Enl@ce: Revista Venezolana de Información, Tecnología y Conocimiento
ISSN: 1690-7515
Depósito legal pp 200402ZU1624
Año 6: No. 1, Enero-Abril 2009, pp. 43-55

Cómo citar el artículo (Normas APA):
De Freitas, V. (2009). Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar. *Enl@ce: Revista Venezolana de Información, Tecnología y Conocimiento*, 6 (1), 43-55

Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar

Vidalina De Freitas[1]

Resumen

Este trabajo se propone conocer las fortalezas y debilidades a las que pudieran estar sometidos los activos de información que están en custodia en la Dirección de Servicios Telemáticos (DST) de la Universidad Simón Bolívar ubicada en Caracas, Venezuela, con el fin de sugerir estrategias que minimicen la ocurrencia de posibles amenazas que en la mayoría de los casos explotan las vulnerabilidades organizacionales. Basado en una metodología de estudio de caso, este estudio permitió recoger información detallada usando una variedad de sistemas de recolección de datos, como entrevistas semi-estructuradas, estructuradas y en profundidad, revisión bibliográfica y arqueo de fuentes. Igualmente, se realizaron visitas a las instalaciones de la dirección evaluada y se revisaron aspectos de seguridad física previstos en las Normas ISO-27001:2007. Se concluye que cada uno de los elementos en custodia de la DST es de suma importancia para la Universidad Simón Bolívar, por lo que se sugiere la aplicación de algunos controles establecidos en las normas ISO, para cada uno de dichos activos.

Palabras clave: ISO-27001:2007, seguridad de la información, análisis y evaluación de riesgo, activos de información

Recibido: 26-06-08 Aceptado: 17-11-08

[1] Ingeniero en Computación. Magíster en Ingeniería de Sistemas. Especialista en telecomunicaciones. Profesora con categoría de Agregada en la Universidad Simón Bolívar. Venezuela. Correo electrónico: vfreitas@usb.ve

Analysis and Risk Assessment of Information: Case Study Universidad Simon Bolivar

Abstract

Nowadays, organizations, with all their technological advances and complex information processes, face many threats that, in most cases, exploit their vulnerabilities. The Simón Bolívar University, located in Caracas, doesn't escape from this reality. The objective of this work is knowing the strengths and weaknesses to which they may be subject information assets that are in custody at the Directorate of Telematics Services (DST) of the Simón Bolívar University, in order to suggest strategies to minimize the occurrence of possible events. This methodology uses a case study that allows you to gather detailed information with a variety of systems for collecting data for a given period. Among the data collection methods are used semi-structured, structured and in-depth review of the literature and archaeological sources. Similarly, visits were made to the facilities and reviewed aspects of physical security under the ISO-27001: 2007. The conclusion is that each element in the custody of the DST is of paramount importance to the University, are thus suggested implementing some controls in the ISO, for each of those assets.

Key words: ISO-27001:2007, Information Security, Analysis and Assessment of Risks, Asset Information

Introducción

El avance tecnológico ha traído consigo un reto mayor para quienes se dedican al combate de programa con características maliciosas, la difusión de nuevas técnicas y metodologías de ataques y amenazas informáticas cada vez más sofisticadas y eficaces. No es un secreto la cantidad de recursos que invierten las organizaciones para evitar intrusiones y manipulaciones que pongan en riesgo, desde la integridad de la data hasta las operaciones propias de la entidad.

Hoy en día, las organizaciones son más dependientes de sus redes informáticas y un problema que las afecte, por pequeño que sea, puede llegar a comprometer la continuidad de las operaciones, situación que inevitablemente se traduce en pérdida económica, retraso en las operaciones y crisis de confianza por parte de los usuarios.

Aunado a lo anterior se encuentra la ausencia de una adecuada política de seguridad de las redes. Este es un problema que está presente por el sólo hecho de subestimarse las fallas que a nivel interno se producen, considerando sobre todo que la propia complejidad de la red es una dificultad para la detección y corrección de múltiples y variados problemas de seguridad que van siendo detectados.

Para Sema Goup (2006), el objeto o propósito de la seguridad de la información consiste en mantener la continuidad de los procesos organizacionales que soportan los activos a resguardar. Así

mismo se intenta minimizar el costo global de la ejecución de dichos procesos como las pérdidas de los recursos asignados a su funcionamiento.

De allí que sea necesario que los responsables de la seguridad de la información en las organizaciones, tomen conciencia de su papel y deban contrastar los riesgos a los que están sometida sus activos. La evaluación, análisis y tratamiento del riesgo permiten llevar el nivel de riesgo de los activos de la organización a valores aceptables (Pessolani, 2007).

Los problemas asociados a la seguridad en redes alcanzan a todo tipo de organización. En particular, a las universidades que manejan grandes volúmenes de información que por su variedad e importancia la hacen blanco de posibles ataques. En estas instituciones, además se forman personas con habilidades que, mal dirigidas, pueden representar una amenaza todavía mayor. La experiencia nos demuestra que la Universidad Simón Bolívar no escapa de esta realidad.

La universidad Simón Bolívar es una institución pública de educación superior, ubicada en Caracas, Estado Miranda, Venezuela. Cuenta actualmente con una población estudiantil de aproximadamente 6789 estudiantes de pre y postgrado, con 424 profesores de planta y 848 empleados.

La Dirección de Servicios Telemáticos (DST) es el ente que resguarda o tiene a su custodia los servidores de las distintas instancias que manejan dichos volúmenes de datos. Es decir, tienen a su custodia los servidores de la Dirección de Administración y Control de Estudios (DACE), los servidores de Finanzas, los servidores de Nómina, los servidores la Dirección de Ingeniería e Información (DII), los servidores de correo, los Servidores de DNS, Página Web (Sede del Litoral), los servidores de Internet e Intranet. Como se puede observar todos estos activos son de suma importancia para el desenvolvimiento de sus operaciones.

De allí su importancia de analizar y evaluar los riesgos a los cuales éstos pueden estar sometidos, para de esa manera poder gestionarlos y minimizar sus posibles efectos.

Metodología utilizada

Este estudio se plantea como la continuación de un trabajo el cual buscaba evaluar la seguridad de la información a la luz de los controles de la ISO 17799:2005 (De Freitas, 2007).

En el presente artículo, se busca evaluar los riesgos a los cuales pueden estar sometidos los activos de información que se encuentran en custodia en la DST. El desarrollo del mismo se llevó a cabo tres fases: la primera consistió en una investigación documental; la segunda en una investigación de campo y la tercera la conformó el análisis, evaluación y tratamiento del riesgo de los activos en custodia de la DST. Siempre en el contexto de un estudio de caso.

Es una investigación documental ya que permite el estudio de problemas con el propósito de ampliar y profundizar el conocimiento de su naturaleza, con apoyo, principalmente, en trabajos previos, información y datos divulgados por medios impresos, audiovisuales o electrónicos [UPEL, p.15].

Es una investigación de campo porque en ella se comienza haciendo un análisis sistemático de los problemas con el propósito de describirlos, interpretarlos, entender su naturaleza y factores constituyentes, explicar sus posibles causas y efectos, y/o predecir su ocurrencia, haciendo uso de los métodos característicos de cualquiera de los paradigmas o enfoques de investigación conocidos o en desarrollo [UPEL, p. 14].

La población estuvo conformada por el personal que labora en la DST.

Se llevó a cabo el levantamiento de información a través de entrevistas en profundidad semi-estructuradas, se aplicaron cuestionarios y se realizaron visitas guiadas a las instalaciones.

Una vez obtenido los datos e información de los diferentes entes involucrados y corroborado con la visita a las distintas instalaciones de la Universidad Simón Bolívar, se procedió a la revisión, análisis e interpretación de los mismos. Para ello se emplearon métricas cuantitativas, pero en la mayoría se realizó usando la métrica cualitativa.

Evaluación del Riesgo

Conocer el riesgo a los que están sometidos los activos es imprescindible para poder gestionarlos, y por ello han surgido una multitud de guías informales, aproximaciones metódicas y herramientas de soporte las cuales buscan objetivar el análisis para saber cuán seguros (o inseguros) están dichos activos y no llamarse a engaño (MAGERIT, 2005).

El riesgo es definido como la probabilidad que una amenaza pueda explotar una vulnerabilidad en particular (Peltier, 2001).

Entre las múltiples metodologías y estándares que han surgido para manejar la seguridad se pueden mencionar: ISO 27001:2005, SEE_CMM, Cobit, ITIL, ISM3, entre otros. Sin embargo, se requiere incorporar los cambios necesarios para que se ajusten a los requerimientos particulares de cada empresa.

En los actuales momentos la norma ISO 27001:2007, presenta un compendio que proporciona una base común para la elaboración de reglas, un método de gestión eficaz de la seguridad y permite establecer informes de confianza en las transacciones y las relaciones entre empresas.

La norma ha sido publicada en dos partes:

- ISO/IEC 27002:2007: Código de buenas prácticas para la Gestión de la seguridad de la información;
- ISO/IEC 27001:2007 - BS 7799 Parte 2: Especificaciones relativas a la gestión de la seguridad de la información.

Lo relacionado con la gestión del riesgo es una parte esencial del ISO 27001:2007. En el Anexo A de esta norma se propone una tabla detallada de los controles (Alexander, 2007), controles que deben ser seleccionados en base a los resultados de la evaluación del riesgo y a las decisiones tomadas concernientes al tratamiento de dicho riesgo.

La gestión del riesgo, generalmente, contempla el cálculo del riesgo, la apreciación de su

impacto en el negocio y la probabilidad de ocurrencia (Hiles, 2004). Luego se derivan pasos para reducir la frecuencia a un nivel considerado aceptable.

Si la empresa no conoce sobre el riesgo que corren sus activos de información, difícilmente llegará a estar preparada para evitar su posible ocurrencia, de allí la importancia de conocerlo y crear controles para disminuir o eliminar su posible ocurrencia.

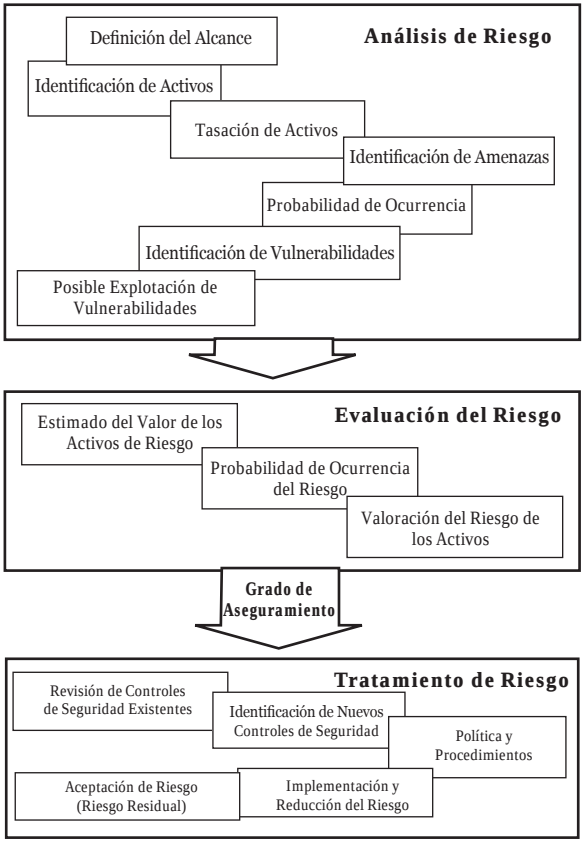
La ISO 27001:2007 recomienda para llevar a cabo una gestión de riesgo, que se defina primero el alcance del estándar en la empresa, y con base en ello, identificar todos los activos de información. Los activos de información deben ser tasados para identificar su impacto en la organización. Luego se debe realizar un análisis para determinar qué activos están bajo riesgo. Es en ese momento que se deben tomar decisiones en relación a qué riesgos aceptará la organización y qué controles serán implantados para mitigar el riesgo (Alberts y Dorofee, 2003). A la gerencia le corresponde revisar los controles implantados a intervalos de tiempo regular para asegurar su adecuación y eficacia. Se le exige a la gerencia que controle los niveles de riesgos aceptados y el estado del riesgo residual (que es el riesgo que queda después del tratamiento del riesgo).

El objetivo final de la evaluación de riesgos es realizar un cálculo de las amenazas a los activos de información, con vistas a seleccionar los controles ISO 27002:2007 o ISO 17799:2005 adecuados para mitigar ese riesgo.

Después de revisar los diferentes métodos, metodologías y herramientas existentes, se propone el esquema que se puede observar en la **Figura 1** para llevar a cabo el mencionado análisis y evaluar su riesgo.

Figura 1

Esquema del Análisis y Evaluación de Riesgo



Fuente: Elaboración propia

Desarrollo del trabajo

Análisis de riesgo. El objetivo del análisis de riesgo es identificar los riesgos basados en la identificación de los activos, de sus amenazas y vulnerabilidades (Alexander, 2007, p. 53).

a) *Definición del alcance del modelo:* el primer paso que se siguió de acuerdo a la metodología propuesta fue definir el alcance de esta evaluación de riesgo. El alcance de esta investigación son los activos que están en custodia de la Dirección de Servicios Telemáticos (DST), de la Universidad Simón Bolívar, Caracas, Venezuela.

La DST es la encargada de los servicios de comunicación de voz y datos, del apoyo técnico en informática no especializada y de la administración de los servicios de misión esencial de la Universidad. Esta unidad para el logro de sus objetivos cuenta con cuatro departamentos, que se encargan de brindar el apoyo y soporte necesarios: Departamento de Atención al Usuario, Departamento de Tecnología Informática, Departamento de Servicios de Red y Departamento de Servicios Telefónicos.

b) *Identificación de activos:* una vez definido el alcance se procedió a identificar los activos. Se identificaron 8 activos de información vitales (ver Tabla 1). Entre los activos de información, según la clasificación de la ISO 17799:2005, se encuentran:

- Activos de información (datos, de manuales de usuario, entre otros)
- Documentos en papel (contratos)
- Activos de software (aplicación, software de sistemas, entre otros)
- Activos físicos (computadoras, servidores, medios magnéticos, enrutadores, entre otros)
- Personal (estudiantes, clientes, empleados, entre otros)
- Imagen de la compañía y reputación
- Servicios (comunicaciones, entre otros)

c) *Tasación de activos:* una vez que se estableció el alcance y se identificaron los activos pertenecientes a una entidad en particular, se procedió a la tasación de dichos activos (esto con la finalidad de poder identificar posteriormente la protección apropiada a los activos, ya que es necesario tasar su valor en términos de importancia a la gestión tanto académica como administrativa de la Universidad Simón Bolívar, o dadas ciertas oportunidades determinar su valor potencial).

La tasación de activos es un factor muy importante en la evaluación del riesgo. La tasación es la asignación apropiada en términos de la importancia que éste tenga para la empresa. Para ello se deberá aplicar una escala de valor a los activos y de esa manera poder relacionarlos apropiada (Alberts y Dorofee, 2003).

En este caso (activos en custodia de la DST), se tasó su impacto con relación a su confidencialidad, integridad y disponibilidad. Se estableció utilizar la escala cualitativa de: Alto, Mediano y Bajo.

d) *Identificación de amenazas:* una vez realizada la tasación, se efectuó la identificación de amenazas.

Una amenaza es la existencia de algún mecanismo, que activado, permite explotar una vulnerabilidad. Una amenaza para poder causar daño a un activo debe estar asociada a una vulnerabilidad en el sistema, aplicación o servicio. Un incidente es cuando coinciden una vulnerabilidad y una amenaza afectando el funcionamiento de la organización (Hiles, 2004; Barnes, 2001), es decir, es la concreción de una amenaza.

Se realizaron reuniones con las personas encargadas de estos activos, con la finalidad de explorar las principales amenazas por cada activo de información.

e) *Probabilidad de ocurrencia de las amenazas:* el siguiente paso fue establecer la posibilidad de ocurrencia de amenazas y el impacto económico que pudiese ocasionar en la organización. La probabilidad de ocurrencia de una amenaza es el número de probables incidentes que pudiese sufrir un activo expuesto a una amenaza sin ningún tipo de contramedida para defenderlo.

Es importante señalar, que no todas las amenazas tienen la misma probabilidad de ocurrencia. Existen amenazas cuya frecuencia es baja y otras que son altas.

Para ello, también se utilizó la escala cualitativa de Alta, Media o Baja probabilidad de ocurrencia.

f) *Identificación de vulnerabilidades:* una vulnerabilidad es un error que representa un problema potencial, es decir, es una condición de debilidad, que le permite a una amenaza producir un daño en la organización.

En esta fase de la investigación se realizaron reuniones con los encargados de los activos, estableciendo por cada amenaza las posibles vulnerabilidades relacionadas con cada activo de información.

g) *Posible explotación de vulnerabilidades:* una amenaza para poder causar algún tipo de daño a un activo, tendría que explotar la vulnerabilidad del sistema, aplicación o servicio. Las vulnerabilidades son condiciones que pueden permitir que las amenazas las exploten y causen daño.

Se llevó a cabo reuniones con los encargados de los activos de información de la DST con la finalidad de obtener su realimentación respecto a las posibles explotaciones que pudiera tener cada amenaza relacionada con los activos.

La evaluación incluyó la identificación de debilidades en el ambiente físico, organizacional, procedimientos, gestión, administración, hardware, software o en equipos de comunicación, que podrían ser explotados por una fuente de amenazas para causarle daño a un activo en particular.

Una vez identificada las distintas vulnerabilidades por cada amenaza, se debe hallar el grado en que la amenaza puede explotar cada vulnerabilidad. Se produjo un listado de aquellas vulnerabilidades consideradas importantes.

Evaluación de riesgo

El proceso de evaluación del riesgo permite a una organización alcanzar los requerimientos del estándar. Este proceso ayuda a cualquier organización que desee establecer un Sistema de

Gestión de la Seguridad de la Información (SGSI) en concordancia con la cláusula 4.2.1 de la norma.

La evaluación de riesgo es el proceso de comparar los riesgos estimados contra los criterios de riesgo establecidos o dados, para determinar el grado de importancia del riesgo.

El objetivo de esta evaluación es la de identificar y evaluar los riesgos. Los riesgos son calculados por una combinación de valores de activos y niveles de requerimientos de seguridad.

El riesgo se evalúa contemplando tres elementos básicos:

Estimado del valor de los activos de riesgo

Probabilidad de ocurrencia del riesgo

Valoración del riesgo de los activos

a) *Estimado del valor de los activos de riesgos:* este punto es fundamental para evaluar el riesgo. El objetivo es determinar el daño económico que el riesgo pudiera causar a los activos evaluados. Esto se llevó a cabo dándole un valor monetario a cada activo de acuerdo al valor de referencia en el mercado y de su importancia para la Universidad. Se estableció un estimado del valor de los activos con los integrantes de la DST.

b) *Probabilidad de ocurrencia del riesgo:* se llevó a cabo reuniones con el jefe del Departamento de Servicios de Red con el fin de visualizar por cada activo sus impactos, amenazas y posibilidad de ocurrencia, así como las vulnerabilidades y su posibilidad de ser explotadas, determinándose la posibilidad de ocurrencia del riesgo por cada activo de información perteneciente a la DST.

c) *Valoración del riesgo de los activos:* por último, se llevó a cabo la valoración del riesgo de los activos.

Para el cálculo del campo total, se dio un valor numérico de de 5 para el término Alto, 4 para el término Medio y 3 para el Bajo. El valor del campo total se obtiene de la suma de los campos "posible Explotación de Vulnerabilidad", más el campo "Valor Activo" más el campo "Posible Ocurrencia" dividido entre tres, el valor obtenido se retorna al término cualitativo.

Siguiendo la metodología, se concluye que todos los activos de información que se encuentran en la DST son activos de información considerados de Alto riesgo, con los cuales habría que identificar (tomando en cuenta el Anexo A de las normas ISO 27001:2007 o de la ISO 17799:2005) sus respectivos controles.

En la **Tabla 1** se puede observar el vaciado del análisis y evaluación de riesgo realizado. La gestión de riesgo permitirá evaluar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que sea aceptado por la dirección (Sema Group, 2006).

Tratamiento de riesgo

El tratamiento de riesgo se define, como el conjunto de decisiones tomadas con cada activo de información. El ISO/IEC Guide 73:2002, lo conceptualiza "como el proceso de selección e implementación de medidas para modificar el riesgo". Las medidas de tratamiento del riesgo pueden contemplar acciones como: evitar, optimizar, transferir o retener el riesgo.

Tabla 1
Realización del Análisis y Evaluación de Riesgo

Activos	Tasación				Amenazas	Probabilidad Ocurrencia	Vulnerabilidad	Posible Explotación de Vulnerabilidad	Valor Activo	Posible Ocurrencia	Total Riesgo
	Confidencialidad	Integridad	Disponibilidad	Total							
Servidores de DACE	A	A	A	A	-Hackers	B	-Software desactualizado o mal configurado	B	A	B	M
					-Virus y/o programas maliciosos	A	-Software desactualizado o mal configurado	A			
					-Seguridad Física	B	-Falla exceda la capacidad instalada	B			
Servidores de Nómina	A	A	A	A	-Hackers	B	-Software desactualizado o mal configurado	B	A	B	M
					-Virus y/o programas maliciosos	A	-Software desactualizado o mal configurado	A			
					-Seguridad Física	B	-Falla exceda la capacidad instalada	B			
Servidores de la DII	A	A	A	A	-Hackers	B	-Software desactualizado o mal configurado	B	A	B	M
					-Virus y/o programas maliciosos	A	-Software desactualizado o mal configurado	A			
					-Seguridad Física	B	-Falla exceda la capacidad instalada	B			
Servidores de Finanzas	A	A	A	A	-Hackers	B	-Software desactualizado o mal configurado	B	A	B	M
					-Virus y/o programas maliciosos	A	-Software desactualizado o mal configurado	A			
					-Seguridad Física	B	-Falla exceda la capacidad instalada	B			
Servidores de DNS, Página Web (Sede del Litoral)	A	A	A	A	-Hackers	B	-Software desactualizado o mal configurado	B	A	B	M
					-Virus y/o programas maliciosos	A	-Software desactualizado o mal configurado	A			
					-Seguridad Física	B	-Falla exceda la capacidad instalada	B			
Servidores de Correo	A	A	A	A	-Hackers	B	-Software desactualizado o mal configurado	M	A	M	A
					-Virus y/o programas maliciosos	A	-Software desactualizado o mal configurado	A			
					-Seguridad Física	B	-Falla exceda la capacidad instalada	B			
Servicios de Intranet	A	A	A	A	-Hackers	B	-Software desactualizado o mal configurado	B	A	B	M
					-Virus y/o programas maliciosos	A	-Software desactualizado o mal configurado	A			
					-Seguridad Física	B	-Falla exceda la capacidad instalada	B			
Servicios de Internet	A	A	A	A	-Hackers	B	-Software desactualizado o mal configurado	M	A	M	A
					-Virus y/o programas maliciosos	A	-Software desactualizado o mal configurado	A			
					-Seguridad Física	B	-Falla exceda la capacidad instalada	B			

Leyenda: Alto (A), Mediano (M), Bajo (B)

De acuerdo a lo establecido en la cláusula 4.2.1 (g), se deben seleccionar objetivos de control y controles apropiados del Anexo A del estándar ISO 27001:2007 o de la ISO 27002:2007 y la selección se debe justificar sobre la base de las conclusiones de la evaluación del riesgo y tratamiento del riesgo.

En el caso de los activos pertenecientes a la DST y en custodias por estos, una vez efectuado el análisis y evaluación del riesgo, se propuso mitigar los riesgos encontrados en los activos de información: a) Servidores de correo y b) Servicios de Internet. El criterio establecido para aplicar los controles apropiados del anexo A sobre estos activos fue el resultado de ALTO RIESGO en la evaluación del riesgo realizada. Los activos de información: c) Servidores de DACE, d) Servidores de Nómina, e) Servidores de la DII, f) Servidores de Finanzas, g) Servidores de DNS, h) Página Web (Sede del Litoral), e i) Servidores Intranet se le consideró un riesgo aceptable, por ser evaluado como un riesgo MEDIO y visualizarlo compatible con las políticas de la organización.

***Enunciado de aplicabilidad**:* se puede observar en la **Tabla 2**, a nivel de ilustración, un enunciado de aplicabilidad como producto del análisis y evaluación del riesgo efectuado a los Servidores de Correo e Internet.

Tabla 2

Enunciado de aplicabilidad

Activo de Información	Justificación
Servidores de DACE	Proporcionar direccionalidad en la seguridad de información
	Minimizar errores humanos en la seguridad de información
	Capacitación del usuario
	Minimizar los incidentes de seguridad y aprender de ellos
	Evitar el acceso físico no autorizado
	Evitar la pérdida de activos e interrupción del servicio
	Evitar la pérdida de activos y contaminación de software malicioso
	Controlar el acceso a la información
	Crear responsabilidades en el usuario
	Crear conciencia acerca del uso de contraseñas
	Evitar el acceso no autorizado a la computadora
	Inclusión de Seguridad de la información en el proceso de gestión de la continuidad de las operaciones
	Evaluar el riesgo
	Implantar planes para mantener y recuperar las operaciones
Servidores de Nómina	Proporcionar direccionalidad en la seguridad de información
	Minimizar errores humanos en la seguridad de información
	Capacitación del usuario

Tabla 2

Enunciado de aplicabilidad (Continuación)

Activo de Información	Justificación
	Minimizar los incidentes de seguridad y aprender de ellos
	Evitar el acceso físico no autorizado
	Evitar la pérdida de activos e interrupción del servicio
	Evitar la pérdida de activos y contaminación de software malicioso
	Controlar el acceso a la información
	Crear responsabilidades en el usuario
	Crear conciencia acerca del uso de contraseñas
	Evitar el acceso no autorizado a la computadora
	Inclusión de Seguridad de la información en el proceso de gestión de la continuidad de las operaciones
	Evaluar el riesgo
	Implantar planes para mantener y recuperar las operaciones
Servicios de Internet	Proporcionar direccionalidad en la seguridad de información
	Minimizar errores humanos en la seguridad de información
	Capacitación del usuario
	Minimizar los incidentes de seguridad y aprender de ellos
	Evitar el acceso físico no autorizado
	Evitar la pérdida de activos e interrupción del servicio
	Evitar la pérdida de activos y contaminación de software malicioso
	Controlar el acceso a la información
	Crear responsabilidades en el usuario
	Concientizar acerca del uso de contraseñas
	Evitar el acceso no autorizado a la computadora
Servicios de Intranet	Proporcionar direccionalidad en la seguridad de información
	Minimizar errores humanos en la seguridad de información
	Capacitación del usuario
	Minimizar los incidentes de seguridad y aprender de ellos
	Evitar el acceso físico no autorizado
	Evitar la pérdida de activos e interrupción del servicio
	Evitar la pérdida de activos y contaminación de software malicioso
	Controlar el acceso a la información
	Crear responsabilidades en el usuario
	Concientizar acerca del uso de contraseñas
	Evitar el acceso no autorizado a la computadora

Conclusiones

Entre las principales conclusiones que se pueden obtener de esta investigación, se encuentran:

El objetivo de la evaluación de riesgo es identificar y ponderar los riesgos a los cuales los sistemas de información, sus activos o servicios están expuestos, con la finalidad de identificar y seleccionar los controles apropiados.

Como se pudo observar, en los casos de los servidores de Correo e Internet, la evaluación del riesgo esta basada en los valores de los activos y en los niveles de los requerimientos de seguridad, considerando la existencia de los controles actuales.

La DST debe promover el establecimiento, implantación, operación, monitoreo, mantenimiento y mejoramiento de ISO 27001:2007 en la Universidad Simón Bolívar.

El encargado de la DST está en conocimiento de la importancia que tienen los activos adscritos a su dependencia, por lo que pone un esfuerzo por preservarlos.

Los activos que están bajo la custodia en la DST, pertenecen a instancias que manejan datos críticos para la Universidad, de allí la importancia de preservarlos.

Para escogencia de los controles se debe justifican con base a las conclusiones obtenidas del análisis, evaluación y tratamiento del riesgo a los cuales se someten los activos de información.

Existen muchos métodos para el cálculo de riesgos de activos de información, pero se debe escoger el que más se adapte a las características de la empresa.

Bibliografía

Alberts, C. y Dorofee, A. (2003). *Managing Information Security Risk*. Pearson Education. Boston.

Alexander, A. (2007). *Diseño de un Sistema de Gestión de Seguridad de Información. Óptica ISO 27001:2005*. Alfaomega Colombiana S.A. Colombia.

Barnes, J. (2001). *A Guide to Business Continuity Planning*. Wiley. London.

De Freitas, V. (2007). *La Universidad Simón Bolívar a la Luz de los Controles de Seguridad de la ISO-17799/27001*. Ponencia presentada en el IV Congreso Iberoamericano de Seguridad de la Información. Mar del Plata. Argentina. Pp 277-296.

Hiles, A. (2004) *Business Continuity Best Practices*. Rothsein Associates. Inc.

ISO/IEC Guide 73:2002. *Risk management - Vocabulary - Guidelines for use in standards*.

ISO/IEC ISO 17799:2005. (2005). *Information Technology - Security Techniques - Information Security Management Systems Requirements Specification*. Recuperado el 15 de Julio del 2008 en http://17799.com

ISO/IEC ISO 27001:2007. (2007). *Information Technology - Security Techniques - Information Security Management Systems Requirements Specification*. Recuperado el 9 de marzo de 2008 en http://iso27000.es

Peltier, T. (2001). *Information Security Risk Analysis*. Auerbach. London.

Pessolani, P. (2007). *Evaluación de Riesgo en las Tecnologías de Información y Comunicaciones orientada a Organismos Públicos*. Ponencia presentada en el IV Congreso Iberoamericano de Seguridad de la Información. Mar del Plata. Argentina. Pp. 245-259.

Sema Group (2006). *MAP-Magerit Versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Secretaría del Consejo Superior de Administración Electrónica. Ministerio de Administraciones Públicas. Madrid. España.

UPEL Universidad Pedagógica Experimental Libertador. (2003). *Manual de Trabajos de Grado de Especialización y Maestría y Tesis Doctorales*. Fedupel. Caracas. Venezuela.