UNIVERSIDAD Privada DR. RAFAEL BELLOSO CHACÍN

Revista Electrónica de Estudios Telemáticos
TÉLÉMATIQUE

SISTEMA DE GESTIÓN DE SEGURIDAD EN REDES LAN

(Safety management system lans)

Recibido: 03/03/2016 **Aceptado:** 02/03/2017

Carrasquero, Elimar
Universidad Rafael Belloso Chacín, URBE, Venezuela
elimar.carrasquero@gmail.com

Pérez, Luis
Universidad Rafael Belloso Chacín, URBE, Venezuela
luisperez3059@gmail.com

RESUMEN

La presente investigación tuvo como objetivo general proponer un sistema de gestión de seguridad en redes LAN para la Universidad Católica Cecilio Acosta (UNICA). Desde el punto de vista metodológico, denominado como proyecto factible, descriptivo, con un diseño no experimental, trasversal y de campo. La población estuvo conformada por catorce (14) sujetos pertenecientes a la organización. Para la recolección de información se utilizó la técnica de encuesta, mediante un cuestionario constituido por cuarenta y dos (42) ítems con cinco alternativas de respuestas de la escala de Likert, con un resultado considerado como muy alto, de acuerdo a una alpha de cronbach de 0,912. De acuerdo a los resultados obtenidos, se evidenció la existencia de debilidades en el sistema de gestión de seguridad en la red LAN en la organización. En consecuencia, se presenta el diseño de una propuesta, cuyo propósito fundamental fue fortalecer la competitividad, interoperabilidad y flexibilidad de las redes LAN, a fin de brindar al usuario servicios de calidad. Cuya propiedad buscaba mantener actualizado en todo momento la dinámica de su sistema de seguridad, pues, dichas redes suelen estar sometidas a cambios constantes propios del desarrollo tecnológico. La propuesta estuvo sustentada en la estructura del proceso de gestión de la seguridad expuesta por Bertolín (2008).

Palabras clave: gestión, sistema, seguridad, red.

ABSTRACT

This research has the general objective to propose a security management system in LAN networks for the Catholic University Cecilio Acosta (UNICA). From the methodological point of view, feasible and descriptive naming order project with a non-experimental, cross-country and design. The population of fourteen (14) subjects of the organization. The survey technique was used to collect information regarding the instrument a questionnaire composed of forty-two (42) items with five response options Likert scale, yielding a (high) result 0.912 was applied. According to the results, there was evidence of weaknesses in the safety management system on the LAN in the organization studied. Consequently, it presents the design of a proposal whose main purpose is to strengthen

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 15 Edición No 2 Julio – Diciembre 2016

competitiveness, interoperability, flexibility LANs in order to provide quality services to the user. Owned seeks to maintain updated all the time dynamics of the security system, as such networks are often subject to changes constants own technological development. The proposal was based on the structure of the process safety management exhibited by Bertolín (2008).

Keywords: management, system, security, network.

INTRODUCCIÓN

A través de los años en Venezuela el avance en la informática ha desempeñado un papel fundamental en todas las áreas de desempeño humano, al punto de convertirse en una herramienta indispensable en la vida cotidiana, igualmente, el seguimiento de las nuevas tecnologías, especialmente entre estas, la computación y las telecomunicaciones. La comunicación entre los seres humanos ha fomentado el desarrollo de las relaciones, tanto laborales como de cualquier índole, siendo este un factor primordial en el proceso de cualquier sociedad.

Igualmente, la constante necesidad por lograr mejores resultados en el menor esfuerzo posible ha llevado a las organizaciones a considerar cada vez más sus gestiones diarias, sus canales de comunicación, su desempeño personal, su productividad y por supuesto su eficacia. Actualmente, las redes de computadoras ayudan a las grandes empresas a tener comunicación con el mundo externo, además de apoyar a compartir recursos de manera institucional, siendo una ventaja para transmitir y distribuir información de vital importancia para cualquier usuario autorizado que disponga de ella de forma segura y así tener la certeza de que únicamente esa información será la utilizada manteniendo un adecuado control de acuerdo a las funciones que se realizan en la institución o de forma doméstica según sea el tipo de usuario.

Así, la seguridad en redes LAN, se ha convertido en uno de los problemas más relevantes en la vida organizacional, más aun, desde la globalización con la intencionalidad de ofrecer mejores servicios a través de estas redes, a fin de generar utilidades apoyadas en el desempeño efectivo de sus miembros de internet. Dada la potencialidad de esta herramienta y de sus innumerables aplicaciones, cada vez más personas y empresas sienten la necesidad de conectarse a este mundo. Por ello, los administradores de red han tenido la necesidad de crear políticas de seguridad, consistentes en realizar conexiones seguras, enviar y recibir información encriptado, filtrar accesos e información, entre otros.

Antes el bosquejo de globalización que las tecnologías de la información han originado, principalmente por el uso masivo y universal del internet, como los servicios involucrados con ellos, las instituciones suelen estar inmersas en situaciones de amenazas y ambientes agresivos, donde el vulnerar y sabotear se convierte en recursos para delinquir en espacios informáticos universales conocidos como hackers, crackers, entre otros. En este sentido, las tecnologías son sometidas severamente, así como frecuentemente a estos atacantes, por cuanto las han transformado en continuos riesgos, que obliga a las instituciones a establecer medidas de emergencia, normas, así como

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 15 Edición No 2 Julio – Diciembre 2016

políticas decisivas para enfrentar estas transgresiones, permitiendo lograr la seguridad informática que toda organización pretende

Por otra parte, las instituciones, al ser cada vez más dependientes de sus redes, emergen problemas de seguridad de gestión, por mínimo que sea puede llegar a comprometer la continuidad de los procedimientos. La falta de medidas de seguridad en las redes es un nudo crítico que carece, pues, cada vez es mayor el número de atacantes con sistemática organización, cada día van adquiriendo habilidades más especializadas que les permiten obtener extraordinarios beneficios.

Por otra parte, la mayoría de las instituciones con infraestructura tecnológica, entre ellas las universitarias, no están preparadas debidamente para determinar con exactitud el nivel de seguridad o inseguridad de su plataforma; como consecuencia se visualiza una incapacidad para detectar sus vulnerabilidades tecnológicas, debido a las posibles amenazas de seguridad. Ante esta incapacidad tecnológica, es difícil determinar los niveles de seguridad de sus redes; del mismo modo establecer políticas que garanticen la confiablidad e integridad de la información.

SISTEMA DE GESTIÓN DE SEGURIDAD DE REDES LAN

Sistema de gestión de seguridad; consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento dentro de una organización. Así la Organización Marítima Internacional, OMI, señala que un sistema de gestión de seguridad “es un sistema estructurado basado en documentos, que permitan al personal de la organización implantar de forma eficaz los principios de seguridad y protección ambiental de la misma”.

Sistema de gestión de seguridad es un proceso continuo multidimensional, que debe tenerse en cuenta en la definición, en la gestión y en la reingeniería de empresas y proceso de negocio. Por otra parte, un sistema de gestión de seguridad, es un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la misma.

NECESIDAD INSTITUCIONAL

“La tecnología por sí sola poco puede hacer, necesita de usuarios para sacar de ella sus potencialidades y ser capaces de superar sus debilidades". Esta afirmación valora cuestiones importantes relacionadas con la presencia e incidencia en las redes LAN; generándose una necesidad institucional la cual debe ser atendida desde perspectivas acorde con el propósito institucional establecido, donde los sistemas de información tienen un lugar preponderante.

En la actualidad la necesidad institucional se relaciona con el sistema de gestión de seguridad, este aumenta ante las amenazas que recibe del entorno, es los sistemas de información ofrecen ciertas ventajas en el cometimiento de actos delictivos y vandálicos, debido al carácter impersonal que puede asumir al atacante, es decir, no requiere de la

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 15 Edición No 2 Julio – Diciembre 2016

presencia o contacto físico con la persona o institución señalada como el objetivo del atacante, basta con sortear algunos impedimentos de carácter técnico para tener acceso a la información, por ello es que las redes de datos constituyen la principal vía de estos ataques.

Las organizaciones y sus sistemas de redes de datos enfrentan múltiples amenazas de seguridad, procedentes de una extensa variedad de fuentes, esta puede incluir; fraudes asistidos por computador, espionaje, saboteo, vandalismo, incendios e inundaciones. Las causas de daño tales como códigos maliciosos y ataques de piratería por computador y denegación de servicio suelen ser los más comunes, volviéndose cada vez más sofisticados. De allí la importancia de dar respuestas contundentes a esta problemática, lo cual el sistema de gestión de seguridad, debe abordar a través de; monitoreo, políticas de seguridad y planificación.

RECURSOS SENSIBLES

Los recursos sensibles se caracterizan por un constante incremento del número, complejidad y diversidad que los componen; donde, los principales problemas relacionados con la expansión de las redes son la gestión de su correcto funcionamiento cada día y la planificación estratégica de su crecimiento. Por todo ello, la gestión de red integrada constituye un conjunto de actividades dedicadas al control y vigilancia de recursos de telecomunicación, bajo el mismo sistema de gestión, se ha convertido en un aspecto de enorme trascendencia en el mundo de las telecomunicaciones.

Los recursos sensibles, lo cuales son asegurar los recursos del sistemas de información (material o programas) de una organización para ser utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación, sólo sea posible a las personas que se encuentren calificadas y dentro de los límites de su autorización. En consecuencia, de los recursos sensibles de mayor preponderancia para ser estudiado en la presente investigación son: mantenimiento, servidores, switches, routers, firewall, bases de datos y sistemas instalados.

CONTROLES DE ACCESO

El control de acceso en las redes LAN, tiene la posibilidad de controlar los permisos a cualquier usuario para acceder a servicios o datos de la organización, definición y gestión de puntos, contraseñas, seguridad perimetral, monitorización de accesos. Por el cual, los mecanismos para el control de acceso pueden ser usados para cuidar recursos físicos acceso a una habitación donde hay servidores, recursos lógicos, una cuenta de banco, de donde solo determinadas personas pueden extraer dinero o recursos digitales, un archivo informático que solo puede ser leído pero no modificado.

Control de acceso, es un término genérico que se utiliza para designar el proceso por el que un sistema de computación o un monitor de referencia controlan la interacción entre los usuarios y los recursos del sistema, de tal forma que los primeros acceden a los recursos deseados. Desde esta perspectiva los controles de acceso constituidos por la

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 15 Edición No 2 Julio – Diciembre 2016

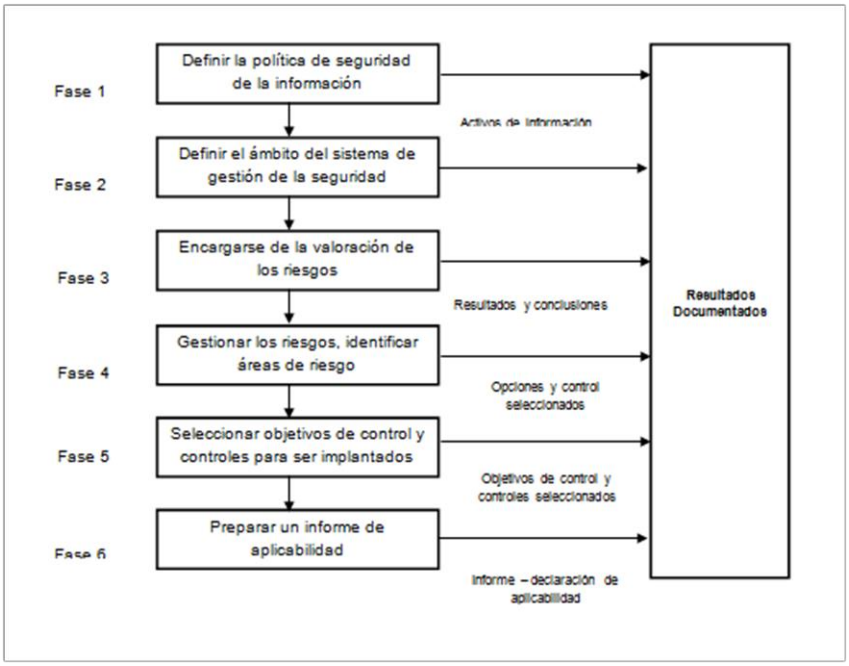
red, sistemas operativos, administración e infraestructura conforman el andamiaje necesario para facilitar un sistema de gestión de seguridad de las redes LAN.

Además, los controles de acceso serán determinados por el responsable de seguridad informática junto con el responsable del área informática, a fin de permitir el acceso solo al personal autorizado.

ESTRUCTURA DEL PROCESO DE GESTIÓN DE LA SEGURIDAD

En el desarrollo de sistema de gestión de seguridad en redes LAN, consisten en un conjunto de varios métodos, con el fin de llevar a cabo para una organización eficiente, segura y confiable, para gestionar la accesibilidad de la información. Para la presente investigación se escogió la estructura del proceso de gestión de la seguridad, es una especificación de un sistema de gestión de la seguridad de la información (SGSI), debido a que se consideró la más adecuada para el desarrollo de la misma.

Figura 1. Estructura del proceso de gestión de la seguridad



Según BS 7799-2 / AS-NZS 4444

Fuente: Bertolín (2008).

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 15 Edición No 2 Julio – Diciembre 2016

Cuadro 1. Operacionalización de la Variable

Variable	Dimensiones	Indicadores
Sistema de gestión de seguridad en redes LAN	Necesidad Institucional	Monitoreo Políticas de seguridad Planificación
	Recursos Sensibles	Mantenimiento Servidores Switch Router Firewall Bases de datos Sistema instalado
	Controles de Acceso	Red Sistema Operativo Administración Infraestructura

Fuente: elaboración propia.

MARCO METODOLÓGICO

En torno al tipo de investigación considerada factible, descriptiva, con diseño no experimental, transversal y de campo. Se consideró la aplicación de un censo poblacional, representado por catorce (14) sujetos que laboran en la organización respectivamente. En cuanto a la recolección de datos se elaborará un instrumento con escala de medición tipo Likert de cinco (5) alternativas de respuestas cerradas: Siempre (S), Casi Siempre (CS), Algunas Veces (AV), Casi Nunca (CN) y Nunca (N) de acuerdo a sus puntajes. En tal sentido, el instrumento se aplicó estando constituido por cuarenta y dos (42) ítems, obteniendo como resultado una confiabilidad de 0,912, indicándose como muy alta.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 15 Edición No 2 Julio – Diciembre 2016

Se elaboró la propuesta, así como las referencias bibliográficas. En cuanto al proceso de realización, el desarrollo de sistema de gestión de seguridad en redes LAN, propuesta por quien plantea seis (6) fases en el desarrollo del sistema de gestión de la seguridad de la información, la cual se encuentra conformada por: definir la política de seguridad de la información; definir el ámbito del sistema de gestión de la seguridad; encargarse de la valoración de los riesgos; gestionar los riesgos, identificar áreas de riesgo, seleccionar objetivos de control y controles para ser implantados, preparar un informe de aplicabilidad.

RESULTADOS DE LA INVESTIGACIÓN

Tabla 1. Cierre de la Variable Sistema de gestión de seguridad en redes LAN

Variable	Media	Dimensiones	Medias
Sistema de gestión de seguridad en redes LAN	**2,90**	Necesidad Institucional	**2,79**
		Recursos Sensibles	**2,74**
		Controles de Accesos	**3,16**
Calificación de Baremo Moderado			

Fuente: elaboración propia.

Los resultados evidencian que la variable Sistema de gestión de seguridad en redes LAN, se evaluaron las dimensiones; necesidad institucional, recursos sensibles, controles de accesos. Por lo tanto, develaron que el mayor puntaje de la dimensión controles de acceso con una calificación de 3,16 seguido a la dimensión necesidad institucional con una calificación de 2,78. Posteriormente, la dimensión recursos sensibles el cual arrojó una calificación de 2,74. Dicha variable alcanzando una media de 2,90 por lo que se ubicaron según la clasificación del baremo, en la categoría moderado.

Finalmente, al detallar se destaca que la variable Sistema de gestión de seguridad en redes LAN, se logró evidenciar que la media es de 2,90 ubicándose esta en la categoría moderado. Del mismo modo, según los resultados obtenidos el sistema de gestión de seguridad es un proceso continuo multidimensional, que debe tenerse en cuenta en la definición, en la gestión y en la reingeniería de empresas y proceso de negocio. Por otra parte, un sistema de gestión de seguridad, es un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la misma.

Se puede definir como la parte de un sistema general de gestión establecido por una organización que incluye la estructura organizativa, la planificación de las actividades, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos para

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 15 Edición No 2 Julio – Diciembre 2016

desarrollar, implantar, llevar a efecto, revisar y mantener al día la política de prevención en materia de accidentes graves.

Sistema de gestión de seguridad; consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento dentro de una organización. Con respecto a los resultados se busca brindar al usuario servicios de calidad. Cuya propiedad mantiene actualizado en todo momento la dinámica del sistema de seguridad, pues dichas redes suelen ser sometidas a cambios constantes propios del desarrollo tecnológico.

PROPUESTA

Plan operativo del sistema de gestión de seguridad en redes LAN para la Universidad Católica Cecilio Acosta (UNICA). Objetivo general: Proponer un plan operativo del sistema de gestión de seguridad en redes LAN para la Universidad Católica Cecilio Acosta (UNICA). objetivos específicos**:** Definir la política de seguridad de la información referente a las redes LAN para la Universidad Católica Cecilio Acosta (UNICA), Especificar el ámbito del sistema de gestión de la seguridad en redes LAN para la Universidad Católica Cecilio Acosta (UNICA), Determinar la valoración de los riesgos en redes LAN para la Universidad Católica Cecilio Acosta (UNICA), Gestionar e identificar las áreas de riesgos en redes LAN para la Universidad Católica Cecilio Acosta (UNICA), Seleccionar los objetivos de control y controles a aplicar en redes LAN para la Universidad Católica Cecilio Acosta (UNICA), Establecer las operaciones de gestión en la aplicabilidad de redes LAN para la Universidad Católica Cecilio Acosta (UNICA).

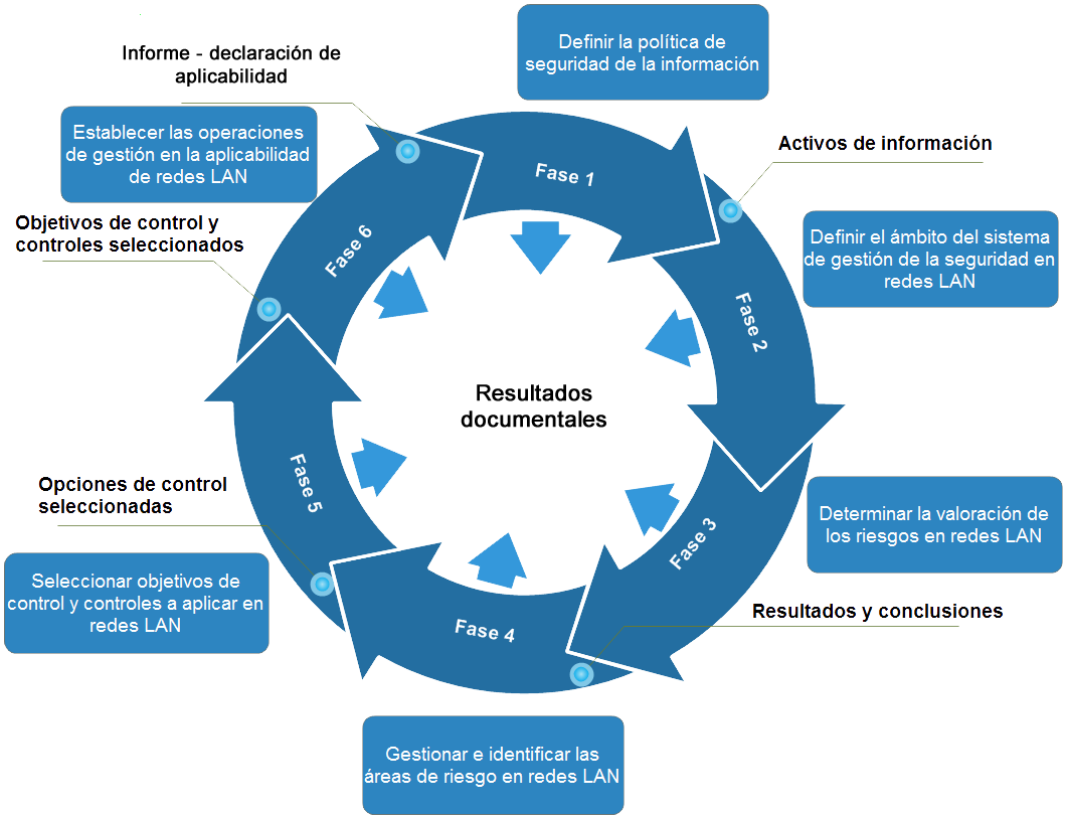
La justificación del presente plan estuvo centrado en facilitar el desarrollo de un sistema de gestión de seguridad en redes LAN, que cumpliera con determinadas normas de calidad y confiabilidad con un enfoque claramente definido acerca de lo requerido en cada organización; por cuanto, los beneficios que se esperan de la aplicabilidad de un plan operativo, dependen significativamente del buen uso dado a las herramientas tecnológicas, por parte del personal responsable en tales tareas, entre las cuales se encontraban: velar por la seguridad, configuración, administración y vida útil de las herramientas tecnológicas utilizadas, a objeto de garantizar la confiabilidad, disponibilidad e integridad de los datos que se manejan dentro de la misma.

PLAN OPERATIVO DE LA PROPUESTA

La propuesta estuvo referida a un plan operativo sobre un sistema de gestión de seguridad en redes LAN para la Universidad Católica Cecilio Acosta (UNICA), fundamentada en la estructura del proceso de gestión de la seguridad según BS 7799-2 / AS-NZS 4444.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 15 Edición No 2 Julio – Diciembre 2016

Figura 2. Estructura del proceso de gestión de la seguridad según BS 7799-2 / AS-NZS 4444.



Fuente: elaboración propia.

FASE I: DEFINICIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La definición de la política de seguridad de la información, el contexto del manejo tecnológico en muchas organizaciones ha sido sustentado específicamente en la promoción de la seguridad en redes LAN, con la intencionalidad gerencial de establecer normas, fomentar la colaboración y proporcionar oportunidades de desarrollo laboral para los responsables de garantizar la seguridad de las redes.

FASE II: ESPECIFICACIÓN DEL ÁMBITO DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD EN REDES LAN

La especificación del ámbito del sistema de gestión de la seguridad en redes LAN, permite asegurar que el personal operario de los equipos o tecnología tengan mayor control sobre las diversos tipos de activos que deben ser gestionados con medidas de seguridad en cuanto a sus datos e información, a fin de evitar la vulnerabilidad del sistema.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 15 Edición No 2 Julio – Diciembre 2016

FASE III: DETERMINACIÓN DE LA VALORACIÓN DE LOS RIESGOS EN REDES LAN

La determinación de la valoración de los riesgos en redes LAN, es importante porque permite asegurar que todos los usuarios durante el desempeño de sus actividades en sistemas de gestión sean identificables de manera única, a través de mecanismos de autentificación. Lo que coadyuva en la confirmación de los permisos de acceso del usuario al sistema.

FASE IV: GESTIÓN E IDENTIFICACIÓN DE LAS ÁREAS DE RIESGOS EN REDES LAN

La gestión e identificación de las áreas de riesgos en redes LAN, es el proceso por el cual se controla, minimiza o elimina situaciones que afectan los activos de la organización, además, facilita la creación de medidas adecuadas para enfrentar los hechos punibles que pueden afectar el desarrollo de las redes LAN. Por ello, todas las medidas a ejecutar se deben documentar para permitir una gestión sistemática, coherente y articulada con las normas establecidas por la organización.

FASE V: SELECCIÓN DE OBJETIVOS DE CONTROL Y CONTROLES A APLICAR EN REDES LAN

La selección de objetivos de control y controles a aplicar en redes LAN, comprenden algunas acciones operativas que se requieren para la implementación técnica, mantenimiento y seguimiento de las medidas de seguridad. De allí, que tanto el control como los controles pueden ser derivados de mecanismos existentes que se encuentran incluidos comúnmente en estándares y normas de seguridad como también pueden ser el resultado de una combinación de controles propuestos para los requerimientos de una organización especifica.

FASE VI: ESTABLECIMIENTO DE LAS OPERACIONES DE GESTIÓN EN LA APLICABILIDAD DE REDES LAN

El establecimiento de las operaciones de gestión en la aplicabilidad de redes LAN, constituye uno de los elementos fundamentales de un sistema de gestión de seguridad de redes LAN, es decir, se puede definir como un proceso que lista los objetivos y controles que se pretende implementar en una organización, a su vez instituir las justificaciones de aquellos controles que no son pertinentes de ser implementados. Es significativo resaltar que la construcción de un listado único requiere de la identificación de riesgos, la definición de controles, identificación de requisitos legales, contractuales, entre otros; sin olvidar la consideración de las necesidades requeridas por cada organización.

FACTIBILIDAD DE LA PROPUESTA

La determinación de la factibilidad responde a los requerimientos del sistema de gestión de seguridad de la red LAN que permite expresar la posibilidad que tiene la Universidad Católica Cecilio Acosta de implantar la presente propuesta para beneficiar y

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 15 Edición No 2 Julio – Diciembre 2016

agilizar su proceso de seguridad, para el cual se establecen tres criterios al momento de tomar una decisión como lo son la factibilidad técnica, económica y operacional.

La factibilidad técnica consistió en realizar una evaluación de la tecnología existente en la organización, este estudio estuvo propuesto a recolectar información sobre los componentes técnicos poseídos por la empresa y la posibilidad de hacer uso de los mismos en el desarrollo del sistema y de ser necesario, los requerimientos tecnológicos que debían ser adquiridos para la mejora y puesta en marcha del sistema. De acuerdo a la tecnología necesaria para la propuesta del plan operativo de la Universidad Católica Cecilio Acosta, se evaluó bajo dos enfoques: hardware y software.

En la factibilidad económica, se determinaron los recursos para desarrollar y mantener en operación el plan operativo, haciendo una evaluación donde se puso de manifiesto el equilibrio existente entre los costos intrínsecos del sistema y los beneficios derivados de este, lo cual permitió observar de una manera más precisa. Como se mencionó anteriormente en el estudio de factibilidad técnica, la organización contaba con las herramientas necesarias para la propuesta del sistema, por lo cual el desarrollo de la misma no requirió de una inversión inicial.

La factibilidad operativa se relaciona con la estructura organizativa que permite la gestión de los recursos humanos, materiales, técnicos, financieros, ético, científicos, tecnológicos, entre otros, para lograr un diseño de seguridad coherente y sistemático en atención a las políticas institucionales que privilegie el adiestramiento continuo y la concienciación de todos los involucrados en materias de seguridad.

CONCLUSIONES

Actualmente, la seguridad de la información es un tema en común en las gerencias de las empresas que utilicen este recurso como fuente principal para sus operaciones. Esto trae consigo la adopción de mecanismos y herramientas destinadas a propiciar seguridad de los datos y agilidad en el procesamiento de la información.

Por lo tanto, el sistema de gestión de seguridad en redes LAN, consistió en la protección de su confiablidad, integridad, de los sistemas de comunicación entre computadoras que permitiera compartir información dentro de la organización. En consecuencia, puede ocasionar severos daños a la integridad de las redes de datos, las cuales son de vital importancia en cualquier organización; pudiéndose afectar los datos relevantes para los usuarios que hagan uso de los diferentes sistemas de información; por ende, la omisión de las políticas de seguridad puede ocasionar que los datos puedan ser manipulados por individuos inescrupulosos con intenciones destructivas.

REFERENCIAS BIBLIOGRÁFICAS

Bertolín, J. (2008). Seguridad de la información. Redes, informática y sistemas de información. España.

Depósito Legal: PPX200002ZU2142 / ISSN: 1856-4194. Volumen 15 Edición No 2 Julio – Diciembre 2016