Enl@ce: Revista Venezolana de Información, Tecnología y Conocimiento
ISSN: 1690-7515
Depósito legal pp 200402ZU1624
E-ISSN: 2542-3274
Depósito legal ppi 201502ZU4693
Año 13: No. 3, Septiembre-Diciembre 2016, pp. 114-130

Cómo citar el artículo (Normas APA):
Salamanca, O. (2016). Sistema de gestión de seguridad para redes de área local para empresas desarrolladoras de software. *Enl@ce Revista Venezolana de Información, Tecnología y Conocimiento*, 13 (3), 114-130

Sistema de gestión de seguridad para redes de área local para empresas desarrolladoras de software

***Salamanca, Oscar*[1]**

Resumen

El propósito de proponer un sistema de gestión de seguridad para redes de área local para empresas desarrolladoras de software, sustenta el objetivo del presente artículo. Metodológica se rige por diversos referentes teóricos, así como lo establecido en las Normas ISO/IEC 27002:2013. Se considerado como proyecto factible, diseño no experimental de campo y transversal descriptivo. Se trabajó con un censo poblacional, conformada por nueve (9) sujetos integrantes de los departamentos de soporte y desarrollo. Para la técnica, se utilizó la encuesta, mediante el diseño de un cuestionario diseñado en treinta (30) expresiones cerradas. Los datos fueron procesados mediante la estadística descriptiva para su análisis y discusión. Los resultados determinan, una clara presencia de oportunidades para superar las debilidades que afectan la seguridad de la red en las organizaciones, así como, se evidenció la carencia de buenas prácticas que fomentaban el riesgo de la información. Se concluye, sobre la importancia del diseño de un sistema de gestión de seguridad de la información, basada en los estándares ISO/IEC 27002:2013, NIST SP800-12 e ITILv3. Se recomienda su aplicación para cumplir con todos los elementos necesarios para mitigar las debilidades en la organización en pro del crecimiento de la empresa.

Palabras clave: sistema de gestión de información; seguridad de redes; empresas desarrolladoras de software; normas ISO/IEC.

Recibido: 16/11/16 Devuelto para revisión: 25/11/16 Aceptado: 5/12/16

1 Magister en Telemática. Ing. en Computación. Universidad Rafael Belloso Chacín-Venezuela. Cursante Modulo 4 de Cisco Certified Network Associate Routing and Switching (CCNA).

Security Management System in the local area network for software development companies

Abstract

The purpose of proposing a safety management system for local area networks for companies developing software, supports the objective of the present article. Methodological is governed by various theoretical references, as well as established in the ISO/IEC 27002:2013. It is considered as a feasible project, non-experimental design of field and cross-sectional descriptive study. We worked with a census of the population, composed of nine (9) members of the department of support and development. For the technique, we used the survey, through the design of a questionnaire designed in thirty (30) expressions closed. The data were processed using the descriptive statistics for analysis and discussion. The results determine a clear presence of opportunities to overcome the weaknesses that affect the security of the network in organizations, as well as the lack of good practices that encouraged the risk of information. It is concluded, on the importance of the design of an information security management system, based on the standards ISO/IEC 27002:2013, NIST SP800-12 and ITILv3. It is recommended that your application to fulfill all elements necessary to mitigate the weaknesses in the organization of the growth of the company.

Keywords: Information management system; network security; companies developing software; ISO/IEC standards.

Introducción

En la medida que evoluciona la humanidad se presentan cambios en las necesidades de las organizaciones, generando en el entorno de las telecomunicaciones nuevas formas de acceder a la información e interconexión de redes. Situación que trae como consecuencia nuevos desafíos para mantener la seguridad en la infraestructura de las empresas en un orden mundial, de este modo el diseño de redes se rige globalmente por estándares internacionales que son utilizados por las organizaciones para mantener una estructura óptima que cumpla con estas directrices.

Con la llegada de Internet (International Network), una red internacional donde convergen diversidad de usuarios con distintos propósitos, la perspectiva de seguridad cambió drásticamente debido a la conexión global de redes, más aún con el auge de recientes dispositivos digitales, donde se crean nuevos modos de interacción, así como modernas formas que vulneran la seguridad y que son complejos de evitar. Por consiguiente, sólo las organizaciones que apliquen métodos de protección eficaces podrán reducir los riesgos de ataques y/o robos de información confidencial.

La transformación del entorno tecnológico, genera novedosos modelos de negocios que son aplicados por las empresas para expandir sus mercados, lo que conlleva a tener relaciones más estrechas con sus proveedores y clientes. Como consecuencia, surgen personas con intereses diferentes que buscan

aprovechar la información privada de las empresas, dañar los sistemas informáticos, destrucción de datos que generan pérdidas económicas y materiales.

Para prever los planteamientos expuestos, la Organización Internacional para la Estandarización (ISO) y la Unión Internacional de Telecomunicaciones (ITU) definen cinco áreas funcionales para la Gestión de Red como lo son: gestión de configuración, gestión de rendimiento, gestión de contabilidad, gestión de fallas y gestión de seguridad. El enfoque de la gestión de seguridad, consiste en administrar los componentes físicos y lógicos de la red por medio de parámetros de protección establecidos, es decir la seguridad física comprende los procedimientos de prevención, así como detección destinados a proteger la accesibilidad física al hardware de la red y la seguridad lógica, trata acerca de mecanismos e implementación de barreras para resguardar el poder acceder a los datos, dividiéndose en seguridad de aplicaciones, seguridad del sistema operativo, seguridad de la red, así como la identificación y autentificación.

Actualmente la innovación constante en las redes locales genera cambios abruptos en el crecimiento del flujo de la información que maneja una organización, considerando una alta demanda en la versatilidad, escalabilidad y adaptabilidad de esta, lo que conlleva a una mayor tendencia de equipos informáticos conectados como tal. En función de ello, surgen nuevos métodos de ataques y retos para la seguridad por parte de los administradores de red, por lo tanto, es vital proteger el activo más importante de una empresa como lo es la información, a través de un sistema de gestión de seguridad en redes, lo cual es necesario para prevenir, y mitigar los riesgos latentes y garantizar el logro de los objetivos empresariales.

Adicionalmente, se menciona que entre las fallas más comunes en el ámbito de seguridad en redes se encuentran, la estructura física de la red, el cableado estructurado no se encuentra organizado e identificado, carencia de metodologías para el mantenimiento de los equipos informáticos, actualizaciones de aplicaciones, sistemas operativos, firewalls, falta de planes de expansión de la red local ni políticas de seguridad definidas, ni procedimientos de seguridad en caso de contingencias que pueden ocasionar congestionamiento en el tráfico de la red.

Todas estas carencias influyen directamente en la seguridad de la red, ya que de no aplicarse estos controles servirían para crear una inestabilidad en la red local e incluso verse comprometida la operatividad de la empresa, al mismo tiempo la seguridad de la información es el punto más álgido de la organización, por constituirse como la base fundamental de los activos de la empresa, razón por la cual, la efectividad de la propuesta del sistema de gestión de seguridad en la red de área local para empresas de desarrollo de software, forma parte del reto por impulsar.

Sistema de Gestión de Seguridad de la Información

La norma ISO/IEC 27002:2013, define un Sistema de Gestión de Seguridad de la Información (SGSI) como las políticas, procedimientos, directrices, y recursos asociados a actividades colectivamente gestionadas por una organización, en la búsqueda de la protección de sus activos de información. Un SGSI, es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización, para alcanzar los objetivos

propuestos.

Desde la perspectiva de Heasuk, Seungjoo y Dongho (2011), conciben que un sistema de gestión de seguridad de la información, ha sido desarrollado para la administración eficaz de la seguridad de la información en una organización. Donde los SGSI, son capaces de hacer frente a una variedad de incidentes de seguridad. Además, también pueden administrar y operar continuamente la seguridad de la información en la tecnología, el hardware, software de los sistemas de información, manteniendo las características más importantes de un sistema seguro como lo son: confidencialidad, integridad, y disponibilidad.

Desde una visión integral, un SGSI consta del diseño, implantación, mantenimiento de un conjunto de procesos para gestionar el poder acceder o a la información, asegurando la confidencialidad, integridad y disponibilidad de la misma, con la finalidad de mitigar los riesgos de seguridad inherentes a la información, contemplando las cuatro fases del Ciclo de Deming como son Planificar (P), Hacer (H), Chequear (C) y Actuar (A); donde el enfoque es asegurar la continuidad de las operaciones en una organización, reduciendo las amenazas a los activos y limitando los impactos de violación de seguridad a su mínima expresión, con la finalidad de mantener un ambiente seguro.

Estándares Internacionales de Seguridad

Actualmente las organizaciones necesitan demostrar que realizan una gestión competente y efectiva del resguardo de los datos que gestionan, por lo tanto, es necesario seguir un conjunto estructurado de normas para garantizar la seguridad de la información. En consecuencia, existen organismos internacionales que regulan estas actividades con el fin de establecer, ante problemas reales o potenciales, disposiciones destinadas a usos comunes para obtener un nivel de ordenamiento óptimo o mejora continua en un contexto dado.

En el ámbito de las tecnologías de la información, han surgido diversos marcos de referencia de mejores prácticas, creados con la finalidad de apoyar a las organizaciones en pro de ofrecer bienes y servicios de alta calidad a través de la integración de las tecnologías de información, procesos, infraestructura, recursos humanos que operen de forma integral, por ende, se abordarán algunas normas y buenas prácticas que rigen el referido proceso.

Seguridad de la información: estándar publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional ISO/IEC 27002:2013

Enjuto (2007) manifiesta que la ISO 27002:2013, es una guía para conocer que se puede hacer para mejorar la seguridad de la información. Esta norma expone una serie de apartados y consideraciones relacionadas con la seguridad. También presenta sugerencias para cada uno de los controles, sin privilegios entre estos, bajo el enfoque de darle prioridad al sistema de gestión.

Asimismo, Calder (2009) expresa que la ISO 27002:2013 se encuentran los aspectos que buscan mitigar el impacto o la posibilidad de ocurrencia de los diferentes riesgos a los cuales está expuesta la organización. Con esta norma las empresas pueden encontrar una guía que sirva para la implementación de los controles de seguridad de la organización y de las prácticas más eficaces para gestionar la seguridad de la información.

En este orden de ideas, la norma ISO/IEC 27002:2013, puntualiza las buenas prácticas a seguir por medio de los mecanismos de control de seguridad que requieren ser implementados en una empresa bajo las directrices del estándar ISO/IEC 27001:2013, con el objetivo de minimizar el impacto en caso de ocurrencia de incidentes, resaltando que se adaptan a cualquier organización. En este sentido, la nueva versión ISO/IEC 27001:2013 contiene un conjunto de lineamientos a seguir para el desarrollo documental de un sistema de gestión de seguridad de la información sin importar su enfoque empresarial, alineando bajo una misma estructura todos los documentos relacionados con los sistemas de gestión y evitando así problemas de integración con otros marcos de referencia.

ITILv3: prácticas para mejorar la gestión de servicios en tecnologías de información

Vinogradsky (2008), define ITIL como un conglomerado de prácticas eficientes destinadas a mejorar la gestión de servicios TI, con el propósito de optimar la calidad de los servicios. Esta compuesto por cinco libros de referencia como son estrategia del servicio, diseño del servicio, transición del servicio, operación del servicio y mejora continua del servicio. Además, Huércano (2014) expresa que es un compendio de publicaciones o librerías, que describen de manera sistemática las buenas prácticas para la gestión de los servicios de TI y ofrece una aproximación sistemática para la entrega de servicios de calidad.

De acuerdo con lo expuesto, ITILv3 es un marco público que describe las mejores prácticas en la gestión de servicios de TI, se centra en la medición y mejora de la calidad del servicio, con un enfoque integrado que proporciona soluciones eficientes como factor clave para el éxito en las organizaciones que implementan las técnicas y procesos contenidas en él; así como, puede ser adaptadas de acuerdo a las necesidades o circunstancias de cada empresa.

Instituto Nacional de Estándares y Tecnología Publicación Especial 800-12.(NIST 800-12)

Conocido a través de sus siglas en inglés NIST como National Institute of Standards and Technology Special Publication 800-12, fue establecido en 1901 por la Oficina Nacional de Normalización para promover la innovación mediante el desarrollo de avances en normas o tecnología, con el fin de incrementar la productividad, así como mejorar la calidad de vida. Además, una de las funciones básicas de la agencia es desarrollar, mantener y conservar la custodia de los patrones nacionales de medición, proporcionar los medios, métodos para comparar los estándares utilizados en la ciencia, ingeniería, comercio, industria, educación con las normas adoptadas o reconocidas por el Gobierno Federal.

Diferentes principios y prácticas en seguridad

comunes tanto en agencias gubernamentales como en corporaciones privadas, están recogidos en una larga lista de publicaciones identificadas bajo la Serie 800, disponibles para su libre descarga. Estas guías o directrices son documentos muy elaborados y de reconocido prestigio, que cubren múltiples aspectos relacionados con la seguridad de la información.

Con relación a la publicación 800-12, se orienta en una visión general de la seguridad en informática para desarrollar un enfoque sólido en la selección apropiada de controles de gestión operacional y técnico, bajo el marco del ciclo de vida de un SGSI, que contempla cinco fases como son iniciación, desarrollo / adquisición, implementación, operación / mantenimiento y disposición.

Seguridad en Informática: estrategia para minimizar vulnerabilidad en sistemas de información

La seguridad en informática, considerada como el conjunto de técnicas aplicadas a los componentes de la red local, persigue el objetivo de minimizar las vulnerabilidades presentes en los sistemas de información acordes a las políticas de la organización. La seguridad en informática es responsable de preservar los dispositivos conectados a la red, así como a la información administrada por esta. Los problemas de seguridad, no deben perturbar la capacidad de una organización para realizar sus operaciones; este es el requisito básico de seguridad que deben tener las organizaciones.

Tipton y Krause (2008), exponen que no se tratan solo acerca de controles tecnológicos; la seguridad no puede orientarse solo en aplicaciones de software o hardware, cualquier intento de implementar controles de tecnología sin tener en cuenta las actitudes sociales de la organización es una fórmula para el desastre. El mejor enfoque para la seguridad eficaz es una capa que abarca el resguardo tanto tecnológico, como el no tecnológico. Según, Peltier, Peltier y Blackley (2014) la seguridad en informática puede cubrir desde el desarrollo de políticas estrictas que una organización va a seguir para proteger la información, hasta el acceso de un usuario a un archivo en el servidor de la empresa.

Desde esta perspectiva, se afianza que la seguridad en informática se enfoca en proteger los tres activos principales como son el software, hardware e información, además de la comunicación entre ellos, las debilidades humanas que interactúan con estos. Como elementos de lo que probablemente es el acrónimo más reconocido en la industria de la seguridad, la confidencialidad, la integridad, y la disponibilidad (CID ó CIA) constituye el fundamento de la seguridad de la información, con el fin de proporcionar una protección adecuada a cualquier fallo de seguridad, generando confianza entre los usuarios o los sistemas de información.

Políticas de Seguridad y seguridad física de los sistemas de información

Las políticas de seguridad, se consideran como parte de la gestión de los lineamientos a seguir por el personal de la organización, con el propósito de superar las amenazas y vulnerabilidades que se puedan presentar y afecten los sistemas de información, por lo que su documentación garantiza su correcto uso. El objetivo, es asegurar que el costo para implementar tales políticas, no exceda el de recuperación de incidentes de seguridad.

Mitnick y Simón (2003) sostienen que las políticas de seguridad son instrucciones claras que proporcionan las directrices al comportamiento de los empleados para la protección de la información, son un componente fundamental en el desarrollo de controles efectivos para contrarrestar las amenazas de seguridad. Estas políticas, son aún más importantes cuando se trata de prevención y detección de ataques de ingeniería social. Los controles de seguridad eficaces se implementan, mediante la capacitación de los empleados, políticas o procedimientos bien documentados.

Por su parte, Paquet (2013) opina que las políticas de seguridad comprenden un conjunto de objetivos para la compañía, reglas de comportamiento de usuarios y administradores, así como, requerimientos para la gestión de sistemas que garanticen la seguridad en redes de forma colectiva. Una política de seguridad, es un documento vivo, es decir que nunca finaliza, se actualiza continuamente a medida que la tecnología y los requerimientos de los empleados cambian.

Con respecto de la seguridad Física, Peltier et al. (2014), que la seguridad física consiste en proteger el sitio donde se encuentra el computador, equipo electrónico y software instalado, incluyendo el acceso controlado a las salas de cómputo, garantizando las condiciones medioambientales para su correcto funcionamiento, ello incluye el control de temperatura, humedad y flujo eléctrico, de manera que se proporcione un suministro ininterrumpido de energía eléctrica.

Para tales efectos la norma ISO/IEC 27002:2013 (2015) la define como evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones de procesamiento de información de la organización, contemplando diversos elementos como lo son: (a) perímetro de seguridad física, (b) controles de acceso físico, (c) seguridad de oficinas, despachos en instalaciones, (d) protección contra amenazas externas y del ambiente, (e) el trabajo en las áreas seguras, (f) seguridad en el cableado, (g) gestión de activos, (h) mantenimiento del equipamiento.

La seguridad física, es considerada como todos los métodos y herramientas destinadas a resguardar la información en la plataforma informática de una organización, con la finalidad de prevenir cualquier tipo de amenaza, para mantener la continuidad operativa de una empresa; donde este tipo de seguridad, es responsabilidad de un equipo multidisciplinario capacitado para estos fines, siguiendo los lineamientos de la entidad donde se encuentran.

Seguridad Lógica: un estándar que respalda las políticas de control

La norma ISO/IEC 27002:2013 (2015), establece la seguridad lógica como la limitación de acceder a la tecnología de información y funciones del sistema de aplicaciones según las políticas de control de la organización. Por su parte, Tipton et al. (2008), indican que consiste en soluciones técnicas con el objetivo de proteger los activos de una entidad; entre los objetivos para la seguridad lógica se encuentran (a) asegurar que los operadores puedan trabajar bajo supervisión, y no puedan modificar los programas, ni archivos que no correspondan, (b) asegurar que se estén utilizando los archivos y programas correctos en y por el procedimiento correcto, (c) que la información transmitida sea recibida solo por el destinatario al cual ha

sido enviada y no a otro, (d) que la información recibida sea la misma que ha sido transmitida, (e) que existan sistemas alternativos secundarios de transmisión entre diferentes puntos para casos de emergencia.

La seguridad lógica, trata de todas las medidas que garantizan el resguardo de los sistemas tecnológicos en una organización por medio de parámetros como respaldo de la información; servidor de controlador de dominio; servidor proxy; restricciones a la instalación de software; controles contra el malware; mantenimiento del software de los equipos; políticas de privilegios de acceso de los usuarios; gestión de contraseñas; control de acceso al código fuente; protocolos de seguridad, entre otros.

En este orden de ideas, el sistema de gestión de seguridad de la información se define como un conjunto de lineamientos en los ámbitos de las dimensiones situación actual, seguridad física y seguridad lógica, que consideran estrategias definidas como son los indicadores de estructura organizacional, políticas de seguridad, control de acceso físico, gestión de activos, respaldo de la información, entre otros, los cuales hacen frente a los riesgos de seguridad en una organización, enfocándose en asegurar la continuidad de las operaciones en una empresa, reduciendo las amenazas a los activos y limitando el impacto de violación de seguridad a su mínima expresión, con la finalidad de mantener un ambiente seguro.

Estrategias metodológicas

La investigación se clasificó dentro de la modalidad de proyecto factible, pues en esta se establecerá una propuesta de un sistema de gestión de seguridad en la red de área local para empresas de desarrollo de software, dirigida a solventar una necesidad previamente detectada en la organización. Se consideró una investigación de campo, debido a que los datos provienen de la realidad, es decir, del lugar en el cual suceden los acontecimientos, como lo es la red local de una organización. Diseño transeccional descriptivo, no experimental, debido a que la variable, así como sus dimensiones e indicadores fueron analizados en su estado natural, es decir, se desarrolló la medición de la variable operacional en consecución de los objetivos estratégicos, sin ser manipulados.

Para la recolección y análisis de los datos, se consideró la aplicación de un censo poblacional, constituida por un total de nueve (9) sujetos. La recolección de los datos que muestran un fenómeno en un tiempo determinado, se realizó mediante el uso de la técnica la encuesta, a través del diseño de un cuestionario conformado por treinta (30) expresiones, con escala de Likert en orientación positiva con el propósito de describir la variable sistema de gestión de seguridad de la información en la red de área local.

Asimismo, fueron definidos los procedimientos para organizar, presentar y analizar los datos obtenidos, que para la presente investigación será un tratamiento estadístico de tipo descriptivo, calculando las medias, distribuciones de frecuencias relativas y absolutas de las respuestas de los sujetos por cada ítem. Del mismo modo, se enmarca bajo el enfoque cuantitativo, ya que en armonía con Palella y Martins (2012) se requiere el uso de instrumentos de medición y comparación, que proporcionan datos cuyo estudio necesita la aplicación de modelos matemáticos o estadísticos.

Análisis y discusión de resultados

Los resultados obtenidos permiten determinar a través de la tabla 2, lo referente con el diagnóstico sobre la situación actual de las empresas de desarrollo de software. Estos responden, específicamente a los indicadores relacionados con la estructura organizacional, políticas de seguridad, vulnerabilidades y amenazas.

Tabla 1

Dimensión Situación Actual

Alternativas	TA		DA		NAD		ED		TD		μ	Nivel
Indicadores	**FI**	***fi***	**FI**	***fi***	**FI**	***Fi***	**FI**	***Fi***	**FI**	***fi***		
Estructura Organizacional	17	62,96	7	25,93	3	11,11	0	0,00	0	0,00	4,44	Muy Alto
Políticas de Seguridad	11	40,74	8	29,63	4	14,81	3	11,11	1	3,70	4,00	Alto
Vulnerabilidades	8	29,63	13	48,15	0	0,00	4	14,81	2	7,41	3,78	Alto
Amenazas	4	14,81	13	48,15	6	22,22	3	11,11	1	3,70	3,44	Alto
Situación Actual	40	**37,04**	41	**37,96**	13	**12,04**	10	**9,26**	4	**3,70**	**3,92**	**Alto**

Fuente: Elaboración Propia (2016)

La clasificación de la dimensión 3,92 se encuentra en un Alto nivel, confirmando lo establecido por Oppenheimer (2011) donde la situación actual consiste en examinar la red existente para juzgar mejor las expectativas para la escalabilidad, rendimiento y disponibilidad, incluyendo aprender acerca la topología y estructura física, que al contrastar los resultados de los indicadores pertenecientes a la dimensión se encuentran en su totalidad en las opciones alto nivel y muy alto nivel.

Con respecto a determinar las áreas sensibles en relación con la seguridad física de los componentes informáticos en la red de área local para empresas de desarrollo de software, se observa en tabla 3 los indicadores relacionados con control de acceso físico, seguridad en el cableado y gestión de activos.

Tabla 2
Dimensión Seguridad Física

Alternativas	TA		DA		NAD		ED		TD		μ	Nivel
Indicadores	**FI**	***fi***	**FI**	***fi***	**FI**	***Fi***	**FI**	***fi***	**FI**	***fi***		
Control de Acceso Físico	8	29,63	7	25,93	5	18,52	4	14,81	3	11,11	3,33	Moderado
Seguridad en el Cableado	3	11,11	11	40,74	8	29,63	3	11,11	2	7,41	3,44	Alto
Gestión de Activos	9	33,33	11	40,74	5	18,52	2	7,41	0	0,00	4,00	Alto
Seguridad Física	20	**24,29**	29	**35,80**	18	**22,22**	9	**11,11**	5	**6,17**	**3,59**	**Alto**

Fuente: Elaboración Propia (2016)

Según puede observarse, la clasificación de la dimensión 3,59 se ubicó en un alto nivel, y en armonía con Peltier et al. (2014) la empresa protege el sitio donde se encuentran los dispositivos pertenecientes a la red local como el computador, equipo electrónico, acceso controlado a los departamentos, existen deficiencias en cuanto a las políticas ejecutadas por el personal encargado, carencia de sistemas de aterramientos de acuerdo a los datos obtenidos por medio de los ítems 13 y 16 del cuestionario.

El estudio realizado para determinar las áreas sensibles con relación a la seguridad lógica de los componentes informáticos en la red de área local para empresas de desarrollo de software, presentó como resultados relacionados con los indicadores: respaldo de la información, mantenimiento de equipos y restricción de acceso a la información.

Tabla3
Dimensión Seguridad Lógica

Alternativas	TA		DA		NAD		ED		TD		μ	Nivel
Indicadores	**FI**	***fi***	**FI**	***fi***	**FI**	***fi***	**FI**	***fi***	**FI**	***fi***		
Respaldo de la Información	3	11,11	11	40,74	9	33.33	4	14,81	0	0,00	3,44	Alto
Mantenimiento de Equipos	2	7,41	5	18,52	9	33,33	7	25,93	4	14,81	2,67	Moderado
Restricción de Acceso a la Información	7	25,93	5	18,52	8	29,63	6	22,22	1	3,70	3.33	Moderado
Seguridad Lógica	12	**14,81**	21	**25,93**	26	**32,10**	17	**20,99**	5	**6,17**	**3,15**	**Moderado**

Fuente: Elaboración Propia (2016)

Resulta evidente la tendencia negativa en un 59,26% , en consecuencia la empresa no cumple con los requerimientos correspondientes a la seguridad lógica. Sin embargo, aun cuando la clasificación de la dimensión 3,15 se ubicó en un grado moderado, la empresa debe mejorar aspectos como el mantenimiento de equipos y restricción de acceso a la información, ya que contradice lo expresado por Boyles (2010) donde señala que la empresa debe contar con controles lógicos de software que estén compuestos de contraseñas que permitan identificar y autenticar al usuario que intenta acceder a los sistemas.

En consecuencia, los resultados obtenidos denotan una clara presencia de oportunidades de mejoras que están afectando la seguridad de la información, razón por la cual, se realizó un análisis de las fortalezas y debilidades fundamentadas en las respuestas de los sujetos encuestados, como base para establecer los lineamientos propuestos para responder a los objetivos específicos, tal como se muestra el cuadro 2.

Cuadro 1

Fortalezas y Debilidades

	(Aspectos Positivos)	(Aspectos Negativos)
Situación Actual	Presencia de una robusta estructura organizacional que sirve de apoyo a la seguridad de los sistemas. Los procedimientos de seguridad son agrupados, coordinados y controlados por personal especializado. Existencia de acuerdos de confidencialidad con el personal que maneja información crítica en la organización.	Carencia de mecanismos de detección de intrusos para evitar ataques en los sistemas informáticos. Déficit de dispositivos como el Firewall para filtrar información. Insuficiencia de software para monitorear los dispositivos de red para impedir propagación del malware. Ausencia de planes de contingencia ante incendios, inundaciones, fallas eléctricas, entre otros.
Seguridad Física	Los equipos informáticos se encuentran asignados a los departamentos de forma exclusiva. Normas que regulan el adecuado uso de los activos e información. Inventario actualizado de los activos de la organización.	Falta de políticas que normen el acceso a la infraestructura e instalaciones en la organización. Deficiencia en los sistemas de aterramiento para las líneas de energía. Escasez de dispositivos para proteger las fluctuaciones de voltaje.

Cont... Cuadro 1

	(Aspectos Positivos)	(Aspectos Negativos)
Seguridad Lógica	Alta presencia de planes de recuperación ante incidentes de seguridad.	Alta presencia de obsolescencia de las tecnologías.
	Almacenamiento de respaldos distintos a la sede principal.	Inexistencia de mantenimientos ajustados a las recomendaciones de los fabricantes.
	Limitación de acceso a la información conforme a los privilegios de los usuarios.	Ausencia de un registro de mantenimientos realizados a los dispositivos de la red.

Fuente: Elaboración Propia (2016)

En función de lo expuesto, los líderes empresariales deben entender que la seguridad de la información comprende mucho más que la protección de antivirus, ya que existen muchos componentes necesarios para un programa robusto de seguridad como lo es un sistema de gestión de seguridad de la información que complemente los procedimientos desarrollados en la organización, y con una correcta administración puede ayudar a mitigar los riesgos en las redes LAN, lo que conlleva a una reducción de costos, mayor productividad y establecer buenas prácticas de seguridad.

En este sentido, las políticas de seguridad en una empresa de desarrollo de software se caracterizan por la madurez y eficacia del programa de seguridad y los controles implementados, donde éstos se realizan en una o varias capas que van desde el acceso físico a las instalaciones hasta la auditoría en las aplicaciones manejadas por el personal de la organización, sin desestimar factores externos que influyen en el SGSI.

Propuesta del diseño del sistema de gestión de seguridad

Para dar respuestas a las carencias identificadas según los resultados analizados sobre la seguridad en redes de área local en empresas de desarrollo de software, se prevé que los mecanismos utilizados en lo concerniente a la seguridad en redes no son suficientes para garantizar un óptimo desarrollo, en consecuencia la definición de estrategias, normas y estándares son considerados como fundamentos básicos para solventar la situación actual.

El diseñó del sistema de gestión de seguridad en la red de área local para empresas de desarrollo de software, para los efectos, es concebido por medio de la combinación de tres prácticas y estándares como son la ISO/IEC 27002:2013, NIST SP800-12 e ITILv3, los cuales permitieron definir los lineamientos propuestos con base de las debilidades encontradas en los resultados de la investigación. Ver figura 1. Asimismo, para el desarrollo como

tal de sistema, se consideró como base las buenas prácticas de ISO/IEC 27002:2013, NIST SP800-12 e ITILv3, de igual forma se emplea el ciclo tradicional en los sistemas de gestión de calidad conocido como P-D-C-A, donde (P) plan/planificar: establecer, (D) do/(hacer): implantar y operar, (C) check/chequear: monitorear y revisar, (A) act/actuar: mantener y mejorar.

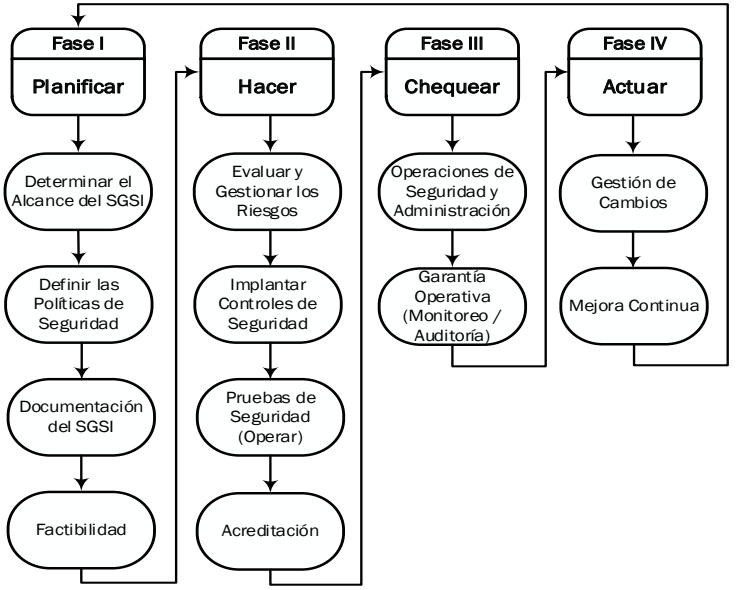

Figura 1
Diseño del sistema de gestión de seguridad.

Fuente: Adaptado de ISO/IEC 27002:2013, NIST SP800-12 (1995) e ITILv3 (2011).

En el marco de la conceptualización de cada una de las fases se establecen:

Fase I: Planificar

Se concibe a través de la definición de los objetivos y procesos necesarios para obtener los resultados esperados, busca las actividades susceptibles de mejorar por medio de precisar el alcance, políticas y documentación en el ámbito de seguridad de la información en la red LAN para empresas de desarrollo de software con la finalidad de establecer un sistema de gestión de seguridad de la información.

Fase II: Hacer

Se concibe la ejecución del plan estratégico, desde la visión de: organizar, dirigir, asignar recursos, supervisar la ejecución, mientras se recopilan datos para verificarlos y evaluarlos en los siguientes pasos. A través de esta fase se implementan las políticas, normas, procedimientos e instrucciones técnicas. Por consiguiente, para la investigación abarca aspectos como evaluar, gestionar los riesgos, implantar controles de seguridad, pruebas de seguridad y acreditación; etapas seleccionadas de las buenas prácticas de seguridad de NIST en la publicación SP800-12.

Fase III: Chequear

Permite planificar y llevar a efecto las actividades que permitan evaluar la efectividad, eficiencia del sistema de gestión de seguridad de la información, se mide el desempeño de los procesos en comparación con los controles implementados, las políticas y experiencias del SGSI, reportar los resultados a los altos directivos para su revisión aun si no cumplen con las expectativas iniciales.

Fase IV: Actuar

Es la fase donde se toman acciones correctivas y preventivas basadas en los resultados de la auditoría y revisión gerencial del SGSI para lograr el mejoramiento continuo, destacando que si son satisfactorios se implantará la mejora de forma definitiva, y si no lo son, habrá que decidir si realizar cambios para ajustar los resultados o descartarlos; una vez terminada esta etapa se debe volver a la primera fase para estudiar nuevas mejoras e implantarlas, por medio de las buenas prácticas ITILv3.

Lineamientos generales o políticas organizacionales

1. Los altos directivos se responsabilizarán por las políticas de seguridad de la empresa en estudio, así como todo el personal que interviene en la organización cumpla y coopere con la implementación de los controles de seguridad a través de una estructura organizacional adecuada para gestionar este fin.

2. Los coordinadores de los departamentos soporte y desarrollo mantendrán responsabilidades definidas en cuanto a la gestión de activos relacionados a los sistemas de información y a la clasificación de esta.

3. El coordinador del departamento de soporte, se encargará de gestionar los controles físicos necesarios respecto al personal relacionado al acceso a la infraestructura e instalaciones de TI en la organización.

4. El gerente de operaciones y los coordinadores de los departamentos de soporte y desarrollo establecerán los planes de contingencia ambientales adecuados para asegurar los activos que contengan información crítica de la empresa.

5. El gerente de operaciones debe velar por el cumplimiento por parte de los coordinadores de cada departamento de exigir a los subordinados cumplan con los controles de seguridad vinculado al uso interno o externo de la información.

6. El coordinador de soporte mantendrá la responsabilidad de gestionar el registro de mantenimiento realizado a cada uno de los dispositivos pertenecientes a la red LAN de la organización.

7. Los coordinadores de soporte y desarrollo garantizarán el cumplimiento de los diversos mantenimientos de software o hardware realizados a los equipos informáticos estén ajustados a las recomendaciones técnicas de los fabricantes.

8. El coordinador de soporte será el encargado de exponer al menos dos presupuestos en caso de adquisición de equipos o remplazo de piezas informáticas con el objetivo modernizar los equipos informáticos.

9. El gerente de operaciones y los coordinadores de los departamentos soporte y desarrollo establecerán las responsabilidades para la gestión de incidentes asociado a la seguridad de la información.

10. El coordinador de soporte realizará los planes necesarios que garanticen una reacción adecuada y oportuna ante fallos de energía, entre los cuales se encuentra verificar o mejorar el sistema de aterramiento en las instalaciones de la empresa en estudio.

11. Los coordinadores de soporte y desarrollo velarán que cada equipo informático de la organización cuente con dispositivos electrónicos como reguladores de voltaje o UPS con la finalidad de protegerlos ante fluctuaciones de energía.

12. Todos los empleados de la organización deben cumplir lo establecido en los documentos del Sistema de Gestión de Seguridad de la Información, de lo contrario podrán ser sancionados según la falta cometida.

Conclusiones y recomendaciones

El desarrollo concebido para proponer un sistema de gestión de seguridad para redes de área local para empresas desarrolladoras de software, permiten concluir que existe una tendencia positiva en los indicadores estructura organizacional y políticas de seguridad, mientras las vulnerabilidades y amenazas se caracterizaron con inclinación negativa, lo que conlleva a seguir los lineamientos o políticas organizacionales planteados para erradicar las debilidades presentes en la organización.

Con respecto a las áreas sensibles relacionadas con la seguridad física de los componentes informáticos se detectó una preferencia positiva hacia la gestión de activos, aun cuando se deben mejorar considerablemente el control de acceso físico y la seguridad en el cableado, con la finalidad de transformar estos indicadores en fortalezas para la organización.

Lo inherente con áreas sensibles, se puede inferir que existe una predilección hacia los mecanismos empleados en lo concerniente al respaldo de la información, entretanto se presentó una tendencia negativa en aspectos como el mantenimiento de equipos y la restricción de acceso a la información, por consiguiente se deben seguir las políticas de seguridad propuestas para reducir estas debilidades.

En consecuencia, se concluye que aun cuando existe un alto nivel de presencia de la variable en estudio en la organización, el diseño del sistema de gestión de seguridad en la red de área local para empresas

de desarrollo de software, se baso en tres prácticas y estándares como son la ISO/IEC 27002:2013, NIST SP800-12 e ITILv3, que cumple cabalmente con todos los elementos necesarios para mitigar las debilidades encontradas en la organización y perfeccionar las fortalezas a su máximo nivel de presencia.

Por lo cual se recomienda, incrementar los programas de formación en materia de seguridad en redes locales a los encargados de estos procesos; así como, fortalecer la evaluación de los riesgos con la finalidad de detectar nuevos factores internos o externos que puedan alterar la operatividad de la empresa. Además, establecer planes de detección de intrusos por medio de herramientas para este fin como un firewall que filtra la información y monitorea los dispositivos que componen la red local. De igual forma, sugiere incentivar las políticas que norman el acceso físico a las instalaciones de la organización, así como el uso obligatorio de dispositivos de identificación.

En líneas generales, promover un eficiente sistema de aterramiento para las líneas de energía en toda la infraestructura de la empresa y fomentar el uso de equipos que permiten proteger ante fluctuaciones de voltaje, seguidos de permanentes programas de mantenimiento de equipos informáticos, considerando el control de registros de acuerdo con el tipo de mantenimiento, además de propiciar la inversión para compensar la obsolescencia de las tecnologías, como también afianzar los mecanismos de seguridad correspondientes al cambio periódico de pasword para el personal de la organización.

Sin dejar de destacar, llevar a la práctica cada una de las fases del modelo de gestión de seguridad en redes locales para empresas de desarrollo de software, que permitan alcanzar la implementación del mismo. Del mismo modo, estimular la creación de estrategias o políticas de seguridad desarrolladas por el personal de los departamentos de desarrollo y soporte con el objetivo de contrarrestar nuevas amenazas.

Referencias

Boyles, T. (2010). **CCNA Security. Study Guide**. Wiley Publishing, Inc. United States.

Calder, A. (2009). **Implementing Information Security based on ISO 27001 /ISO 27002. A Management Guide. Best Practice**. Van Haren Publishing. Nederland.

Enjuto, J. (2007). **Diferencias entre ISO 27001 e ISO 27002**. Recuperado el 11 de junio del 2016 de http://secugest.blogspot.com/2007/09/diferencias-entre-iso-27001-e-iso-27002.html.

Heasuk, J.; Seungjoo, K. y Dongho, W. (2011). **Advanced Information Security Management Evaluation System**. *KSII Transactions on Internet and Information Systems*. 5(6)

Huércano, S. (2014). **ITIL V3. Manual Integro**. Biable Management, Excellence and Innovation. B-able. Sevilla, España.

ISO/IEC 27002:2013. **Estándar Internacional. Tecnología de la Información - Técnicas de seguridad - Código de buenas prácticas para controles de seguridad de la información**. Organización Internacional para la Estandarización Instituto Uruguayo de Normas Técnicas. Montevideo. Fondonorma.

Mitnick, K. y Simón, W. (2003). **The Art of Deception. Controlling the Human Element of Security. Foreword by Steve Wozniak**. John Wiley & Sons Editorial, United States.

Oppenheimer, P. (2011). **Top-Down Network Design**. Third Edition. Cisco Press. United States.

Palella, S. y Martins, F. (2012). **Metodología de la Investigación Cuantitativa**. Editorial FEDUPEL. Caracas, Venezuela.

Paquet, C. (2013). **Implementing Cisco IOS Network Security (IINS)**. Second Edition, Cisco Press. United States.

Peltier, T.; Peltier, J. y Blackley, J. (2014). **Information Security Fundamentals**. Second Edition. Auerbach Publications. United States.

Tipton, H. y Krause, M. (2008). **Information Security Management Handbook**. Sixth Edition. Auerbach Publications. United States.

Vinogradsky, V. (2008). **The ITIL Framework: And How It Can Improve Your Service Desk.** Recuperado el 11 de junio del 2016 de https://www.alloy-software.com/news/TheITILFramework.pdf