Indicadores en el Modelo de Seguridad de la Información

Leonel Ayala Sáenz
Postgrados – Especialización en Seguridad Informática
Universidad Piloto de Colombia
ayato007@hotmail.com

***Resumen*- En este documento se contemplan algunos conceptos básicos para la definición de métricas, los cuales pueden ser tenidos en cuenta por las organizaciones, para que de acuerdo con su naturaleza, los utilicen para definir métricas, no solo para tener conocimiento del desempeño del modelo de seguridad de la información, sino que les permitan implementar indicadores en las otras áreas o procesos que conforman las organizaciones. Igualmente, se contemplan aspectos tales como los conductores de medición de seguridad en el negocio, modelado de medidas de seguridad y qué define una buena métrica. Se hace una breve descripción de las características de los indicadores de gestión entre los que se contemplan aspectos tales como por qué debemos medir, para que debemos medir, atributos, tipos y categorías de los indicadores. Se expone una metodología para la construcción de indicadores y finalmente, se incluyen ejemplos de indicadores que se podrían utilizar para la medición del control y la evolución del modelo de seguridad de la información.**

***Abstract*— In this paper some basic concepts for defining metrics are contemplated, which may be considered by organizations, according to their nature, used to define metrics, not only to have knowledge of the performance of the security model information, but allow them to implement indicators in other areas or processes that make organizations. Similarly, aspects such as safety test leads in business modeling security measures are contemplated and what defines a good metric. A brief description of the characteristics of management indicators including aspects such as why should we measure, so that we measure, attributes, types and categories of indicators contemplated done. A methodology for the construction of indicators exposed and finally, examples of indicators that could be used to measure and control the evolution of the security model of information are included.**

PALABRAS CLAVE

Amenazas, indicador, malware, medición, métricas, modelado, vulnerabilidades,

I. INTRODUCIÓN

El uso masivo de las tecnologías de la información y las telecomunicaciones, en todos los ámbitos de la sociedad, han creado nuevos ambientes, donde se generan conflictos, y donde existen amenazas que atentan contra la confidencialidad, integridad y disponibilidad de la información. En las organizaciones, el uso de estas tecnologías genera riesgos en sus procesos, que obligan a la creación e implementación de métodos que ayuden a sus administradores y a la alta gerencia a identificar de manera acertada las fallas en dichos procesos. La utilización de métricas de seguridad, permiten identificar los niveles de cumplimiento de los controles y procedimientos establecidos en cada uno de sus procesos, generando información que ayuda a tomar decisiones acertadas para la gestión del riesgo de manera más objetiva y el cumplimiento de los objetivos establecidos para el negocio.

Ya que los indicadores, se vuelven una herramienta generadora de información, los funcionarios de la organización, deben tener cuidado en establecer que es lo que se debe medir, para qué se debe medir y cómo se va a medir. Si los indicadores no se encuentran adecuadamente diseñados, los resultados pueden inducir al error. Por lo tanto en el modelo de seguridad de la información, se debe cuantificar y medir los riesgos generados en este proceso, tan efectivamente como se realiza en los demás procesos de la organización.

En este documento, el lector encuentra información que le puede ayudar a aclarar los conceptos de lo que es una métrica, para que sirve y como se puede elaborar, sin que esto quiera decir que es un manual para el desarrollo e implementación de indicadores. Se incluyen algunos ejemplos de métricas que se podrían llegar a implementar en el proceso del modelo de seguridad de la información, los cuales podrían utilizar como marco de referencia para que una vez analizados se identifique la necesidad de implementarlos en su organización.

II. GENERALIDADES

Desde los principios de la era moderna de la computación, la seguridad se ha dejado en mano de los expertos en seguridad informática, principalmente de profesionales que por sus conocimientos, asumen la responsabilidad de mantener segura la información. El crecimiento en la dependencia de la sociedad, en los sistemas de información, entre otros Internet, ha llamado la atención sobre la vulnerabilidad evidente de ésta frágil infraestructura. Para la mayoría de las organizaciones, la seguridad es una "prioridad de la alta dirección". En los últimos años, la Ley Sarbanes-Oxley[1] y la pandemia de seguridad de Windows han causado que los niveles de financiación aumenten significativamente. En el año 2002, el presupuesto de la seguridad de la empresa promedio, donde no se incluye el personal, en Estados Unidos era aproximadamente de USD $1.1 millones, que se tradujo en un total de USD $196 gastados en seguridad anual por empleado[2]. Los presupuestos han aumentado anualmente en

[1] La Ley Sarbanes Oxley nace en Estados Unidos con el fin de monitorear las empresas que cotizan en bolsa de valores, evitando que las acciones de las mismas sean alteradas de manera dudosa, mientras que su valor es menor. Su finalidad es evitar fraudes y riesgo de bancarrota, protegiendo al inversor.

[2] Según artículo de A. Carey, "Worldwide Information Security Services Forecast, 2001–2006," IDC report no. 26899, Apr. 2002.

casi un 20% desde entonces, pero la mayor parte del gasto se ha realizado en la adquisición de los productos de seguridad y no en el proceso de seguridad de la información.

Entonces, ¿por qué no se orientan los esfuerzos hacia el proceso de seguridad de la información? Los expertos en seguridad de la información, se realizan preguntas sencillas, que son fácilmente respondidas en el contexto empresarial:

¿La seguridad en la organización, es mejor este año?
¿Qué puedo conseguir con el presupuesto asignado?
¿Cómo nos encontramos con respecto a la competencia?

Aunque la seguridad de la información tiene algunos detractores, algunas de las empresas líderes y sectores de la industria, lo ven como un medio viable para hacer frente a los riesgos de seguridad de la información. En el modelo de antaño, se percibía el temor a las consecuencias catastróficas de un ataque a la información, la incertidumbre acerca de su vulnerabilidad y las dudas sobre la capacidad de las garantías organizacionales para la toma de decisiones de seguridad.

Teniendo en cuenta los factores de miedo, incertidumbre y duda, se crea la necesidad de establecer métodos de medición, que permitan establecer objetivos claros, que deberían alcanzar las organizaciones, para establecer los avances de maduración en la implementación del modelo de seguridad de la información.

Por lo anterior, en el documento se contemplan aspectos tales como:

Conductores de medición de seguridad en el negocio: analiza la importancia de las métricas de seguridad y las presiones comerciales que impulsan a las organizaciones a adoptarlas.

Modelado de medidas de seguridad: se definen "modeladores de seguridad", en qué se diferencian de "medidores de seguridad" y porque debemos aprovechar las experiencias de otros campos, para desarrollar indicadores eficaces.

¿Qué hace una buena métrica? Define cinco cualidades esenciales que garantizan lo que la métrica de seguridad debe tener.

III. CONDUCTORES DE MEDICIÓN DE SEGURIDAD EN EL NEGOCIO

Los indicadores de seguridad sensatos, buscan ir más allá del miedo, la incertidumbre y la duda, a un marco en el que las organizaciones pueden incrementar la estimación del riesgo, el alcance de los daños, entender el rendimiento de su seguridad organizacional y evaluar los costos de las métricas de seguridad en contra de su efectividad esperada.

Para gestionar el riesgo, se deben tener en cuenta los siguientes cuatro aspectos que impulsan a las empresas lejos del miedo, la incertidumbre y la duda:

Fragilidad de los activos de información: La mayoría de las organizaciones, se han dado cuenta que la eficacia de la operación, depende de la información. Cada ejemplo conocido de corrupción de información crítica, daño o destrucción, intensifica su preocupación por esta dependencia. Por lo tanto, está extendiendo el conocimiento de seguridad de la información y la voluntad de hacerle frente a los riesgos.

Seguridad demostrable: Las organizaciones se sienten incapaces de medir con precisión la idoneidad o eficacia de las diferentes opciones de seguridad. Las métricas de seguridad consistentes están disponibles, por lo tanto, la organización puede invertir en mejorar la seguridad.

Las presiones de costos: Las presiones económicas y el creciente costo de las soluciones de seguridad, significa que los proveedores de seguridad deben competir en precio con otros proyectos de infraestructura de tecnología. El análisis de costo/beneficio y los cálculos de retorno de la inversión, se están convirtiendo en requisitos estándar para cualquier venta de solución para seguridad de la información.

Rendición de cuentas: Los entes de control, reconociendo la creciente exposición de las organizaciones a los riesgos de seguridad de la información, están exigiendo la implementación de soluciones que ayuden al cumplimiento de las normas y establecimiento de buenas prácticas que ayuden a la gestión del riesgo.

IV. MODELADO DE MEDIDAS DE SEGURIDAD

Cuando los datos son escasos, el enfoque estándar es construir modelos y contar con la opinión de expertos para complementar los datos. Algunos modeladores bien informados, podrían ayudar a determinar lo que los indicadores de seguridad deberían tener. El modelado, se refiere naturalmente a medida. En la seguridad informática, la mayoría de los observadores que mencionan las "métricas de seguridad", piensan desde el punto de vista de modelado de amenazas, riesgo percibido y pérdidas. La minoría, se preocupa menos de los aspectos de modelado y prefieren simplemente medir. Los modeladores piensan en función del riesgo, los incentivos económicos y por qué suceden las cosas. Los medidores más en datos empíricos, correlación, intercambio de datos y la causalidad (ver tabla I).

TABLA I
LOS MODELADORES Y MEDIDORES

Modeladores	Medidores
Ecuaciones de riesgo	Datos empíricos
Esperanza pérdida transversal	Análisis de series de tiempo
Álgebra lineal	Correlación
Superficies de ataque	Prácticas esenciales
Flujo de información	Intercambio de información
Incentivos económicos	Gasto económico
Vendedores	Empresas
Por qué?	Antes y después

Se han generado muchas discusiones alrededor de la preocupación de modelos para la medición del riesgo, pero aún no se llega al acuerdo de generar una lista de métricas, que se pueda tomar como guía, para el desarrollo de indicadores.

No se han determinado, antecedentes matemáticos, que permitan llegar a modelos lo suficientemente elaborados que permitan explicar cómo, por qué, o cuál es el riesgo que una

organización debe soportar. Los buenos modelos nos proporcionan razones para la medición. Algunas organizaciones pueden entregar pistas acerca de los modelos que se deben utilizar para el modelo de seguridad de la información. Dichos modelos, se podrían actualizar y ajustar a medida que se disponga de nuevos datos o tal vez sustituir la opinión de los expertos ejecutando mediciones objetivas. Puede tomarse como un proceso evolutivo, por lo cual no hay razón para que las organizaciones empiecen desde cero.

V. ¿QUÉ HACE UNA BUENA MÉTRICA?

La seguridad de la información es una disciplina que aún tiene que someterse a un serio examen analítico, para determinar cómo equilibrar el costo de los controles contra el costo del riesgo. Obtener las medidas adecuadas depende de realizar las preguntas correctas. Para la seguridad de la información, las organizaciones se preguntan lo siguiente:

¿Qué tan efectivos son mis procesos de seguridad de la información?
¿Estoy mejor con respecto al año anterior?
¿Cómo me comparo con las otras organizaciones?
¿Tengo asignado el presupuesto adecuado?
¿Cuáles son las opciones para la transferencia de riesgos?

En la tabla II, se muestra un ejemplo de cómo se podrían calcular las métricas utilizadas en organizaciones de diferentes sectores industriales. En estos indicadores, se pueden identificar tres características:

TABLA II
EJEMPLOS DE MÉTRICAS DE NEGOCIOS

Disciplina o Mercado	Cláves métricas	Cálculo
Transporte	Costo de transporte de carga por kilómetro	Total gastado en el camión dividido por el kilometraje.
	Coeficiente de ocupación	Porcentaje de utilización de la capacidad total.
	Millas vacías	Porcentaje de los viajes que realiza, sin carga.
Almacenamiento	Costo de almacenamiento por metro cuadrado.	Total de los costos de operación de almacén dividido por tamaño.
	La rotación de inventario.	Costo total de los bienes vendidos al año dividido por el valor promedio de inventario para el período.
E-commerce	Tasa de conversión del sitio web	Porcentaje de visitantes únicos al sitio web que compran algo.
Cable y el costo de suscripción vía satélite	Cable y el costo de suscripción vía satélite para adquirir	Costo de toda la comercialización, subsidios y descuentos dividido por el número de clientes adquiridos.
	Ingreso promedio por usuario	Ingreso promedio por usuario

1) Son fáciles de explicar y calcular directamente.
2) Todos están expresados en términos de tiempo, dinero o una medida derivada de estos.
3) Se prestan fácilmente a la evaluación comparativa.

Si las organizaciones compartieran información de las encuestas realizadas por las consultorías, podrían adquirir conocimiento sobre su propio desempeño en relación con las otras organizaciones. La evaluación comparativa de las organizaciones, es una saludable práctica que podría establecerse como pilar de la administración moderna. Los datos de referencia son económicos de conseguir, son expresados como números, contienen unidades de medida, son objetivos y consistentes.

La seguridad de la información, no cuenta con un equivalente, ni la tradición, ni el tiempo para efectuar una evaluación comparativa de rendimiento en las organizaciones. Los números que existen corresponden a las vulnerabilidades y amenazas reportados en los informes generados por empresas especializadas como Symantec, Qualys, entre otros, que solamente proporcionan detalles a nivel macro sobre la existencia de malware o los parches que se deben instalar, pero esta información no puede ser utilizada por las organizaciones para evaluar su efectividad en comparación con otras.

VI. CARACTERÍSTICAS DE LOS INDICADORES DE GESTIÓN

Se puede considerar un indicador de gestión, un dato que refleja las consecuencias de las actividades desarrolladas por las decisiones tomadas en una organización.

Los indicadores de gestión, deberán manifestar como resultado, cifras veraces y confiables, ya que el análisis nos podría llevar a un resultado errado. Por otra parte, si los indicadores son impreciso, la interpretación podría llegar a complicarse. Un indicador de gestión, permite identificar si un proyecto o el proceso dentro de una organización están cumpliendo con los objetivos propuestos.

Un indicador de gestión es:

a) Un instrumento o mecanismos utilizado para evaluar si se están o no cumpliendo con los objetivos estratégicos.
b) Una unidad de medida gerencial que permite evaluar los resultados de una organización, frente a sus objetivos y responsabilidades con las directivas.
c) Un generador de información, que permite analizar el desempeño de cualquier proceso y verificar el cumplimiento en términos de resultados.
d) Un generador de alertas que permiten determinar desviaciones en el cumplimiento de los objetivos.

A. ¿Por qué debemos medir y para qué?

Lo que no se mide, no se puede controlar y si no se puede controlar, no se puede dirigir y si no se puede dirigir no se puede mejorar.

Las empresas vienen experimentando un continuo proceso de cambios, generados por los avances tecnológicos, pasando de un ambiente de protección regulada a ambientes abiertos altamente competitivos. Estos constantes cambios en el ambiente de negocios crean la necesidad que las organizaciones, para mantener e incrementar su participación en el mercado en las mismas o mejores condiciones, elaboren una clara metodología de cómo analizar y evaluar sus procesos, es decir tener definido un sistema de medición de desempeño.

La medición de desempeño, se podría definir generalmente, como una serie de tareas orientadas a medir, evaluar, ajustar y regular, las actividades de una organización.

B. ¿Por qué debemos medir?

Para facilitar la toma de decisiones.

Para no tomar decisiones basado en suposiciones o intuiciones. Para medir la eficiencia de la organización.

Para conocer si cada área o proceso, se encuentra en el camino correcto.

Para mejorar los aspectos donde se determina debilidad y aplicar acciones de mejora.

Para conocer en tiempo real que sucede en la organización (¿somos eficientes?).

C. ¿Para qué debemos medir?

a) Para interpretar lo que está sucediendo.
b) Para actuar oportunamente, cuando las variables se salen de los límites establecidos.
c) Para determinar la necesidad de ejecutar cambios y/o acciones de mejoras y poder evaluar sus consecuencias prontamente.
d) Para analizar las tendencias y apreciar la productividad a través del tiempo.
e) Para establecer la relación existente entre productividad y rentabilidad.
f) Para generar o re-direccionar planes financieros.
g) Para relacionar la productividad con el nivel salarial.
h) Para medir la situación de riesgo en la que se encuentra la empresa.
i) Para proporcionar las bases del desarrollo estratégico y de la mejora focalizada.

D. Atributos de los Indicadores.

Cada indicador o medidor, debe cumplir con los siguientes criterios:

Medible: Expresa que la característica debe ser cuantificable en términos del grado o frecuencia de la cantidad.

Entendible: Debe ser de fácil entendimiento para todos aquellos que lo utilizan.

Controlable: El indicador debe permitir la capacidad de influir en ellos, debe ser controlable dentro de la estructura de la organización.

E. Tipos de Indicadores:

De acuerdo con el contexto de orientación, si es dirigida hacia los procesos, un indicador puede ser de procesos o resultados. Un indicador de procesos, se define para, medir que sucede con las actividades. Un indicador de resultados, se define para medir las salidas del proceso.

Igualmente, los indicadores se pueden clasificar en indicadores de eficiencia e indicadores de eficacia. Un indicador de eficiencia se define para medir el nivel de ejecución del proceso, está enfocado en el cómo se ejecutaron las tareas y mide el rendimiento de los recursos utilizados por un proceso. Se relacionan directamente con la productividad.

Un indicador de eficacia, se define para medir el logro de los resultados propuestos, es decir, informa si se ejecutaron de manera correcta las actividades que se debían realizar en el proceso. Un indicador de eficacia, se define para saber qué se debe hacer, por lo tanto es fundamental conocer y definir operacionalmente los requerimientos del cliente, en cuanto al proceso, para poder comparar el resultado obtenido contra el resultado esperado.

F. Categoría de los Indicadores:

De acuerdo con la categoría, podemos establecer los siguientes indicadores:

Indicadores de cumplimiento: Están relacionados con el cumplimiento en la ejecución de tareas y/o actividades (p.e. monitoreo a usuarios inactivos de funcionarios en vacaciones). Este monitoreo se debe ejecutar hasta el final, para que el indicador se cumpla.

Indicadores de evaluación: Están relacionados con el método o razón que ayudan a identificar nuestras fortalezas, debilidades y oportunidades de mejora (p.e. evaluar el procedimiento de monitoreo). Se evalúa el rendimiento obtenido al ejecutar una tarea, trabajo o proceso.

Indicadores de eficiencia: Están relacionados con las razones que indican el uso de los recursos utilizados en la ejecución de tareas, trabajo o proceso (p.e. tiempo utilizado en la ejecución de la tarea de monitoreo). Lo anterior, teniendo en cuenta que la eficiencia tiene que ver con la actitud y capacidad para realizar un trabajo con el mínimo de recursos.

Indicadores de eficacia: Están relacionados con los métodos o razones que indican capacidad o acierto en el resultado de las actividades o tareas ejecutadas. La eficacia tiene que ver con hacer efectivo un intento u objetivo. (p.e. calidad de los resultados obtenidos en el monitoreo).

Indicadores de gestión: Están relacionados con la metodología que permite administrar realmente un proceso. La gestión, tienen que ver con administrar y/o establecer acciones concretas para ejecutar con éxito la planeación de los trabajos.

G. Propósitos y Beneficios de los Indicadores.

La finalidad de los indicadores, es contribuir en las organizaciones a definir un camino que oriente las actividades que se deben desarrollar para cumplir con los objetivos establecidos.

Los sistemas de medición, como recurso de trabajo, deben cumplir con los siguientes objetivos:

a) Comunicar la estrategia.
b) Comunicar los objetivos.
c) Identificar los problemas y las oportunidades.
d) Diagnosticar problemas.
e) Ayudar a entender los procesos.
f) Ayudar a definir las responsabilidades,
g) Mejorar los controles en la organización.
h) Desarrollar iniciativas y actividades a desarrollar.
i) Medir comportamientos.
j) Facilitar la segregación de funciones.

La razón de la creación de un sistema de medición, es, comunicar, entender y orientar, las estrategias definidas por la organización, las actividades a que se deben desarrollar y la consecución de buenos resultados. Los sistemas de medición, son integrados por lo común, por los siguientes procesos: planificación, asignación de recursos (presupuesto), información, monitoreo (control), evaluación y compensación (ajustes).

Una de las dificultades más comunes, en los sistemas de medición, es su alineación; lo anterior, debido a que los procesos son liderados por áreas diferentes, responsables distintos, que generalmente no se coordinan entre sí. Se

presenta el caso que el proceso de planeación lo ejecuta de forma independiente el área de planificación, mientras que los procesos de asignación de recursos, información y seguimiento los ejecuta el área financiera y los procesos de evaluación y compensación son administrados por el área de recursos humanos.

La falta de coordinación entre las diferentes áreas, genera inconsistencias en el instante de jerarquizar, comunicar, ejecutar y medir las estrategias planteadas. Esto pasa, debido a que lo que para un área de la organización es importante no lo es para las otras, lo que para unas áreas es urgente para las otras no lo es, situaciones que dificultan la integración de todos los mecanismos que propone la organización en pro del cumplimiento de los objetivos trazados.

Para la implementación de una estrategia que permita alcanzar el objetivo definido para el futuro, implica una combinación apropiada de estructura y control. La estructura define las actividades e indica cómo se deben coordinar, sin embargo no provee la motivación suficiente para que funcione, por lo tanto surge la necesidad de generar controles.

Los sistemas de medición, son necesarios para motivar los comportamientos y acciones deseables para la organización y porque no todos los funcionarios están dispuestos o son capaces de hacer lo mejor, en busca de los resultados deseados.

H. Qué se debe esperar de un sistema de Indicadores.

Los sistemas de indicadores, son un recurso que una vez son implementados en la organización, deben proveer resultados, por lo tanto, se podría esperar entre otros, lo siguiente:

a) Que sea un generador de alertas.
b) Que permita identificar las tendencias y las causas de los comportamientos productivos.
c) Que permita establecer la relación entre el valor agregado y costo laboral para definir la cantidad y el costo adecuado del recurso humano.
d) Que permita relacionar factores como productividad del capital humano, capital físico, rentabilidad, endeudamiento y liquidez, para obtener un adecuado equilibrio.
e) Facilitar la toma de decisiones, para construir conocimiento, que sirva de guía a los funcionarios de la organización, a cumplir con las políticas y operar adecuadamente los procesos productivos.

Las áreas deben definir los indicadores con base en los procesos propios y para su definición, se debe contemplar:

a) Funciones: Propias del área, definidas de acuerdo con su razón dentro de la organización, como guía principal para entender su rol en la gestión global dentro de la misma.
b) Procesos: Teniendo en cuenta que los procesos incluyen básicamente una entrada (datos, información), un proceso propiamente dicho y una salida (resultados, conocimientos).
c) Estructura: La manera en que se encuentran organizados los elementos que componen el área para operar en forma adecuada.
d) Desempeño: Está definido por lo que se entrega al área, lo que genera y lo que se espera como resultado.
e) Clientes: El resultado (datos, información, productos) generado por el área, tienen como receptores unos clientes con necesidades y expectativas con respecto a lo que ésta les entrega.

I. Condiciones básicas que debe reunir un Indicador.

Un indicador deberá ser relevante, la información que genera debe ser imprescindible y cumplir con el objetivo de informar controlar, evaluar, para ayudar a una adecuada toma de decisiones. Los cálculos que se utilizan en el indicativo, no deben arrojar resultados ambiguos, lo que debe permitir que sean auditables para evaluar su confiablidad siempre que sea necesario; igualmente, deberá ser inequívoco para evitar interpretaciones contradictorias. El concepto que debe expresar el indicador, debe ser claro y mantenerse en el tiempo, el indicador deberá ser pertinente, es decir, adecuado a lo que se pretende medir y la información generada por él mismo, debe estar disponible en el momento que se requiera para una toma de decisiones.

La objetividad en los indicadores es otra importante característica, debido a que se debe evitar estar condicionados por factores externos (públicos o privados) o el accionar de terceros. Por tal razón, deberán ser evaluados periódicamente por entes externos. Para determinar variaciones relativamente pequeñas, el indicador deberá ser eficaz. Dicha propiedad, es la sensibilidad que exige que su construcción debe ser de calidad, para que automáticamente permita identificar cambios en los datos. Asimismo, deberá ser preciso, permitiendo un margen de error aceptable.

Los indicadores deberán ser accesibles, ya que su elaboración tiene un costo, el cual debe ser superado por los beneficios que generan sus resultados, de fácil interpretación y cálculo sencillo.

Resumiendo, los indicadores deberán proporcionar información en cantidad y calidad razonables (relevancia) para no obtener conclusiones distorsionadas de la realidad (inequívoco), estando disponible en el momento propicio para la toma de decisiones (pertinencia y oportunidad), teniendo en cuenta que los costos de elaboración no superen los resultados potenciales de la información generada.

VII. METODOLOGÍA PARA CONSTRUCCIÓN DE INDICADORES

Las metodologías, ayudan a sistematizar el trabajo y a identificar los puntos clave para desarrollar los objetivos que se definieron, de manera exitosa. En este numeral, se propone una metodología, que podría ser utilizada para la elaboración de un conjunto de indicadores. Cuando en una organización se propone una metodología de elaboración de indicadores, ésta debe ser aprobada por la mayoría de los miembros de las áreas que participarán en dicha actividad, con el fin que todos utilicen una misma terminología, y así evitar confusiones que lleven a interpretaciones erradas entre los diferentes niveles de la organización.

Para la elaboración de indicadores, la metodología debe definir:

1. La elaboración de una plantilla donde se describan los aspectos principales del indicador tales como nombre del indicador, descripción, objetivo, fuente de datos, entre otros, con tener un inventario de los indicadores definidos.

Adicionalmente, se debe contemplar la formulación de las siguientes preguntas:

2. ¿Qué se debe hacer?

Se deben seleccionar las actividades que se consideran prioritarias. De acuerdo con un criterio previamente establecido, se trata de identificar un valor de medición (p.e. de 0 a 10), que permita priorizar todas las actividades.

3. ¿Qué se desea medir?

Una vez identificadas las actividades, las cuales deben estar descritas y valoradas, se deberán seleccionar los receptores (destinatarios) de la información, teniendo en cuenta que cada indicador es diferente sustancialmente en función de quién los utilizará.

4. ¿Quién utilizará la información?

Importante identificar quiénes serán los funcionarios dentro de la organización, a los cuales se les deberá entregar la información resultado del indicador.

5. ¿Cada cuánto tiempo?

Dependiendo de la actividad y del destinatario de la información, se deberá definir una frecuencia (mensual, trimestral, semestral, anual), para su presentación.

6. ¿Con qué o quién se compara?

Se deberán establecer referentes de acuerdo con la estructura del indicador, proceso o resultado, los cuales pueden ser internos o externos a la organización y que podrán ser utilizados para efectuar comparaciones.

En el proceso de elaboración de los indicadores se deben contemplar e identificar los factores clave del éxito, los cuales son las capacidades controlables por la organización en los que se destaca para lograr los objetivos, como son: capacidad de conseguir satisfacción de los clientes o usuarios, la capacidad para generar servicios de calidad, capacidad para disminuir los tiempos de entrega de manera confiable y la capacidad para retroalimentarse y aprender.

VIII. ¿CÓMO PODEMOS MEDIR LA SEGURIDAD?

En el mejor de los casos, las métricas de seguridad tradicionales son accidentales; en el peor de los casos, dan una aparente sensación de seguridad, que tiene como resultado una implementación ineficiente o insegura de indicadores de seguridad. Para proporcionar una imagen más completa y ordenada del estado del modelo de seguridad de la información en una organización, es necesario realizar una combinación entre madurez y calidad.

A lo largo del tiempo, la medida (métricas de seguridad) de la eficacia de los esfuerzos en seguridad de la información ha sido siempre difícil de evaluar. La medida de calidad del modelo de seguridad se evalúa, sólo cuando la organización se ve afectada por una crisis. Pero es precisamente para evitar esto, que se realizan verdaderos esfuerzos en lo relacionado con la seguridad.

Una pieza del rompecabezas de métricas de seguridad definidas para el modelo de seguridad de la información, es la medida de los avances obtenidos en el programa de seguridad, frente al modelo de madurez. Este enfoque está dirigido a la medición de cosas significativas para la organización y el acercamiento al cumplimiento de los objetivos, que corresponden a dos de las características antes mencionadas.

TABLA III
RESUMEN GENERAL DEL MODELO DE MADUREZ DE SEGURIDAD

Categorías	No. de elementos medidos	Factores cubiertos por los elementos
1. Gestión general de la seguridad	11	Necesidad, estrategia, compromiso, roles y responsabilidades, políticas y procedimientos.
2. Clasificación y control de activos	5	Valoración, evaluación de riesgos, propiedad, etiquetado y manejo, inventario.
3. Seguridad relativa al personal	8	Contratación y finalización de contrato, roles y responsabilidades, investigación de antecedentes, formación, reporte, revisión.
4. Seguridad física y del entorno	12	Perímetros, riesgos ambientales, evaluación de riesgos, controles de acceso, seguridad, eliminación, y destrucción de activos, monitoreo, gestión de incidentes, concienciación, cooperación.
5. Control de accesos.	11	Perímetros, evaluación de riesgos, controles de acceso, autenticación, necesidad de acceso, responsabilidad del usuario, actualización de accesos, monitoreo, dispositivos móviles, gestión de incidencias.
6. Desarrollo y mantenimiento de sistemas	9	Estándares, modelo de ciclo de vida, revisión, análisis de diferencias, planificación de requerimientos, integridad y certificación de pruebas, repositorio de código, gestión de versiones, retirada.
7. Gestión de comunicaciones y operaciones	16	Estándares, todos los métodos de comunicaciones electrónicas, procedimientos operativos, monitoreo, backups, gestión de excepciones, actualizaciones y parches, helpdesk, gestión de cambios, sistemas criptográficos, gestión de soportes, código maligno, aceptación de sistemas, librería de documentación, planificación de capacidades.
8. Seguridad organizacional	11	Función de seguridad, monitoreo, asesoría, auditoría, comité de seguridad, concienciación, segregación de funciones, pruebas de penetración y vulnerabilidad, gestión de incidentes, cooperación.
9. Gestion de continuidad de negocio	7	Evaluación de riesgos, gestión de prioridades, backups, planificación de continuidad de negocio y recuperación de desastres, pruebas, actualizaciones.
10. Cumplimiento	10	Reglamentaciones, contratos, propiedad intelectual, etiquetado y manejo, retención de registros, auditoría, sanciones.

En la tabla III, se presenta un ejemplo de un modelo detallado de madurez de seguridad, donde se tiene en cuenta

un enfoque de sistema de gestión que sigue un estándar para desarrollar un programa de seguridad completo, lo que implica la inclusión o no de un gran número de elementos.

Teniendo en cuenta que se tiene muy poca valoración subjetiva, los resultados son objetivos y por lo tanto pueden ser difundidos. Si ciertos elementos son ejecutados (programas de auditoría), nos podrían llevar a la ejecución de otros controles de calidad; por lo tanto no se está midiendo solamente la calidad o eficacia en la implantación de los elementos. Se considera importante, aclarar que para un elemento se puede definir más de un indicador.

A continuación, se relacionan algunos indicadores que se pueden implementar en las organizaciones con el fin de tener conocimiento del estado del modelo de seguridad. De acuerdo con las cifras resultado del cálculo de los indicadores, las organizaciones deberán evaluar las actividades y controles que se tengan implementados y de ser necesario realizar los ajustes correspondientes o validar la necesidad de crear nuevos controles. Es necesario aclarar que los indicadores que aquí se incluyen, son un ejemplo de cómo se podrían implementar en una organización, pero esto no quiere decir que no existan metodologías diferentes para el diseño de métricas, las cuales deberían ser implementadas de acuerdo con la naturaleza y necesidades propias de cada negocio.

Para facilitar el entendimiento de los indicadores, por aquellas personas de las organizaciones que van a hacer uso de ellos, es necesario aclarar que la hoja de vida de cada indicador deberá estar compuesta por dos partes: una de diseño (ver tabla IV), que comprende la descripción del indicador y la otra de medición (ver tabla V), donde se generan los resultados de la medición efectuada.

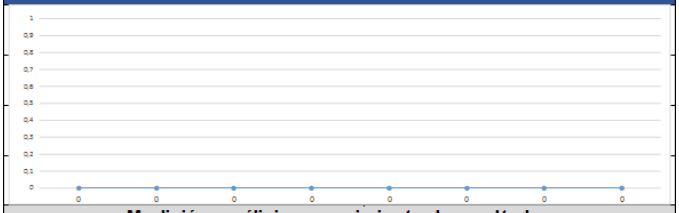
TABLA IV
DISEÑO HOJA DE VIDA INDICADOR

DISEÑO HOJA DE VIDA INDICADOR					
Diseño del indicador					
ID		*Fecha actualización*		*Versión*	
Nombre					
Objetivo					
Medida					
Fuente de datos					
Fórmula de cálculo					
Método de cálculo, análisis y reporte					
No.	*Paso*	*Responsable*	*Frecuencia*		
Criterios para el análisis de datos					
Meta					
Valor fórmula			Sentido		
Indicador		=>100%	Entre 80% - 99%	Entre 0 -79%	

En el diseño, se encuentran los siguientes elementos: identificación, que es el código asignado por la organización; fecha de actualización, donde se registra la fecha de creación del indicador y posterior fecha de actualización; versión, que nos indica cuantas veces ha sido modificado; nombre, que se le da al indicador; objetivo, que describe para que fue creado el indicador; medida, que indica breve descripción de lo que va a medir el indicador; fuente de datos, que nos permite identificar la actividad o el dispositivo tecnológico que está generando la información que utilizará el indicador; fórmula de cálculo, ecuación matemática que se debe ejecutar para obtener el resultado del indicador. En el método de cálculo, análisis y reporte, se describen los pasos que se deben realizar para la ejecución del indicador, el responsables y la frecuencia de medición definida para el indicador. En los criterios para el análisis de datos, se define la meta que se debe cumplir el proceso que se está midiendo; el valor de la fórmula expresado en porcentaje, y el indicador propiamente dicho, el cual se expresa en forma de semáforo, para visualmente determinar si se está o no cumpliendo con la meta definida; un sentido creciente o decreciente, el cual se define de acuerdo con la naturaleza del indicador.

En la medición, se encuentra un espacio, en el cual se debe insertar una gráfica de los resultados del indicador, con el fin que se tenga un entendimiento visual de dicho resultado; en la medición, análisis y seguimiento de resultados, se encuentra el periodo evaluado, la meta propuesta para ese periodo, el resultado en cifras (numero o porcentaje), un espacio para una descripción breve del análisis efectuado a los resultados y una breve descripción del plan de actividades que se va a ejecutar para el cumplimiento del objetivo del proceso, en caso que este no se cumpla. Igualmente se dispone de un espacio en donde el análisis y el plan de actividades se pueden registrar de manera más específica.

TABLA V
MEDICIÓN HOJA DE VIDA INDICADORES

MEDICIÓN - HOJA DE VIDA INDICADORES				
				
Medición, análisis y seguimiento de resultados				
Periodo	**Meta**	**Estado / Resultado**	**Análisis**	**Acciones**
Análisis			***Acciones***	

A continuación se incluyen algunos de los indicadores que se podrían definir para la medición de algunas de las actividades realizadas en el modelo de seguridad de la información:

a) Ejecución del programa de seguridad.

Este indicador permite conocer el porcentaje de cumplimiento de las iniciativas de seguridad implementadas versus el programa de plan de actividades definido para el modelo de seguridad de la información aprobado por el comité de seguridad de la información (ver tabla VI).

TABLA VI
INDICADOR EJECUCIÓN DEL PROGRAMA DE SEGURIDAD

Diseño del indicador	
ID	SI - 1.1.1
Fecha de Actualización	15 de Febrero de 2015
Versión	1
Nombre:	Ejecución del programa de seguridad
Objetivo:	Conocer el cumplimiento (porcentaje) de las iniciativas de seguridad implementadas respecto al programa de seguridad de la información.
Medida:	Porcentaje de avance de iniciativas de seguridad respecto al avance planteado en el plan de trabajo definido en el comité de seguridad.
Fuente de datos	Plan de trabajo definido por el comité seguridad de la información.
Fórmula de cálculo	(Porcentaje ejecutado del plan de trabajo / Porcentaje esperado de avance del plan de trabajo) * 100

b) Documentación de seguridad

Este indicador permite identificar el número de actividades ejecutadas con respecto a las detalladas en los documentos referenciados (ver tabla VII); lo cual ayuda a controlar que las actividades que desarrollan los funcionarios, son las descritas en los manuales y procedimientos elaborados para los procesos de la organización.

TABLA VII
INDICADOR DOCUMENTACIÓN DE SEGURIDAD

Diseño del indicador	
ID	SI - 1.1.2
Fecha de Actualización	15 de Febrero de 2015
Versión	1
Nombre:	Documentación de seguridad
Objetivo:	Velar por la documentación actualizada de las actividades desarrolladas por los responsables de las funciones de seguridad de la información e informática.
Medida:	Porcentaje de documentación de las actividades desarrolladas en las funciones de seguridad de la información e informática.
Fuente de datos	Manuales de Funciones; Manual Organizacional de Seguridad de la Información; Cronograma Operativo de Seguridad; Personas responsables de la función de seguridad
Fórmula de cálculo	(Número de actividades de seguridad de la información e informática documentadas y revisadas / Número total de actividades realizadas)*100

c) Nivel de cultura de seguridad de la información

Este indicador permite establecer el nivel de cultura de seguridad de la información, de los funcionarios de la organización, a partir de tres variables: conocimiento, compromiso y comportamiento (ver tabla VIII).

TABLA VIII
INDICADOR NIVEL DE CULTURA DE SEGURIDAD

Diseño del indicador	
ID	SI - 1.1.3
Fecha de Actualización	15 de Febrero de 2015
Versión	1
Nombre:	Nivel de cultura de seguridad.
Objetivo:	Identificar el nivel de cultura de seguridad de los Colaboradores de la Entidad.
Medida:	Porcentaje de nivel de cultura de seguridad de los usuarios de acuerdo con la medición de conocimiento, compromiso y comportamiento establecidos por la Entidad.
Fuente de datos	Evaluaciones escritas; Plan de Capacitación; Listados de Asistencias a capacitaciones de Seguridad; Base de datos incidentes; Encuesta de seguridad
Fórmula de cálculo	(Conocimiento + Compromiso + Comportamiento) / 3 (Conocimiento = Porcentaje total de Colaboradores que obtuvieron calificaciones entre 8 y 10 en la evaluación de Seguridad) (Compromiso = Porcentaje total de Colaboradores que asistieron a las capacitaciones programadas de acuerdo al plan establecido) (Comportamiento = Porcentaje total de Colaboradores que se comportan adecuadamente, teniendo en cuenta la cantidad de incidentes presentados y/o los resultados de la encuesta de seguridad.

IX. CONCLUSIONES

Las organizaciones deben prestar especial atención al desarrollo e implementación de los indicadores en sus procesos. Recordemos que lo que no se mide, no se puede controlar, lo que puede generar inconvenientes a las directivas de las organizaciones para establecer estrategias de mejora.

Con el continuo cambio que se vienen presentando en el mundo de los negocios y que afecta a las organizaciones a nivel tecnológico, comercial y de infraestructura, obliga a cambiar el punto de vista de la protección que se debe implementar y para estar preparados para ambientes altamente competitivos. Por esta razón las organizaciones deben contar con herramientas que les brinden información confiable para analizar y evaluar la evolución de los procesos propios del negocio. Herramientas como los indicadores, serán de gran ayuda para una adecuada toma de decisiones.

La importancia de los sistemas de medición, radica en que son necesarios para motivar los comportamientos y acciones deseables para la organización, incentivando la creación de estrategias que motiven a los funcionarios a orientar sus esfuerzos, para cumplir con los objetivos del negocio.

REFERENCIAS

[1] Andrew Jaquit foreword Daniel E. Geer, Chapter 2 Defining Security Metrics in Security Metrics: Replacing Fear, Uncertainty, and doubt, ext printed in the United States on recycled paper at RR Donnelley, Crawfordsville, Indiana First printing, March 2007.

[2] https://jcvalda.wordpress.com/2012/12/10/definicion-y-

caracteristicas-de-los-indicadores-de-gestion-empresarial/

[3] http://www.redalyc.org/articulo.oa?id=78419688001

[4] http://www.isaca.org/Journal/Past-Issues/2005/Volume-2/Pages/Como-Puede-Medirse-la-Seguridad.aspx.

[5] http://www.gestiopolis.com/administracion-estrategia-2/definicion-caracteristicas-indicadores-gestion-empresarial.htm

[6] http://www.monografias.com/trabajos55/indicadores-gestion/indicadores-gestion2.shtml

REFERENCIAS TABLAS

TABLA I - LOS MODELADORES Y MEDIDORES. Fuente: Andrew Jaquit foreword Daniel E. Geer, Chapter 2 Defining Security Metrics in Security Metrics: Replacing Fear, Uncertainty, and doubt.

TABLA II - EJEMPLOS DE MÉTRICAS DE NEGOCIOS. Fuente: Andrew Jaquit foreword Daniel E. Geer, Chapter 2 Defining Security Metrics in Security Metrics: Replacing Fear, Uncertainty, and doubt.

TABLA III - RESUMEN GENERAL DEL MODELO DE MADUREZ DE SEGURIDAD. Fuente: http://www.isaca.org/Journal/Past-Issues/2005/Volume-2/Pages/Como-Puede-Medirse-la-Seguridad.aspx.

TABLA IV - DISEÑO HOJA DE VIDA INDICADOR. Fuente: El autor.

TABLA V - MEDICIÓN HOJA DE VIDA INDICADORES. Fuente: El autor.

TABLA VI - INDICADOR EJECUCIÓN DEL PROGRAMA DE SEGURIDAD. Fuente: El autor.

TABLA VII - INDICADOR DOCUMENTACIÓN DE SEGURIDAD. Fuente: El autor.

TABLA VIII - INDICADOR NIVEL DE CULTURA DE SEGURIDAD. Fuente: El autor.