RISI 8(1), 2011 (25-30)
Revista de Investigación de Sistemas e Informática
Facultad de Ingeniería de Sistemas e Informática
Universidad Nacional Mayor de San Marcos
ISSN 1815-0268 (Versión Impresa)
ISSN 1816-3823 (Versión electrónica)

La seguridad de la información

Information security

Percy Vivanco Muñoz, Augusto Cortez Vásquez, Víctor bustamante Olivera

Universidad Nacional Mayor de San Marcos
Facultad de Ingeniería de Sistemas e Informática

pvivancom@gmail.com, cortez_augusto@yahoo.fr, vbustamante@gruposantodomingo.com.pe,

ReSUMeN

La seguridad de los sistemas de información es un tema muy complejo que requiere la preparación de estrategias que permitan que la información circule libremente, garantizando al mismo tiempo la seguridad del uso de los sistemas de información en toda la comunidad. El proceso de garantía de seguridad esta relacionada con establecer un nivel de con fianza en el sistema que podría ser muy variable. Está es una cuestión de juicio profesional basado en evidencias sobre el sistema, su entorno y su proceso de desarrollo. Se puntualizará en el presente artículo todo lo relacionado a la seguridad de la información, custodia de datos, la auditoría de sistemas; así como el enfoque para medir el desempeño de las medidas de seguridad, el avance y progreso de las estrategias y la consecución de sus objetivos. Se considerará el impacto que tiene la falta de seguridad en la productividad enfocándose en el Modelo del Análisis para el Retorno de la Inversión de Seguridad (ROSI) derivado del conocido indicador financiero ROI (Retorno sobre la Inversión). Este modelo busca justificar la inversión en seguridad de la información en términos monetarios.

Palabras clave: seguridad de información, Análisis de retorno de inversión, seguridad informática.

AbStRACt

The security of information systems is a very complex issue which requires the preparation of strategies that allow information to flow freely, while ensuring the safety of using information systems throughout the Community. The safety assurance process is related to establishing a level of confidence in the system that could be very variable. This is a matter of professional opinion based on evidence about the system, its environment and its development process. Are spelled out in this article all about the security of information, data escrow, auditing systems, as well as the approach to measure the performance of the security, progress and advancement strategies and achieving its objectives. They consider the impact of insecurity on productivity by focusing on the Model Analysis for the Return on Security Investment (ROSI) derived from the financial indicator known ROI (Return on Investment). This model seeks to justify the investment in information security in monetary terms.

Keywords: information security, analysis for the return on investment, computer security.

1. INtRodUCCIóN

A partir de la Segunda Guerra Mundial, el campo de la seguridad de la información ha crecido y evolucionado considerablemente, convirtiéndose en una carrera acreditada a nivel mundial, a tal punto que tanto las personas como las organizaciones encargadas de la elaboración de soluciones informáticas buscan el desarrollo de sistemas de información de calidad, enfocándose en software y hardware que permitan las comunicaciones y la integración desde diversas partes del mundo.

La constante actualización para asegurar la información es bastante más amplia, que no es simplemente una cuestión técnica sino responsabilidad de la alta gerencia y los cuadros directivos de una institución u organización.

Por ello es substancial resaltar la importancia que tienen estos sistemas de información en la sociedad y por ende la valoración que tiene dentro de medios gubernamentales, políticos, empresariales o educativos.

El funcionamiento de un sistema seguro depende normalmente de que el sistema esté disponible y su funcionamiento sea fiable[1], un sistema puede convertirse en no fiable si sus datos son corrompidos por algún intruso [3].

2. CoNteNIdo

La seguridad de la información tiene como fin la protección de la información y de los sistemas del acceso, uso, divulgación, y destrucción no autorizada. Los términos "seguridad de información", "seguridad informática" y "garantía de la información"; son usados con frecuencia y aunque su significado no es el mismo, persiguen una misma finalidad al proteger la confidencialidad, integridad y disponibilidad de la información. Sin embargo, entre ellos existen algunas diferencias sutiles. Estas diferencias radican principalmente en el enfoque, las metodologías utilizadas y las zonas de concentración.

La seguridad de la información[2] involucra la implementación de estrategias que cubran los procesos en donde la información es el activo primordial. Estas estrategias deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran.

La seguridad informática[3] consiste en garantizar que el material y los recursos de software de una organización se utilicen únicamente para los propósitos para los que fueron creados y dentro del marco previsto. Se resume, por lo general, en cinco objetivos principales:

- **Integridad**: garantizar que los datos sean los que se supone que son.
- **Confidencialidad**: asegurar que sólo los individuos autorizados tengan acceso a los recursos que se intercambian.
- **disponibilidad:** garantizar el correcto funcionamiento de los sistemas de información.
- **evitar el rechazo:** garantizar que no se pueda negar una operación realizada.
- **Autenticación:** asegurar que sólo los individuos autorizados tengan acceso a los recursos.

Los conceptos de seguridad informática y seguridad de información implican un panorama y una visión más amplia en un marco de riesgos de negocio respecto a una perspectiva tradicional de seguridad técnica, ya que, por un lado en la seguridad de la información los riesgos del negocio no sólo incluyen vulnerabilidades y amenazas sino que se incluyen los riesgos organizacionales, operacionales, físicos y de sistemas de TI y comunicaciones.

Dicho esto, como se evalúa los gastos y riesgos que implican la seguridad informática y la seguridad de la

1 El concepto de sistema fiable se utiliza para denotar la probabilidad de que durante un determinado periodo de tiempo el sistema funcione correctamente tal y como lo espera el usuario.

2 La seguridad de la información se refiere a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma. No debe confundirse con el concepto de seguridad informática, ya que esta última sólo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diferentes medios o formas.

3 La seguridad informática es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

información. ¿Es posible justificar económicamente las inversiones en seguridad de la información?

Un primer punto importante de considerar es la justificación de las inversiones en seguridad, ¿Qué impacto tiene la falta de seguridad en la productividad? ¿Qué impacto tendría una interrupción de seguridad catastrófica? ¿Cuál es la solución más costo-efectiva? ¿Qué impacto tendría la solución sobre la productividad?

Un segundo punto es ¿Cómo medir el desempeño de las medidas de seguridad y realizar la gestión correspondiente en la búsqueda de mejores resultados? ¿Cómo se evalúan los criterios que definen los elementos esenciales para la evaluación de la seguridad de la información?

Para evaluar las interrogantes del primer punto me enfocaré en el **Modelo del Análisis para el Retorno de la Inversión de Seguridad (RoSI)** derivado del conocido indicador financiero ROI (Retorno sobre la Inversión). Este modelo busca justificar la inversión en seguridad de la información en términos monetarios. Para ello se tiene presente que los efectos de una implementación de seguridad en general no surgen en forma directa como beneficios económicos para una empresa, sino en todo caso como una reducción en las pérdidas que producen incidentes de seguridad como ataques, fallas o errores.

El esquema de trabajo de ROSI parte de considerar que cada incidente produce pérdidas que se pueden estimar. Para ello se hacen cálculos del escenario original frente a cada incidente, y de lo que resultaría de aplicar salvaguardas o contramedidas para mitigarlo adecuadamente. La diferencia entre ambos resultados es el valor o beneficio de dichas salvaguardas. Entonces ROSI (análogamente al ROI) es igual a la relación entre el retorno y el costo de las contramedidas (la inversión en el ROI). El retorno o ganancia incremental, resulta ser el valor (beneficio en el ROI) menos el costo de dichas contramedidas.

ROSI = (mitigar el riesgo – Costo) / Costo

Se deduce que si el retorno de la inversión es positivo, tenemos una inversión que es significativo considerar, de lo contrario, si los costos superan los beneficios, la inversión no es recomendable.

En lo referente a las pérdidas por ataques o fallas generalmente se elaboran con la métrica de gestión de riesgos conocida como ALE. Para ello se estiman los valores probables del impacto monetario y de la frecuencia anual de ocurrencia para cada incidente, de modo tal que el producto de ambas variables resulta ser el ALE correspondiente.

SLe = AV * eF

Asset Value (AV) = Valor del Activo

Exposure Factor (EF) = Factor de Exposición

Single Loss Expectancy (SLE) = Expectativa de pérdida x evento

ALe = SLe * ARo

Single Loss Expectancy (SLE) = Expectativa de pérdida x Evento

Annual Rate of Occurrence (ARO) = Ratio (frecuencia) Anual de Ocurrencias esperadas

Annual Loss Expectancy (ALE) = Expectativa de pérdidas Anualizadas

Luego se multiplican estos elementos para obtener el (ALE) de esa vulnerabilidad.

Si bien es cierto que este mecanismo funciona adecuadamente cuando se disponen de suficientes datos históricos propios de dichos incidentes, ante la no existencia de estos datos se puede recurrir a fuentes externas, aunque generalmente no son completas y pueden estar referidas a ambientes de negocios diferentes al que se analiza. Además no es seguro que lo ocurrido se repita de la misma manera, ya que hay incidentes que declinan en su aparición por las salvaguardas o de las propias amenazas, así como incidentes nuevos que antes no se presentaban.

Hay un dicho muy conocido que dice "lo que no se puede medir, no se puede gestionar" y este es el segundo punto que se tocará, cómo medir el desempeño de las medidas de seguridad y realizar la gestión correspondiente en la búsqueda de mejores resultados, y es que la dificultad se centra en poder medir el avance y progreso de las estrategias y la consecución de sus objetivos.

Una forma de hacerlo es a través de las métricas, una métrica de seguridad puede definirse como el conjunto de preceptos y reglas necesarios para poder medir de forma real el nivel de seguridad de una organización, estas implantan medidas, controles e indicadores que garantizan la gestión de seguridad. El Instituto Nacional

de Estándar y Tecnología (NIST) elabora y promueve patrones de medición, normas y tecnología con el fin de realzar la productividad y acelerar el desarrollo y despliegue de sistemas, fiables, útiles e interoperables, y seguros, y es a través de estas métricas que se procede al mapeo de controles y gestión de políticas, de las Normas ISO 20071 para encontrar las métricas NIST adecuadas que provean un buen soporte para la autoevaluación y casos de uso de la gestión de controles necesarios.

Podemos nombrar algunas métricas como por ejemplo:

- Métricas para medir el porcentaje de riesgos identificados evaluados como de importancia alta, media o baja, más "no evaluados".
- Tendencia en número de riesgos relativos a seguridad de la información en cada nivel de importancia.
- Costos de seguridad de la información como porcentaje de los ingresos totales o del presupuesto de TI.
- Porcentaje de riesgos de seguridad de la información para los cuales se han implantando totalmente controles satisfactorios.

Pero, más allá de las métricas mencionadas incluyendo las condiciones de qué medir y cómo; hasta aquí no se pude contar con un mecanismo que nos sirva de control y gestión efectiva para las medidas de seguridad, entonces, es imperativo diseñar el modelo ideal para conducir las actividades de seguridad en un tema de investigación fundamental para alcanzar la eficacia y la eficiencia de la gestión de seguridad de información y así cumplir con los objetivos de la institución y/o empresa, para eso, se debe recurrir a otras herramientas de otras áreas de negocio, es decir herramientas de gestión de la estrategia, en conclusión se hace necesario utilizar indicadores no financieros que apoyados en la metodología del Balanced ScoreCard nos ayuden a concentrar los esfuerzos en crear verdadero valor a medio y largo plazo.

El Cuadro de Mando Integral (Balanced Scorecard) es considerada una de las mejores herramientas para implementar un plan estratégico en una compañía ya que responde a la incertidumbre de si la implementación de su estrategia planeada está avanzando o no. Esta herramienta-metodología se basa en la implementación de un mapa estratégico gobernado por la relaciones causa--fecto; lo importante es que ninguna perspectiva funciona de forma independiente, sino que nosotros podemos tomar la iniciativa actuando en cualquiera de ellas. [2]

En términos generales el primer paso se basa en la definición de los objetivos financieros para alcanzar la visión, para lo cual se debe indicar que estos objetivos constituirían el efecto de nuestra forma de actuar con los clientes/usuarios y, a su vez, el logro de sendos objetivos dependerá necesariamente de cómo hayamos programado y planificado los procesos internos. Por último, el BSC plantea que el logro unificado de todos estos objetivos tiene como pilar una formación de aprendizaje - formación y crecimento continuo.

elementos de un balanced Scorecard

Misión, visión y valores. La aplicación del Balanced Scorecard empieza con la definición de la misión, visión y valores de la organización. La estrategia de la organización sólo será consistente si se han conceptualizado esos elementos. En muchos casos estos ya están definidos y son mucho más sostenibles en el tiempo que los otros elementos del modelo.

A partir de la definición de la misión, visión y valores se desarrolla la estrategia, que puede ser representada directamente en forma de mapas estratégicos, o conceptualizada, antes, en otro formato.

Lo importante no es si el desarrollo de la estrategia forma parte del modelo, lo realmente importante es si hay una estrategia definida y adecuada. Si lo está, será el punto de partida para el desarrollo de los elementos del modelo; en caso contrario, el primer paso consistirá en la definición de la estrategia. [1,5].

Las Perspectivas

- **Perspectiva financiera:** es la primera perspectiva, cuya orientación principal es maximizar el valor de los accionistas y medir la creación de valor en la organización, en este caso la rentabilidad sobre la inversión.
- **Perspectiva del cliente** En esta perspectiva la organización identifica los segmentos de clientes/usuarios y de mercado en los que ha elegido competir. Permite que los productos y servicios estén mejor alineados con las preferencias de los clientes.
- **Perspectiva interna** En esta perspectiva se identifican los procesos críticos y estratégico para el logro de los objetivos planteados en las perspectivas externas, financiera y de clientes. En conclusión, se identifican los procesos críticos en los que la

organización debe sobresalir con excelencia para satisfacer los objetivos de los stakeholders, incluyendo la retención de los clientes/usuarios en los segmentos seleccionados y la generación de óptimos rendimientos financieros que incrementen el valor para los accionistas.

- **Perspectiva de aprendizaje y crecimiento (innovación).** La perspectiva desarrolla objetivos e indicadores para impulsar el aprendizaje y el crecimiento de la organización. Los objetivos establecidos en las perspectivas financieras, del cliente y de los procesos internos identifican los aspectos en los cuales la organización ha de ser excelente.

Mapas estratégicos y objetivos. Llamamos mapa estratégico al conjunto de objetivos estratégicos que se conectan a través de relaciones causales. Los mapas estratégicos son el aporte conceptual más importante del Balanced Scorecard.

Siempre los objetivos financieros son la cumbre del mapa estratégico ya que es el fin de toda estrategia "rentabilidad a largo plazo", y razón de ser de las empresas. [4]

Figura 1. Mapa estratégico aplicado a la seguridad de la información.

3. ReSULtAdoS

De todo lo anteriormente desarrollado, nos hemos visto involucrados a un análisis puramente estratégico de una empresa, mas estos objetivos estratégicos determinaran los Objetivos Operacionales que se aplicarán a distintas áreas y/o funciones de una organización.

Estos objetivos estratégicos establecen objetivos operacionales relacionados con la seguridad de la Información Que una vez establecidos, se derivarán en los indicadores, que son los llamados a verificar su cumplimiento, estos indicadores, las metas correspondientes deseadas y las Iniciativas a tomar para lograr el cumplimiento son el resultado que el BSC nos presenta para poder establecer un diálogo con ejecutivos en base a aspectos de la seguridad y que son o llegan a ser de interés para la alta gerencia, demostrando que la seguridad de la información no solo es un problema técnico solamente, sino que establece la participación de las demás áreas de una empresa así como en los niveles gerenciales medios y superiores.

Los objetivos operacionales de seguridad así como los Indicadores de una organización pueden ser establecidas por los objetivos de control de las normas ISO 27001/27002, siendo las Iniciativas de Seguridad los propios controles de estas normas.

Todos los objetivos del BSC no llegaran a ser objetivos de control y/o que todas las Iniciativas llegarán a ser controles de las normas. En realidad el tablero de comando no pretende ser una imagen completa de la seguridad de la información a nivel normativo, sino más bien correlacionar los aspectos más críticos de la seguridad con los procesos de negocios de la empresa.

4. CoNCLUSIoNeS

El artículo presentó un análisis puramente estratégico que deriván en objetivos operacionales que se aplicaran a distintas áreas y/o funciones de una organización. Estos objetivos operacionales están relacionados con la seguridad de la información que una vez establecidos, se derivarán en los indicadores que son los llamados a verificar su cumplimiento. Los objetivos operacionales de seguridad así como los Indicadores de una organización pueden ser establecidas por los Objetivos de Control de las normas ISO 27001/27002, siendo las iniciativas de seguridad los propios controles de estas normas.

PERSPECTIVAS	OBJETIVOS CONTROL	INDICADORES	METAS			INICIATIVAS
			AÑO X	CUMPL. META	NIVEL CUMPL.	
FINANZAS	1. Asegurar operatividad segura	Reducción de pérdidas por vulnerabilidad	30%	11%	37%	Gestión de cambios
	2. Optimizar utilización de recursos	Reducción de gastos por utilización de insumos	35%	17%	49%	Gestión de control de utilización
CLIENTES	1. Aumentar percepción positiva de la seguridad por los "consumidores"	Acceso a dispositivos y controles de seguridad de clientes	50%	32%	64%	Tratamiento de seguimiento de atención a clientes
	2. Entregar sistemas de procesos seguros	Reducción de compensación por responsabilidad civil por daños y perjuicios	90%	45%	50%	Implementación de potenciación de medidas de supervisión
PROCESOS INTERNOS	1. Incrementar entornos compartidos	Habilitación de dispositivos en linea para supervisión de usuarios	40%	20%	50%	Gestionar entornos interconectados
	2. Aumentar la productividad de consumidores internos	Reducción de horas/hombres en atención de incidentes	60%	45%	75%	Control de porductividad
	3. Reducir riesgos de propagación de virus	Reducción de vulnerabilidad de pérdida de información	40%	19%	48%	Verificar operatividad de caracteristicas de sistemas de información
APRENDIZAJE Y CRECIMIENTO	1. Asegurar aprendizaje de errores e incidentes pasados	Atención de incidentes solucionados con base a incidentes anteriores	50%	45%	90%	Plan de seguimiento
	2. Cumplir compromisos asumido de manera intrínseca por los miembros	Nivel de concientización	60%	45%	75%	Plan de concientización

5. dISCUSIóN

La mayoría de las vulnerabilidades en los sistemas informáticos se originan en fallos humanos en lugar de problemas técnicos. La seguridad de la información tiene un efecto significativo para el hombre respecto a su privacidad, la que puede cobrar distintas dimensiones dependiendo de la cultura del mismo. Puesto que estamos hablando de la vulnerabilidad de los sistemas informáticos, debemos de considerar que para mejorar la protección y seguridad, se necesita adoptar una perspectiva socio-técnica y pensar en cómo se usan realmente los sistemas y no solamente en sus características técnicas. Asimismo se debe establecer la participación de las demás áreas de una empresa en sus diferentes niveles gerenciales medios y superiores.

6. ReFeReNCIAS bIbLIoGRáFICAS

[1] Duncan MacKenzie, Kent Sharkey. Aprendiendo Visual Basic.Net en 21 Lecciones Avanzadas; L3

[2] Ordoñez Ruben 2010 ,L1 Cambio, Creatividad e Innovación; Ediciones Granika, 2010

[3] Sommerville Ian, 2006 Edit. Addison Wesley Ingenieria de software Madrid.

[4] Pete Deemer, Gabrielle Banefield, Craig Larman, Bas Vodde The SCRUM Primer; Scrum Training Institute L4

[5] Corral Rodrigo. Scrum y la gestión de la configuración; http://geeks.ms/blogs/rcorral/archive/2009/01/29/exprimiendo-scrum-scrum-y-la-gesti-243-n-de-la-configuraci-243-n-i.aspx U1