Gestión del riesgo en Seguridad Informática

Pinzón, Iraldo
iraldopinzon@hotmail.com
Universidad Piloto de Colombia

***Abstract*--This articlewasperformed in order to provideguidance to companies and especiallythe IT department to managetherisk of informationsecurity. Riskmanagement in thecomputerfieldseeks to sensitizeallcompanies and especiallyColombian, theissue of security and riskmanagementisrelated to themanagement of data, information and assetsinformatic. Riskmanagementiscarriedoutconsidering a phase of analysis, whichseeks to understand: the active, system and data; findingvulnerabilities and threats, withthemainobjectiveriskassessment, findingtheirlikelihood and businessimpact. Once obtainedtherisks, itclassified, youtakeeach of thehazardsfound and controlsimplemented, in order to obtainanacceptablerisk, whyanalyzes and evaluatestheoperation and measuretheeffectiveness in thereductionprocessrisk. Itisimportant to considersecuritypolicies, regulations and institutional rules of the country in allimplementations in order to supportthemission of thebusiness.**

Resumen—Este artículo se realizó con el fin de brindar orientación a las empresas y en especial al área de TI,para gestionar el riesgo de seguridad informática.La gestión de riesgo en el campo informático busca sensibilizar a todas las empresas y, en especial a las colombianas,en el tema de la seguridad y la administración del riesgo está relacionada con el manejo de datos, activos e información.La gestión de riesgos se realiza teniendo en cuenta una fase de análisis, con la que se busca conocer: los activos, el sistema y los datos; encontrando sus vulnerabilidades y amenazas, teniendo como objetivo principal la determinación del riesgo, encontrando su probabilidad e impacto del negocio.Una vez obtenidos se realiza la clasificación, se toma cada uno de los riesgos encontrados y se implementan controles, con el fin de obtener un riesgo aceptable, motivo por el cual se analizay evalúael funcionamiento, así medir la efectividad en el proceso de reducción de riesgo.Es importante tener en cuenta las políticas de seguridad, normatividad del país y reglas institucionales en todas las implementaciones con el fin de apoyar la misión del negocio.

Índice de términos—Gestión del riesgo, vulnerabilidad, amenaza, mitigar, controles, seguridad informática, riesgo residual.

I. INTRODUCCIÓN

La gestión del riesgo informático en una organización tiene como principal objetivo construir bases muy sólidas para alcanzar la misión, proteger la información y todos los activos informáticos.Las empresas en la actualidad realizan procesamiento de información con ayudas tecnológicas para brindar apoyo a la misión del negocio, por lo tanto es importante realizar una buena gestión del riesgo para proteger los activos de información.

Un buen proceso de gestión del riesgo es un ítem fundamental de la seguridad de TI, uno de los pilares debe ser la protección de la organización y su capacidad para apoyar la misión del negocio de forma segura, por eso se pretende concientizar de la existencia y la necesidad de gestionarlos ofreciendo una metodología, por medio de la cual se descubre y planifica el tratamiento del riesgo de una manera adecuada para mantenerlos bajo control, igualmente prepara a las empresas o áreas encargadas de seguridad informática para procesos los de evaluación, auditoria o certificación.

II. OBJETIVOS DE LA GESTIÓN DEL RIESGO

Es importante tener en cuenta hacia donde orienta la gestión del riesgo, a continuación los principales objetivos:

A. Concientizar a todos los responsables de los sistemas informáticos sobre la existencia de los riesgos y su obligación de mitigarlos.

B. Aplicar una metodología adecuada y mantener el ciclo PHVA.

C. Apoyar a laorganización en todos los procesos de evaluación, auditoria o certificación.

D. Ayudar la planeación de controles para mantener los riesgos aceptables.

III. ¿Qué es gestión del riesgo en seguridad informática?

Se entiende por riesgo de seguridad informáticatoda amenaza que explote alguna vulnerabilidad de uno o varios activos y pueda afectar el funcionamiento de un sistema, teniendo en cuenta la probabilidad que ocurra el evento y el impacto en caso de materializarse, en alguna de las tres características principales de la seguridad informática las cuales se describen a continuación.

*Integridad:*Es una condición que garantiza que la información solo puede ser modificada por quien esté autorizado, esta debe ser consistente o coherente.

Confidencialidad: La información solo debe ser visible por quien la requiera y esté autorizado, hace referencia a la privacidad de la información.

*Disponibilidad:*Condición que garantiza que la información pueda ser accedida en cualquier momento que sea requerida. Está directamente relacionada con la continuidad del negocio.

La gestión del riesgo comprende la adecuada administración de los mismos, donde el objetivo principal es minimizarlo obtener un riesgo aceptable esto no es solo una responsabilidad del área de seguridad, muchas áreas la cumplen papeles muy importantes entre ellas tenemos:

- Alta dirección
- Jefe de Informática
- Gerentes
- Directores y oficiales de seguridad
- Profesionales de TI
- Formadores de conciencia de seguridad

Las directrices de seguridad y correcta gestión del riesgo deben empezar desde la alta gerencia, concientizando a toda la empresa de su importancia y el buen papel que desempeña cada uno de los integrantes. Algunas de las áreas en que habitualmente ha incursionado la seguridad se pueden definir así:

- Seguridad física.
- Control de accesos.
- Protección de los datos.
- Seguridad en las redes.

IV. Evaluación del riesgo

La evaluación de riesgos es el proceso general de identificación, análisis y valoración.En la evaluación de riesgo se determina el grado de la amenaza potencial y el riesgo asociado, se debe definir el alcance el resultado de este proceso para ayudar a identificar los controles apropiados, el proceso se realiza como mínimo una vez al año no solo por cumplimiento de normas si no porque es una buena práctica, aportando a la mejora continua, hay que tener en cuenta que esta evaluación debe ser lo suficiente flexible para permitir cambios cuando se justifique por cambio de políticas o de nuevas tecnologías.

El proceso de evaluación es un ciclo el cual se puede resumir en un mapa conceptual (ver Figura 1) en su caracterización del riesgo se propone ejecutar en algunos pasos importantes que se describen a continuación:

Figura 1. Proceso de evaluación del Riesgo [2]

A. *Sistema de caracterización:* En este paso es importante determinar el alcance de la evaluación de los riesgos, debe realizar la identificación de los activos a tener en cuenta: Hardware, software, la información, personas que apoyan y utilizan el sistema de TI, criticidad de los sistemas, sensibilidad de los datos y controles actuales entre otros; para la recopilación de la información se pueden usar métodos como la entrevista, cuestionarios, revisión de documentación o la combinación de estos.

Existe información adicional a tener en cuenta como la política de seguridad de la compañía, practicas generales de la industria y normatividad del país.

B. *Identificación de las amenazas*. Una amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño sobre los elementos de un sistema o afectación de alguno de los activos identificados, se recomienda indagar sobre el historial de este tipo de amenazas, relacionar el listado de amenazas.

C. *Identificación de vulnerabilidades.*Una vulnerabilidad es un defecto o una debilidad de un sistema informático, en su diseño, implementación o controles aplicados, que pueden ser utilizadas para causar algún tipo de daño, estas debilidades pueden aparecer en cualquiera de los activos, esta identificación se realiza por medio de unas pruebas de seguridad y una lista de verificación de acuerdo al sistema o activo evaluado.

D. *Análisis de controles:*El objetico principal es verificar el funcionamiento de los controles actuales y controles previstos, para mitigar o minimizar el riesgo, los controles se aplican a todos los activos identificados pueden ser técnico u operacionales, estos pueden ser preventivo, correctivos e incluso predictivos.

E. *Determinar el riesgo:* Es determinar la probabilidad que una vulnerabilidad potencial pueda afectar el funcionamiento del sistema o afecte alguno de los pilares de la seguridad; Confidencialidad, integridad o disponibilidad. Con el fin de facilitar la determinación del riesgo se clasifica en tres niveles: Alto, medio y bajo.

Alto: Si una observación o hallazgo se evalúa como de alto riesgo, hay una fuerte necesidad de medidas correctivas. Un sistema existente puedecontinúan operando, sino un plan de acción correctiva debe ser puesto en marchatan pronto como sea posible.

Medio: Si una observación está clasificado como de riesgo medio, las acciones correctivas sonnecesaria y un plan debe ser desarrollado para incorporar estas accionesdentro de un período razonable de tiempo.

Bajo: Si una observación es descrita como de bajo riesgo, el sistema debedeterminar si aún se requieren acciones correctivas o decidenaceptar el riesgo.

F. *Análisis de impacto:*Es importante analizar el impacto, estese identifica con la afectación o pérdida de la integridad, disponibilidad o confidencialidad, analizando el impacto en la misión, evaluando la criticidad de un activo o datos y la sensibilidad de los mismos.

El impacto se mide como la explotación de una vulnerabilidad y puede afectar tanto en funcionamiento o económicamente e incluso la imagen de una compañía que en algunos casos es intangible, dependiendo de las consideraciones se puede evaluar de manera cualitativa o cuantitativa, se recomienda el segundo ya que nos proporciona mediciones en cantidades permitiendo hacer un análisis de costo beneficio.

G. *Matriz de riesgo:*Se debe generar la matriz del riesgo a cada uno de los activos, se debe categorizar de una manera organizada con el fin de sacar los reportes, de acuerdo a la probabilidad de que se materialice el riesgo y el impacto que puede ocasionar, no solo económico también de imagen, prestigio perdida de clientela entre otros, la matriz se puede realizan de manera cualitativa o cuantitativa, de acuerdo a la metodología Margerit recomienda la segunda opción por el manejo de

cantidades y de fácil comprensión y ayuda a la hora de tomar decisiones por parte de la gerencia.

*H. Recomendaciones de Control:*El objetivo principal es mitigar o eliminar los riesgos identificados, ofreciendo recomendaciones y llevándolos a un nivel aceptable, es de notar que no todos los controles recomendados son de obligatorio cumplimiento debe existir la evaluación costo beneficio.

I. Documentación: Una vez que la evaluación de riesgos se ha completado (amenaza a los recursos y vulnerabilidades identificadas, riesgosevaluados, y los controles recomendados), todos los resultados deben ser muy bien documentados, a va ser el apoyo para la alta dirección para la toma de decisiones.

V. MITIGACIÓN DEL RIESGO

En este proceso se prioriza, evalúa la aplicación de controles de reducción de riesgos recomendados por el proceso de evaluación de riesgos. El tratamiento de los riesgos es un ciclo comprendido por cuatro pasos (PHVA), que consiste en planear, hacer, verificar y actuar. Para mitigar el riego existen cinco formas las cuales se relacionan a continuación.

1) *Asumir el riesgo:*Se entiendo como la aceptación del riesgo potencial y se continúa operando el sistema de TI.

2) *Evitar el Riesgo:* Se evita eliminando la causa del riesgo, ejemplo dejar de utilizar un sistema porque hay un riego identificado.

*3) Reducir el Riesgo:*La forma de reducir un riesgo es con la implementación de controles, minimizando el impacto o la probabilidad.

*4) Planificacióndel Riesgo:*La gestión del riesgo se realiza mediante el desarrollo de un plan de mitigación de riesgos que prioriza,implementa y mantiene controles.

5) Transferir el Riesgo: El riesgo se transfiere por el uso de opciones para compensar una pérdida, una de las más relevantes es la compra de un seguro.

A. Estrategia para aplicar controles

A cada uno de los activos se debe categorizar en la matriz de una manera organizada para sacar los reportes.Al tratar los riesgos se deben iniciar a mitigar los más importantes de acuerdo a la evaluación, le deben dar prioridad a los de mayor impacto los cuales requieren de acción correctica de inmediato, durante este proceso se estudia la viabilidad y la eficacia seleccionando el control más adecuado. Con el fin de ayudar a la gerencia en la toma de decisiones se lleva a cabo un análisis de costo beneficio. Una vez seleccionado los controles se asignan las personas responsables para ejecutar dicho control, debe ser personal idóneo con las capacidades de ejecutarlo.

Se desarrolla un plan de implementación detallado describiendo los riesgos, los controles seleccionados, la priorización, programación con fechas y recursos.
Es recomendable usar al anexo A de la Norma ISO 27001 donde se describen 133 controles y deberían ser los mínimos que sedeberán aplicar, o justificar los que se crean que no aplican, pero esto no da por completa la aplicación de la norma dentro del proceso de análisis de riesgos aparecen aspectos que quedan sin cubrir por algún tipo decontrol. Por lo tanto, si a través de la evaluación de riesgos se determina que es necesaria la creaciónde nuevos controles, la implantación del SGSI impondrá la inclusión de los mismos, sino seguramenteel ciclo no estará cerrado y presentará huecos claramente identificables.

B. Riesgos residuales

Es llamado riesgo residual aquel que permanece después de la implementación de los controles, cada compañía puede definir el alcance de la reducción del riesgo por medio de los controles con la reducción de la amenaza o minimizando el impacto.

Con la implementación de nuevos controles o mejorando los actuales se puede bajar los riesgos residuales en caso de no ser un riesgo aceptable

VI. Conclusiones

La seguridad informática no solo es una responsabilidad del área de tecnología, debe fluir desde la gerencia hacia todos los procesos del negocio.

La gestión del riesgo es un proceso cíclico que nunca termina.

El riesgo es inherente a todos los recursos informáticos, realizando una buena gestión es la única forma de medir y mitigar.

REFERENCIAS

[1] ISO/IEC 27001/2005, Information technology - Security techniques - Information security management systems – Requirements

[2] Juan Carlos Reyes, Proceso de evaluacióndelriesgo. Recuperadode: http://www.acis.org.co/fileadmin/Base_de_Conocimiento/VIII_JornadaSeguridad/17-ElAnalisisRiesgosBaseSistemaGestionSeguridadInformacionCasoMagerit.pdf

[3] NIST Publicación 800-12, An introduction to computer Security Risk management guide for information Technology System, Manual de la NIST.

[4] NIST Publicación 800-30 Risk management guide for information Technology System, Recomendaciones del institutonacional de estandares y tecnología.

Autor
Iraldo Pinzón Parada
Ingeniero Electrónico (ECCI)
Especialista en Seguridad Informática (Universidad Piloto de Colombia)