Publicaciones en Ciencias y Tecnología. Vol 4, 2010 N^0 2, pp.33–37, ISSN:1856-8890,Dep.Legal pp200702LA2730

El Análisis de Riesgo en la seguridad de la información

[*]Manuel Mujica, [**]Yenny Alvarez

Recibido: 21 de Marzo 2009, Aceptado:10 de Julio 2009

Resumen

El propósito de este artículo consiste en ofrecer un conjunto de reflexiones conceptuales sobre la seguridad de la información y específicamente sobre el análisis de riesgos y su importancia en las organizaciones. Por lo que, el recurso más importante y afectado en toda organización pública y privada, grande o pequeña, es la información, por lo cual toda organización debe estar alerta e implementar sistemas de seguridad basados en un análisis de riesgo para evitar o mitigar las consecuencias no deseadas. El análisis de riesgo es un proceso que permite identificar las amenazas y vulnerabilidades de una organización con el objetivo de generar controles que minimicen los efectos de los riesgos, el cual implica determinar qué o cuáles activos proteger, de qué o de quién hay que protegerlos y cómo hacerlo.
El análisis de riesgos debe realizarse de forma continua dado que es necesario evaluar periódicamente si los riesgos identificados y la exposición a los mismos se mantienen vigentes; y es de vital importancia porque permite identificar los impactos futuros en la estructura de riesgos de la organización. Internacionalmente existe una norma, ISO 27005:2008 publicada en junio del año 2008, que establece criterios sobre la gestión del riesgo de la seguridad de la información y proporciona un marco normalizado que sirve de guía para definir metodologías propias para cada organización, esta norma sirve de apoyo a la norma ISO 27001:2005 que proporciona un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI).

Palabras clave: Seguridad de información, análisis de riesgos, vulnerabilidades, amenazas.

Abstract

The purpose of this paper is to provide a set of conceptual thinking on information security and specifically on risk analysis and its importance in organizations. So, the most important and affected resource in any public or private, large or small organization, is the information collected, processed, stored and made available to users on computers and transmitted over networks, so that any organization must be alert and learn to implement security systems based on a risk analysis to prevent or mitigate the unintended consequences, because the risk is measurable. Risk analysis is a process that identifies threats and vulnerabilities of an organization with the goal of creating controls that mitigate or minimize the effects of risks, that involves to determine which assets to protect, from what or from who have to be protected and how to do it. The risk analysis should be made continuously since it is necessary to assess regularly whether the identified risks and exposure to those calculated earlier are still valid, and it is of vital importance because it can allow to identify future impacts on the risk structure of the organization. Internationally there is a standard, ISO 27005:2008 published in June of 2008, which establishes criteria for risk management of information security and provides a standardized framework that provides guidance in defining its own methodologies for each organization, this rule serves support to ISO 27001:2005 which provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a management system for information security (ISMS).

Keywords: Information Security, risk analysis, vulnerabilities and threats.

[*] *Departamento de Redes UNEXPO,Universidad Nacional Experimental Politécnica "Antonio José de Sucre", Barquisimeto, Lara 3001*
[**] *UPEL-IPB, Barquisimeto, Venezuela*

Introducción

El siguiente artículo proporciona información inherente al tema de la seguridad de la información, específicamente en el área de análisis de riesgos en los Sistemas de Gestión de Seguridad de la Información (SGSI[1]) que son manejados por las diferentes organizaciones, con el fin de asegurar el activo fundamental de sus sistemas, como lo es la información, para reducir al mínimo las vulnerabilidades y las pérdidas para permitir la mejora continua en la toma de decisiones y la mejora del rendimiento.

Las organizaciones hoy día, con la tecnología y complejidad en el manejo de la información, donde posiblemente enfrentan diferentes amenazas que probablemente explotan sus vulnerabilidades, la confidencialidad, integridad, disponibilidad y el no repudio de la información en la empresa, es primordial para el aumento de su competitividad; por lo que están obligadas, si desean continuar operando, a establecer SGSI que permitan identificar sus activos vitales de información, e implantar los controles pertinentes. Por lo tanto, es importante establecer un análisis de riesgo que permita a la organización identificar las amenazas a los que se encuentran expuestos sus activos, para estimar la frecuencia de materialización y valorar el impacto que tendría en la organización.

Aunado a ello, es fundamental conocer que el análisis de riesgo es crucial para el desarrollo y operación de un sistema de gestión de seguridad de información, ya que justo en esta etapa es donde la organización debe construir su "modelo de seguridad", que no es más que la representación de todos sus activos y sus dependencias jerárquicas, así como, todo aquello que pudiera ocurrir (amenazas) y que tuviera un impacto en la organización.

Es importante considerar el análisis de riesgo como el núcleo de toda organización en cuanto a la seguridad de la información, la cual permite establecer un nivel adecuado de seguridad, que se aspira lograr en la protección de los activos, de qué o quién protegerlos y cómo hacerlo, teniendo como guía la normativa International Standards Organization (ISO [2] 27005:2008) que establece criterios sobre la gestión del riesgo proporcionando un marco normalizado para definir metodologías propias de análisis de riesgo, y la normativa ISO 27001:2005 que proporciona un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI.

De esta manera como contribución se ofrece el planteamiento de diferentes autores sobre la temática, que consiste en definiciones, objetivos, beneficios, características, y normativa del análisis de riesgo.

Desarrollo

Análisis de Riesgo

La alta dependencia de los sistemas de información trae cada vez más, preocupación en las organizaciones debido a los riesgos que generan la complejidad de los sistemas, posibles accidentes, errores o ataques, y la constante evolución en un entorno cambiante; por lo que la ejecución de estos riesgos puede afectar la continuidad de los servicios (internos y externos), la protección de la información en general, así como la validez y eficacia de los procesos que se basan en transacciones electrónicas; por lo tanto, es necesario aplicar un análisis de riesgo para crear las políticas de seguridad basadas en una metodología para controlar los elementos que permiten reducir la exposición a los riesgos protegiendo los activos de una organización.

Según la norma ISO/IEC 17799:2005 [1], se define Riesgo, como "la combinación de la probabilidad de un evento y sus consecuencias" (pp. 14).

En concordancia con lo anterior, Dorta [2], define riesgo como "posibilidad de sufrir una pérdida o no". De las definiciones anteriores, se infiere que riesgo es toda probabilidad de que una amenaza ocurra

[1]Sistema de gestión de seguridad (SGSI), esa parte del sistema gerencial, basada en un enfoque de riesgo comercial, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información ISO/IEC27001:2005

[2]International Standarization Organization (ISO), es una organización internacional no gubernamental, compuesta por representantes de los organissmos de normalización nacionales, que producen normas internacionales industriales y comerciales . http:/www.iso.org

durante un período definido ocasionando impactos económicos, materiales, entre otros.

Por otro lado, la norma ISO/IEC 17799:2005 [1], define análisis de riesgo como el "uso sistemático de la información para identificar las fuentes y calcular el riesgo" (pp. 14), mientras que la norma ISO/IEC Guía 73:2002 lo define como el "proceso general de análisis del riesgo y la evaluación del riesgo".

En este sentido, el análisis de riesgo es un elemento fundamental para determinar las medidas de seguridad de un activo de información o sistema, ya que identifica los riesgos y estima el impacto potencial que supone su propia destrucción o la pérdida de la información o mayor aun una afectación en cuanto a la disponibilidad, confidencialidad, integridad y no repudio de la información, esto en concordancia con lo planteado por Royal [3], quien expresa que:

No todas las exposiciones necesitan ser o deberían ser controladas, el control total no es un costo eficaz y generalmente es muy ineficiente, sin embargo, si el diseñador no tiene idea de que la exposición presenta el mayor riesgo en términos de frecuencia de ocurrencia y costo, no tiene otra alternativa que controlar cada exposición (pp. 83).

Por otro lado, se deben crear registros de los impactos potenciales que pueden derivarse de las amenazas de los activos, por lo que se debe establecer un vínculo entre los activos, las amenazas y lo que es importante para la organización (objetivos de negocio), que proporcionan una base sobre la que analizar los riesgos.

En el mismo orden de ideas, Martínez [4], expone que el análisis de riesgos "es perfectible, por lo que siempre tendrá ventajas, desventajas y diferentes objetivos de acuerdo al entorno y punto de vista de la institución, empresa o comunidad en la cual se aplique" (pp. 44).

De las definiciones anteriores se deduce que el análisis de riesgo es una actividad o proceso que tiene por resultado consolidar las vulnerabilidades para identificar los pasos a seguir para su corrección, identificar las amenazas que pueden explotar esas vulnerabilidades para mitigarlos, identificar los impactos potenciales que pudieran tener los incidentes y así aprovechar las vulnerabilidades encontradas, y determinar las recomendaciones para corregir o reducir las amenazas, por lo tanto implica determinar qué se necesita proteger (cuáles activos), de qué hay que protegerlos y cómo hacerlo. Así como también se debe considerar la relación costo- beneficio, permitiendo que las medidas de seguridad sean evaluadas con relación a su aplicabilidad y beneficio que se agregará al negocio de la organización, para orientar la implementación de la política de seguridad solo en las situaciones en que la relacióncosto-beneficio lo justifique.

Objetivos del análisis de riesgo

Royal [3], expresa que el proceso de análisis de riesgo deber ser efectuado en cualquier momento y cumplir con los siguientes objetivos (pp. 83): Identificar, evaluar, y manejar los riesgos de seguridad; debe estimar la exposición de un recurso a una amenaza específica; determinar cual combinación de medidas de seguridad proporcionará un nivel de seguridad razonable a un costo aceptable; tomar mejores decisiones en seguridad informática y enfocar recursos y esfuerzos en la protección de los activos de información.

Beneficios del análisis de riesgo

El realizar un análisis de riesgos en las organizaciones trae consigo una serie de beneficios que se ven reflejados en el costo-beneficio de la misma, éstos varían de organización en organización y van de acuerdo a las políticas de cada una, pero en líneas generales se resumen de la siguiente manera:

- Asegurar la continuidad operacional de la empresa
- Saber manejar las amenazas y riesgos críticos
- Mantener una estrategia de protección y de reducción de riesgos
- Justificar una mejora continua de la seguridad informática.

- Costos de seguridad justificados
- Permitir que la seguridad se convierta en parte de la cultura de la organización
- Apoyar la comunicación y facilitar la toma de decisiones, certeza económica/financiera.

Limitantes del análisis de riesgo

Según Martínez [4], el proceso de análisis de riesgos presenta una serie de limitantes como son: complicaciones para concienciar objetivos, ligereza en la aplicación de los análisis en el campo, escasa difusión, poca concienciación, gran diversidad de métodos de análisis, inversión de tiempo y recursos a las actividades, las soluciones al problema de seguridad no son instantáneas, y una sola metodología no es aplicable a todos los ambientes.

Fases del análisis de riesgo

El proceso de análisis de riesgos según lo expresa Martínez [4], debe cumplir con tres etapas:

Fase 1: **construir perfiles de amenazas basados en activos**: activos críticos, requerimientos de seguridad para los activos críticos, amenazas a los activos críticos, prácticas de seguridad actuales, vulnerabilidades actuales de la organización.

Fase 2: **identificar vulnerabilidades de infraestructura**: componentes clave, vulnerabilidades actuales de la tecnología.

Fase 3: **desarrollar planes y estrategias de seguridad**: riesgos de los activos críticos, medidas de riesgo, estrategias de protección, planes de mitigación de riesgos.

Normativas que rigen el análisis de riesgos

ISO/IEC 27001:2005 [5] (Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos). Aprobado y publicado como estándar internacional en Octubre del 2005 por Específica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de seguridad de información (SGSI).

ISO/IEC 27005:2008 [6] Norma que proporciona directrices para la gestión del riesgo de seguridad de la información en una organización, sin embargo, esta norma no proporciona ninguna metodología específica para el análisis y la gestión del riesgo de la seguridad de la información.

ISO/IEC 27002:2005 [1] (Antigua ISO/IEC 17799: Tecnología de la información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información)

Conclusiones

Actualmente con la creciente innovación tecnológica que llega a las organizaciones, es de vital importancia tomar conciencia en cuanto a la existencia de los riesgos que amenazan los activos y que tales riesgos se pueden medir, para lograr mantener un nivel de seguridad aceptable en la organización; empezando por las cosas más simples, que consumen menos recursos, pero que atacan muchísimos riesgos; debido a la existencia de numerosas empresas que invierten más en una seguridad perimetral para que no roben información desde afuera sin tomar en cuenta la protección interna.

Es por ello que toda organización debe estar en alerta y saber implementar sistemas de seguridad basados en un análisis de riesgos para identificar las amenazas a la que se encuentran expuestos los activos, estimar la frecuencia de ocurrencia de tales amenazas y valorar el impacto que tendría en la organización la ejecución de dichas amenazas, minimizando los riesgos; y en contraparte, el análisis de riesgo es un proceso analítico donde intervienen un gran número de variables por lo que una sola metodología no es

aplicable a todas las organizaciones, es por esto que es recomendable apoyarse en las normas ISO/IEC 27005:2008 [6], ISO/IEC 27001:2005 [5], ISO/IEC Guía 73:2002 [8] que sirven de guía para que cada organización arme su propia metodología de análisis de riesgos y finalmente implanten su propio sistema de gestión de seguridad de información.

Referencias

[1] ISO/IEC 17799:2005 *Information technology - Security techniques - Code of practice for information security management.*

[2] Dorta, J. (2004) *La evaluación de los riesgos como componente básico del sistema de Control Interno*. Espaũa.

[3] Royal, F. (1988). *Seguridad en los sistemas informáticos*. Madrid, Espaũa: Díaz de Santos, S.A.

[4] Martínez, L. (2002). *Introducción al análisis de riesgos*. Distrito Federal, México: Limusa, S.A

[5] ISO/IEC 27001:2005. *Information technology - Security techniques - Information security management systems - Requirements.*

[6] ISO/IEC 27005:2008.

[7] Information technology – Security techniques – Information security risk management.

[8] ISO/IEC Guía 73:2002. *Risk management – Vocabulary – Guidelines for use in standards*