Modelo de Sistema de Gestión de Seguridad para la Red de Datos de una Institución del Estado Peruano

Model of Security Management System for Data Network of a Peruvian State Institution

José Steve Burga Guardales[1]

Facultad de Ingeniería Electrónica y Eléctrica, Universidad Nacional Mayor de San Marcos, Lima, Perú

***Resumen*- Las redes de datos, los sistemas de información y comunicación son importantes activos para cualquier organización por ser el soporte tecnológico de la información en el mundo digital. El presente artículo brinda los lineamientos para un modelo de un sistema de gestión de seguridad para redes de datos, cuyos resultados permitan determinar la cantidad de riesgos por cada servicio informático a nivel de las capas 3 y 4 del modelo OSI en una institución del Estado Peruano; gestionado las amenazas, vulnerabilidades y riesgos a los que puede estar expuesto la red de datos de la organización en estudio.**

***Abstract*- Data networks, information systems and communication are important assets for any organization as a technological support of information in the digital world. This article provides guidelines for a model of security management system for data networks. The results allow determining the amount of risks for each informatic service related with the 3 and 4 layers of the OSI Model of a Peruvian State institution; managing the threats, vulnerabilities and risks that the data network of the organization under study may be exposed.**

***Palabras Claves*- Red de datos, amenazas, vulnerabilidades, riesgos.**

***Key Words*- Data network, threats, vulnerabilities, risks.**

I. INTRODUCCIÓN

En los últimos años, se ha producido una masificación del uso de las Tecnologías de la Información y Comunicaciones - TIC, utilizados tanto a nivel profesional como personal, usando las redes de datos e Internet, al cual accedemos por diversos dispositivos tales como computadoras personales, notebooks, tablets, dispositivos móviles, etc.

Sin embargo, desde que las instituciones empezaron a utilizar redes de datos y sistemas informáticos como el soporte tecnológico para realizar sus distintos procesos de negocio de manera automatizada, han enfrentado diversas amenazas que atentaron contra los mismos. En consecuencia, las organizaciones tomaron estrictas medidas de seguridad a fin de mantener la continuidad de la operación de sus servicios informáticos y de la misma organización.

De acuerdo con William Stallings [1], un cambio relevante que ha afectado a la seguridad de la información es la introducción de sistemas distribuidos y la utilización de redes y servicios de comunicación para transportar datos entre terminales de usuario y computadores y de computador a computador.

A. Marco Teórico del estudio.

1. Sistema de Gestión

Un sistema de gestión es una estructura probada para la gestión y mejora continua de las políticas, los procedimientos y procesos de la organización. Ayuda a lograr los objetivos de la organización mediante una serie de estrategias, que incluyen la optimización de procesos, el enfoque centrado en la gestión y el pensamiento disciplinado [2].

2. Definición de Seguridad

El término seguridad proviene del latín *securitas*, que significa '*certeza*' o '*conocimiento claro y seguro de algo*'. Cuando se utiliza esta palabra en una locución adjetiva ('*de seguridad*') significa que se está refiriendo a un dispositivo o mecanismo diseñado para evitar que éste falle, garantizando su buen funcionamiento [3].

3. Seguridad de la Información

La seguridad de la información protege a ésta de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la

[1] José Steve Burga Guardales, e-mail: jose.burga.g@hotmail.com
Recibido: Marzo 2014 / Aceptado: Mayo 2014.

organización y maximizar el retorno de las inversiones y las oportunidades de negocio [4].

Los principios básicos en la seguridad de la información son [5]:

- **Confidencialidad** - sólo ciertas personas pueden tener acceso a determinada información en la empresa.
- **Integridad** - sólo personas autorizadas pueden cambiar o añadir datos a información específica.
- **Disponibilidad** - la información está disponible sólo para aquellos que poseen cierta autoridad, en momentos en que se la necesite.

Asimismo, las principales definiciones en el tratamiento de la información son:

- **Activo de información:** Es todo aquello que tiene valor para la organización y por lo tanto requiere protección: documentos en papel, software, dispositivos físicos, servicios, imagen institucional, etc.
- **Amenaza:** Es la causa potencial de un incidente no deseado que puede resultar en daño al sistema, a la organización o a sus activos, la cual puede ser accidental o intencional. Los activos están sujetos a muchos tipos de amenazas que explotan sus vulnerabilidades, tales como: tecnológicas, humanas, desastres naturales, etc.
- **Vulnerabilidad** - Es una debilidad o ausencia de control. Por sí sola no causa daños, pero si no es administrada, permitirá que una amenaza se concrete.
- **Impacto** - Es el cambio adverso en el nivel de los objetivos alcanzados por la organización, que pueden ser: oportunidades perdidas, costos financieros, imagen y reputación, etc. [6].
- **Riesgo** - Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información y que tenga un impacto a la organización.

4. Estándares en seguridad de la información

Los principales estándares en la gestión de seguridad de la información, los cuales son la base para el desarrollo de la metodología planteada en el Capítulo II, son la serie de normas ISO/IEC 27000, que proporcionan un marco de gestión de la seguridad de la información la cual es aplicable a todos los tipos y tamaños de organizaciones como por ejemplo: empresas comerciales, instituciones del gobierno u organizaciones sin fines de lucro. [7].

5. Seguridad en Redes de Datos

De acuerdo con las buenas prácticas de gobierno de TI - COBIT [8], se define a la seguridad de la red de datos como el uso de técnicas de seguridad y procedimientos de administración asociados (utilizando firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes. Asimismo, de acuerdo a la NTP ISO/IEC 17799, se indica que la gestión de la seguridad en redes asegura la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo.

6. Normas Técnicas Peruanas

En el Perú, se cuentan con un conjunto de Normas Técnicas Peruanas (NTP por sus siglas) referente a la seguridad de la información basadas en las normas internacionales ISO, siendo la principal norma técnica en el ámbito de la seguridad de la información la NTP ISO/IEC 27001:2008. EDI. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos.

Esta norma tiene como objetivo el ofrecer un modelo para establecer, implementar, operar, mantener y mejorar un efectivo sistema de gestión de seguridad de la información, siendo de uso obligatorio en todas las entidades del estado integrantes del Sistema Nacional de Informática, aprobado mediante la Resolución Ministerial 129-2012-PCM.

B. Planteamiento del Problema

Como parte de la aplicación de los principios de gobierno electrónico, las instituciones del Estado Peruano cuentan con diversos servicios informáticos que brindan a los ciudadanos, permitiendo aumentar la eficacia y eficiencia de la gestión pública, e incrementar sustantivamente la transparencia del sector al que pertenecen.

Debido a que todos los servicios informáticos de una institución tienen como base la utilización de una red de datos, que permite brindar la debida atención al ciudadano, se requiere poder gestionar las vulnerabilidades, amenazas a las que puede estar expuesta, así como sus impactos y riesgos sobre los servicios informáticos de materializarse una amenaza.

C. Objetivo del estudio

El objetivo del presente estudio es brindar los lineamientos para un modelo de un sistema de gestión de seguridad para redes de datos, que coadyuve a mantener la continuidad de operación de los principales servicios informáticos en una institución del Estado Peruano.

D. Justificación

Las instituciones del sector estatal presentan la misma necesidad de poder mantener la operatividad de la red institucional, tanto como las empresas privadas.

Teniendo en consideración que la red de datos de toda organización brinda el soporte tecnológico para el funcionamiento de los diversos servicios informáticos de la organización, se hace necesaria una metodología de seguridad para la red de datos que permita el establecimiento de objetivos de control para la gestión de riesgos.

II. METODOLOGÍA

El alcance del estudio está centrado en el análisis de los activos de información correspondientes a servicios informáticos que son considerados como críticos, así como los componentes de la red de datos que permiten su operación, en una institución del Estado Peruano.

Se ha considerado cuatro etapas en el diseño del modelo de gestión, el cual se muestra en la Fig. 1.

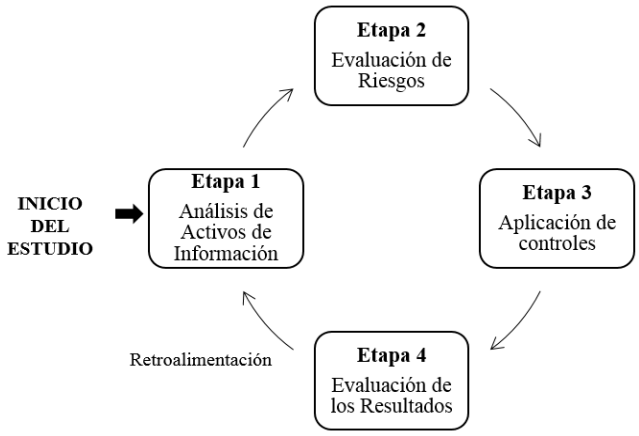

Fig. 1. Etapas del estudio.

El análisis de riesgos se realiza considerando las amenazas y vulnerabilidades a las que pueden estar expuestos los activos de información seleccionados respecto a las capas 3 y 4 del modelo OSI, así como sus impactos a la institución seleccionada.

A. Etapa 1. Análisis de activos de información

1. Activos de información

Como se ha mencionado anteriormente, los activos de información, objetos del estudio, son los referidos a los servicios críticos informáticos que utiliza la institución en su labor diaria en el proceso de atención al ciudadano, por lo que se debe de realizar un inventario de servicios informáticos y determinar cuáles son los considerados como críticos.

En tal sentido, es necesario asignar un valor para los parámetros de confidencialidad, integridad y disponibilidad para cada servicio seleccionado asignándole un valor de la Tabla I, de acuerdo al impacto que tienen para la organización ante una pérdida o falla de los mismos.

TABLA I

VALORES DE TASACIÓN PARA LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

Valor	Descripción
5	Impacto Irreversible
4	Impacto grave
3	Impacto considerable
2	Impacto parcial
1	No impacta

La tasación a cada servicio informático se calculará usando la ecuación (1) donde *Vc*, *Vi* y *Vd* son los valores asignado para la confidencialidad, integridad y disponibilidad respectivamente.

$$Ts = \frac{Vc + Vi + Vd}{3} \quad (1)$$

Debido a que los posibles valores se encontrarán en el rango de 1 al 5, se ha establecido 3 segmentos posibles para establecer el nivel del resultado obtenido, el cual se muestra en la Tabla II.

TABLA II

NIVELES PARA RESULTADOS OBTENIDOS

Segmentos posibles del valor obtenido	Nivel
3.68 – 5.00	Alto
2.34 – 3.67	Medio
1.00 – 2.33	Bajo

Serán considerados como servicios críticos informáticos a aquellos que hayan obtenido el nivel "*alto*" en la tasación.

2. Información de infraestructura de red

El objetivo en esta parte del análisis es obtener información de cómo está constituida la infraestructura tecnológica de la institución en estudio.

En tal sentido, dependiendo del tamaño de la organización podremos encontrar:

- Un centro de datos para los servidores institucionales. Aquí se encontrarán los servicios informáticos a analizar.
- Red LAN, MAN y WAN
- Salida a Internet

Se debe determinar cuáles son los activos tecnológicos a nivel de la red de datos que se requieren para que, tanto un usuario interno de la institución como un ciudadano, pueda hacer uso del servicio informático catalogado como crítico.

3. Amenazas y vulnerabilidades

Se requiere determinar las principales amenazas a los que pueden ser vulnerables los servicios informáticos y cuya causa tenga origen en alguna falla de un elemento de la infraestructura tecnológica de la institución desde el punto de vista de la capa de red.

Asimismo, es necesario conocer los controles existentes de tipo preventivo, detectivo y reactivo, que serán considerados como los niveles de capacidad que tiene el servicio informático para hacer frente a las amenazas, y que permitirá poder determinar el nivel de vulnerabilidad en el que se encuentra el servicio. De acuerdo a la información obtenida, se realiza una valorización de los niveles de capacidad conforme lo mostrado en la Tabla III

TABLA III
NIVELES DE CAPACIDAD DE LOS SERVICIOS INFORMÁTICOS

Capacidad del activo	**Valor**
Ninguno: Control no implantado	5
Incompleto: Control implantado parcialmente que no logra conseguir su objetivo completamente	4
Realizado: Control implantado que logra cumplir el objetivo requerido	3
Gestionado: Control que se encuentra implantado y documentado, además de ser gestionado.	2
Optimizado: El control establecido como estándar por la institución y satisface totalmente los requerimientos con eficiencia y eficacia.	1

La vulnerabilidad, para cada amenaza determinada, será considerada como la debilidad o ausencia de control que presente el servicio informático, pudiendo establecer su nivel de vulnerabilidad como el promedio de su capacidad detectiva (*Cd*), capacidad preventiva (*Cp*) y capacidad correctiva (*Cc*) mediante la ecuación (2).

$$Nv = \frac{Cd + Cp + Cc}{3} \qquad (2)$$

B. Etapa 2. Evaluación de riesgos

1. Análisis de la probabilidad de amenazas

Se debe determinar la probabilidad de ocurrencia de una amenaza detectada de acuerdo a la frecuencia con la que ésta pueda presentarse, para lo cual se establecerá la escala mostrada en la Tabla IV

TABLA IV
FRECUENCIA DE UNA AMENAZA

Valor	**Nivel**	**Frecuencia**
5	Muy alto	Una vez al día
4	Alto	Una vez a la semana
3	Medio	Una vez al mes
2	Bajo	Una vez cada 6 meses
1	Muy bajo	Una vez al año o más

Con los datos anteriores, para un servicio informático, la probabilidad de ocurrencia de una amenaza puede ser determinada como la media geométrica del nivel de vulnerabilidad Nv y valor asignado para la frecuencia de la amenaza Fa, tal y como se indica en la ecuación (3).

$$Pa = \sqrt{Nv \times Fa} \qquad (3)$$

De acuerdo a los valores obtenidos es posible categorizar el nivel de la probabilidad de ocurrencia del riesgo utilizando la misma escala mostrada en la Tabla II

2. Evaluación de impacto

Se evalúa los tipos de impactos de materializarse una amenaza para cada servicio informático, de acuerdo a la naturaleza de la organización. Para una institución del Estado Peruano puede considerarse los siguientes aspectos:

- Impacto técnico de la amenaza.
- Impacto en la atención al ciudadano.
- Impacto a la imagen institucional.

Para cada uno de estos tipos de impacto se ha de valorizar en niveles de acuerdo a la Tabla V.

TABLA V
NIVELES DE IMPACTO A CONSIDERAR

Valor	**Impacto técnico**	**Impacto en la atención al ciudadano / imagen institucional**
5	Total	Muy alto
4	A nivel externo (accesible de Internet)	Alto
3	A nivel de la red interna	Medio
2	Local (una oficina)	Bajo
1	Individual	Muy bajo

El nivel de impacto a la institución de una amenaza estará dado por la ecuación (4) en donde *It*, *Ic* e *Ii* son los impactos técnicos, en la atención al ciudadano y a la imagen institucional respectivamente.

$$Ni = \frac{It + Ic + Ii}{3} \quad (4)$$

3. Determinación del riesgo

Finalmente, es necesario conocer en qué estado de riesgo se encuentra el servicio informático en relación al impacto que pueda generar una amenaza de materializarse, por lo que se establece el valor del riesgo como la media geométrica de la probabilidad de ocurrencia de una amenaza Pa y el nivel de impacto Ni, tal y como se indica en la ecuación (5).

$$Re = \sqrt{Pa \times Ni} \quad (5)$$

Dependiendo del resultado obtenido, el estado en el que se encuentra el servicio informático se clasificará de acuerdo a la Tabla VI

TABLA VI
CLASIFICACIÓN DEL ESTADO DEL SERVICIO INFORMÁTICO

Segmentos posibles para el valor del riesgo efectivo	Estado
3.68 – 5.00	Crítico
2.34 – 3.67	Moderado
1.00 – 2.33	Aceptado

C. Etapa 3. Aplicación de controles

En primer lugar, los tipos de controles a considerar son los siguientes:

- **Aceptar**: no hacer nada, aceptar la amenaza tal como se presenta. No se aplican controles.
- **Reducir**: minimizar la posibilidad de materializarse una amenaza.
- **Evitar**: reducir a su mínima expresión la posibilidad de materializarse una amenaza.
- **Transferir**: a un tercero el tratamiento de la amenaza.

1. Requerimientos de control

De acuerdo a los resultados obtenidos en la evaluación del riesgo efectivo para los servicios informáticos, se deberá de atender principalmente aquellos que se encuentren en un nivel crítico. Los principales aspectos a contemplar son los siguientes:

- Controles para el monitoreo de la red, para determinar la disponibilidad de los equipos de comunicaciones y servicios informáticos, navegación a internet y consumo de ancho de banda
- Controles para la seguridad de la red, con políticas de firewall y detección y protección contra intrusos a nivel de red

2. Elección de los controles

Se debe de realizar la elección de los controles que permitan minimizar o reducir a su mínima expresión las amenazas logrando disminuir el valor del riesgo efectivo a los servicios informáticos.

En esta parte del análisis, la elección de controles para el cubrimiento de riesgos que requiera algún tipo de adquisición por parte de la entidad, debe tener en consideración el tiempo para realizar los procesos de adquisición de bienes, licencias y renovaciones, así como los trámites administrativos que contempla la legislación vigente de acuerdo a la Ley de Contrataciones y Adquisiciones Estado y a la Ley No 28612 "*Ley que norma el uso, adquisición y adecuación del software en la administración pública*"

3. Aplicación de los controles

Los controles seleccionados han de ser aplicados de acuerdo a las amenazas determinadas, indicando qué tipo de control será y qué capacidad será reforzada: capacidad preventiva, detectiva o reactiva.

D. Etapa 4. Evaluación de resultados

La evaluación de resultados consiste en realizar un análisis final luego de haber establecido los controles anteriormente seleccionados, realizando el mismo procedimiento indicado en las etapas 1, 2 y 3, y determinar el resultado final del riesgo efectivo a los servicios institucionales, de modo tal de determinar si en efecto se ha cumplido con los objetivos de control planteados.

Los nuevos controles aplicados durante el presente proceso de análisis deberán ser documentados, formando parte del sistema de gestión de seguridad de la red de datos, teniéndose éstos podrán ser mejorados en el tiempo hasta lograr la optimización de los mismos, de modo tal que satisfagan completamente las necesidades de la organización con eficiencia y eficacia.

III. RESULTADOS

La investigación muestra los lineamientos para un sistema de gestión de seguridad para la red de datos.

La metodología descrita permite determinar el estado de riesgo en el que se encuentran cada servicio informático analizado desde la perspectiva de la red de datos, pudiendo consolidar y agrupar el número de riesgos críticos, moderados y aceptados obtenidos durante el proceso de análisis, lo que brinda a gerentes

de TI y a la alta dirección poder tomar las decisiones que correspondan frente a los riesgos que puedan presentarse a los servicios críticos que utiliza la institución en la atención diaria a los ciudadanos.

IV. CONCLUSIONES

El presente estudio se muestra como una propuesta factible que permite establecer un modelo de un sistema de gestión como un marco de trabajo para administrar sistemáticamente la seguridad de la red de datos de una organización del Estado Peruano.

La aplicación de controles ha de reducir el número de riesgos asociados a los activos de información de la red de datos de la organización en estudio, estableciendo una línea base de la gestión de sus respectivos riesgos.

Las tecnologías de protección utilizadas como controles deben adecuarse al tamaño y al presupuesto de la organización.

Finalmente, el sistema planteado para la gestión de seguridad de una red de datos no es un proyecto, es un proceso continuo en la organización. Los controles adoptados deben de ser evaluados constantemente de modo que validen el estado de riesgo en el que se encuentran los servicios informáticos así como el poder detectar nuevas amenazas.

REFERENCIAS

[1] William Stallings, "Comunicaciones y Redes de Computadores", 7ma. Edición, Reimpresión, *Pearson Prentice Hall*, 2008.

[2] BSI Group, portal de México [Online]. Disponible en: www.bsigroup.com.mx/es-mx/Auditoria-y-Certificacion/Sistemas-de-Gestion/De-un-vistazo/Que-son-los-sistemas-de-gestion/

[3] Diccionario de la lengua española – Real Academia Española Disponible en: http://lema.rae.es/drae/?val=seguridad

[4] Norma técnica Peruana NTP-ISO/IEC 17799. "*EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información*", *INDECOPI*, 2da Edición, 2007.

[5] Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 "*EDI. Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la Información. Requisitos*", *INDECOPI*, 1ra Edición, 2009.

[6] International Standard ISO/IEC 27005:2008, "*Information technology-Security techniques-Information security risk management*", ISO/IEC, 1ra Edición, 2008.

[7] International Standard ISO/IEC 27000 "*Information technology — Security techniques — Information security management systems — Overview and vocabulary*", ISO/IEC, 2da Edición, 2012

[8] IT Governance Institute, "COBIT 4.1", versión 4.1, *IT Governance Institute*, 2007.