Publicaciones en Ciencia y Tecnología **Vol 2 N 1** (2008), 1–7

DISEÑO DE UN PLAN DE SEGURIDAD INFORMÁTICA PARA LA UNEXPO

*MANUEL MUJICA

Resumen

La investigación se basó en diseñar un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" (UNEXPO) sede Rectoral. Los incidentes de seguridad en los servicios de información tales como: ataques de DoS, SPAM, pérdida de información y computadoras infectadas, soportó la premisa planteada y se utilizó como modelo de referencia la norma ISO/IEC 27001 e ISO/IEC 17799. La metodología utilizada fue la de proyecto factible. Se realizaron análisis estadísticos, técnicas de recolección y análisis de la información dando como resultado mejoras consolidadas en los aspectos de seguridad de la información.
Descriptores: Plan de Seguridad Informática, ISO/IEC 27001, ISO/IEC 17799.

Abstract

The research was based on designing a plan for the Computer Security Experimental National University Polytechnical "Antonio José de Sucre" site Rectoral. Incidents of security information services such as DoS attacks, SPAM, loss of information and computers infected, endured the premise raised and used as a reference model ISO / IEC 27001, and ISO / IEC 17799. Methodology of the project was feasible. Statistical analyses were performed, technical collection and analysis of information resulting in consolidated improvements in the areas of information security.
Key Words: Plan Security, ISO / IEC 27001, ISO / IEC 17799.

**Departamento de Redes UNEXPO,Universidad Nacional Experimental Politécnica "Antonio José de Sucre", Barquisimeto, Lara 3001*

1 Introducción

El concepto de seguridad en informática se basa en confidencialidad, autenticación y disponibilidad de la información, estos elementos son afectados constantemente, PandaLabs [1], publicó que el veintiuno por ciento (21%) del correo electrónico que reciben las empresas son SPAM y que el cinco por ciento (5%) del tráfico total de la red está infectado por algún tipo de software malicioso. Los empleados utilizan el acceso a Internet con fines personales, lo cual se tradujo en pérdidas por lucro cesante para las empresas de más de trescientos ochenta (380) millones de dólares durante el ao 2.005. Además, se descubrió que el sesenta y seis por ciento (66%) de las visitas a páginas con contenidos pornográficos se efectúan durante la jornada laboral, no sólo provocando pérdidas sino consumiendo el ancho de banda. Esto evidencia la necesidad de las organizaciones de contar con planes de seguridad de la informacin basados en normas y/o estándares, en particular, el caso de estudio en la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" en la sede Rectoral.

2 Desarrollo

En las últimas décadas se han propiciado cambios en el área tecnológica que han impulsado la automatización de los procesos de las distintas organizaciones, siendo uno de estos cambios el uso masivo de redes de computadoras. Este proceso se ve amenazado constantemente por vulnerabilidades que aparecen reiteradamente en los sistemas de información y también como consecuencia de inadecuadas políticas de seguridad o falta de éstas para el manejo de los servicios de información. Visto el problema repercute negativamente en el ámbito financiero e incluso en la imagen organizacional.

Las Universidades Venezolanas como organizaciones las cuales prestan servicios de información, han utilizado como parte de sus herramientas tecnológicas las redes de computadores. Es evidente que éstas no escapan de los problemas de seguridad de la información planteados con antelación, tal y como se ha podido corroborar por observación directa del investigador en la UNEXPO, donde han ocurrido incidentes de seguridad en los servicios de información tales como: ataques de denegación de servicio, presencia de correo SPAM, perdida involuntaria de información institucional, computadores infectados de virus, troyanos y la no existencia de un plan de seguridad de la información que logre minimizar los riesgos ante estas amenazas. Es por lo expuesto, que se propuso el diseño de un Plan de Seguridad Informática y se estableció como marco de referencia la norma ISO/IEC-27001 [2] y la norma ISO/IEC-17799 [3].

Entre los enfoques teóricos que sustentaron el estudio, se pueden mencionar: Seguridad, Norma ISO/IEC 27001:2005, Norma ISO/IEC 17799:2005, entre otras. El enfoque epistémico se basó en la teoría de sistemas, ya que concibe la estructura como una concepción, que según Hurtado [4], "es aquella donde la realidad es vista bajo una concepción sistemática, en la cual la integración de elementos cumple funciones y configura estructuras".

Segn G'omez [5] para que un sistema se pueda definir como seguro se debe dotar de cuatro características al mismo:

- Integridad: requiere que la información solo pueda ser modificada por las entidades autorizadas. La modificación incluye escritura, cambio, borrado, creación y reactuación de mensajes trasmitidos.
- Confidencialidad: requiere que la información sea accesible únicamente por las entidades autorizadas.
- Disponibilidad: requiere que los elementos del sistema informático estén disponibles para las entidades autorizadas cuando los necesiten.
- No repudio: ofrece protección a un usuario frente a otro usuario que nieguen posteriormente que se realizó cierta comunicación. Esta proteccin se efectúa por medio de una colección de evidencias irrefutables que permitirán la resolución de cualquier disputa. El no repudio de origen protege al receptor de que el emisor niegue haber enviado el mensaje, mientras que el no repudio de recepción protege al emisor de que el receptor niegue haber recibido el mensaje.

La Norma ISO/IEC 27001 ha sido preparada con la finalidad de proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). La adopción de un SGSI debe ser una decisión estratégica para una organización. El diseñno e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados, el tamaño y estructura de la organización. Se espera que estos y sus sistemas de apoyo cambien a lo largo del tiempo. Se espera que la implementación de un SGSI se extienda en concordancia con las necesidades de la organización.

La aplicación de un sistema de procesos dentro de una organización, junto con la identificación y las interacciones de estos procesos y su gestión, puede considerarse un "enfoque del proceso". El estándar internacional adopta el modelo del proceso Planear-Hacer-Chequear-Actuar (PDCA del ingles), el cual se puede aplicar a todos los procesos SGSI. La figura 1 y tabla 1 muestran cómo un SGSI toma como insumo los requerimientos y expectativas de la seguridad de la información de las partes interesadas y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que satisfacen aquellos requerimientos y expectativas.

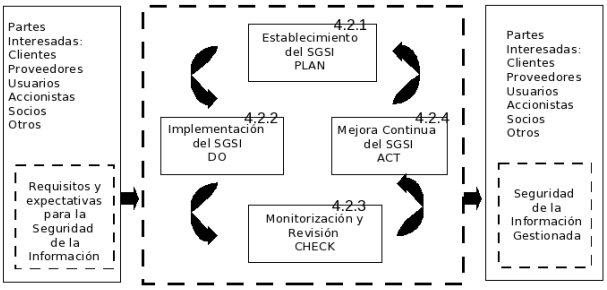

Figure 1: Modelo PDCA aplicado a los procesos SGSI. ISO/IEC-27001:2005

Planear (establecer el SGSI)	Establecer política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.
Hacer (implementar y operar el SGSI)	Implementar y operar la política, controles, procesos y procedimientos SGSI.
Chequear (monitorear y revisar el SGSI)	Evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia para su revisión
Actuar (mantener y mejorar el SGSI)	Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoria interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI

Tabla 1: Descripción del Modelo PDCA aplicado a los procesos SGSI

La adopción del modelo PDCA también reflejará los principios tal como se establecen en los Lineamientos OECD [6] que gobiernan los sistemas y redes de seguridad de la información. Este estándar internacional proporciona un modelo sólido para implementar los principios en aquellos lineamientos que

gobiernan la evaluación del riesgo, diseñno e implementación de seguridad, gestión y re-evaluación de la seguridad.

La norma ISO/IEC 17799 es un estándar internacional que establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos delineados en este estándar internacional proporcionan un lineamiento sobre los objetivos de gestión de seguridad de la información generalmente aceptados.

Los objetivos de control y los controles de este estándar internacional son diseñnados para ser implementados y satisfacer los requerimientos identificados por una evaluación del riesgo. Este estándar internacional puede servir como un lineamiento práctico para desarrollar estándares de seguridad organizacional y prácticas de gestión de seguridad efectivas y para ayudar a elaborar la confianza en las actividades inter-organizacionales. Este estándar contiene 11 cláusulas de control de seguridad conteniendo colectivamente un total de 39 categorías de seguridad principales y 133 controles que presenta para el tratamiento del riesgo.

En lo concerniente al marco metodológico utilizado el estudio se ubicó en la modalidad de proyecto factible, por ser una investigación desarrollada en el espacio y en el tiempo determinado, previo análisis y diagnóstico de la situación, y por cuanto pretendió satisfacer necesidades de tipo institucional, como lo fue el diseñar un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica "Antonio José de Sucre" sede Rectoral, tomando como referencia la norma ISO/IEC-27001:2005 y la norma ISO/IEC-17799:2005. El diseño de la investigación se realizó a través de las fases de la formulación de un proyecto factible: Fase I Diagnóstico; Fase II Factibilidad; Fase III Diseñno del Plan de Seguridad Informática y Fase IV Evaluación del Plan de Seguridad Informática.

La recolección de los datos se hizo mediante la aplicación de dos (2) instrumentos: una (1) entrevista estructurada, la cual constó de dieciséis (16) preguntas abiertas y (1) un cuestionario estructurado con diez (10) ítems cerrados para medir actitudes y opiniones con el método de escalamiento tipo Likert. Finalmente se detalló la situación presentada a través de la observación directa, no participante y sistemática.

Con el fin de evaluar los ajustes requeridos para validar el contenido de los instrumentos utilizados, se sometió a la validez de criterios por juicio de expertos. Para efectos de la confiabilidad del instrumento se aplicó una prueba piloto y los resultados obtenidos se aplicó el cálculo del coeficiente de confiabilidad Alpha de Cronbach. Se obtuvo un Alpha = 85,86%, que es de "Fuerte confiabilidad".

La definición del SGSI para la UNEXPO comenzó con la identificación del alcance del SGSI y de la política de seguridad de la información. Para la evaluación del riesgo se identificaron y tasaron los activos: La identificación se elaboró mediante el análisis de la metodología de las elipses. La tasación se realizó en función de su impacto a su confidencialidad, integridad y disponibilidad con una escala cualitativa entre Alto (A), Medio (M) y Bajo (B). En el tabla 2 se realiza un ejemplo del resumen de los activos a los que se les realizó la tasación.

Activos de información	A	M	V
Hardware	22	39	103
Sotware	13	2	25
Documentación	1	0	11
Total	13	41	139

Tabla 2: Tasación de Activos

La identificación de requerimientos de seguridad y la evaluación de la posibilidad de que las amenazas y vulnerabilidades ocurrieran se realizó una vez obtenido la tasación de activos y para lo que se utilizó el análisis y evaluación del riesgo, como lo muestra en ejemplo el tabla .

Donde Ts: Tasasión, Pos: Posibilidad, Ame: Amenazas, Vul: Vulnerabilidad, Exp: Expotación, Ps: posible, C:Configuración, Int: Integridad, Ds: Disponibilidad, Ocu: Ocurrencia, Ener: Energía, gnral:General, Sg: seguridad, Err:Error, Conf: Configuración, pers: Personal, eléc: Electrica, act: Activo.

Activos		TS		Total	Ame	Pos de	Vul	Posible Exp. de	valor	Ps	Total
	C	Int	Ds			Ocu		vul	act	ocu	gnral
Medios de Comunicación	A	A	A	falta de pers	fallas de fun	A	Ener eléc	A			
					A	poca	A Ds				
					falta de Sg	M	Err de conf	A			

Tabla 3: Realización del análisis y evaluación del riesgo

Se realizó una selección de opciones de tratamiento de riesgos apropiadas y una selección de controles para reducir el riesgo a nivel aceptable. Para lo cual se definió en el enunciado de aplicabilidad, ver ejemplo en el tabla .

Activo de información	objetivo de control	control	justificación
Medios de Comunicación	**A.6.1**. Organización interna	**A.6.1.1** Compromiso de la gerencia con la seguridad de la información **A.6.1.3** Asignación de responsabilidades de la seguridad de la información	Proporcionar direccionalidad en la seguridad y evitar errores humanos
	A.7.1 Responsabilidad por los activos	**A.7.1.1** Inventarios de activos **A.7.1.3** Uso aceptable de los activos	evitar perdida de activos e interrumpción del servicio
	A.8.2 Durante el empleo	**A.8.2.2** capacitación y educación en seguridad de la información **A.8.2.3** Proceso disciplinario	Minimizar los incidentes de seguridad y aprender de ellos
	A.12.2 Procesamiento correcto en las aplicaciones	**A.12.2.1** Validación de data de insumo **A.12.2.2**. Control de procesamiento interno **A.12.2.3**Integridad del mensaje	Asegurar la operación correcta de los medios de procesamiento de información

Tabla 4: Enunciado de aplicabilidad

Se Ejecutó los procedimientos de monitorización para detectar errores de proceso, identificar fallos de seguridad de forma rápida y acciones a realizar: En concordancia con lo establecido McNab [7] propone una metodología para la evaluación de seguridad de redes basado en los estándares más importantes de los Estados Unidos y para el Reino Unido específicamente "National Security Agency's INFOSEC Assessment Methodology (NSA IAM)" y "Communications and Electronics Security Gruop (CESG CHECK)" respectivamente.

La NSA IAM propone un entorno de trabajo definido en tres niveles de evaluación relacionado con el testeo de redes informáticas basadas en IP: (a) Evaluación: Este nivel implica realizar una descripción con la cooperación de la organización, incluyendo acceso a su documentación de políticas, procedimientos, etc. (b) Valoración: Es un proceso práctico que implica la realización de pruebas con herramientas de exploración y penetración de redes, usando conocimientos técnicos específicos y con consentimiento de la institución. (c) Equipo Rojo: Es una evaluación sin la cooperación de la institución de carácter externo a la red objeto de la penetración, e implica pruebas de penetración.

La CESG CHECK del mismo modo permite proporcionar servicios de evaluación en seguridad cubriendo aspectos como políticas, procedimientos, etc. Ambas metodologías fueron abordadas, a fin de proporcionar un refinado resultado de la evaluación del Diseño del Plan de Seguridad de Información implementado en la Institución. En este sentido, se puede inferir que existen en estas metodologías de evaluación dos grandes áreas: **la técnica** desarrollada en este punto utilizando el nivel de "Equipo Rojo" de la NSA IAM, descrita en la figura y para cuyas acciones se utilizaron las herramientas varias de seguridad y **la gerencial** la cual podría estar basada en CESG CHECK para futuras investigaciones.

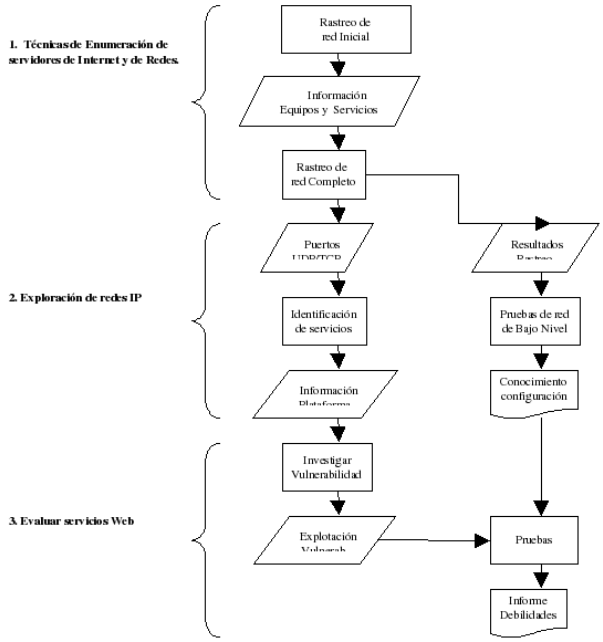

Figure 2: Diagrama de flujo para la evaluación de la seguridad en redes. McNab (2004)

3 Conclusiones

Dentro de los aspectos más resaltantes que se pueden mencionar, está una mejora total del setenta y uno por ciento (71%) una vez aplicado el plan de seguridad informática diseñada para la institución, hecho que refleja positivamente la efectividad del mismo. Todo esto como resultado de que se implementaron

soluciones de seguridad basado en los dominios de la norma ISO/IEC 27001:2005, tales como: políticas de seguridad, políticas de respaldos, normas y procedimientos, inventario de activos de información, consolidación de dominio para la autenticación, definición de perfiles de usuarios, servidor de archivos, servidor de antivirus corporativo, servidor de actualizaciones de seguridad, servidor proxy, normalización de estaciones de trabajo, firewall, implementación de una red conmutada a través de VLAN, documentación e ingeniería de detalle de la red entre otros.

Las recomendaciones se elaboraron sobre la base de los elementos y acciones que se evidenciaron a través del desarrollo de la investigación, de las que se pueden mencionar: (a) desarrollar el Business Continuity Plan (BCP) o Plan de Continuidad del Negocio, así como también, el Business Impact Analysis (BIA) o Análisis de Impacto del Negocio y (b) Como recomendación final se ratifica la necesidad de implementar una solución de Cluster Server y configurar una solución de Infraestructura PKI, entre otros.

References

[1] PandaLabs. *Informe trimestral PandaLabs*, [On-Line] Disponible en: http://www.pandasoftware.com/ [consultado Agosto 2.006].,

[2] ISO/IEC 27001:2005 - Tecnología de la Información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requerimientos. Organización Internacional de Estándares (ISO).

[3] ISO/IEC 17799:2005 - Tecnología de la Información - Técnicas de seguridad - Código para la práctica de la gestión de la seguridad de la información Organización Internacional de Estándares (ISO).

[4] Hurtado, M. *Metodología de la investigación holística*, Caracas - Venezuela. ED.: SYPAL, 2.000

[5] Gómez, J. *Seguridad en GNU/Linux*, Todo Linux No. 60 año 5, Madrid - Espaa, ED.: Studio Press, 2.006.

[6] Lineamientos OECD para Sistemas y Redes de Seguridad de la Informacin - Hacia una Cultura de Seguridad. [On-Line] Disponible en:www.oecd.org. Pars - Francia [consultado Junio 2.006].

[7] McNab, C. *Seguridad de redes*, (Madrid - España, ED.: Anaya Multimedia, 2.004)