responder a las potenciales amenazas.

Es importante considerar que las medidas que se diseñen deberán sustentarse en el tamaño y la complejidad de la entidad financiera que se esté analizando. Deberán también tenerse en cuenta aspectos como relación costo y beneficio de realizar la

[2] Véase referencia bibliográfica N° [02]

medición. Por último, la documentación es un paso que ninguna organización debe omitir ya que permitirá la repetición, la sustentabilidad y la integración de los datos obtenidos.

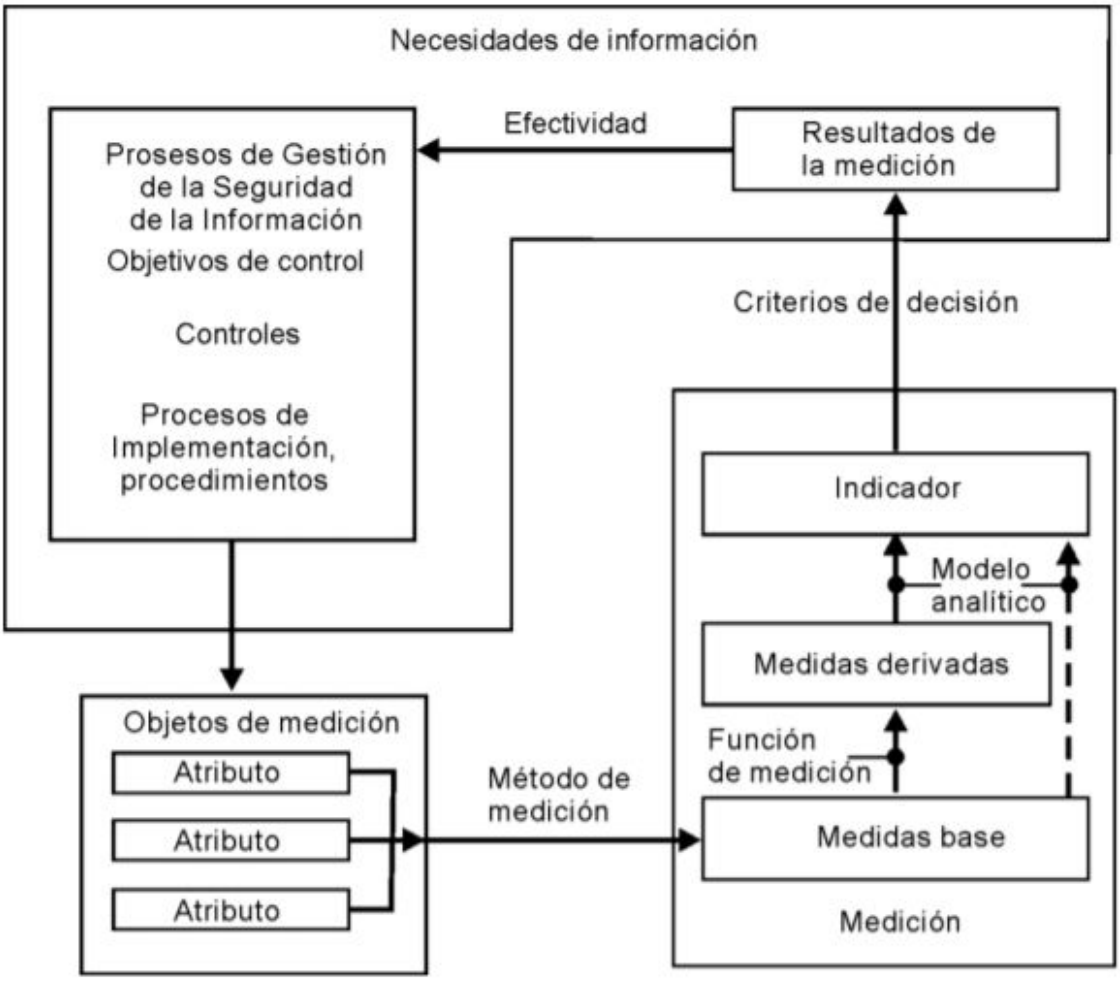
Los modelos de medición de la seguridad de la información que propone la ISO/IEC 27.001, están basados en la ISO/IEC 15939 y resulta de interés describir para una mejor comprensión del lector ya que más adelante serán utilizados de base para las mediciones desarrolladas en este trabajo.

“El modelo de medición de la seguridad de la información es una estructura que vincula una necesidad de información con los objetos de medición pertinentes y sus atributos. Los objetos de medición pueden incluir procesos, procedimientos, proyectos y recursos planificados o implementados. El modelo de medición de seguridad de la información describe cómo los atributos concernientes son cuantificados y convertidos en indicadores, los cuales proveen la base para la toma de decisiones[3].” (Instituto Argentino de Normalización y Certificación, Septiembre de 2010, p. 14)

La siguiente figura representa el modelo de medición de la seguridad de la información propuesto por la normativa.

Tabla 3

[3] Véase referencia bibliográfica N° [03]



A continuación procederemos a desarrollar cada uno de los conceptos a los que hace referencia este Modelo de Medición de la Seguridad de la Información propuesto por la normativa en cuestión ya que son de vital importancia para comprender lo que la normativa nos propone.

Medidas base: lo considera como la medida más simple que es posible alcanzar. Es la consecuencia de la utilización de este método aplicado a los atributos que se han elegido respecto del objeto que se está midiendo.

Objeto de medición: el mismo puede tener más de un atributo y de ellos solo una porción menor tendrá valores que serán útiles para ser asignado a una medida base.

Método de medición: hace referencia a una secuencia lógica de operaciones que se utiliza, en la mayoría de los casos, para poder cuantificar el valor que le corresponde a un atributo en relación a una escala de medición previamente determinada. Es posible aplicar este concepto a un determinado atributo de un objeto de medición.

La normativa presenta una tabla en donde muestra la relación entre los conceptos detallados anteriormente. La misma hace referencia a que un objeto de medición posee un atributo que le permite identificar una muestra que representara lo que el control que se está midiendo pretende mostrar. Luego, estos atributos pueden relacionarse con uno o más métodos de medición que describirán acciones concretas a llevar a cabo. Finalmente, la medida base identificará la unidad que se tendrá en cuenta para cuantificar el modelo de medición.

Entonces, un resumen que ilustra a cada uno de estos conceptos es que, mientras que los objetos de medición son redactados en forma descriptiva, el atributo hace alusión a características detectables dentro de lo que en estadística se considera una población. El método de medición comienza a enunciarse con un verbo y la medida base es aún más específica que el atributo identificando, qué es lo que se debe medir.

La ISO/IEC 27.004 describe a su vez, sobre muchos otros aspectos referentes a las métricas en Seguridad de la Información, tales como cuáles son los métodos, que se debe medir, desarrolla técnicas para hacerla y también para mostrarlas a directivos. Sin embargo, también existen otros marcos de trabajo que hacen su aporte a la temática la cual consideramos de interés incluir en este trabajo.

Lo que arriba se describe son solo extractos de la normativa que servirán de base para el desarrollo de esta tesis y que sustentan en forma teórica la metodología que se utilizará para el desarrollo de métricas puntuales en una entidad financiera de la República Argentina.

Objetivos de Controles para Tecnologías de Información y Tecnologías Relacionadas (C.O.B.I.T)

Este documento recopila y nos acerca buenas prácticas en materia de Seguridad de la Información que se presenta como un marco de trabajo aplicado a áreas específicas tal como el control y la supervisión, no solo en Seguridad de la Información, sino en un área más general que abarca la Tecnología de la Información y considera a aquella como parte esencial de esta última. El marco de trabajo está bajo la autoría y supervisión de la Asociación de Auditoría y Control de Sistema de Información (I.S.A.C.A) previamente citada en este trabajo.

C.O.B.I.T desarrolla dos temas que resultan de interés para este trabajo. Por un lado, versa acerca sobre la construcción y la finalidad de las métricas de Tecnología de Información (T.I) y, por otro lado, habla del Modelo de Capacidad de Procesos. Vale aclarar que en versiones anteriores del marco dicho modelo tenía el nombre de Modelo de Madurez. Explicaremos brevemente estos conceptos ya que pueden arrojar luz más adelante, en el texto del trabajo.

Este marco de trabajo que consideramos holístico propone establecer metas corporativas, el proceso de establecimiento de las mismas excede a los límites de este trabajo, pero una vez que están establecidas también nos invita a hacer un seguimiento de ellas a través de métricas. Es allí donde se propone dividir dentro de las métricas corporativas y de T.I y utilizar diferentes métricas que nos permitan entender el grado de avance o cumplimiento que tenemos con cada una de las metas propuestas. A su vez, se debe tener en cuenta que las mismas deben ser alcanzables y pertinentes dentro del contexto y el área organizacional donde están siendo aplicadas y se recomendó generar un cuadro de mando para utilizar como guía.

Un área de una empresa puede tener más de una meta; y una meta, a su vez, puede tener una o más métricas asociadas. Es así como por ejemplo para el área de T.I se pueden determinar tres metas y para cada meta se puede establecer dos, tres o cuatro métricas para medir el logro de cada meta.

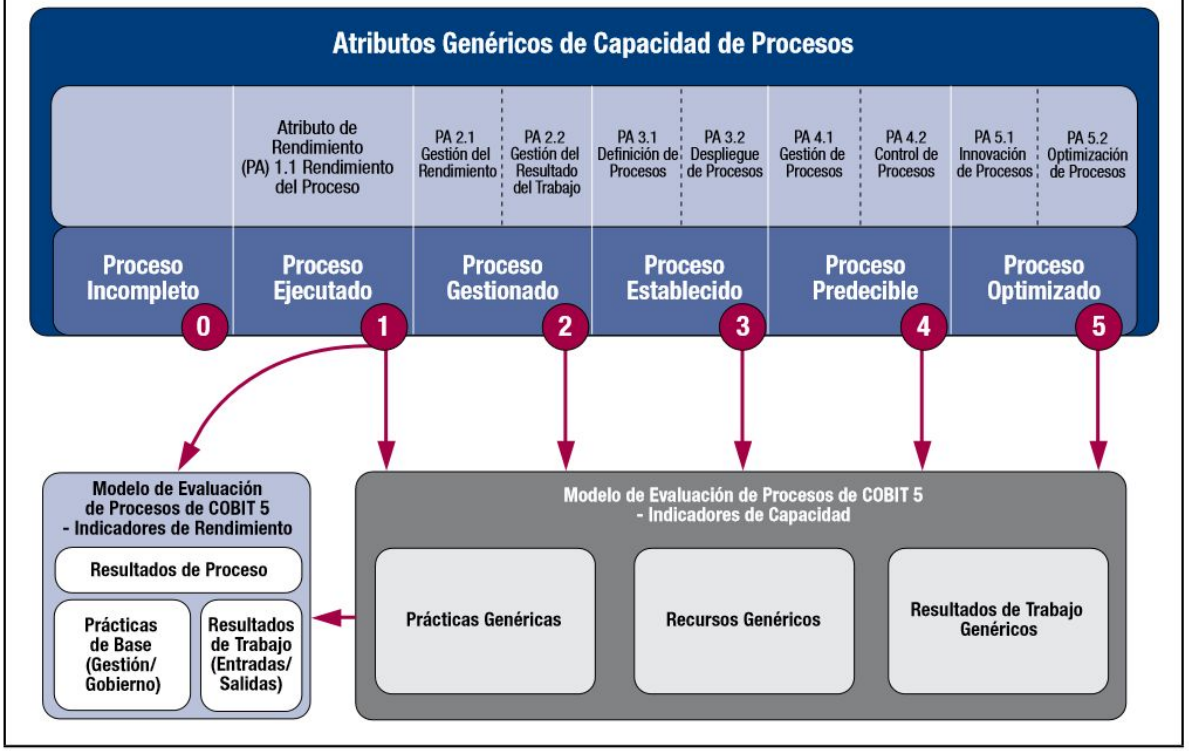
Refiriéndonos ahora al modelo de Capacidad de los Procesos de C.O.B.I.T 5 podemos decir que este introduce algunos cambios con respecto al modelo anterior.

Sin embargo, ambos modelos están orientados a medir el estado en que se encuentran los procesos de T.I o su grado de avance, y para determinar cuál es la distancia que hay entre el estado actual y el estado en el que se desearía estar. Esto permitirá delinear un camino de acción de mejora para llevar a la empresa al nivel de madurez deseado.

El nuevo Modelo de Capacidad de Procesos propone seis niveles, es así como los diferentes procesos de la organización pueden alcanzar cualquiera de ellos. Es requisito que, para alcanzar el nivel siguiente, se haya completado el nivel anterior. La siguiente figura muestra este enfoque con más claridad:

Tabla 4

Figura 19—Resumen del Modelo Capacidad de Procesos de COBIT 5



Acerca de este proceso el Marco C.O.B.I.T indica que “Existen seis niveles de capacidad que se pueden alcanzar por un proceso, incluida la designación de “proceso incompleto” si las prácticas definidas en el proceso no alcanzan la finalidad prevista:

> 0 Proceso incompleto - El proceso no está implementado o no alcanza su propósito. A este nivel, hay muy poca o ninguna evidencia de ningún logro sistemático del propósito del proceso.
>
> 1 Proceso ejecutado (un atributo) – El proceso implementado alcanza su propósito.
>
> 2 Proceso gestionado (dos atributos) – El proceso ejecutado anteriormente está ya implementado de forma gestionada (planificado, supervisado y ajustado) y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.
>
> 3 Proceso establecido (dos atributos) – El proceso gestionado descrito anteriormente está ahora implementado usando un proceso definido que es capaz de alcanzar sus resultados de proceso.

4 Proceso predecible (dos atributos) – El proceso establecido descrito anteriormente ahora se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso.

5 Proceso optimizado (dos atributos) – El proceso predecible descrito anteriormente es mejorado de forma continua para cumplir con los metas empresariales presentes y futuros.[4]"

Esta información será de utilidad para poder desarrollar más adelante el trabajo, fundamentar los argumentos y basarnos en teorías aceptadas y buenas prácticas en la materia para poder construir la propuesta propia.

CAPÍTULO II: Análisis del contexto y organización de la entidad financiera.

Introducción

Hemos seleccionado para el desarrollo de este trabajo a una entidad financiera Argentina que opera de forma similar a una entidad bancaria a la cual denominaremos "Entidad Financiera Nacional" (C.F.N.) para mantener en forma anónima cuestiones relacionadas a su funcionamiento, su estructura organizacional, su organigrama, los recursos de Tecnología de Información que utiliza entre muchas otras que no deben ser reveladas para preservar la privacidad de la organización.

Se pretende poder colaborar con la organización en el desarrollo de métricas que le sean útil al área de Seguridad de la Información a la hora de tomar decisiones, incrementar la madurez, explotar la utilidad de las herramientas, dar visibilidad a los

[4] Véase referencia bibliográfica N° [04]

controles entre objetivos que quizás aún no están establecidos, pero pueden surgir en un futuro.

Como ya se ha dicho, el objetivo no es solo satisfacer aspectos puntuales con el desarrollo de métricas específicas, sino poder aportar una metodología para futuras implementaciones en entidades financieras en el ámbito de la República Argentina.

Dicha organización cuenta con aproximadamente dos mil quinientas identidades, las cuales son gestionadas a través de un directorio activo. Recientemente comenzaron a desarrollar algunos de sus proyectos en la tecnología de la nube, lo que ha representado un gran desafío para el área de seguridad informática.

Es una empresa familiar, que aún es dirigida por sus dueños quienes están involucrados en el día a día de la operatoria. Comenzó sus operaciones en la década de los años 80 y hoy tiene presencia nacional con alrededor de cien sucursales distribuidas en todo el país.

Los clientes de esta entidad financiera pueden operar en sus sucursales, a través de terminales y canales electrónicos, billeteras virtuales y aplicaciones móviles para acceder a determinados servicios. Los servicios relacionados a transacciones internacionales quedan excluidos de esta investigación.

Contexto Organizacional de “Entidad Financiera Nacional” (E.F.A)

Esta organización está inmersa en el contexto actual de la República Argentina, quien al día de la fecha no solo se ve impactada por la situación de fuerza mayor como el Covid 19, sino que atraviesa de forma cíclica crisis económicas de las cuales las entidades financieras han aprendido a cuidarse, como así a sobrevivir.

En cuanto a la Tecnología de la Información, Argentina es un país que posee recursos humanos con formaciones muy sólidas en las materias. Si combinamos

este factor con el hecho de que los sueldos de las entidades financieras son unos de los más altos del país y sufren actualización que generalmente acompañan o igualan a la inflación, este sector se convierte en uno de los más atractivos para los trabajadores del área.

Si bien en general las entidades financieras aún manejan lenguajes de programación muy antiguos, como puede ser COBOL, y tienen regulaciones estrictas del Banco Central de La República Argentina que muchas veces limita la capacidad de innovación, por la calidad de información que estas entidades manejan y la actividad principal (el dinero) la inversión de herramientas para la protección de esta información suele ser elevada.

La entidad financiera en análisis ha tomado relevancia en los últimos años y ha llegado a convertirse en una banca comercial. La misma es de capitales privados pertenecientes a la República Argentina. Tiene su sede central el corazón económico y financiero de la Capital Federal de dicho país y, además, posee sesenta y cinco sucursales en diferentes provincias.

A la fecha, la entidad no posee subsidiarias ni sucursales en el extranjero, pero no se descarta que pueda expandir sus fronteras en un futuro. En su rol de banco comercial opera en sectores como el de empresas, personas, comercio exterior, apoya microemprendimientos, negocios fiduciarios, inversiones y trading, entre otros.

Dicha entidad financiera figura entre las veinte más importante de la República Argentina a la fecha y lidera la lista de aquellos con mayor crecimiento en los últimos años en el país.

Sintetizando, el contexto de país en el que está inmerso esta entidad no siempre es favorable. No obstante, esto no siempre se ve reflejado en las tecnologías de la Información que soportan las operaciones. Si bien no tienen un alto grado de innovación, si lo suelen tener de recursos.

Gerencia de Seguridad de la Información o Protección de Activos Informáticos (P.A.I.)

La normativa a la cual están sujetas los bancos en forma obligatoria es la "Comunicación "A" 4609", sus modificatorias o complementarias, y la última comunicación incorporada: "A" 6209, emitidas por el Banco Central de la República Argentina. Acorde con el texto de esta misma normativa, se realizan las auditorías pertinentes a las entidades financieras que operan en el país. La Comunicación consta de ocho secciones y es un "Texto ordenado actualizado de las normas sobre "Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras"[5]" (BCRA, 2017)

Dentro de esta normativa, en la sección tres, podremos encontrar un apartado en especial que regula la existencia del área de Protección de Activos de Información que hace referencia a la gestión de la seguridad. Allí se especifica que la misma deberá administrar y controlar la seguridad en referencia a los accesos físicos y lógicos en los diferentes ambientes y recursos de tecnología de información, tales como: equipamientos, herramientas, plataforma utilizadas en las diferentes sucursales, transferencias electrónicas, etc.

Entre los aspectos que destaca la regulación del B.C.R.A está el de mejoramiento continuo, que para poder llevar a cabo esta tarea es necesario poder tener visibilidad de lo que se ha hecho hasta el momento. En operaciones con un alto volumen, la posibilidad de visualizar claramente para tomar decisiones la brindan las métricas o los indicadores claves de desempeño que nos proponemos desarrollar en este trabajo.

La estrategia de Seguridad es un punto marcado en esta normativa, y la medición y el seguimiento respecto del cumplimiento de dicha estrategia deberá ser provisto por las métricas a desarrollar.

[5] Véase referencia bibliográfica N° [05].

El área de P.A.I. dentro de E.F.N. Está conformada por aproximadamente 15 personas entre las cuales se encuentra un Director de Seguridad de la Información, tres líderes de equipo y once analistas. El primero de los equipos responde a la gestión de identidades, la cual se hace de forma manual e incluye tareas como el alta, baja o modificaciones de usuarios, el desbloqueo de los mismos, la administración de las políticas de los grupos, entre otros.

Vale aclarar que al no tener un gestor de identidades, estas tareas se realizan de forma manual y una demora en las mismas puede ocasionar que un cajero no pueda operar en su sucursal o que un analista de riesgos se demore en los procesos de análisis crediticio de la carpeta de un cliente.

El segundo equipo mantiene herramientas de seguridad que son indispensables a la hora de garantizar la seguridad perimetral, tales como el cortafuegos para el cual debe gestionar las reglas o el gestor de accesos de privilegios para aquellas cuentas de servicios o sistemas que accedan como administradores y debe tener un registro de esa sesión.

Por último, el equipo al cual este trabajo pretende hacerle un aporte significativo. Es el referente a controles y monitoreo. En una entidad financiera este equipo cobra aún más fuerza que en cualquier otro porque no hará solo un aporte a la madurez de la Seguridad de la Información, sino que también debe llevar un estricto control sobre ciertos puntos que son exigidos y auditados por el ente regulador, en este caso el B.C.R.A.

En el siguiente apartado de este mismo capítulo nos dedicaremos a ahondar sobre las tareas de este último equipo.

Área de controles

Como se dijo anteriormente, este es el área que tendrá a cargo la ejecución de los controles y el desarrollo de las métricas o de los indicadores claves de desempeño

que utilizar E.F.N. Algunos de ellos son de índole mandatorio y otros se harán para garantizar la satisfactoria y eficiente aplicación del Plan Estratégico de Seguridad que se haya desarrollado.

Si ahondamos en las tareas de las cuales este área es responsable, cuestiones como la actualización de parches en los diferentes sistemas operativos, o las versiones de los sistemas operativos utilizados deben ser controlados de forma estricta así como la rotación de claves y la utilización de usuarios con altos privilegios. En relación con los controles efectuados la Comunicación "A" 4609 menciona:

> Adicionalmente, los controles efectuados por el área deben establecerse formalmente a través de reportes operativos, que permitan la supervisión continua y directa de las tareas y el análisis del logro de las metas definidas. Estos reportes deben mantenerse en archivo por un término no menor a 2 (dos) años, utilizando para ello soportes de almacenamiento no reutilizables y preferentemente sometidos a algoritmos de función irreversible o como normalmente se denomina "funciones hash[6]". (BCRA, marzo de 2017, p. 7)

En la Comunicación "B" 9042, que amplía el texto de la Comunicación "A" 4609 se puede encontrar el siguiente texto:

> El área de protección de activos de información es la responsable primaria de efectuar las actividades regulares de monitoreo y controles de verificación. Las frecuencias de administración y procesamiento de los programas de aplicación y sus registros de datos resultantes. Asimismo, se deben controlar especialmente los usuarios con niveles de accesos privilegiados, su utilización de revisión dependerá del valor de la información administrada y del riesgo asociado a la aplicación o servicio tecnológico. Se deben evaluar los accesos a las funciones y su asignación. Los incidentes y debilidades en materia de seguridad deben registrarse y comunicarse inmediatamente a través de adecuados canales de información, con el objeto de analizar sus causas e implementar mejoras en los controles informáticos a fin de evitar su futura ocurrencia[7]. (BCRA, marzo de 2017, p.7)

[6]Véase referencia bibliográfica N° [06]
[7] Véase referencia bibliográfica N° [06]

El área está compuesta por una líder y tres analistas que ejecutan las tareas operativas diarias. Reportan al gerente de Seguridad Informática que a su vez reporta al director de Tecnología. El gerente de Seguridad Informática tiene reuniones mensuales con el área de auditoría y riesgo tecnológico para poder conversar y llevar un seguimiento de los temas y puntos levantados por ambas partes, así como tener actualizado el catálogo de tareas que el área desempeña.

Conclusiones del análisis

Si bien la E.F.N. cuenta con un área destinada a la Seguridad de la Información y eso agrega valor y sienta bases sólidas sobre las cuales crecer y construir, consideramos que este trabajo puede aportarles procedimientos y metodologías para desarrollar métricas e indicadores claves de desempeño que le permita mejorar sus procesos, incrementar sus niveles de madurez, dar a conocer principios de seguridad esenciales entre sus trabajadores y, además, detectar cuales son los principales puntos de control para poder trabajar sobre ellos y mejorarlos.

La entidad es receptiva a mejoras, está en un proceso de automatizaciones de procesos y tareas repetitivas que insumen más tiempo del deseado de sus analistas. Se espera que cuando dichas automatizaciones estén implementadas satisfactoriamente, los analistas que previamente desarrollaban la tarea dispongan de tiempo adicional para poder volcarlo a mejoras.

Esta tesis no pretende imponer ningún cambio a la organización, no obstante, persigue el objetivo de arrojar claridad sobre las tareas, los proyectos y los procesos que desempeña el área y aquellos puntos de mejora. A su vez también creemos que le va a permitir entender cuán alineada están sus prácticas en referencia a los marcos teóricos tenidos en cuenta en el primer apartado de este trabajo.

CAPÍTULO III: Indicadores Operativos

Introducción

En los últimos tiempos, cada vez son más las organizaciones que se dan cuenta de la importancia que apareja contar una Gestión Estratégica de la Seguridad de la Información. Los ataques que se perpetran crecen, la información abunda y se transforma en un bien preciado. Los altos directivos son conscientes de esta tendencia y buscan implementar acciones concretas que les permitan, o bien entender donde están posicionados en la materia, o bien ejecutar acciones concretas para comenzar a diseñar un plan.

Toda acción que se ejecute en materia de Seguridad de la Información debe ser controlada y medida para poder tomar decisiones al respecto. Sin embargo, la Entidad Financiera Nacional, a la cual se pretende agregar valor y ayudar a diseñar sus métricas e indicadores claves de desempeño en esta tesis, debe ejecutar controles y tener mediciones. Caso contrario, el organismo de contralor del país podría sancionarla.

A continuación, desarrollaremos algunos conceptos sobre los Indicadores Operativos, uno de los cuales la organización debe poseer para responder con las solicitudes correspondientes.

Conceptos Teóricos

En el apartado referente al Marco Teórico de este mismo trabajo, se hizo una introducción general a las métricas y los indicadores. Lo que en este capítulo se pretende es ahondar sobre conceptos teóricos de los indicadores operativos en particular, para entender a que hacen referencia y que abarcan de la organización.

Una de las formas de definir a los indicadores, es como métricas generales que permiten evaluar el riesgo o la eficiencia de un Sistema de Gestión de Seguridad de

la Información (SGSI), implementado de acuerdo con alguna de las normativas y buenas prácticas vigente y normalmente aceptadas en el ámbito o a una combinación de ellas.

Los indicadores pueden ser volcados en un cuadro de mando que permita gestionarlos y administrarlos de forma más clara. En este trabajo se realiza dicho cuadro en una planilla de cálculo en donde se vuelcan todos los indicadores asociados a sus respectivos objetivos de control. En este cuadro también deberá poder verse la frecuencia con la cual el indicador operativo será medido y su progreso en el tiempo. En el caso de ser posible, se recomienda establecer también un objetivo al que se aspira a alcanzar que se alinee con un correcto funcionamiento del SGSI.

La ISO/IEC 27.004 define a un indicador como "medida que provee una estimación o evaluación de atributos específicos, derivados de un modelo analítico con respecto a la necesidad de información definida[8]" (IRAM, 2010, p.10). Otro de los conceptos que nos resultan interesantes, es aquel que considera que es muy difícil evaluar aquello que no se puede medir, y propone para poder medir un proceso que cuente con indicadores.

En general, los indicadores claves de desempeño buscan cuantificar si se ha podido alcanzar el cumplimiento de un objetivo basándonos en la efectiva y eficiente ejecución de un proceso. Sin embargo, los indicadores operativos por sí solo no se podrán relacionar linealmente con el cumplimiento de un objetivo de negocio. Pero es importante considerarlos ya que nos permitirán ejecutar los controles, que son importante para el SGSI y además, pueden aportar a la medición de indicadores tácticos o estratégicos.

Importancia de utilizarlos en el área de Seguridad Informática

[8] Véase referencia bibliográfica N° [03].

Consideramos buenos indicadores operativos aquellos que nos arrojan información valedera, concreta, oportuna y medible o que son una ponderación entre acciones que se ejecutaron acorde al procedimiento y aquellas que, por el contrario, se ejecutaron de forma incorrecta. También podemos agregar a esto las métricas sobre los niveles de servicio referentes al tiempo y costo de aprovisionamiento.

Es importante aclarar que aunque la entidad tenga la capacidad de generar cientos de indicadores operativos, esto no garantiza que se esté controlando más, mejor o eficientemente. El objetivo de los indicadores operativos es sentar bases para construir indicadores claves de desempeño y, en este sentido, se deben generar los mínimos necesarios para alcanzar el objetivo planteado.

Se debe considerar también que, en algunos casos, es posible que el Indicador Operativo aporte un simple dato concreto que permita cuantificar una determinada acción de la compañía y que, luego con unirse a otros, permitan entender, componer o responder a cuestiones tácticas o estratégicas.

Los indicadores operativos para convertirse en información de utilidad, deben estar direccionados a medir acciones que estén controladas por la empresa y tengan absoluta independencia del entorno. Los indicadores que consideramos útiles son arrojados, en líneas generales, realizando una ponderación que considera las acciones que se llevaron a cabo de forma correcta y aquellas que fueron ejecutadas de forma incorrecta. Vale aclarar que dentro de las acciones incorrectas incluimos los falsos negativos y positivos que surgen de forma frecuente en nuestro análisis.

En pocas palabras, los indicadores operativos de seguridad informáticas resultan sumamente útiles a la hora de generar información y agregar valor, es por esto que la propuesta de generar todos aquellos que se consideren necesarios para cada control o proceso resulta de suma importancia. Es fundamental tener en vista que no los vamos a utilizar de forma directa para la construcción de los indicadores claves de desempeño, sino que aportarán a los diagnósticos que permitan identificar aquellos controles, procesos o procedimientos que están funcionando correctamente o, por el contrario, detectar dónde se debe aplicar un cambio en aquellos sobre los cuales los indicadores claves hayan prendido una alarma.

Incidentes y capacitaciones relativa a la operación de los canales electrónicos

Dentro del campo de aplicación profesional de la Tecnología de la Información, Auditoría y Seguridad de la Información, es cada vez más frecuente conocer que algunos de los canales electrónicos que los bancos tienen a disposición han sido vulnerados.

Si bien las métricas sobre estos canales exceden el alcance de este trabajo, nos parece interesante mencionar cuales son los riesgos a los cuales estas organizaciones están expuestas para que puedan tomar medidas de mitigación. Ya sea a través de capacitación, concientización, formación o revisión de procesos.

Los principales canales que recientemente (2020) han sido atacados y, en algunos casos, vulnerados en la República Argentina se enumeran y describen brevemente a continuación:

Sistema de administración de terminales de autoservicio (TAS)

Dentro del ámbito financiero, se entiende por este sistema como aquel que está diseñado para brindarle servicios a los clientes en las diferentes operaciones que el mismo esté habilitado a realizar. Este sistema le da la posibilidad al banco de gestionar sus dispositivos de cara al cliente, adaptándolas a las diversas necesidades específicas que pueden presentar los distintos tipos de clientes (personas, comercios, exportadoras, importadoras, etc) y, a su vez, enfocar los esfuerzos de acuerdo con la estrategia de atención que se haya definido.

hoy en día se busca de forma permanente agilizar las transacciones, evitar las grandes filas de personas y, en línea con el nuevo paradigma, automatizar. En consecuencia, todas aquellas operaciones que puedan ser volcadas a un canal de autoservicio se harán. Sin embargo, recurrir a este método no tiene que desproteger al usuario abriendo un posible nuevo vector de ataque.

A tales fines, es mi sugerencia que los autoservicios sean tratados, monitoreados y gestionados como infraestructura crítica poniendo especial atención en la operación de sus "software", las autenticaciones, autorizaciones, trazabilidad de las operaciones, accesibilidad física, entre otras cuestiones.

Cajeros Automáticos (ATM)

Es elemental que en una primera instancia pongamos en común lo que entendemos por un cajero automático. A los efectos de este trabajo consideramos que:

> "Es una computadora especializada que le permite administrar su dinero de manera conveniente. Por ejemplo, casi todos los ATM le permiten retirar dinero, y muchos le permiten hacer depósitos. En algunos ATM, puede imprimir un estado de cuenta (un registro de la actividad o las transacciones en su cuenta), verificar los saldos de sus cuentas (la cantidad de dinero que hay en sus cuentas en este momento), transferir dinero entre sus cuentas e incluso comprar sellos. Habitualmente puede acceder a la mayoría de los servicios en un ATM operado por su propio banco.[9]" (Wells Fargo, 2020)

Los cajeros automáticos están sujetos a diferentes tipos de ataques, entre los cuales pueden listarse las siguientes categorías: fraudes, ataques a la seguridad física de los mismos y ataques sobre los procesos lógicos que operan los mismos.

Los fraudes hacen referencia a la impersonalización de un usuario por otro, haciendo uso de credenciales o "token" que hayan sido previamente comprometidos a través de los múltiples medios conocidos, como puede ser el *"skimming"*, *"phishing"* o la ingeniería social.

Los ataques a la seguridad física de los cajeros automáticos, apuntan a extraer el dinero que estas computadoras almacenan en su interior. Generalmente, estos

[9] Véase referencia bibliográfica N° [07]

ataques vienen aparejados de destrucciones materiales de las vidrieras que los protejen y el cajero automático en sí mismo.

Existen antecedentes donde se han atado los cajeros automáticos a un camión con una soga detrás y se los ha semiempotrado de la pared para luego asaltar el dinero contenido por los mismos.

Por último, se considera también los ataques lógicos a estas computadoras. Estos requieren de un mayor entendimiento de los procesos que estos cajeros están llevando adelante. Se puede ejecutar mediante el robo de información confidencial del usuario o, también, atacando la integridad de la información que gestiona el cajero.

Aquí se dejan registradas algunas recomendaciones de seguridad para tener en cuenta al usar ATM (Wells Fargo, 2020):

- “Evite usar ATM en lugares apartados o desolados. Use ATM ubicados en el interior de bancos o supermercados, donde haya otras personas a su alrededor. Use ATM en lugares públicos y bien iluminados.
- Preste atención a lo que sucede a su alrededor cuando retire dinero. Si advierte algo fuera de lo normal, regrese más tarde o utilice otro ATM.
- Si le parece que alguien ha manipulado el ATM, no lo use. (Esto podría significar que un delincuente ha colocado un “*skimmer*” [duplicador] en el ATM para robar su información financiera). Si una persona sospechosa le ofrece ayuda para usar el ATM, rechácela y váyase.
- Cuando ingrese su PIN, cubra el teclado para que nadie más pueda verlo.
- Después de completar su transacción, recuerde retirar su tarjeta, el efectivo y cualquier documento impreso, como recibos o estados de cuenta.

- Guarde su dinero y su tarjeta ATM antes de salir del ATM. Evite siempre mostrar su dinero en efectivo. Verifique siempre que la cantidad que retiró o depositó sea la misma que la cantidad impresa en el recibo.
- Llévese sus recibos para que posibles delincuentes no sepan cuánto retiró o cuánto dinero hay en su cuenta.
- Al usar el ATM del autobanco, mantenga cerradas las puertas y encendido el motor[10]"

La capacitación y concientización de los usuarios respecto de los puntos detallados precedentemente, como también con el personal de seguridad y del banco, y la incorporación del área de seguridad de la información en la revisión de los procesos lógicos que los cajeros automáticos ejecutan, es elemental para poder mitigar el riesgo y prevenir estos ataques.

Puntos de venta (POS)

Esta tecnología es conocida como una combinación de "software" y "hardware" que permite ejecutar una transacción de compra venta, generalmente con tarjeta. Existen dos canales por los cuales se pueden concretar dichas transacciones: los canales en línea o los tradicionales en forma presencial en el local.

Dependiendo cual sea el canal que se utilice, habrá una variación sustancial de los riesgos a los cuales queda expuesto el usuario o el comercio. En términos generales, ambos pueden ser estafados, debiendo abonar algún cargo que no les corresponde del lado del titular de la tarjeta, y no pudiendo cobrar una mercadería entregada, del lado del vendedor.

[10] Véase referencia bibliográfica N° [07].

Los POS pueden ser vulnerados por “malware”, es decir un “software” malicioso que toma control sobre el sistema principal con el objetivo de hacerlo ejecutar una acción para lo cual el mismo no fue diseñado, la fuerza bruta, ingeniería social, “hardware” que se conecte al POS o una combinación de ellos.

Algunas recomendaciones útiles para el uso seguro y correcto implementación de estos dispositivos son: velar porque las contraseñas sean fuertes, configurar el POS un número limitados de intentos de inicio de sesión y limitar el acceso al software lo máximo posible siguiendo la premisa de menor privilegio posible.

Banca Internet (BI)

Los posibles vectores de ataque a la banca internet son tantos como puntos débiles se puedan encontrar en un sistema, en un usuario, en una combinación de ellos, en una mala implementación, entre muchas otras causales.

Es aún indeterminado el espectro de amenazas a los que este sistema está sometido, y a título personal, creo que será difícil en el futuro cercano limitarlo a una lista de alternativas. Sin embargo, la digitalización cada vez fuerza más al mundo a migrar hacia estos canales. Debemos ser conscientes de que son una gran oportunidad y también una debilidad.

Como profesionales de seguridad, debemos hacer nuestro mejor esfuerzo por dar a conocer cuáles son los riesgos a los que los usuarios se exponen y, adicionalmente, capacitar a los usuarios internos de las respectivas entidades financieras para que sean capaces de diseñar y desarrollar los procesos con los eslabones de seguridad ya incorporados a las diferentes capas que sostienen el sistema.

Principales Indicadores Operativos en Seguridad de la Información

A la hora de construir un indicador operativo, la compañía debe tener en claro cuales son sus objetivos estratégicos referidos al área de tecnología de la información y de seguridad ya que, con estos indicadores, se pretende construir una base sólida que luego permita elaborar mediciones de mayor complejidad.

La actividad principal de la empresa tomará un papel fundamental a la hora de elegir qué indicadores se ejecutarán y con qué periodicidad, ya que ninguna empresa cuenta con la infraestructura, los recursos ni sería eficiente construir indicadores que no sean utilizados o aporten información valiosa.

A continuación, listamos algunos de los indicadores de seguridad de la información que pueden servir de ejemplo. No son de ninguna manera los únicos que existen. En las conclusiones finales, se podrán encontrar indicadores operativos elaborados específicamente para la Entidad Financiera Nacional a la que este trabajo se aboca.

- Cantidad de incidentes de seguridad que fueron reportados en el periodo.
- Cantidad de ataques prevenidos por las herramientas de seguridad de la compañía (Cortafuegos, IPS).
- Cantidad de actualización es de parches de seguridad que se realizaron sobre sistemas Linux.
- Tiempo promedio de respuesta para atender los incidentes.

A su vez, se detallan a continuación los indicadores operativos que se proponen en el conclusiones finales que fueron diseñados a la medida de la Entidad Financiera que se trata en este trabajo. Se podrá leer también una breve descripción de los mismos:

Alta de usuarios: este indicador pretende medir la cantidad de altas de usuarios que dan visibilidad acerca de las operaciones y luego correlacionar datos. Esta información se debe dividir entre usuarios internos y externos.

Baja de usuarios: aquí se persigue el objetivo de medir la cantidad de bajas de usuarios dando visibilidad acerca de las operaciones y luego correlacionar datos.

Este punto también debe ser susceptible de ser divido en usuarios internos y externos.

Modificación de usuarios: con este indicador la Entidad Financiera podrá medir la cantidad de modificaciones de usuarios permitiendo dar visibilidad acerca de las operaciones y luego correlacionar datos.

Inicio de sesión: teniendo en cuenta estos logs, se podrá medir la cantidad de inicio de sesión, su duración y la IP desde donde fue realizada. Esto dará visibilidad a la organización en general, y permitirá tomar acciones en caso de algún incidente o anomalía en particular.

Cierre de sesión: aquí mediremos la cantidad de cierre de sesión, su duración y la IP desde donde fue realizada. Este es un indicador que pretende dar visibilidad a la compañía sobre volumen y la persistencia de las sesiones al ser comparado con el indicador detallado previamente.

Gestión de usuarios de servicios por plataforma: en este caso se contabilizará la cantidad de nuevos usuarios de servicios y la cantidad de veces que los existentes accedieron, teniendo la posibilidad de visualizar la información en un tablero y aplicarle filtros por sucursal, aplicación, etc.

Gestión de usuarios de servicios de base de datos: con este indicador se contabilizará la cantidad de nuevos usuarios de servicios y la cantidad de veces que los existentes accedieron. Al igual que en el indicador anterior, el objetivo es poder construir un tablero nutrido de información que permita a los mandos medios y altos tomar decisiones en base a la información así como también manipularla fácilmente para poder apreciarla desde distintos ángulos.

Gestión de usuarios de servicios de aplicativos: estos usuarios son críticos y consideramos importante contabilizar la cantidad de nuevos usuarios de servicios y la cantidad de veces que los existentes accedieron. De esta manera se podrá tener un mayor control y trazabilidad de los mismos.

Gestión de usuarios de servicios de comunicaciones: al igual que en el caso anterior, contabilizar la cantidad de nuevos usuarios de servicios y, la cantidad de veces que los existentes accedieron, permitirá comprender cuál es la demanda que tiene la organización respecto de estos usuarios y la debida gestión que debe implementar.

Caducidad de usuarios de servicios: en este punto se pretende comprender qué usuarios quedaron obsoletos o fuera del circuito frecuente de uso. Este indicador medirá sobre todos los tipos de usuarios de servicios, considerando que cantidad no fueron utilizados por dos meses con el objetivo de darlos de baja evitando vulnerabilidades por la existencia de usuarios con accesos y en desuso.

Versión de los sistemas operativos: tener un inventario claro de los recursos utilizados permitirá asegurar la infraestructura y sus componentes de forma apropiada. Es por eso que este indicador recolecta y listara las versiones de los sistemas operativos utilizados en los servidores identificados como críticos. Con este detalle se podrá planificar actividades como el parcheo, la "*hardenización*" o la homologación de software y aplicaciones, entre otras.

Actualización de parches de los sistemas operativos: la información recolectada en el indicador anterior colaborará con la tarea que debe ejecutarse y medirse en este caso. Es fundamental identificar la fecha, versión y módulos actualizados en la última descarga de parches de los sistemas operativos para poder entender cual es la situación actual de la infraestructura y cómo debe plantearse el mantenimiento de la misma.

Renovación de certificados SSL/TLS: la encriptación en tránsito es fundamental para garantizar la integridad de la información que se trafica. La gestión de estos certificados implica hacer un exhaustivo seguimiento de las fechas de vencimiento de los mismo, corroborando que todos ellos aún están vigentes y logrando visibilidad de la cantidad de certificados que han sido renovados en el periodo. Aún más

destacable, es poder prever los próximos vencimientos e iniciar las gestiones pertinentes de renovación.

Conclusiones

La construcción de los indicadores operativos es la primera que debe realizarse en cuanto a la tarea en sí de mediciones. Por su puesto que la misma debe ser ejecutada una vez que la estrategia de seguridad de la información está definida y debe ser revisada de forma periódica.

Contar con información referente a la operación le permitirá a la organización tener una visión respecto de donde está posicionado en términos de volumen y, a su vez, podrá cuantificar y magnificar las operaciones diarias. Es probable que los resultados arrojados conformen un gran volumen de información, con lo cual es crítica la forma y herramienta que se elija para mostrar la información a los altos directivos.

Una mala elaboración y ejecución de los indicadores operativos impactan negativamente, sin lugar a duda, en los indicadores tácticos y estratégicos que dependen de ellos. Entonces, si bien estos primeros indicadores no requieren de gran conocimiento técnico para su ejecución, si se recomienda poner el foco en el diseño, el análisis y la revisión de los mismos.

CAPÍTULO IV: Indicadores Tácticos

Introducción

Para poder entender el objetivo de este capítulo, partimos de la premisa de que si sabemos que algo sucede, pero no lo podemos medir, entonces estamos hablando de un nivel de conocimiento escaso o deficiente. Para refrescar, entendemos a la seguridad como aquello que protege a la compañía frente a un potencial daño, que persigue la disminución o ausencia del riesgo. Sumando a esto lo previamente definido a los indicadores, podemos concluir que las métricas de seguridad nos mostrarán el grado de seguridad relativa a un proceso, control o procedimiento.

Como se mencionó anteriormente, los indicadores operativos son ideales para cuestiones técnicas y puntuales, cuantificables de forma sencilla. El resultado que arrojan, en general, es más un dato concreto que una información que permita tomar decisiones. Pueden darnos una guía acerca si una plataforma se maneja adecuadamente, si una herramienta está correctamente implementada o si se está realizando una tarea de acuerdo con el procedimiento.

Los indicadores estratégicos, sin embargo, pretenden aportar una visión integral a los altos mandos y acorde a los objetivos estratégicos planteados, para brindar información para la gestión de la seguridad de la información. De esta forma empiezan a acercarse a conceptos tales como la manera en la que se están gestionando los riesgos en la organización, grado de involucramiento y alineamientos con requisitos de seguridad en los proyectos, capacitación y concientización de los usuarios, cumplimientos de políticas y alcance de resultados respecto de la estrategia.

Junto a los indicadores estratégicos, los indicadores tácticos permitirán a los mandos directivos o gerenciales tomar e implementar las decisiones que consideren necesarias y/o aplicar un cambio en el rumbo. Desarrollaremos a continuación algunos conceptos claves que sugerimos considerar al momento de elaborar un indicador táctico.

Conceptos teóricos sobre los indicadores tácticos

Los indicadores tácticos persiguen el objetivo de generar una mejor visión sobre los activos que el área de seguridad de la información administra, y colaboran de forma activa y constante con el monitoreo sobre la efectividad respecto del alcance de los objetivos permitiendo que los responsables tomen las decisiones necesarias para cumplir con la estrategia pautada.

Debemos recordar que, en términos generales, la planificación táctica tiene directa correlación con el plan que se debe llevar a cabo en el mediano plazo. Consideramos a mediano plazo un lapso de uno a tres años, dependiendo de la organización, de su actividad principal y del tiempo estimado en la planificación estratégica. El plan a nivel táctico debe estar alineado en su totalidad con la planificación estratégica que realizó la compañía. Dicho alineamiento facilitará su cumplimiento y potenciará las acciones llevadas a cabo tal fin.

Si nos remitimos al origen de la palabra técnica, proviene del griego. En sus raíces deviene del verbo “tessai”, que al traducirlo puede entenderse como ordenar. Inevitablemente este concepto se vincula con la estrategia en el sentido de proponer medios para poder alcanzar el cumplimiento de un objetivo. En otras palabras, las tácticas se utilizan como instrumentos para poder implementar el plan de acción ideado en la estrategia de la organización.

Si lo aplicamos al área de seguridad informática en el contexto de una entidad financiera, la táctica nos permite conectar el plan estratégico vinculado estrechamente con cuestiones abstractas que marcan un norte para la organización, con aquellas acciones determinadas que deben ejecutarse a nivel operativo.

Principales indicadores tácticos en Seguridad de la Información

Los indicadores tácticos son conectores entre el plan estratégico y el nivel operativo. Al oficiar de vínculo, se deben identificar y relacionar las variables para una correcta integración. Con lo cual en mi opinión como profesional deben cumplir dos requisitos, por un lado entender cabalmente y estar alineados con los pilares que plantea la organización en su estrategia, y por el otro, deben ser sencillos de traducir a acciones concretas que permitan desarrollar las operaciones diarias en la materia.

No está demás aclarar que este tipo de indicadores no son algo que puedan ser definidos de forma general, la determinación de los mismos va a depender de la estrategia de la organización, la actividad principal de ella, la estructura del área de seguridad informática, entre otras cosas. Por todo lo expuesto, proponemos los siguientes indicadores para una entidad financiera con la estructura descrita en el capítulo II y las regulaciones vigentes del país.

A continuación, se detallan los indicadores tácticos identificados:

- Grado de cumplimiento de la configuración de las políticas de directivos de grupo en los dispositivos de personal propio y terceros.
- Eficacia del control y homologación de aplicaciones autorizadas en los dispositivos que almacenen información de la compañía.
- Cantidad de políticas de filtrado de correo electrónico no deseado o phishing.

Además de estos indicadores comúnmente aceptados dentro del ámbito y que pueden ser aplicables en forma general a cualquier organización, para la entidad financiera objeto de aplicación profesional en este trabajo, se han desarrollado y propuesto los siguientes indicadores (los cual pueden ampliarse en las conclusiones finales de la presente tesis):

Estado de los proyectos del área de Seguridad de la Información: llevando adelante la medición de este indicador, se pretende tener un panorama esclarecedor en cuanto al grado de avance de los proyectos del área de seguridad de la información, así como la participación que el arte tiene en proyectos de la entidad financiera.

Estado de los proyectos: En este punto, se pretende visualizar cual es el porcentaje de adhesión de los proyectos de la organización a las recomendaciones de Seguridad de la información logrando visibilidad sobre la implementación de las propuestas para asegurar los desarrollos.

Tiempos de aprovisionamiento de roles: seguridad de la información es también un área que dentro de las organizaciones presta servicios a sus clientes internos, es decir a los usuarios de la compañía. Poder medir el nivel de servicio prestado es elemental para entender si se está cumpliendo con los objetivos estratégicos que se han planteado. Aquí se pretende saber cuál es el tiempo que le implica al área de gestión de identidades aprovisionar un rol, segregado por los tiempos que tardan en la aprobación todos los involucrados en el flujo del mismo.

Altas por sucursal y plataforma: utilizando el indicador operativo acerca de las altas, que se detalló en el capítulo anterior, en este punto se pretende generar información para poder entender qué sistemas son los más requeridos y obtener tendencia por regiones según las altas en las diferentes regiones donde la entidad tiene sucursales para poder orientar los esfuerzos a aquellas regiones que tengan mayor demanda o plataformas más requeridas o utilizadas.

Resolución de incidentes: la resolución de incidentes no es una tarea que se limita a cerrar el caso, hacer todo el análisis acerca de su causa raíz y entender cuales son los principales vectores de ataques es fundamental para poder detectar a tiempo y estar preparados para responder a cualquier anomalía. En este sentido, obtener una lista de las categorías sobre las cuales se generaron incidentes permitirá tener información para procesar, por ejemplo, determinar cuántos de ellos fueron incidentes y cuantos falsos positivos, así como poder entender la calidad de los mismos y posibles puntos de control o fallo de la compañía.

Detección de incidentes: desarrollamos este indicador para poder identificar mensualmente si las herramientas de detección y prevención de incidentes han operado correctamente y cuántos potenciales ataques han frenado.

Aprovisionamiento a los sistemas críticos: en este indicador se tendrán en cuenta las altas del día abarcando los tres sistemas críticos de la compañía: el mail, la mensajería interna y el acceso a la intranet. De esto se deberá prestar especial atención a cuantos accesos fueron dados en tiempo y cuántos han fallado.

Filtrado de correo electrónico: después de la ejecución de los pasos necesarios para este indicador, la entidad financiera obtendrá estadística de filtrado y detección de correo electrónico no deseado y los que han sido reportados como sospechosos por los usuarios. Como política de la empresa, los correos reportados deberán ser analizados y, si corresponde, agregados a una lista corporativa de filtrado de correo.

Control y homologación de aplicaciones autorizadas: dentro de las medidas básicas que la empresa considera importante para asegurar sus sistemas, se encuentra contar con sistemas homologados que fueron previamente analizados por las áreas correspondientes y garantizan los estándares que la empresa persigue. La detección en una muestra representativa de dispositivos y servidores sobre la instalación de sistemas o aplicaciones que no están homologados por la entidad es uno de los controles que se deben implementar para poder hacer un seguimiento del cumplimiento de esta política.

Configuración de las políticas de directivos de grupo: Es imprescindible controlar el correcto impacto de las políticas de directivas de grupo de la compañía en los dispositivos de personal propio y terceros, velando porque las mismas sean acorde a los estándares de la entidad financiera. Con este indicador se logrará detectar y enumerar proactivamente desvíos.

Firma del acuerdo de confidencialidad de personal externo: este indicador responde a una exigencia del Banco Central de la República Argentina hacia con todas las entidades financieras autorizadas que operen en territorio nacional. Por lo tanto, es de carácter mandatorio monitorear este aspecto. Lo que se propone es, de acuerdo con las altas arrojadas en el indicador operativo, cotejar con la cantidad de acuerdos de confidencialidad firmados para concluir si todos los terceros ingresados en el

sistema y activos han firmado el acuerdo correspondiente, caso contrario poder tener información confiable para remediarlo.

Conclusiones

Los indicadores tácticos permitirán entender cómo la organización avanza en la ejecución y cumplimiento del plan estratégico a través de acciones concretas que, generalmente, no estarán vinculadas a operatoria diaria o a tareas rutinarias. Un indicador táctico puede alertarte sobre una deficiencia en los sistemas que en la operatoria diaria puede no ser detectadas.

Este tipo de indicadores apunta a brindar información a los mandos medios para poder apuntalar la operatoria diaria y hacer foco sobre aquellos rumbos que deben ser modificados. A su vez, permiten tener visibilidad del grado de apego al plan estratégico hecho por la organización y van a nutrir de información a los indicadores que responden a aquel.

Es para mi importante destacar que si los indicadores tácticos que están correctamente diseñados permiten dar visibilidad sobre el avance de los proyectos de seguridad informática como también de aquellos donde la seguridad informática tenga injerencia o está convocada a modo de consulta. Esta área es clave para securizar la organización de forma homogénea y no solo en aquellos aspectos en donde el área de seguridad está destinada a focalizar, ya sea por normativa o por estrategia.

CAPÍTULO V: Indicadores Estratégicos

Introducción

Un indicador puede entenderse como parámetros basados en métricas que permiten monitorear el avance hacia los diferentes objetivos que se haya planteado la organización. Trasladando esta idea, un indicador estratégico se sustenta en métricas que permitan monitorear el progreso para alcanzar los objetivos estratégicos que hayan sido fijados para la compañía.

Aquello que se pretende lograr a nivel estratégico a lo largo del tiempo es posible de ser medido con indicadores. Aquellos objetivos de esta índole van a derivar en operacionales, y a su vez estos poseerán sus propias metas, indicadores e iniciativas propias.

Demás está decir que, para poder construir los indicadores estratégicos y ejecutar su medición, es necesario que previamente se hayan planteado claros objetivos estratégicos que le permitan al área de seguridad trabajar acorde a sus objetivos.

Conceptos teóricos sobre los indicadores estratégicos

Los indicadores estratégicos suelen ser planteados por la alta gerencia y comunicados a los mandos medios para que puedan desarrollar tácticas que se alineen con la estrategia. Dicha estrategia permite dar visibilidad a proveedores, clientes, órganos de control y demás interesados acerca de las medidas tomadas para garantizar la seguridad de la información y los activos de la compañía.

La estrategia de una organización no siempre es sencilla de traducir a números o a hechos concretos que sean cuantificables para poder ser medidos. Sin embargo, los indicadores deben tener en cuenta quién utilizará esa información, con que periodicidad será consumida, cuales son los factores claves de éxito, entre otras cosas.

La estrategia de una organización no es algo que pueda ser ejecutado en el corto plazo, en consecuencia los indicadores estratégicos requieren de una medición continua a través del tiempo que permita que sean comparables con el pasado y arroje una visión para poder, no solo tomar decisiones sino también entender en dónde está la compañía posicionada en función del lugar en donde planificó estar.

Esta clase de indicadores requiere de la capacidad de tener una visión macro de los objetivos de Seguridad de la Información de la compañía y, utilizando una metáfora, “no solo ver los árboles, sino poder todo el bosque al que conforman”. Los indicadores que miden la evolución de la estrategia deben estar en consonancia, y es posible que en algunos puntos convergen, con otros indicadores más generales del área de Tecnología de la Información.

Principales indicadores estratégicos en Seguridad de la Información

Los principales indicadores estratégicos son aquellos que permiten dar visibilidad sobre el progreso de la estrategia delineada a principio del ciclo. Es importante que esta estrategia sea debidamente comunicada hacia toda la organización en forma de cascada para que cada uno de los empleados esté comprometido con la misma y al tanto del objetivo superior que está persiguiendo con cada acción que realice.

La estrategia de Seguridad de la Información permitirá a la compañía marcar el rumbo general de hacia dónde se dirige y qué objetivos quiere cumplir en el mediano plazo. La estrategia siempre puede ser revisada y modificada de acuerdo con el contexto.

El objetivo de los indicadores que proponemos en este trabajo es para dar un seguimiento acerca de cómo evoluciona la ejecución de las acciones que llevarán al cumplimiento de la estrategia, pero también entender a tiempo y de forma proactiva si hay desvíos en el alcance de estos objetivos para poder tomar acciones correctivas.

Algunos de los indicadores generales a cualquier organización que proponemos son:

- Estado de los proyectos: porcentaje de adhesión de los proyectos de la organización a las recomendaciones de Seguridad Informática.
- Tiempos de aprovisionamiento de roles: cual es el tiempo de aprovisionamiento de un rol segregado por los tiempos que tardan en la aprobación todos los involucrados en el flujo.
- Altas por sucursal y plataforma: utilizando el indicador operativo acerca de las altas, generar información para poder entender qué sistemas son los más requeridos y obtener tendencia por regiones según las altas en las diferentes regiones donde la entidad tiene sucursales.
- Resolución de incidentes: obtener una lista de las categorías sobre las cuales se generaron incidentes. Determinar cuántos de ellos fueron realmente incidentes y cuantos falsos positivos.

Más allá de los indicadores detallados arriba, que tienen vigencia en el campo de la Seguridad de la Información, no debemos olvidar que en este trabajo de aplicación profesional se pretende aportar a la problemática de la E.F.N. A tales fines, se desarrollaron indicadores estratégicos, que se vinculan con los tácticos y operativos, como se menciona anteriormente en este trabajo.

Es elemental entender la correlación y asociación que tienen entre ellos para poder llevar a cabo una efectiva estrategia de Seguridad de la Información. Es por esto que, en este capítulo, además de detallar los indicadores estratégicos los vinculamos con algunos de los técnicos y operativos propuestos:

Capacitación externa e interna: en este punto es importante considerar la cantidad de horas de cursos tomados, realizando una apertura de aquellos que se refieren al área técnica y aquellos de áreas blandas o gerenciales. Esto le permitirá a la entidad entender si cumple con el requisito mínimo propuesto por el área de recursos humanos. Este indicador estratégico puede alinearse con el táctico referente al control y homologación de aplicaciones autorizadas, ya que el uso autorizados de las mismas está estrechamente vinculado al conocimiento que posea tanto el área de Seguridad de la Información, como sus usuarios.

Actualización de procesos críticos: en este caso, al idear este indicador, se busca garantizar la calidad y certificar los niveles de actualización y obsolescencia de los procesos críticos del área. En este ejemplo, podemos considerar un proceso crítico el aprovisionamiento de roles y/o sistemas críticos, ambos indicadores tácticos. Estos a su vez se nutren de información que se desprende de indicadores operativos, tales como: alta, baja y modificación de usuarios, actualización de parches de los sistemas operativos, etc.

Evaluación de la robustez de los algoritmos de encriptación utilizados en las conexiones: en este indicador se garantizará la correcta gestión, implementación y usabilidad de los certificados utilizados. Considerando que los mismos no sean vulnerables u obsoletos, así como que las características del mismo aseguren el tráfico. Esta estrategia para proteger la integridad se alinea con el indicador operativo referente a la gestión de los mismos, ya que el vencimiento de uno de ellos dejará el sitio desprotegido, eventualmente bloqueado y al usuario expuesto.

Procesos documentados: hacer un seguimiento sobre los procesos de seguridad de la información que está documentado es de vital importancia para la mejora continua, el registro y la garantía de la operación. Desde el punto de vista táctico, el grado de avance de los proyectos debe estar debidamente documentado, así como la detección y resolución de incidentes.

Campañas de hacking ético: estas campañas son llevadas a cabo con el objetivo de obtener los resultados acerca de la campaña de phishing dividida por sector teniendo en cuenta quienes lo reportaron, quienes hicieron click y quienes llegaron hasta la instancia de comprometer sus contraseñas. Desde un punto de vista táctico, este indicador estratégico se practica realizando la filtración de correos electrónicos.

Concientización: este es un punto fundamental para cualquier compañía, que busca garantizar la primera línea de defensa, es decir los usuarios. Ellos deben ser concebidos como un aliado, y deben ser capacitados para poder llevar adelante su labor de forma segura. Se propone entonces relevar el contenido generado en

términos de concientizar a la compañía. Puede ser en formato de mails, videos, charlas o eventos. Se propone realizar tres campañas de concientización masivas, donde se logre llegar, sumando todas las audiencias, a toda la compañía.

Seguridad en los proyectos del banco: aquí se buscará contabilizar la cantidad de proyectos donde se incluyó la seguridad, en qué etapa fue llamada, y en qué porcentaje se han cumplido las propuestas en cuanto a la arquitectura de seguridad hechas por el área.

Puntos de auditorías resueltos y levantados: para las entidades financieras de la República Argentina el cumplimiento de la normativa vigente es obligatorio y auditado de forma externa. En línea con esto, este indicador pretende que de acuerdo a las auditorías del periodo, puedes tener trazabilidad acerca de los puntos de auditoría del BCRA que se han levantado en contraposición contra aquellos.

El estado de los proyectos lo consideramos un punto crítico para entender cómo es la participación del área de seguridad en los diferentes proyectos de la compañía. A su vez no permite entender el grado de adhesión a las recomendaciones que damos, la interacción con el resto de las áreas, si consideran útil nuestro aporte, o si somos un freno a la hora de avanzar.

En cuanto a los tiempos de aprovisionamiento de los roles, esto nos permite entender cómo es el servicio de seguridad de la información que brindamos de cara al cliente interno. Estratégicamente el área cuenta con ser un facilitador, con poder securizar sin ralentizar acompañado los procesos de la compañía y aportando seguridad. No obstante, si por brindar seguridad elaboramos complejos procesos que dejan a la gente por horas sin poder hacer su trabajo estratégicamente hay algo que amerita ser replanteado.

Este indicador facilitará tener visibilidad para entender si debemos invertir recursos en la atención al cliente que estamos brindando. Vale aclarar que este es solo un ejemplo de un conjunto de indicadores que permitan visibilizar esta área el cual se

considera clave en la estrategia acerca del posicionamiento del área en la compañía.

Entender donde radica el mayor volumen de altas en cuanto a sucursales y plataformas se refiere, nos habilitará una comprensión cabal acerca de donde deben ser invertidos los mayores recursos, que sistemas deben ser los primero en tener un mayor grado de automatización ya que son los más usados, en cuales debemos implementar mejoras en función de la demanda que haya de los mismos y otros asuntos referidos al impacto en mayor volumen de gente de acuerdo a las regiones con mayores altas, entre otros tópicos.

Por último, nos encontramos con el indicador acerca de las categorías sobre las cuales se resolvieron los incidentes. Esto puede derivar en información acerca de incidentes externos, fallas de los sistemas que afecten la disponibilidad, permisos a usuarios que hayan sido otorgados de forma incorrecta u otro tipo de incidente el cual debería ser investigado con la debida diligencia para poder mitigarlo en el futuro.

Quienes diseñan y quienes consumen los Indicadores Estratégicos

Los indicadores estratégicos son diseñados por los mandos medios y presentados a la alta gerencia o directivos de la organización. En última instancia son ellos quienes los consumen. Es importante considerar en este punto que la forma en que se muestran los indicadores es de suma relevancia.

De esta manera, deben tener un impacto visual, ser fácilmente entendibles para poder interpretar la situación actual o tomar medidas cuando los números no se ajustan a los límites establecidos ya sea introduciendo cambios o mejoras. También en el campo específico de la seguridad de la Información pueden aportar a la tarea de medir la situación de riesgo en la cual se encuentra la empresa. A su vez aportarán una base en cuanto al progreso en el desarrollo estratégico y la mejora focalizada.

Conclusiones

La estrategia de una organización no es algo dinámico y cambiante, si bien por supuesto que puede ajustarse y/o reformularse, es algo que se plantea y se planea para alcanzar en el mediano o largo plazo, es decir entre tres y cinco años. Se persigue durante mucho tiempo. Pequeñas acciones se llevan a cabo día a día para construir el camino que lleva a lograr un objetivo común o superior.

Es un engranaje perfectamente armado el sistema que conecta a los indicadores operativos, tácticos y estratégicos. Unos se nutren de otros y se retroalimentan. Sin embargo, son los indicadores estratégicos los que resumen, incluye y abarca a los otros dos. En esta línea de pensamiento, es altamente probable que si se encuentran grandes desvíos en los indicadores operativos estos se trasladen a los tácticos y esto impacte en el cumplimiento o en la ejecución de la estrategia planteada.

Por eso es importante que dentro de la compañía la estrategia no sea una “isla” que solo conozca la alta gerencia y que, en cambio, todos los integrantes del área tengan claros los objetivos que se alinean con las acciones concretas que están llevando a cabo.

Por último, pero no menos importante, los números que arrojen los indicadores debe ser mostrado en un tablero sencillo de visualizar. Que permita cambiar filtros y jugar con los números para poder ver un mismo indicador desde distintos ángulos. Es decir, por región, sucursal, sistema o cualquier otro corte que aporte a la toma de decisiones. la alta gerencia que consume estos indicadores no dispone de abundante tiempo para analizar una tabla dinámica o una base de datos. Es por esto que la forma en que estos indicadores sean expuestos es clave para producir un impacto y una correcta influencia en la toma de decisiones.

CAPÍTULO VI: Indicadores de la Seguridad de la Información en el entorno de la Nube

Introducción

Desde hace alrededor de cinco años que en el ámbito de la seguridad de la información y de tecnología en general, se viene escuchando con fuerza una nueva tendencia: sistemas de computación en la nube.

En un principio, cuando esta idea desembarcó en el ámbito, los profesionales de Seguridad de la Información nos resistimos a la idea de que nuestra información esté alojada en el servidor de un proveedor externo, al cual nosotros no tendríamos acceso físico y desconocíamos los requerimientos de seguridad que la protegían.

En el año 2017, en la conferencia anual que brinda Gartner en Estados Unidos, se mencionó que este nuevo paradigma de la nube había llegado para quedarse. Fue así como en el año 2018 el Banco Central de la República Argentina comenzó a modernizar su regulación incluyendo este nuevo concepto en su normativa.

La realidad es que la tecnología evoluciona rápido y, el que no se adapta no sobrevive o paga sobreprecios. Rápidamente las entidades financieras comenzaron a adoptar esta nueva tecnología, incorporar metodologías ágiles que a las que esta plataforma invita y, también, a incorporar roles como el DevOps o SecOps sumamente asociado a la forma de trabajar que plantea la nube donde la escalabilidad y el despliegue continuo son dos rasgos fundamentales.

El objetivo de este capítulo es no ignorar esta nueva forma de trabajar y esta herramienta y proponer también indicadores que debe considerarse desde el punto de vista de la seguridad de la información en una infraestructura montada en la nube donde las fronteras de bordes se licuan, el acceso a los servidores no es posible y la gestión de identidades se hace con un modelo orientado a objetos diferente del paradigma al que estamos acostumbrados.

¿Que plantea este nuevo paradigma y porque los incluimos en este trabajo?

Hoy en día hablar de la nube implica hablar de un nuevo paradigma. Así lo explica el equipo de Simbiotia (2

9):

> El filósofo estadounidense Thomas Kuhn plantea que un cambio de paradigma científico se producía cuando los supuestos básicos generales, las teorías, leyes y técnicas aplicadas hasta el momento por los miembros de una comunidad científica, resultan a todas luces incapaces para explicar algunos fenómenos, anomalías y dudas que van surgiendo en relación con una materia.
>
> Cuando estas dificultades se mantienen y son constantes, chocan con el paradigma universalmente aceptado por las comunidades científicas, generando así una crisis que sólo puede ser resuelta con la aparición de un nuevo paradigma. Una nueva forma de entender dicha ciencia o materia, no solo por parte de un científico aislado, sino por toda la comunidad científica, que abandona el antiguo paradigma conocido y adopta otro nuevo[11].

Adaptado al campo de la Seguridad de la Información que quizás está un poco alejado de la ciencia abstracta estudiada como tal y más cercano a un campo de aplicación práctica, el concepto de la nube y todo lo que ella propone ha sido ampliamente aceptado por la comunidad y ha llegado para quedarse. Pero, ¿qué propone la nube que fue tan disruptivo con lo anterior?

La nube propone escalabilidad horizontal y vertical en el aprovisionamiento de infraestructura en segundos, propone pagar por los servicios consumidos, propone

[11] Véase referencia bibliográfica N° [08].

un “todo” como servicio. Puedes insertar en la palabra todo lo que te guste: infraestructura como servicio, plataforma como servicio, seguridad como servicio, código como servicio y así podríamos continuar.

Hay seis grandes proveedores de esta tecnología a nivel mundial: Amazon Web Service, Microsoft Azure, Google Cloud, Alibaba Cloud, IBM Cloud, Oracle, en cuanto a nube pública. También está la posibilidad para las grandes empresas con “hardware” ya adquirido, de adoptar este concepto, internalizar y montar su propia nube privada dentro de la compañía.

A nivel seguridad las soluciones en la nube despejan varios problemas que en las soluciones “on-premise” consumían mucho tiempo de en la curva inicial de un proyecto, migración o instalación. Los microservicios referidos a la gestión identidades, gestión de llaves de encripción o seguridad en redes, por citar solo tres ejemplos, ya vienen resueltos en la nube y todo lo que hay que hacer es cargar algunos datos o diseñar previamente una arquitectura sólida.

Estos tiempos que ahorra la nube, permite redireccionar los recursos para ocuparse de otro grado de análisis en los controles, el monitoreo o las mejoras. Los indicadores sobre el entorno de computación en la nube apuntan a dar visibilidad sobre la posición de la seguridad, la magnitud de la utilización de la misma, pero, por sobre todas las cosas, con este capítulo pretendemos incluir este concepto con un punto clave e innovador que cualquier empresa debe considerar en el presente.

Conceptos teóricos sobre los Indicadores de la Nube

Los indicadores en la nube son transversales a todos los analizados en este trabajo, es decir: los operativos, tácticos y estratégicos. Esto se debe a que una infraestructura, una plataforma o un programa.

Normativa Vigente

Actualmente para la nube, más allá de las normativas y buenas prácticas generales que lentamente se van adecuando a este nuevo entorno, existen en el país una que considero debe ser mencionada a los fines de este trabajo de aplicación profesional.

Debido a que el caso de aplicación profesional se está realizando sobre una Entidad Financiera Nacional con envergadura bancaria, la misma está sujeta a las normativas y comunicaciones que surjan del Banco Central de la República Argentina.

A los efectos de omitir lo que la entidad regulatoria ha estado delineando en este último tiempo y debido al agregado de valor que la misma le aporta al conocimiento general, introduzco en este trabajo el contexto de la comunicación "A" 6354 (BCRA, noviembre de 2017). La misma detalla en sus párrafo inicial: "Expansión de entidades financieras" y "Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras[12]".

Considero que esta normativa brinda un marco de trabajo para aquellas entidades bancarias que se encuentra ante un proceso de migración eficiente al nuevo mundo digital y sobre todo al paradigma de la nube como herramienta.

Sin ir más lejos en su sección siete la norma habla sobre la tercerización de servicios de tecnología en sus diferentes aspectos. Tales como: infraestructura, base de datos, monitoreo, retención de información y "backup", respuesta a incidentes y ciclo de vida de desarrollo.

Principales Indicadores de la Nube en Seguridad de la Información

Hoy en día la nube agiliza la construcción y entrega del producto, así como el proceso de desarrollo. Esta habilidad, si bien considero que hace más eficiente la tarea y provee de nuevas herramientas, no deja de tener riesgos nuevos y distintos

[12]Véase referencia bibliográfica N° [05].

asociados. Siendo conscientes de que esos riesgos existen, somos capaces de mitigarlos, asumirlos, transferirlos o aceptarlos.

A los fines de esclarecer la posición de cada empresa sobre estas nuevas tecnologías y de colaborar con la E.F.N, propongo se tengan en cuenta los siguientes indicadores correspondientes a un ambiente en la nube:

Micro Servicios de la nube utilizados: con este indicador se busca dar visibilidad de la cantidad y el tipo de microservicios de seguridad que cada nube ofrece, y están activos en los distintos proyectos donde el área de seguridad está involucrada.

Cantidad de recursos con cumplimiento: lo que se pretende aquí tiene relación directa con el cumplimiento normativo que aplique. Busca un análisis de seguridad, sobre la totalidad de los recursos habilitados en la nube. Como por ejemplo, cuántos de ellos están bajo el cumplimiento de las buenas prácticas de seguridad de la información y cuántos no.

Configuraciones de la infraestructura: explotando la escalabilidad que brinda la nueva y el "deploy" automatizado, las posibilidades de realizar configuraciones en la infraestructura de acuerdo con normas y políticas de forma general se hace alcanzables. Este indicador pretende revisar periódicamente dichas configuraciones con el objetivo que se actualicen a las nuevas funcionalidades de la herramienta.

Conclusiones

La nube ha llegado para quedarse y romper con el viejo paradigma. No es suficiente con que la herramienta, es decir la computadora de alguien más, sea contratable a demanda y escalable tanto horizontal como verticalmente.

Es también imprescindible en mi opinión que los altos mandos de las empresas estén dispuestos a hacer un cambio en sus modelos mentales, una inversión para la migración que conlleva y un entendimiento cabal del plan a largo a plazo que tendrá un retorno de la inversión que lo amerita.

En mi opinión profesional, la nube no es lo más eficiente para todas las empresas ni en todos los casos técnicos. La nube cubre ciertas necesidades en casos específicos mejores que otros.

Lo que si me animo a concluir desde lo profesional, es que la era digital ha llegado. Esto quiere decir que quien no se suba a bordo de la digitalización quedará excluido desde el punto de vista técnico y desprotegido desde el punto de vista de la seguridad. Esta aseveración se basa, entre otros puntos, en que la obsolescencia a quienes no se modernicen los dejará fuera del sistema.

CAPÍTULO VII: Grado de madurez según los indicadores aplicados.

Introducción

Al revisar este trabajo con mi tutor, consideramos que el mero hecho de proponer y desarrollar nuevos indicadores que sirvan para el seguimiento y la medición de las tareas profesionales ejecutadas en una entidad bancaria específica de Argentina en el área de Seguridad de la Información no bastaba como aporte al campo de estudio de la materia para una tesis de maestría. Es por ello que decidí avanzar un paso más en la materia, y proponer elaborar un modelo de madurez específico el cual derive de analizar la información que se desprende de los indicadores planteados en este trabajo.

Si bien los indicadores propuestos en esta tesis, por un tema de extensión, son solamente una muestra del vasto universo que existe y se podría elaborar y ejecutar en una empresa de esta envergadura, si el lector sigue la lógica de los mismos, la metodología que se propone en este trabajo y se nutre de la teoría aquí recopilada, creemos que será capaz de desarrollar tantos como la organización lo requiera adaptado a cada plan estratégico en particular pudiendo considerar la normativa que le compete a la institución o bajo la cual es auditada.

Es por esto que en este capítulo nos dedicaremos a plantear, desarrollar el contenido y justificar el diseño de un modelo de madurez que pueda ser adaptado a la existencia de los indicadores operativos, tácticos y estratégicos que la compañía tenga permitiéndole, no solo medir y tomar decisiones, sino entender de forma global donde están posicionados respecto del objetivo óptimo o de la máxima madurez posible de alcanzar.

Diferentes aristas de un mismo modelo. Analogía del cubo mágico y la madurez.

Entendiendo la madurez como un cubo mágico, considero cada cara del cubo como una posible arista de la madurez del área de seguridad de la información de la entidad financiera. Luego, más adelante en este mismo capítulo, voy a ponerle nombre a cada una de estas aristas entrando en un mayor grado de detalle y descripción. Siguiendo la analogía, considero que a mayor grado de madurez, más homogeneidad habrá de cuadraditos del mismo color en dicha arista del cubo. Entonces cada uno de esos cuadrados pequeños que componen una de las caras del cubo, será un indicador correctamente ejecutado en el área que le corresponda a la arista.

Si bien tenemos indicadores estratégicos, tácticos y operativos no es lineal la madurez de un área. Es decir, las áreas que pretendo determinar son transversal a estas tres categorías y serán contribuidas por ellas. Claro está que si quiero entender cómo avanza mi plan estratégico me remitiré a los indicadores de este sector. Las categorías que se pretenden desarrollar aquí son de incumbencia tanto de la estrategia, como de la táctica y de la operación y no se puede tener una visión integral, holística y completa de ellas sin conocer los datos, el avance y los resultados obtenidos en cada una de ellas. Porque no dependen solo del éxito de una de ellas sino de las tres.

Las diferentes aristas que proponemos para entender y medir el grado de madurez de la compañía en términos de seguridad de la información, en cinco aspectos principales, salvando las diferencias con un cubo, son:

1. Capacitación y “Awareness” (Ciber Resiliencia)
2. Proyectos (Mejoras de procesos operativos)
3. Cumplimiento normativo
4. Automatización de tareas
5. Propuesta e implementación de mejoras

A continuación, procederé a desarrollar a que hago referencia con cada una de ellas.

1. **Capacitación y concientización**

Creo firmemente que los usuarios o empleados de la compañía son la primera línea de defensa. Si ellos no asimilan y comprenden la importancia de proteger y resguardar activos para la organización, no importa cuánto inviertas en herramientas que protejan tus activos digitales o cuantos recursos tengas asignado a la tarea de securizar la información, la organización es vulnerable. Con todo esto, la necesidad de educar y capacitar a los usuarios en la materia y a los mismos integrantes del equipo de seguridad, se volvió una tarea imperiosa para cualquier organización.

La capacidad que una organización tenga de protegerse de ataque como el phishing o el “ransomware” son directamente proporcional a cuan entrenados estén sus empleados en cosas tan simples como no compartir sus credenciales, no hacer “click” en un enlace malicioso de un correo electrónico y poder reportarlo o, subir a la nube personal documentos de la organización para trabajarlos más tarde. Por dar solo algunos ejemplos de los errores cotidianos con los que nos encontramos todos los días y que hacen que nuestra organización sea más vulnerable a los ataques.

Soy de las profesionales de seguridad que cree que si un usuario compartió sus credenciales la responsabilidad no es del empleado, la responsabilidad es de las personas que trabajamos en el área de seguridad que no fuimos capaces de transmitirle a ese eslabón fundamental de la cadena la importancia que tienen esas credenciales y la cantidad de puertas que permite abrir a quien las posea. Como todos sabemos, la cadena se rompe por su eslabón más débil, y si no protegemos el eslabón “usuario” estamos obviando una parte fundamental. La tarea de mostrarle a ese usuario como proteger los activos de la organización es nuestra y debe ser llevada a cabo con meticulosidad y constancia.

El grado de educación que predomine en la compañía y la capacidad que la empresa tenga de mantener un programa continuo de formación y capacitación aludiendo a temas interesantes que cautivan el interés de los empleados, en donde se pueda dejar un mensaje que impacte, no solo a nivel corporativo sino también

personal que resulte cautivador y que pueda ser llevado a prácticas corporativas, mostrará la madurez en la cual se sitúa la organización con respecto a este tema.

Hay distintos indicadores desarrollados en la planilla de cálculo adjunta a este trabajo que pueden arrojar luz sobre el estado de madurez en el cual se encuentra la compañía. Desde ya que la concientización es una práctica que se debe aplicar de forma continua, ya que no basta con la ejecución una sola vez de forma aislada.

2. Proyectos

Los proyectos que lleva adelante la compañía, tanto del área de tecnología como propios de seguridad de la información, así como aquellos que pertenecen a otras áreas completamente distintas como puede ser recursos humanos o riesgo crediticio generalmente implica el manejo de información sensible o requiere acceso a sistemas críticos.

No siempre las empresas entienden la importancia de incorporar la óptica de seguridad de la información en un proyecto, más considerando que la misma suele implicar una inversión mayor y a lo mejor extensión de los plazos. En primer lugar, es importante aclarar que la incorporación de seguridad de la información en una etapa tardía o productiva tiene un costo aproximado de treinta veces mayor a una incorporación en su fase de desarrollo.

Por otro lado, no se debe perder de vista que en una entidad financiera las normativas del Banco Central de la República Argentina aplican para todas las áreas y no pueden ser obviadas, ya que un punto levantado en una auditoría es de suma gravedad.

A su vez, con esta arista se busca monitorear la cantidad de proyectos propios del área de seguridad de la información, la temática de los mismos, su duración, su efectividad y su debida evolución a través del tiempo.

3. Cumplimiento normativo

Las entidades financieras de la República Argentina tienen la obligación de cumplir con la normativa del Banco Central quien lleva a cabo exhaustivas auditorías de forma periódica (generalmente cada dos años). La autorización para operar depende del cumplimiento de esta normativa. Entender y diseñar las operaciones para un mejor cumplimiento es elemental.

Si bien el grado de sujeción a la norma debe ser elevado, es decir se parte de una base exigente, en este aspecto se busca que los indicadores alcancen la madurez suficiente para permitirle a la organización tomar acciones preventivas y no correctivas, eliminar retrabajo, facilitar la búsqueda y generación de documentación, entre otros aspectos a considerar.

4. Automatización de tareas

En la actualidad se busca que aquellas operaciones repetitivas donde no hay un agregado de valor por el mero hecho de ejecutarlo, puedan ser automatizadas para redireccionar los recursos y esfuerzos hacia un mayor grado de análisis u alguna otra tarea que no pueda ser procesada por la misma computadora.

Lo primero que resulta interesante aclarar, es que un mayor grado de automatización no significa una disminución del personal sino una redistribución de las tareas y la disponibilidad de mayor tiempo para dedicarle a los proyectos, a tareas de análisis e interpretación, a mejoras o a trabajar sobre la madurez del de seguridad de información en búsqueda del incremento de la misma.

Lo segundo en materia de automatización, y ya sumergiéndonos en cuestiones más técnicas, es lo referente a las diferentes formas que existen de automatizar. Hoy en día se puede hacer a través de la compra de una herramienta costosa, como un gestor de identidades. Pero también se puede lograr con el desarrollo de un “script” que genere reportes que de otro modo se generarían de forma manual.

Como en cualquier implementación de nuevas metodologías, lo importante es contar con el apoyo de los mandos medios y las herramientas para hacerlo. Los indicadores que me permitan medir el grado de automatización de mis procesos, controles y operaciones darán lugar a entender el nivel de madurez con respecto a la automatización en el área de seguridad de la información.

Es interesante considerar también que la automatización de procesos tiene una curva de entrada elevada, pero luego tiene un retorno generoso. Es decir, al principio puede resultar complicado automatizar un proceso, pero es probable que al ser algo repetitivo se esté ahorrando en el futuro muchas horas de ejecución. Al menos es interesante plantearse este análisis.

5. Propuesta e implementación de mejoras

La mejora continua y las iniciativas del área de seguridad de la información que no responden a una agenda predeterminada al comenzar el año, sino a detecciones de los analistas de las tareas diarias de mejores formas de ejecutar las tareas componen un grupo de potenciales proyectos o iniciativas.

La mejora continua en los procesos y las operaciones son herramientas vitales para incrementar la eficiencia de un área y con ella la madurez de la misma. Incorporar una herramienta, automatizar una tarea repetitiva, incorporar un servidor remoto para disminuir tiempos locales de procesamiento o proponer una lista homologada de tareas a tener en cuenta en cualquier proyecto donde intervenga el área de Seguridad de la Información, son algunos de la variedad de ejemplos que se puede dar en la materia.

No debemos olvidar que en algunos casos la rutina diaria, mantener la rueda girando y los incidentes que puedan surgir suelen ocupar el cien por ciento de la agenda. Sin embargo, es importante destacar, que debe separarse un espacio para pensar, analizar y detectar puntos de mejora. Aunque a lo mejor ese año no puedan

ser implementados, se recomienda que sean incorporados a lista de futuras mejoras a considerar.

Lo estratégico como el norte para la organización.

Más allá de los diferentes enfoques que le podamos dar al grado de madurez, es interesante tener en vista que la estrategia marcará el rumbo y delimitará el camino de las decisiones que se tomen en el futuro. Razón por la cual proponemos considerar tres aspectos cuando evaluamos la madurez del área de Seguridad de la Información:

- **Mejoras de procesos operativos**

La mayoría de los directores del área de Seguridad de la Información pueden relatar su historia acerca de lo importante que es comprender que la seguridad de la información es un área de servicios.

No es atípico toparse con profesionales que ejercen como analistas o líderes de equipo de seguridad que conciben la seguridad como algo imprescindible, mandatorio e inevitable. En mi opinión, este punto de vista no hace más que desvirtuar uno de los principales objetivos del área en la mayoría de las empresas: brindar un servicio.

Si comenzamos a cambiar nuestros modelos mentales y concebimos al área de seguridad de la información como un área que debe brindar un servicio, garantizar ciertos estándares de cumplimiento hacia con el cliente interno y velar, no solo por la seguridad, sino por la eficiente y oportuna provisión del servicio, es posible que reenfoquemos la concepción que nosotros mismos tenemos acerca de nuestro deber.

En el contexto de este capítulo de la tesis, remarcó este punto a fines de considerar en un planeamiento estratégico la importancia de velar por prestar un buen servicio desde el área de Seguridad de la Información.

- **Protección de la Seguridad de la Información**

El segundo aspecto que considero sumamente relevante es la protección de la seguridad de la información, abordada desde dos aspectos, uno tradicional y otro innovador: la eficiencia y la automatización, respectivamente.

Cuando nos referimos a la eficiencia, hacemos referencia a llevar a cabo las tareas con la óptima gestión de los recursos disponibles. Sobre todo, considerando que el tiempo y los trabajadores son recursos sumamente escasos que deben ser bien administrados para poder obtener los fines planeados.

La automatización hace referencia a un nuevo paradigma donde se persigue despejar la agenda de los analistas para que tengan un mayor grado de análisis y no repitan de forma manual aquellas tareas que pueden ser automatizadas. Hoy en día la metodología que propone integración y entrega continua la automatización de herramientas de seguridad es una alternativa viable y comúnmente aceptada.

Es también la utilización de “scripting” para poder sustituir tareas repetitivas por tareas de análisis y que aporten valor, permitiendo que aquellas que pueden ser llevadas a cabo por una computadora sean ejecutadas de esta manera.

- **Ciber Resiliencia**

Este concepto nos acerca a la idea de que situaciones imprevistas que golpean a la organización de forma no esperada van a suceder, porque los imprevistos siempre existen, lo importantes es entender y haber reflexionado acerca cómo se va a reaccionar cuando esto ocurra.

Uno de los cursos de acción posibles es: identificar cuales son los activos críticos e implementar sobre ellos medidas de control que me permitan tener una mayor visibilidad y así anticipar o detectar cualquier potencial incidente.

Metodología de ponderación de la madurez.

En las conclusiones finales de este trabajo podrán encontrar una tabla donde propongo diferentes indicadores Estratégicos, Tácticos, Operativos y de la Nube, los mismos fueron explicados previamente en los oportunos capítulos junto con un contexto teórico que permita entender la razón de ser de cada uno de ellos.

A los efectos de poder darles a los indicadores un valor que permita a la compañía entender cuán efectivos son y donde queda posicionada una vez obtenido los resultados de estos, se proponen dos medidas de ponderación:

1. **Medir la Performance:**

La Performance será medida en función de umbrales de tiempo y de cantidad, el ratio de medición irá de 1 a 5 donde 1 es lo mínimo y 5 lo máximo. A continuación, desarrollare un ejemplo práctico tomando como muestra un indicador para clarificar:

Supongamos que estamos la cantidad de inicios de sesión, su duración y la IP desde donde fue realizada. En este caso, el umbral de tiempo del indicador en cuanto a su performance estará asociado con el tiempo que tomó la medición de este de acuerdo con lo esperado. Este indicador es uno de los que perfectamente puede ejecutarse de forma automatizada. Pues bien, si la ejecución automática hubiese fallado y alguien lo hubiese ejecutado completamente de forma manual la performance en términos de umbrales de tiempo sería igual a 1. Si por el contrario el indicador hubiera operado correctamente y los datos se hubieran obtenido en los tiempos esperados, entonces sería de 5.

En cuanto a los umbrales de cantidad, siguiendo con el caso previamente tomado, estos dependen de si todas las bases de datos que debían ser consultadas entregaron los datos correctamente y de si fue posible producir como resultado del indicador la información esperada considerando los datos recibidos.

2. **Medir la Madurez**

Por otro lado, la madurez tal como la planteamos en este trabajo, será medida en función de umbrales de expectativa y de implementación. El ratio de medición irá de 1 a 5 donde 1 es lo mínimo y 5 lo máximo. Para poder tomar una medida de esto, será necesario que previamente se establezcan niveles de automatización y mensura, tanto de expectativas como de implementación.

Luego, los niveles que hayan sido alcanzados en la ejecución real se coteja contra los esperados para poder otorgarle un ponderación de a 5 de acuerdo al grado de cumplimiento de las expectativas pautadas.

Conclusiones

La diferencia de estos tres aspectos planteados previamente con las aristas del cubo, es que, las aristas del cubo atraviesan a la seguridad de forma transversal y estos aspectos hacen foco en aquellas cuestiones que se deben tener en cuenta al pensar lo estratégico en una E.F.N.

Si bien como profesional considero que los planes sufren modificaciones y no hacen para apegarse a ellos de forma acérrima, estoy de acuerdo con la necesidad de hacer planes para saber hacia dónde se dirige la organización y ser capaces de cambiar el rumbo de la marcha a tiempo en caso de que se observe algún desvío.

La estrategia es el núcleo de donde se desprenden el resto de los planes, es sumamente importante dedicarle tiempo a su diseño, medición y seguimiento. Las decisiones críticas y determinantes surgirán de aquí.

CAPÍTULO VIII: Conclusiones finales

Hoy en día las entidades bancarias están sufriendo un cambio de paradigma en la forma de operar. El advenimiento de la era digital junto con las nuevas modalidades transaccionales que impuso la pandemia de COVID-19 en el mundo, traen aparejados grandes desafíos en términos de seguridad de la información.

Los proyectos, se diseñan, construyen, implementan y operan en tiempos que, en algunos casos, no superan los seis meses. Esto hace que a aquellas áreas de seguridad de la información que no acompañen este dinamismo, no les queda otra opción que rezagarse en la inclusión de sus buenas prácticas y recomendaciones. Porque como profesionales que somos, debemos entender que los resultados en el negocio son los que más impacto tienen. Negarnos a eso, es no aceptar la realidad.

Adicionalmente, y como para potenciar esta experiencia transformadora, soluciones como la nube, la entrega continua y las herramientas de código abierto están siendo comúnmente aceptadas. No se desarrolla un juicio de valor indicando que esto es bueno o es malo, es la realidad que está pasando.

Salir del enfoque tradicional basado en riesgo, operaciones manuales, información resguardada por perímetros, la “anti-automatización” por miedo a la pérdida de puestos de trabajo, la oposición al contrato de responsabilidad compartida de la nube, por mencionar algunos nuevos desafíos, ya no es una opción. En mi opinión, quien se resista a ese cambio quedará obsoleto, expuesto, vulnerable, análogo a un sistema operativo que ya no actualiza su versión de antivirus.

Aprender herramientas nuevas, incorporar nuevas formas de trabajo, cambiar modelos mentales son formas de sobrevivir, pero además de hacerlo de la forma más segura posible. Si bien la seguridad en un 100% no existe, trabajamos todos los días para tratar de garantizarla en su máximo porcentaje.

En este contexto cambiante, vorágine, digital y más acelerado que nunca, poder contar con indicadores que reflejen nuestras operaciones resolverá, en mi opinión,

varias encrucijadas a las cuales los directivos se encontrarán expuestos y les permitirá tomar decisiones de forma rápida y adaptada al entorno en donde trabajan acompañando mejor al negocio de la organización.

Los indicadores son diseñados, construidos y ejecutados por el área de seguridad de la información pero no en todos los casos están dirigidos para esta sección. Es decir, poder darle con los indicadores que se proponen en este trabajo visibilidad al resto de las áreas de tecnología o bien a superiores, permitirá demostrar necesidades, justificar recursos, explicar tendencias, decidir cursos de acción y modificar desvíos, ni más ni menos.

A continuación, se detallan todos los indicadores propuestos en la presente tesis:

			Performance		**Madurez**	
Tipo	**Nombre**	**Objetivo**	**Tiempo**	**Cantidad**	**Expectativa**	**Implementación**
Operativo	Alta de usuarios	Medir la cantidad de altas de usuarios que permita dar visibilidad acerca de las operaciones y luego correlacionar datos. Esta información se debe dividir entre usuarios internos y externos.	Umbrales	Umbrales	Nivel de (automatización y mensura)	Nivel de (automatización y mesura)
Operativo	Baja de usuarios	Medir la cantidad de bajas de usuarios que permita dar visibilidad acerca de las operaciones y luego correlacionar datos	1-5	1-5	1-5	1-5
Operativo	Modificación de usuarios	Medir la cantidad de modificaciones de usuarios que permita dar visibilidad acerca de las operaciones y luego correlacionar datos	1-5	1-5	1-5	1-5
Operativo	Inicio de sesión	Medir la cantidad de inicio de sesión, su duración y la IP desde donde fue realizada	1-5	1-5	1-5	1-5
Operativo	Cierre de sesión	Medir la cantidad de cierre de sesión, su duración y la IP desde donde fue realizada	1-5	1-5	1-5	1-5

Operativo	Gestión de usuarios de servicios por plataforma	Contabilizar la cantidad de nuevos usuarios de servicios y la cantidad de veces que los existentes accedieron	1-5	1-5	1-5	1-5
Operativo	Gestión de usuarios de servicios de base de datos	Contabilizar la cantidad de nuevos usuarios de servicios y la cantidad de veces que los existentes accedieron	1-5	1-5	1-5	1-5
Operativo	Gestión de usuarios de servicios de aplicativos	Contabilizar la cantidad de nuevos usuarios de servicios y la cantidad de veces que los existentes accedieron	1-5	1-5	1-5	1-5
Operativo	Gestión de usuarios de servicios de comunicaciones	Contabilizar la cantidad de nuevos usuarios de servicios y la cantidad de veces que los existentes accedieron	1-5	1-5	1-5	1-5
Operativo	Caducidad de usuarios de servicios	Acerca de todos los tipos de usuarios de servicios, que cantidad no fueron utilizados por dos meses	1-5	1-5	1-5	1-5
Operativo	Versión de los sistemas operativos	Listar las versiones de los sistemas operativos utilizados en los servidores identificados como críticos	1-5	1-5	1-5	1-5
Operativo	Actualización de parches de los sistemas operativos	Identificar la fecha, versión y módulos actualizados en la última descarga de parches de los sistemas operativos	1-5	1-5	1-5	1-5
Operativo	Renovación de certificados SSL/TLS	Corroborar las fechas de vencimientos de todos los certificados y tener visibilidad de la cantidad de certificados que han sido renovados en el periodo	1-5	1-5	1-5	1-5
Táctico	Estado de los proyectos del área de Seguridad Informática	Grado de avance de los proyectos del área	1-5	1-5	1-5	1-5
Táctico	Estado de los proyectos	Porcentaje de adhesión de los proyectos de la organización a las recomendaciones de Seguridad Informática	1-5	1-5	1-5	1-5
Táctico	Tiempos de aprovisionamiento de roles	Cual es el tiempo de aprovisionamiento de un rol segregado por los tiempos que tardan en la aprobación todos los involucrados en el	1-5	1-5	1-5	1-5

		flujo				
Táctico	Altas por sucursal y plataforma	Utilizando el indicador operativo acerca de las altas, generar información para poder entender qué sistemas son los más requeridos y obtener tendencia por regiones según las altas en las diferentes regiones donde la entidad tiene sucursales	1-5	1-5	1-5	1-5
Táctico	Resolución de incidentes	Obtener una lista de las categorías sobre las cuales se generaron incidentes. Determinar cuántos de ellos fueron realmente un incidente y cuantos un falso positivo	1-5	1-5	1-5	1-5
Táctico	Detección de incidentes	Identificar mensualmente si las herramientas de detección y prevención de incidentes han operado correctamente y cuántos potenciales ataques han frenado	1-5	1-5	1-5	1-5
Táctico	Aprovisionamiento a los sistemas críticos	De las altas del día, y considerando los tres sistemas críticos de las compañía, cuantos accesos fueron dado en tiempo y cuántos han fallado	1-5	1-5	1-5	1-5
Táctico	Filtrado de correo electrónico	Obtener estadística de filtrado y detección de correo electrónico no deseado y los que han sido reportado como sospechosos	1-5	1-5	1-5	1-5
Táctico	Control y homologación de aplicaciones autorizadas	Detectar en una muestra representativa de dispositivos y servidores si hay instalados sistemas o aplicación que no están homologados por la entidad	1-5	1-5	1-5	1-5
Táctico	Configuración de las políticas de directivos de grupo	Controlar el correcto impacto de las políticas de directivas de grupo de la compañía en los dispositivos de personal propio y terceros, acorde a los estándares de la entidad financiera.	1-5	1-5	1-5	1-5

Táctico	Firma del acuerdo de confidencialidad de personal externo	De acuerdo a las altas arrojadas en el indicador operativo acerca de las altas de terceros, cotejar con la cantidad de acuerdo de confidencialidad firmados para concluir si todos han firmado el acuerdo de confidencialidad. Detectar desvíos	1-5	1-5	1-5	1-5
Estratégico	Capacitación externa e interna	Considerar la cantidad de horas de cursos tomados, abierto por aquellos que se refieren al área técnica y aquellos de áreas blandas o gerenciales. Permitirá comparar si cumple con el requisito mínimo propuesto por el área de recursos humanos.	1-5	1-5	1-5	1-5
Estratégico	Actualización de procesos críticos	Garantizar la calidad y certificar los niveles de actualización y obsolescencia de los procesos críticos del área	1-5	1-5	1-5	1-5
Estratégico	Evaluación de la robustez de los algoritmos de encriptación utilizados en las conexiones	Revisar que los certificados utilizados no sean vulnerables u obsoletos, así como que las características del mismo se adecuen a las necesidades de seguridad del tráfico	1-5	1-5	1-5	1-5
Estratégico	Procesos documentados	Contabilizar la cantidad de procesos que están documentados y cuando fueron actualizados	1-5	1-5	1-5	1-5
Estratégico	Campañas de hacking ético	Obtener los resultados acerca de la campaña de phishing dividida por sector teniendo en cuenta quienes lo reportaron, quienes hicieron click y quienes llegaron hasta la instancia de comprometer sus contraseñas	1-5	1-5	1-5	1-5
Estratégico	Concientización	Relevar el contenido generado en términos de concientizar a las compañías. Puede ser en formato de	1-5	1-5	1-5	1-5

		mails, videos, charlas o eventos. Se propone realizar tres campañas de concientización masivas, donde se logre llegar, sumando todas las audiencias, a toda la compañía.				
Estratégico	Seguridad en los proyectos del banco	Contabilizar la cantidad de proyectos donde se incluyó la seguridad, en qué etapa fue llamada, y en qué porcentaje se han cumplido las propuestas en cuanto a la arquitectura de seguridad hechas por el área.	1-5	1-5	1-5	1-5
Estratégico	Puntos de auditorías resueltos y levantados	De acuerdo con las auditorías del periodo, puedes tener trazabilidad acerca de los puntos de auditoría del BCRA que se han levantado en contraposición contra aquellos preexistentes que se han logrado cerrar.	1-5	1-5	1-5	1-5
Nube	Mico Servicios de la nube utilizados	Tener visibilidad de la cantidad y el tipo de microservicios de seguridad que cada nube ofrece, activo en los distintos proyectos donde el área de seguridad está involucrada.	1-5	1-5	1-5	1-5
Nube	Cantidad de recursos con cumplimiento	En un análisis de seguridad, sobre la totalidad de los recursos habilitados en la nube, cuántos de ellos están bajo el cumplimiento de las buenas prácticas de seguridad de la información.	1-5	1-5	1-5	1-5
Nube	Configuraciones de la infraestructura	Explotando la escalabilidad que brinda la nueva y el "deploy" automatizado, las posibilidades de realizar configuraciones en la infraestructura de acuerdo con normas y políticas de forma general se hace alcanzables. Este indicador pretende revisar	1-5	1-5	1-5	1-5

		periódicamente dichas configuraciones con el objetivo que se actualicen a las nuevas funcionalidades de la herramienta.				

Referencias bibliográficas.

[01] Bakshi, S. (1 de noviembre de 2016). Performance Measurement Metrics for IT Governance. ISACA, 6, Sección Desarrollo de métricas de performance. Recuperado de: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/performance-measurement-metrics-for-it-governance

[02] COSO II, Committee Of Sponsoring Organizations (2013, Mayo). Internal Control, Integrated Framework. Sección Monitoreo. Recuperado de: https://archivo.consejo.org.ar/comisiones/com_43/files/coso_2.pdf

[03] instituto Argentino de Normalización y Certificación (Septiembre de 2010). Esquema 1 de Norma IRAM-ISO/IEC 27004. Recuperado de: http://www.frlp.utn.edu.ar/materias/habprof/teoria/27004%20IRAM-ISO-IEC.pdf

[04] ISACA (2012) COBIT 5. Recuperado de: COBIT5-Framework-Spanish (1).pdf

[05] Banco Central De La República Argentina (3 de noviembre de 2017). Comunicación "A" 6354. Recuperado de: http://www.bcra.gov.ar/pdfs/comytexord/A6354.pdf

[06] Banco Central De La República Argentina (29 de marzo de 2017). Comunicación "B" 9042. Recuperado de: http://www.bcra.gov.ar/pdfs/texord/texord_viejos/v-rmsist_17-07-09.pdf

[07] Wells Fargo (2020). Cajero automático (ATM). El futuro está en tus manos. Recuperado de: https://handsonbanking.org/es/resources/cajero-automatico-atm/#:~:text=ATM%20son%20las%20sigla%20en,su%20dinero%20de%20manera%20conveniente.&text=Habitualmente%20puede%20acceder%20a%20la,operado%20por%20su%20propio%20banco

[08] Simbiota (2019). Cambio de paradigma: transformando las relaciones en entornos sanitarios". Recuperado de: https://www.simbiotia.com/cambio-de-paradigma/

Bibliografía general.

INCIBE. (21 de 09 de 2015). *Instituto Nacional de Ciberseguridad*. Recuperado el 01 de 2020, de https://www.incibe.es/protege-tu-empresa/blog/mide-seguridad-informacion

Meyer, C. O. (15 de Marzo de 2015). *Criptored*. Recuperado el Julio de 2019, de http://www.criptored.upm.es/descarga/metricas_y_nuevos_escenarios.pdf

The Apprentice Store. (19 de Noviembre de 2018). *Cyber Security Services*. Recuperado el Febrero de 2020, de https://devtst1.theapprenticestore.co.uk/cyber-security-services/

Body, Industry Consultation. (2015). Regulatory Responses to ATM Cyber-Security. *Industry Consultation Body*, 2-5. Obtenido de https://ec.europa.eu/transport/sites/transport/files/modes/air/single_european_sky/doc/20150910_icb_position_on_regulatory_response_to_atm_cybersecurity.pdf

Olga Kochetova, A. O. (22 de Septiembre de 2016). *Securelist*. Recuperado el Diciembre de 2019, de https://securelist.com/future-attack-scenarios-against-atm-authentication-systems/76099/

Lykou, G. (2019). Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management: Theories, Methods, Tools and Technologies. En D. G. George Iakovakis, *Aviation Cybersecurity and Cyber-Resilience*(págs. 245-260). Springer Nature Switzerland. Obtenido de portal.eu/phocadownload/TSG_Positions/Industry%20Developments%20in%20ATM%20Cyber-Security%202017%20Issue.pdf

Body, I. C. (03 de Noviembre de 2017). Industry Developments in ATM Cyber-Security. 15. Obtenido de https://meet.google.com/linkredirect?authuser=0&dest=http%3A%2F%2Fwww.icb-portal.eu%2Fphocadownload%2FTSG_Positions%2FIndustry%2520Developments%2520in%2520ATM%2520Cyber-Security%25202017%2520Issue.pdf

Krebs On Security. (11 de Mayo de 2020). *Krebs On Security*. Recuperado el Agosto de 2020 , de Ransomware Hit ATM Giant Diebold Nixdorf: https://krebsonsecurity.com/2020/05/ransomware-hit-atm-giant-diebold-nixdorf/

Cybersecurity & Infraesctructure Security Agency. (24 de Octubre de 2020). *Cybersecurity & Infraesctructure Security Agency*. Recuperado el Noviembre de 2020 , de https://us-cert.cisa.gov/ncas/alerts/aa20-239a

Ikeda, S. (03 de September de 2020). US Intelligence Agencies Warn of North Korean Hackers Running Cyber Attacks Against Banks, Stealing Billions. *CPO Magazine*, 3.

SGSI. (s.f.). Obtenido de Blog especializado en Sistemas de Gestión de Seguridad de la Información: https://www.pmg-ssi.com/2019/07/principales-indicadores-en-seguridad-de-la-informacion/

Pacheco, J. (20 de Septiembre de 2017). *HEFLO*. Recuperado el Enero de 2020, de https://www.heflo.com/es/blog/planificacion-estrategica/indicadores-rendimiento-procesos/

Reyna, O. A. (15 de Febrero de 2010). *Candado Digital*. Recuperado el Septiembre de 2019, de http://candadodigital.blogspot.com/2010/02/indicadores-clave-de-desempeno-para.html

Paus, L. (16 de Septiembre de 2016). Cómo generar métricas de seguridad efectivas en la empresa. *Welivesecurity*, 2.

Siteware. (16 de Junio de 2020). Todo sobre la gestión de indicadores estratégicos, tácticos y operativos en empresas. *Siteware*.

Kolga, R. (s.f.). *Cybersecurity insiders*. Obtenido de https://www.cybersecurity-insiders.com/why-successful-point-of-sale-pos (Siteware, 2020)-attacks-will-only-increase/

European Union Agency Foe Cybersecurity. (21 de September de 2016). *European Union Agency Foe Cybersecurity*. Recuperado el Noviembre de 2019, de ENISA: https://www.enisa.europa.eu/publications/info-notes/point-of-sle-attacks

Wikipedia. (5 de Noviembre de 2020). *Wikipedia*. Obtenido de https://en.wikipedia.org/wiki/Point-of-sale_malware

Orr, J. (30 de Agosto de 2019). Incident Of The Week: Russell Stover's Chocolates Latest To Disclose Retail Point-Of-Sale Machine Breach. *Cyber Security HUB*, 1. Obtenido de https://www.cshub.com/malware/articles/incident-of-the-week-russell-stovers-chocolates-latest-to-disclose-retail-point-of-sale-machine-breach

Dam, C. (s.f.). *Teskalabs*. Obtenido de https://teskalabs.com/blog/point-of-sale-security-issues-retail

Trend Micro . (2015). 5 Facts You Might Have Missed About PoS Attacks of Recent Years. *Trend Micro* . Obtenido de https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/5-facts-you-might-have-missed-about-pos-attacks-of-recent-years

Lord, N. (29 de Septiembre de 2020). *Digital Guardian* . Obtenido de https://digitalguardian.com/blog/what-pos-security-protecting-data-pos-environments

Zhang, E. (6 de Noviembre de 2017). Recuperado el Marzo de 2020 , de https://digitalguardian.com/blog/what-point-sale-pos-malware-how-it-works-and-how-protect-your-pos-system

Association For Testing & Softwere Quality Assurance . (s.f.). Obtenido de https://atsqa.org/certifications/atsqa-testing-essentials?gclid=CjwKCAjw-5v7BRAmEiwAJ3DpuO_3R7rh-q8UmdTZsvFVx1BmQibX8FYhfgRCmR2PfnmiyepaTerHXxoCiSAQAvD_BwE

Kaspersky Lab . (2017). Point of Threat or Point of Sale: Threats Targeting PoS Terminals. *Kaspersky Enterprise Cybersecurity*.

Trapx Security . (s.f.). *Trapx Security* . Obtenido de https://trapx.com/cyber-attackers-target-retail-and-point-of-sale-systems-pos/

Attivo Networks . (2020). *Attivo Networks* . Obtenido de https://attivonetworks.com/documentation/Attivo_Networks-Point_of_Sale_System_Attacks.pdf

Gamelah Palagonia, F. (2013). *Privacy Professionals LLC* . Obtenido de https://www.nihca.org/wp-content/uploads/2010/02/CPR-Risks.A-POS-Perspective.pdf

Bisson, D. (25 de Noviembre de 2015). Catch Says POS Malware Incident Might Have Exposed Customers' Data. *Scurity Boluevard*.

Johansson, A. (s.f.). *Benelux Intelligence Community*. Obtenido de https://www.bi-kring.nl/101-business-intelligence-archief/1026-the-4-major-cybersecurity-threats-to-business-intelligence

Huntsman. (s.f.). *Huntsman*. Obtenido de https://www.huntsmansecurity.com/solutions/cyber-security-solutions/business-intelligence-reporting-for-cyber-security/

Secbi . (s.f.). Obtenido de https://www.secbi.com/technology/

Bi-Survey. (s.f.). Obtenido de https://bi-survey.com/big-data-security-analytics

Bi.zone . (s.f.). Obtenido de https://bi.zone/research/

Lord, N. (17 de Julio de 2020). Bibliografíacybersecurity Incident Response Planning: Expert Tips, Steps, Testing & More. *Digital Guardian*.

Areitio, J. (s.f.). *Seguridad de la Información. Redes, informática y sistemas de la información.*

COA . (s.f.). Obtenido de https://www.coasa.com.ar/our-works/tas/

Fujitsu Technology Solutions. (2017). *Fujitsu*. Obtenido de https://www.fujitsu.com/es/Images/WP_Seguridad_en-red-ATMs_final.pdf

Ecommerce Platforms. (s.f.). *Ecommerce Platforms*. Obtenido de https://ecommerce-platforms.com/es/glossary/point-sale

Myers, L. (28 de Julio de 2014). ¿Está protegido tu Punto de Venta contra ataques? *We live security* . Obtenido de https://www.welivesecurity.com/la-es/2014/07/28/esta-protegido-tu-pos-contra-ataques/

De conceptos. (s.f.). *De conceptos* . Obtenido de https://deconceptos.com/ciencias-sociales/tactica#:~:text=El%20origen%20etimológico%20de%20la,para%20llegar%20a%20un%20objetivo.