AUDITORÍA DE LA GESTIÓN DE SEGURIDAD DE LA WAN DE LA CACPE LOJA A NIVEL FÍSICO Y LOGICO

Ing. Carlos Miguel Jaramillo Castro
Unidad de Gestión de Postgrados; Escuela Politécnica del Ejército, Sangolquí, Ecuador

Resumen:

La Cooperativa, es una entidad financiera nacida hace más de 20 años, desde su aparición en el mercado, ha impulsado nuevos servicios para la ciudadanía, para lo cual ha implementado equipos y sistemas informáticos, que han aportado considerablemente en el desarrollo de cada uno de los procesos. En la actualidad, ha implementado un Data Center, donde se encuentran los activos informáticos, sistemas informáticos, en los que se procesa toda la información. También se encuentran ubicados los sistemas de redes, telecomunicaciones y servicios, que son utilizados por el personal ubicado a nivel de las provincias de Loja, El Oro y Zamora Chinchipe. De la información que se genera, procesa y acopia en los servidores y sistemas de almacenamiento, son de carácter confidencial y sumamente critica. Para garantizar la seguridad de esta información, se ha tomado en consideración la implementación de controles que garanticen la confidencialidad, integridad y disponibilidad de la misma. El objetivo es evaluar la gestión de la seguridad tanto a nivel físico como el lógico, para lo cual se utilizó normativas y estándares aceptados a nivel internacional, para mejorar las condiciones de seguridad en el ámbito informático. Para la aplicación de las normativas y la obtención de resultados, se ha utilizado la metodología descriptiva. Para la recolección de información se utilizó normas como la ISO 27002, con la metodología White Box de Auditoría. Finalmente, para la obtención de resultados se utiliza la metodología basada en riesgos con lo cual se obtuvieron los porcentajes de riesgos altos, medios o bajos.

ACTIVO INFORMÁTICO, AUDITORÍA INFORMÁTICA, SGSI, ISO/IEC 27001:2005, HALLAZGOS.

Abstract

The Cooperative, is a financial institution founded over 20 years ago, since its appearance in the market has prompted new services for the public, for which it has deployed teams and computer systems, during this time has contributed significantly to the development of each of its processes. Currently, has implemented a Data Center, which are arranged each computing assets, plus computer systems where all information is processed. Within the same network systems, telecommunications and services that are used by the main office, but its agencies and branches also located in the provinces of Loja, El Oro and Zamora Chinchipe. From the information generated, processed, and collected on servers and storage systems, we can mention the following: customers, credit, accounting, investment, among others, which is confidential and highly critical. To ensure the security of this information is taken into account the implementation of controls to ensure the confidentiality, integrity and its availability, which is proper managed by authorized persons. The goal set for this work was to evaluate the safety management, both physical and logical level, for which regulations and internationally accepted standards are used and have been implemented by many different kind companies to improve security conditions in the computer field. For the implementation of policy and outcome, we used descriptive methodology. To collect information standards such as ISO 27002, the White Box Audit methodology was used. Finally, to obtain the results risk-based methodology is used, whereby the percentages of high, medium or low risk were obtained.

COMPUTER ACTIVE, COMPUTER AUDIT, ISMS, ISO/IEC 27001:2005, FINDINGS.

Secciones

I. Introducción

Con el crecimiento acelerado de las tecnologías de información, la utilización de servidores, desempeña un papel importante en el negocio de las empresas, provocando a su vez, un incremento de la dependencia de los mismos, en los distintos procesos, donde la calidad es fundamental, para conseguir rentabilidad en la producción.

La necesidad de realizar pruebas de calidad de la seguridad, converge hacia el aseguramiento de la eficiencia y confidencialidad de la información. La auditoría de sistemas, permite detectar deficiencias, en las organizaciones que utilizan tecnologías de información y en los sistemas que se desarrollan u operan en ellas.

II. Metodología

Para el desarrollo del presente proyecto, se ha utilizado metodologías, tanto de investigación como de auditoría, como lo son las principales de investigación: encuestas, entrevistas y la observación, con la cual se recolecta toda la información que posteriormente será analizada, para obtener los resultados de la auditoría.

En el proceso de consolidación de la información, para realizar el proceso de la auditoría se realizaron actividades de:

- Inspección
- Análisis
- Visita
- Observación

- Confirmación
- Revisión Analítica

Para todo esto, se utilizó la metodología de auditoria de sistemas denominada White Box, por lo que los propietarios de los activos informáticos, facilitaron el acceso a la información y a las instalaciones.

Por último, para determinar los niveles de las seguridades, se utiliza la evaluación de riesgos, con la cual se determinan los riesgos, a partir de dos perspectivas: probabilidad e impacto. En la evaluación de riesgos, el auditor considera eventos previstos e inesperados y los riesgos inherentes, que es el riesgo en una organización, en ausencia de acciones, que podrían alterar el impacto o la frecuencia, de ocurrencia de los riesgos y los riesgos residuales, que resulta después, que la gerencia ha implantado, efectivamente acciones para mitigar el riesgo inherente, estos son evaluados.

Con la evaluación, se obtiene un catálogo de riesgos, ponderando la probabilidad de ocurrencia e impacto en los objetivos de control. Para la evaluación de las seguridades físicas y lógicas se utilizará los siguientes niveles de impacto, probabilidad y riesgo.

III. Evaluación de resultados y discusión

En la era de la información, todo ordenador es accesible desde Internet y en especial los servidores, se exponen diariamente a un elevado número de ataques. Servidores poco actualizados, con contraseñas débiles o sin una correcta planificación de la seguridad es una víctima segura, y para evitar esto, es necesario

implementar controles de seguridad que minimicen el impacto dentro de cada proceso del negocio.

Una vez analizada toda la información, se ha determinado que las seguridades físicas que posee la Cooperativa de Ahorro y Crédito de la Pequeña Empresa de Loja, en su Data Center aplicando las normativas como la ISO/IEC 27002:2005, poseen niveles de cumplimiento de controles adecuados en ciertas categorías y otras que se deben mejorar.

En lo que respecta a las seguridades lógicas, una vez analizada la información recolectada, se han determinado, que también existen cumplimiento de los controles, de las normas utilizadas para la evaluación de las seguridades, pero se debe tener en cuenta que se debe implementar una mejora continua para su constante mejora.

De los controles revisados, es recomendable que se realice un seguimiento total, de las falencias encontradas, con la finalidad de crear planes o metodologías, para la implementación de controles, que ayuden a mejorar la seguridad, así como evaluaciones constantes, que ayuden a medir la eficiencia y eficacia de los controles implementados, con la finalidad de continuar con los mismos o actualizarlos.

IV. Trabajos relacionados

Dentro de los trabajos realizados en empresas creadas, y, que se encuentran funcionando en la actualidad tenemos:

La auditoría informática de la “Empresa Municipal de Agua Potable y Alcantarillado de Ambato” en el año 2007, implementada en los departamentos: financiero, tesorería, proveeduría, agencia norte y sur la misma, que fue desarrollada

y culminada en su totalidad, determinando las falencias en sus sistemas de cómputo, realizando las respectivas recomendaciones.

(2007). Espinoza, M. *Auditoría Informática de la Empresa Municipal de Agua Potable y Alcantarillado de Ambato.* Recuperado de http://repo.uta.edu.ec/bitstream/handle/123456789/214/t288s.pdf?sequence=1

Igualmente, entre los años 2011 al 2012, se realizó una auditoría de seguridad informática, a la empresa de alimentos “Italimentos Cía. Ltda.”, en la ciudad de Cuenca, la misma que fue culminada con éxito y como resultado final, se pudo determinar el nivel de seguridad en cada uno de los procesos críticos de la empresa.

(2011). Cadme, C. *Auditoría de seguridad informática ISO 27001 para la empresa de alimentos "Italimentos Cía. Ltda.".* Recuperado de: http://dspace.ups.edu.ec/handle/123456789/2644

Cabe indicar que en el mundo, se han realizado trabajos, proyectos y estudios de auditoría informática muy relevantes, los mismos que han tenido gran impacto a nivel mundial, sobre todo, en la generación de nuevos estándares y controles, con lo cual se asegura que las seguridades físicas y lógicas, sean las más adecuadas, garantizando así la protección de la información.

V. Conclusiones y trabajo futuro

Una vez terminada la recolección de la información y realizado el respectivo análisis de la misma, se ha llegado a la conclusión de que la Cooperativa de Ahorro y Crédito de la Pequeña Empresa de Loja, dentro de los niveles de seguridades físicas y lógicas de la red WAN, en especial del Data Center, ha dado muestras de que, en muchas áreas, se han implementado controles, para garantizar la seguridad de los

activos informativos y sobre todo de la información que se genera, procesa y almacena dentro de los mismos.

De igual manera, algunas áreas se han dejado de lado y no se han implementado ningún tipo de control, lo que da lugar a que se genere una brecha en la seguridad, que debe ser atendida de forma inmediata. Es necesario, que en el futuro una vez implementados los controles necesarios, se vuelva a realizar otra auditoria para determinar si los niveles de seguridad han cambiado.

VI. Agradecimientos

A las personas que me han extendido su mano cuando yo los necesitaba. A la CACPE Loja, especialmente al Economista Jorge Piedra Armijos, Gerente de la entidad, quien me abrió las puertas para la elaboración de la auditoría; y a la Ing. Verónica Quinde España, Directora de Tecnología de la CACPE Loja, por su colaboración, brindando la ayuda e información necesaria para la culminación de este proyecto. Al Ing. José Luis Torres MBA y a la Ing. Nancy Velásquez MSc., por su guía y conocimientos que me ayudaron para la culminación total del tema propuesto

VII. Referencias Bibliográficas

Estándar internacional ISO/IEC 27001. (2005). *Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos*

Estándar internacional ISO/IEC 27001. (2005). *Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información.*

Espinoza (2007), *Base de Datos.* Recuperado. http://repo.uta.edu.ec/bitstream/handle/123456789/214/t288s.pdf?sequence=1

Aglone3. (2013). *Política de seguridad de la información.* Recuperado de https://iso27002.wiki.zoho.com/5-1-Pol%C3%ADtica-de-seguridad-de-la-informaci%C
3%B3n.html

Cadme (2012), *Base de Datos.* Recuperado. http://dspace.ups.edu.ec/handle/123456789/2644

Aglone3. (2013. *Seguridad Física y del Entorno.* Recuperado. https://iso.27002.wiki.zoho.com/9-1-%C3%81reas-seguras.html