MODELO DE SEGURIDAD DE GESTIÓN DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001, PARA EL DATA-CENTER DE LA FACULTAD DE INGENIERIA EN CIENCIAS APLICADAS, EN LA UNIVERSIDAD TÉCNICA DEL NORTE

Cristian Alfonso Perugachi Espinosa
Universidad Tecnica del Norte

Resumen— El presente proyecto describe el proceso de elaboración de un modelo de gestión de seguridad de la información basado en la norma ISO/IEC 27001 para el Data-Center de la facultad de ingeniería y ciencias aplicadas, de esta manera estructurar políticas y controles basados en los lineamientos y objetivos de control presentados y orientados a la parte lógica de la arquitectura de red.

Se utilizo una caracterización de los equipos mediante la utilización de la metodología MAGERIT, la cual indica de forma cada fase de la recolección de información centrando su atención a la identificación de las características de los activos, la estructura organizacional, las amenazas y las salvaguardas que se encuentran implementadas en el centro de datos. Una vez realizado el proceso de caracterizar el escenario inicial se realiza un cálculo del riesgo potencial que indica si es necesario tomar acciones.

En la parte de diseño se procede a seleccionar las políticas y objetivos de control previstos en la norma ISO/IEC 27001 que mejor se adapten a la infraestructura, para responder de manera específica a cada objetivo se elaboraron manuales, procesos y se seleccionó Endian Firewall como el software a implementar.

Se puede constatar por medio de la aplicación de la metodología MAGERIT que los parámetros iniciales de riesgo para amenazas humanas accidentales y deliberadas se encontraban entre 8,6 y 9,3 respectivamente. Al implementar las políticas seleccionadas este riesgo se puede obtener que el riesgo disminuyera a rangos de 4,6 y 41 tanto en origen humano accidental y deliberado, lo que implica una mejora, pero no descarta que se elabore una planificación constante para mantener los niveles de riesgo bajos.

I. INTRODUCCIÓN

La Facultad de Ingeniería en Ciencias Aplicadas acaba de implementar dentro de su infraestructura un Data-Center para alojar servidores y una red de servicios basados en el servidor de cloud computing privado.

El proyecto centrará su atención en lo que se refiere a la seguridad lógica de los servidores del Data-Center, entre los cuales se encuentran los servidores de cloud computing, un concepto nuevo dentro de las tecnologías de la información y que permite utilizar la virtualización de servidores para optimizar los recursos de la red de datos.

Se debe tener en cuenta que la topología de red en su diseño actual no contempla ningún tipo de seguridad además del firewall básico integrado en cada servidor, para los accesos LAN, WAN e internet hacia los servidores del Data-Center, permitiendo que se presenten los siguientes escenarios por acción de agentes internos o externos: ataques de denegación de servicio que incide en la disponibilidad de la información; ataques de suplantación de identidad afectando la confidencialidad de la información; infecciones de malware que incide en la integridad de la información.

Alojados dentro del Data-Center se encuentran servidores independientes y virtualizados que ofrecen aplicativos para interactuar con los usuarios finales de la red de datos, pero no se han realizado pruebas de monitorización que determinen la capacidad de flujo de datos soportado, ni de los puertos utilizados por cada uno de los servidores.

Las políticas de seguridad en el Data-Center no están establecidas, lo cual genera que los cambios realizados en la topología de la red para agregar, eliminar y modificar no cumplan con un procedimiento estandarizado en base a normativas internacionales de seguridad, las que establecen además plan de acción en caso de existir vulnerabilidades en la seguridad lógica.

II. MARCO TEÓRICO

A) ISO 27001

Antecedentes

- Se publicó como estándar internacional por la Organitation for Standarization y la comisión internacional Electrotechnical Commission en octubre del año 2005.
- Este estándar o norma es el resultado de la evolución de varios estándares de seguridad de la información, los cuales son:
- Normas “BS” (1901) publicadas por el British Standards Institution con carácter de internacional.
- BS 7799-1 (1995) Mejores prácticas para ayudar a las empresas a administrar la seguridad de la información, no se agregó una certificación ni una manera de conseguirla.
- BS 7799-2 (1999) Agrega los parámetros para conseguir una certificación.
- ISO/IEC 17799 (2000) La Organización Internacional para la Estandarización (ISO) utiliza los parámetros de la BS 7799-1.
- BS 7799-2 (2002) Se agrega la acreditación internacional.
- ISO/IEC 27001 (2005) Aparece la normativa como estándar internacional certificable.
- ISO/IEC 27001 (2007) Nueva versión.
- ISO/IEC 27001 (2009) Documento adicional con modificaciones leves a la norma.
- ISO/IEC 27001 (2013) Evolución de la norma en estructura, evaluación y tratamiento de riesgos.

Descripción

La norma se refiere a garantizar la seguridad de la información en todos los aspectos que abarca la misma, es decir la seguridad tanto física como lógica de los datos, para esto la normativa plantea varios objetivos de control los cuales deben ser establecidos e implementados siguiendo un plan de desarrollo constante y evolutivo, además de ser necesario contar con políticas de seguridad de la información.

El objetivo principal de esta normativa es garantizar las propiedades de la información que son confidencialidad, integridad, disponibilidad de los datos para de esta manera asegurar el activo más importante de una empresa o institución que son los servicios e información de la base de datos.

III. SITUACIÓN ACTUAL

La Universidad Técnica del Norte en su infraestructura cuenta con un Data-Center principal ubicado en el edificio central, conformado por varios equipos de red, y servidores entre los que se puede destacar el servidor de telefonía IP, servidor web, servidor DHCP, Firewall CISCO ASA 5520, y el switch core primario y secundario (respaldo) que comunica con cada facultad además de las dependencias externas por medio de enlaces inalámbricos. La topología física general de la Universidad Técnica del Norte la podemos observar en la Figura 1.

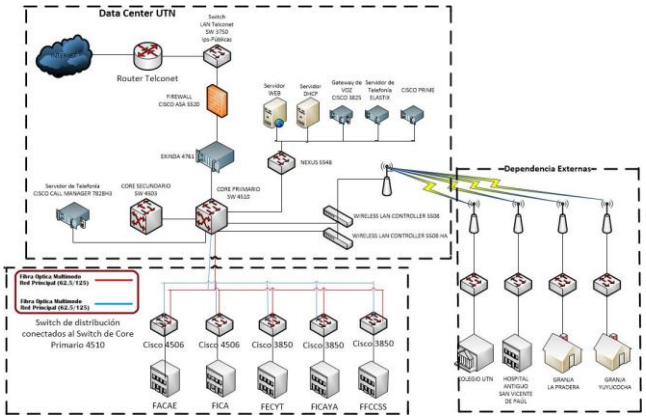

Figura 1. Diagrama Red UTN

En la facultad de ingeniería y ciencias aplicadas de la universidad técnica del norte se realizó la implementación de un Data-Center para ubicación de equipos de red encargados de la interconexión de los laboratorios y el centro de datos del edificio central y su posterior enlace con la red externa o Internet, además de los servidores integrados. La topología Física se observa en la Figura 2.

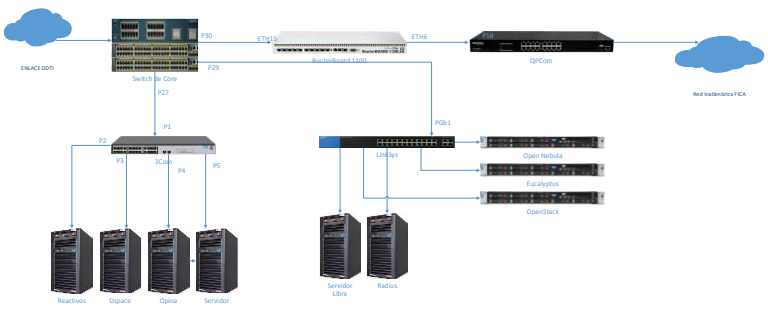

Figura 2. Topología Data-Center

IV. DISEÑO

Para la elaboración de políticas se sigue los lineamientos de la norma ISO/IEC 27001 en donde nos indica el establecimiento del modelo de gestión de seguridad de la información, dentro de este apartado se procede a identificar los objetivos de control tomados en cuenta para la realización del manual de procedimientos y las herramientas implementadas para el cumplimiento de cada una, los objetivos de control se los selecciono de la norma ISO/IEC 27001 en base a los riesgos que necesitan ser abordados inmediatamente los cuales son amenazas de origen humano tanto accidental como deliberado enfocados a la seguridad lógica del Data-Center.

Los objetivos de control seleccionados son:

A) Política de Seguridad de la Información
B) Organización de seguridad de la información
C) Gestión de los Activos
D) Gestión de Comunicaciones y Operaciones
E) Control de Acceso
F) Gestión de incidentes en la seguridad de la información
G) Cumplimiento

El manual de políticas de seguridad para el Data-Center se elaboraron en base a la norma ISO/IEC 27002, tomando en cuenta los objetivos de control mencionados para de esta manera darle una presentación formal a todos los objetivos de control que se tomara en cuenta para el establecimiento del modelo de seguridad de la información.

V. IMPLEMENTACION

Para la implementación del software y el direccionamiento es importante destacar el direccionamiento actual de la topología lógica la cual se puede observar en la tabla 1, hay que denotar que se presentara un direccionamiento propio para generar la DMZ de cada uno de los servidores alojados, la propuesta de direccionamiento se encuentra determinada en la Tabla 2.

Tabla 1. Propuesta direccionamiento

RED	Subred	IP	Gateway
INTERNA DATA-CENTER	10.24.8.0/24		10.14.8.1
OPINA	10.24.8.0/24	10.24.8.X	10.14.8.1
VOZ/IP	10.24.8.0/24	10.24.8.X	10.24.8.1
REACTIVOS	10.24.8.0/24	10.24.8.X	10.24.8.1

Se implementará la arquitectura lógica presentada en la Figura 3 y se utilizará el direccionamiento presentado en la Tabla 2.

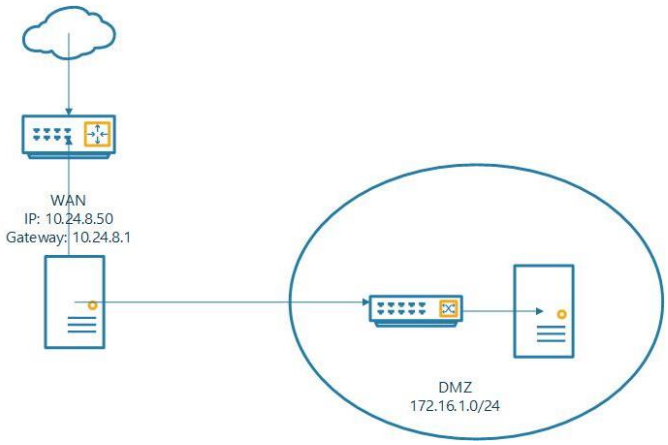

Figura 3. Topología Lógica con DMZ

Tabla 2. Direccionamiento servidores Data-Center

RED	Subred	IP	Gateway
IP ENDIAN	10.24.8.0/24	10.24.8.50	10.14.8.1
DMZ	172.16.2.0/24	172.16.2.1	172.16.2.1
OPINA	172.16.2.0/24	172.16.2.15	172.16.2.1
VOZ/IP	172.16.2.3/24	172.16.2.3	172.16.2.1
REACTIVOS	172.16.2.7/24	172.16.2.7	172.16.2.1

Para la configuración del software hay que acceder por medio del interfaz web por medio de la dirección ip asignada al interfaz Verde o LAN temporal que se utilizara para configuración de las interfaces, la dirección asignada es https://172.16.1.1:10443, en la primera ocasión de acceso se requiere un usuario y contraseña que por defecto son admin y endian respectivamente.

VI. CONCLUSIONES

- La norma ISO/IEC 27001 permite adaptar sus objetivos de control a la organización conformada por los activos que integran el Data-Center de la Facultad de ingeniería y ciencias aplicadas en lo que respecta a los objetivos de control referente a la seguridad de la información y a su vez mediante los procesos para la elaboración de un manual de políticas que regula la parte administrativa del personal a cargo de los

servidores y equipos que procesan los datos y los servidores.

- Con la estandarización de los procesos en el Data-Center por medio de los manuales de políticas, manuales de procedimientos y los formatos para la elaboración de los procesos se reduce los tiempos de respuesta ante amenazas en la seguridad de la información, además de permitir una documentación de cada actividad realizada, reducir las amenazas de origen humado accidental y deliberado las cuales se encontraban inicialmente en parámetros de 8,6 y 9,3 respectivamente indicando un riesgo potencial medio, y al finalizar la implementación se redujeron a 4,6 y 4,1 indicando nivel bajo.
- La facultad de ingeniería y ciencias aplicadas mantiene una infraestructura interna de servidores y equipos de procesamiento de información con crecimiento y desarrollo constante, al tratarse de una organización publica para el análisis de riesgos inicial se utilizó MAGERIT que es un método desarrollado por el gobierno español que permite de una manera estructurada identificar las condiciones del Data-Center.
- Seleccionar MAGERIT como el método para analizar los riesgos permitió simplificar el proceso de identificar los activos que posee el Data-Center, su clasificación, la importancia para la organización, las amenazas a las que se expone y también si existen salvaguardas que protejan cada elemento y proceso; a su vez permite elaborar mediante un método de cálculo de tablas las condiciones iniciales de la infraestructura.
- Debido a las condiciones de la organización tanto en materia de infraestructura lógica como en estructura organizacional los objetivos de control seleccionados permiten mejorar las características iniciales del Data-Center, además de permitir una constante evolución y mejora continua de las herramientas y procesos seleccionados.
- Endian Firewall es la herramienta de código abierto que actualmente permite cumplir con la mayoría de objetivos de control presentados en el diseño de la metodología de gestión de seguridad de la información, además permite utilizar sus herramientas de manera libre y solo se ve limitado por las características físicas del equipo seleccionado para su implementación.
- No existen sistemas de seguridad de la información perfectos, porque los equipos de procesamiento de datos, así como los equipos donde se implementan los servidores dependen de condiciones tanto físicas como lógicas, por lo que cualquier proceso implementado debe estar en constante evaluación, planificación y desarrollo para reducir los riesgos de ataques o vulnerabilidades que se puedan presentar por evolución de la tecnología.

VII. REFERENCIAS

- Allsopp, W. (2009). Unauthorised Access: Physical Penetration Testing For IT Security Teams. Chichester: WILEY.
- Amutio Gomez, M. A. (2012). MAGERIT-version 3.0 Metodología de analisis y gestión de riesgos de los sistemas de información Libro I-Metodo. En M. A. Amutio Gomez, MAGERIT-version 3.0 Metodología de analisis y gestión de riesgos de los sistemas de información Libro I-Metodo (pág. 175). Madrid: Ministerio de Hacienda y Administraciones Públicas.
- AVAST. (2015). avast.com. Obtenido de https://www.avast.com/es-es/c-spyware
- CERTuy. (23 de Abril de 2013). cert.uy. Obtenido de https://www.cert.uy/inicio/sobre_seguridad/glosario/
- Escudero, J. (10 de 12 de 2017). Emprendedores. Obtenido de Emprendedores: http://www.emprendedores.es/gestion/como-calcular-tu-precio-hora
- IBM. (2017). bm.com. Obtenido de https://www.ibm.com/support/knowledgecenter/es/ssw_i5_54/rzair/rzairemcommnd.htm
- Informáticos, D. (2015). delitosinformaticos.info. Obtenido de http://www.delitosinformaticos.info/delitos_informaticos/glosario.html
- KASPERSKY. (2017). kaspersky. Obtenido de https://support.kaspersky.com/sp/viruses/general/614
- Marion AGÉ, F. E. (2015). Seguridad Informatica: Ethical Hacking. Barcelona: Ediciones ENI.
- OVH. (24 de 10 de 2017). OVH Innovation is Freedom. Obtenido de OVH Innovation is Freedom: https://www.ovh.com

- Pablo González, G. S. (2015). Pentesting con Kali 2.0. Madrid: 0XWORD.
- Pérez, P. G. (2014). Ethical Hacking. Madrid: 0xWORD.
- Tori, C. (2008). Hacking Ético. Buenos Aires: Maestroianni.
- UNE 71504:2008. (2008). Metodología de análisis y gestión de riesgos para los sistemas de información.
- Uygur, S. U. (2014). Penetration testing with BackBox. Birmingham: Packt Publishig.

VIII. BIOGRAFÍA

Cristian A. Perugachi E. nació en Ibarra en Ecuador, el 5 de Junio de 1990. Sus estudios de primaria los realizó en la Unidad Educativa "Madre Teresa Bacq" Se graduó como Bachiller General y estudió Electrónica y redes de comunicación en la Facultad de Ingeniería en Ciencias Aplicadas (FICA) de la Universidad de Técnica del Norte de la ciudad de Ibarra - Ecuador