ISSN 0798 1015

REVISTA ESPACIOS

HOME Revista ESPACIOS ÍNDICES / Index A LOS AUTORES / To the AUTORS

Vol. 40 (Nº 28) Año 2019. Pág. 30

Caracterización de los Centros de Procesamiento de Datos (CPD) de las Pequeñas y Medianas Empresas (PyMEs)

Characterization of Data Processing Centers (DPC) of Small and Medium-Sized Enterprises (SME's)

MACHUCA VIVAR, Silvio Amable 1; MENDOZA PÁRRAGA, Ingrid Yulexi 2; SAMPEDRO GUAMAN, Carlos Roberto 3 y LALAMA FLORES, Robert Vinicio 4

Recibido: 17/06/2019 • Aprobado: 15/08/2019 • Publicado 26/08/2019

Contenido

RESUMEN:
La investigación desarrollada siguió un enfoque cuali-cuantitativo que permitió expresar con dimensión numérica el estado de la estructura de los Centros de Procesamiento de Datos (CPD) de las pequeñas y medianas empresas (PyMES) estudiadas y a partir de la interpretación de estos datos ofrecer una caracterización; con el propósito de demostrar así los posibles riesgos a que se someten las empresas mediante un análisis crítico de sus condiciones tecnológicas.
Palabras clave: centros de procesamiento de datos, pequeñas y medianas empresas, tecnología

ABSTRACT:
The research carried out followed a qualitative and quantitative approach that allowed us to express with a numerical dimension the state of the structure of the Data Processing Centers (DPC) of the small and medium-sized enterprises (SMEs) studied and, based on the interpretation of these data, to offer a characterization; with the purpose of demonstrating the possible risks to which companies are subjected through a critical analysis of their technological conditions.
Keywords: data processing centers, small and medium-sized enterprises, technology.

1. Introducción

Gracias al desarrollo y apogeo de las Nuevas Tecnologías de la Información y la Comunicación (NTIC), los progresos en los servicios y modelos de comunicaciones e información, el empleo sostenido y extendido a escala planetaria de la Internet, también se han incrementado los ataques a los sistemas informáticos, lo que ha llevado a las organizaciones a diseñar mecanismos que les faciliten la implementación de análisis que

adviertan, controlen y disminuyan los riesgos relacionados con la infracción o fragilidad de su información. Para esta labor resulta importante dominar los componentes que conforman cada modelo, entre ellos se encuentran los recursos del sistema de información requeridos para que la organización funcione cabalmente (Abril et al.,2013).

Frecuentemente se crean nuevos instrumentos que afectan a la seguridad de la información de las entidades, por esta razón resulta necesaria una estrategia completa de seguridad, de formas de advertir fugas y falencias en los sistemas. A esto se añaden vulnerabilidades internas que conforman un factor de riesgo no menor, y por ende, se manifiesta una elevada posibilidad de pérdida de recursos monetarios y efectos en la confiabilidad por parte de usuarios, clientes y socios de la organización. No se pueden dejar de lado los componentes de riesgos por desastres que al no estar pronosticados y sin planes de contingencia y/o de recuperación pueden producir daños irremediables en tiempo y costos de recuperación. Esto, que resulta apenas cuantificable, puede incluso estipular la continuidad de una empresa (Burgos y Campos, 2009).

Como apunta Dávalos (2013) en la actualidad las organizaciones con el objetivo de reguardar la información han estructurado y determinado la arquitectura de seguridad empresarial, asentada en el liderazgo de la seguridad y progresiva hacia abajo a través de capas, contrariamente al Modelo de Oficiales de Seguridad de la Información - OSI, que se fracciona en siete capas encapsuladas e independientes; mientras que en el Modelo de Seguridad Empresarial, sus capas son interdependientes: 1) Física, transmite hileras de bits en el medio físico, 2) Enlace de datos, provee transferencia de unidades de información al otro lado del enlace físico, 3) Red, conecta y enruta unidades de información, 4) Transporte, provee integridad en la trasmisión de datos punta a punta, 5) Sesión, establece, mantiene y administra las sesiones, por ejemplo: la sincronización del flujo de datos, 6) Presentación, provee la representación de datos entre sistemas, 7) Aplicación, provee servicios para las aplicaciones como transferencia de archivos.

Los Sistemas de Gestión de la Seguridad de la Información bajo las necesidades que requiere la norma ISO 27001, constituyen la plataforma para la gestión de la seguridad de la información. Dicha norma define un SGSI que avala el conocimiento, asimilación, gestión y reducción de riesgos de seguridad de la información para la entidad, de manera documentada, consecuente, estructurada, repetible, eficaz y acomodada a las transformaciones que se originen en los riesgos, contexto y tecnologías. La implementación de un SGSI requiere adaptarse a un nuevo modelo definido como enfoque de gestión, desde la aplicación de controles que componen la norma ISO 27002 hasta insertar productos certificados, conservando la mezcla inteligente de factores tales como las políticas, normativas, líneas, códigos de la práctica, tecnología, cuestiones humanas, legales y éticas (Martelo et al. 2015).

El presente estudio se encarga de demostrar así los posibles riesgos a que se someten las empresas mediante un análisis crítico de sus condiciones tecnológicas.

---

2. Metodología

La investigación desarrollada siguió un enfoque cuali-cuantitativo que permitió expresar con dimensión numérica el estado de la estructura de los Centros de Procesamiento de Datos (CPD) de las pequeñas y medianas empresas (PyMES) estudiadas y a partir de la interpretación de estos datos ofrecer una caracterización; con el propósito de demostrar así los posibles riesgos a que se someten las empresas mediante un análisis crítico de sus condiciones tecnológicas.

Se siguió un diseño no experimental, ya que el alcance de la investigación fue fundamentalmente descriptivo y explicativo sustentado en la aplicación de métodos teóricos y prácticos. Los primeros en calidad de procesos del pensamiento estuvieron presentes durante todo el proceso investigativo y permitieron analizar los resultados encontrados mediante la investigación de campo, en la cual se realizaron encuestas, entrevistas, también se implementó el método de la observación.

Los instrumentos utilizados para la aplicación de la encuesta, entrevista y la observación se

elaboraron tomando en cuenta los componentes que garantizaron la seguridad de los CPD desde las siguientes perspectivas:

-Seguridad Física: se observó la ubicación del CPD, el control de acceso, el sistema de vigilancia, los sistemas contra incendios y climatización. Aspectos que garantizan la protección ante desastres naturales u ocasionadas por el hombre. También incluye, disturbios, sabotajes internos y externos.

-Seguridad de la Red: se observó cómo tienen estructurados los cables, router, switch que permiten defender la red frente a las amenazas. Incluye además el uso de contramedidas físicas para proteger la infraestructura de red contra el acceso no autorizado, el uso inadecuado, la modificación y destrucción.

-Seguridad Lógica: consideró el uso de firewall, antivirus, el sistema de detención de intrusos y el sistema de análisis de seguridad activos.

Se tomó como referencia una población de 54 PyMES comerciales ubicadas en el Cantón Santo Domingo, registradas en el SRI, desde el mes enero del 2017. Siguiendo el muestreo probabilístico se seleccionaron 44 empresas de las cuales se obtuvo información mediante la aplicación de encuestas a sus respectivos gerentes y entrevistas a los técnicos de plantas que las atienden.

Para comprobar y profundizar en los resultados obtenidos mediante la encuesta y la entrevista se utilizó el estudio de caso, sustentado en una observación estructurada que permitió constatar el estado del CPD. Se estudiaron dos casos PyMES de minimarket (A) y otra de venta de equipamiento y materiales de construcción, ferreterías (B) seleccionadas a partir del muestreo no probabilístico, por conveniencia, considerando la apertura para el desarrollo de la investigación y los resultados en su actividad productiva, de este modo una es considerada como exitosa y la otra con limitaciones.

Se emplearon los números absolutos y porcentajes con su estimación, además, por intervalos de confianza, con el empleo del 95% del nivel de confianza y calculado este intervalo por el método de la Normal.

Los resultados más reveladores encontrados al acopiar la información mediante la investigación de campo realizada a administradores de las PyMES comerciales se presentaron a través de tablas, tomando en cuenta los principales indicadores que se determinaron para el estudio.

---

3. Resultados

El 100% de los gerentes reconoció que es importante mantener un control sobre la información, de forma mensual o anual para evitar la pérdida de datos y permitir que el área administrativa lleve un seguimiento y almacenamiento del flujo de información y recursos que surge a partir de esto.

Se aprecia en la tabla 1 que hubo 24 gerentes (82%, para un intervalo de confianza al 95% del 69% al 94%) que manifestaron no tener un conocimiento de los equipos técnicos necesarios, pero sí reconocen la importancia de tener un control sobre la información. La causa de no dedicarle prioridad a una estructura de CPD, pudiera estar relacionada con la creencia de que sería muy costoso y no toman en consideración que a largo plazo esta inversión evita pérdidas considerables y en algunas ocasiones irrecuperables pues deben tomar en cuenta que el crecimiento a futuro de la empresa debe realizarse sobre la base del análisis de los datos almacenados. En consecuencia, deben invertir paulatinamente en una estructura completa y así evitar daños a futuro porque nadie esta salvo de pérdidas por desastres naturales (inundaciones, terremotos, incendios) u otras provocadas por el hombre (robo de información, manipulación de datos). Al respecto Vieites (2013) señala que se debe tener una gestión de riesgo, que consiste en una etapa de evaluación previa de los recursos del sistema de información, con el propósito de garantizar el rigor y objetividad en el cumplimiento de su función. Solamente ocho gerentes dijeron que sí tenían conocimiento.

Más del 50% de los gerentes (24, para un intervalo de confianza al 95% del 39% al 71%) dijo que toma en cuenta primordialmente la seguridad física como prioridad, ya que es la

más visible; de este modo sí conocen la necesidad de garantizar estructura física completa como son: la ubicación del CPD, el control de acceso, el sistema de vigilancia, los sistemas contra incendios y la climatización, así como la necesidad de considerar que para la instalación de los equipos no tiene que existir humedad y vulnerabilidad estructural. Esto puede ser debido a su poco conocimiento sobre temas informáticos. Hubo 16 gerentes (36%, para un intervalo de confianza al 95% del 21% al 52%) que la seguridad de red es la más importante para una estructura básica de un CPD.

En la seguridad de la infraestructura de red los implementos más importantes que deben tener las PyMES son: cableado, router, switch que permiten defender la red frente a las amenazas. Se notaron dificultades en estos aspectos, ya que el área administrativa no invirtió mucho en esta parte por lo que los equipos adquiridos no son los idóneos y se adquieren solo pensando en lo que estiman justo y necesario, de este modo cuando se daña uno de estos equipos no se cuentan con un repuesto para caso de emergencia; esta situación trae como consecuencia que la empresa pierda incluso días sin laborar ya que no podrían arreglar al instante el problema debido a la demora en la gestión de los trámites para la adquisición de nuevos equipos, por eso es aconsejable tener repuestos para poder solucionar de inmediato y no tener pérdidas.

En el caso de la seguridad lógica solamente cuatro gerentes afirmaron que es la más importante. Siempre es fundamental saber sobre la seguridad lógica de una empresa o que es necesario para implementarla, pero los gerentes no toman en cuenta esta parte, es más, desconocen cuáles son consideradas como principales. La empresa al no contar con una seguridad lógica puede dejar en la vulnerabilidad a la información, ya que esta se encarga de filtrar las conexiones que ingresan a la red interna, evita que usuarios de Internet que no han sido autorizados para ingresar a la red de la empresa puedan tener acceso. Al respecto Peña (2013) enfatiza en lo significativo que es firewall como política de protección a la información capaz de brindar un análisis a Internet y evitar que no puedan encriptarse datos vulnerables al sistema, con lo que se garantiza mayor seguridad a la estructura de red que tenga la empresa.

Tabla 1
Respuestas de los gerentes
acerca de los equipos técnicos

Respuestas de gerentes		**No.**	**%**	**Límites del intervalo de confianza al 95%**
Conocimiento de los equipos técnicos	Sí	8	18	6 a 31
	No	36	82	69 a 94
Los importantes para una estructura básica de un centro de procesamiento de datos	Seguridad física	24	55	39 a 71
	Seguridad de red	16	36	21 a 52
	Seguridad lógica	4	9	3 a 22

Puede verse en la tabla 2 que las estructuras de CPD fueron valoradas por los propios gerentes de sus empresas como regular y malas (18 gerentes, para un 41% e intervalo de confianza al 95% de 25% al 57%, respectivamente), lo cual puede considerarse como una potencialidad, pues sí reconocen que presentan problemas en este sentido, sin embargo, no hacen nada por mejorar, lo cual pudiera ser debido a la existencia de limitaciones económicas. Solo ocho gerentes consideraron que la estructura de su CPD era buena.

Tabla 2
Gerentes según valoración
de la estructura de su CPD

Valoración de la estructura de su CPD	No.	%	Límites del intervalo de confianza al 95%
Mala	18	41	25 a 57
Regular	18	41	25 a 57
Buena	8	18	6 a 31

En cuanto al reconocimiento de los riesgos se observa en la tabla 3 que más del 80% (36 gerentes, para un 82% y un intervalo de confianza al 95% del 69% al 94%) dijo que no reconocen los riesgos a los que se exponen.

Tabla 3
Gerentes según reconocimiento
de los riesgos

Reconocimiento de los riesgos	No.	%	Límites del intervalo de confianza al 95%
Sí	8	18	6 a 31
No	36	82	69 a 94

Los resultados expresan que las PyMES comerciales estudiadas dentro del Cantón Santo Domingo cuentan con dificultades en todos los indicadores relacionados con la estructura básica de un CPD, lo cual establece una alerta a las áreas administrativas sobre la necesidad de tener un CPD que garantice un debido procesamiento interno, una correcta gestión y la capacidad en analizar prioridades dentro de las PyMES, para dotar a la empresa de una tecnología de protección de datos en función de desarrollar planes que conlleven al éxito en un mercado cambiante.

Lo anterior se confirma justamente desde la función esencial que cumple el CPD, que permite llevar un control diario de todo el proceso productivo de una empresa mediante el almacenamiento de la información que se genera, lo cual permite cada mes o año comparar el nivel de ingresos que tiene la empresa y poder detectar logros o posibles pérdidas y sobre esta base trazar estrategias deliberadas para asegurar un crecimiento constante. Pero si no se cuenta con una estructura adecuada de un CPD se podría perder la información, algo que afectaría en su desarrollo ocasionando un gran gasto por no invertir desde el inicio.

3.1. Resultados del estudio de caso

Las empresas que se tomaron en cuenta para esta comparación son un minimarket (A) y la otra es un almacén dedicado a la venta de equipamiento y materiales de construcción, ferreterías (B), cada una de ellas realiza un diferente tipo de actividad. La empresa (A) provee ventas de diferentes tipos de consumo es por ello que la información que se genera es de suma importancia, cuenta con el personal específico para al área de TIC´S lo que permite establecer las diferentes medidas de seguridad para la información, cabe recalcar que también cuenta con el espacio físico adecuado para el funcionamiento de un CPD. Por su parte la empresa (B) está empezando a tomar medidas de sobre la estructura de CPD, no cuenta con mucha seguridad en su estructura, no obstante, se pudo conocer que están haciendo cambios para mejorar esta situación.

El estudio de caso confirmó los resultados de las encuestas; se pudo conocer que los administradores de las empresas estudiadas conocían qué peligro corre la información y

confirmaron además que han sufrido su pérdida en reiteradas ocasiones, situación que les ha permitido tomar conciencia de lo fundamental que es tener una buena estructura básica de un CPD.

El estudio realizado a las empresas A y B encaminado a valorar cómo llevan el control de información, y el uso que le dan a la misma mediante la comparación entre ambas permitió conocer que la empresa B cuenta con un encargado del CPD por tiempo completo, sin embargo, su CPD no posee una estructura específica, como tampoco una seguridad de red y lógica, lo cual no garantizó la protección de datos e información. De igual modo no llevan un control de mantenimiento de las maquinas, sólo lo hacen si se da algún problema. El encargado del área de tecnologías de información y comunicación (TIC´S) mencionó que mediante una inversión se pudiera mejorar la estructura del CPD, lo que evidenció que el área administrativa no quiere invertir en este tipo de equipos dentro de la empresa, por lo que con frecuencia se producen pérdidas de información y se exponen al ingreso de hackers, situación que incide en que la empresa se ve imposibilitada para trazar sus planes perspectivos sobre bases sólidas.

La empresa A cuenta con una mayor protección al servidor, no tienen ningún inconveniente en guardar información de la empresa, el tipo de seguridades con que cuenta es la de encriptación de claves para resguardar su información. El encargado realiza un respaldo diario por medio de una base de datos y semanal por archivos. Su tecnología se renueva cada cinco años y se valora su CPD como bueno y funcional.

Los resultados encontrados confirman las ideas planteadas por Formorso (2012), quien establece que la estructura básica de un CPD debe contar con herramientas adecuadas para el monitoreo y la administración de la estructura que genera aplicaciones productivas y que detectan fallas a tiempo.

Se pudo conocer que la empresa A estableció una estructura de red en estrella, que hace más fácil administrar la información. Cuenta además con servidores donde se guarda la información correspondiente, para su seguridad lógica poseen un firewall que protege su red de cualquier intruso que quiera infiltrarse por medio de internet. Tienen ubicadas cámaras de red en puntos estratégicos, para cuidar la integridad de las áreas impidiendo el acceso de personas externas, además poseen una buena estructura de cable, en una se encuentran los de la red y en otra los eléctricos.

Esta empresa ha tomado en cuenta la necesidad de tener un detector de incendios, que es uno de los elementos de seguridad que no debe pasarse por alto ya que puede existir un corte circuito y poner en riesgo toda información. Para la protección del área de TIC´S cuentan con una seguridad biométrica para evitar que personas no autorizadas puedan ingresar a esta área, tienen un control de llaves de los gabinetes en el CPD y cuentan además con la implementación de un sistema eléctrico (UPS) que garantiza el suministro de electricidad después de un corte de luz.

Una situación diferente se apreció en la empresa B que con su nuevo personal de TIC´S solo tienen dos servidores. La empresa tiene lo justo y lo necesario para que el CPD esté funcionando; posee en la actualidad un servidor que es para la base de datos y otra para la facturación electrónica. No cuenta con un firewall lo cual deja en vulnerabilidad a la red. Llama la atención que sólo utilizan antivirus para los servidores y los correos electrónicos; tienen cámaras de seguridad, pero muy pocas, solo para el área de TIC´S, en cajas y parqueadero. Los cables de red eléctricos no tienen una buena estructura. El área de TIC´S no cuenta con una seguridad biométrica ya que sólo tienen una puerta con llaves; esta situación permite que cualquier persona tenga la facilidad de ingresar a esta área. Los gabinetes no están protegidos, no llevan el control de las llaves; no obstante, la empresa está tomando en cuenta las situaciones que se producen ante las suspensiones del fluido y están estableciendo el uso de UPS.

De acuerdo con lo expresado anteriormente cada empresa tiene sus principales métodos de protección, para que puedan generar un crecimiento diario y a largo plazo, de este modo poder establecer una estructura básica constituye una prioridad. Los encargados de TIC´S deben explicar el porqué es necesario comprar cada equipo, especificando el valor útil que va a tener en la empresa y así los gerentes podrán tomar las medidas adecuadas para que

no exista ninguna filtración de personas externas o perdida de información.

La comparación realizada permite advertir que la empresa que ha prestado atención al perfeccionamiento de la estructura de su CPD, cuenta con mayores logros económicos y perspectivas de desarrollo, mientras que la que presenta falencias tecnológicas se enfrenta a dificultades continuas que limitan su crecimiento sobre bases sólidas, no obstante, se advierte el reconocimiento por parte de la gerencia de la necesidad de perfeccionar su CPD.

4. Discusión

Diversos estudios (Martínez et al. 2009 Ordaz et al. 2012) investigan los enfoques de diferentes modelos implementados en empresas, con el objetivo de lograr una óptima seguridad de la información, a través del correcto manejo de procesos informáticos y recursos tecnológicos.

Autores como Medina et al. (2012) no dudan en que la productividad consigue una elevada incidencia con el empleo eficaz de la administración de la información y la calidad de la información, pues sus dos hipótesis trazadas son reconocidas en un nivel de confianza del 99%. Así también, es la variable con un mayor nivel de R2, o sea, que el 36.5% de los resultados son debido a la correlación entre las tres variables implicadas.

Con el objetivo de ofrecer un óptimo servicio e información a sus usuarios, proveedores, socios y terceros, quienes se favorecerían con una mayor organización, control y seguridad en sus inversiones, Posso y Barrios (2014) diseñan y aplican un Sistema de Control Interno como parte fundamental para el desarrollo de las actividades contables y financieras de la entidad.

Lepage (2014), autora de un modelo de gobierno de TI con enfoque de seguridad de información para empresas prestadoras de servicios de salud bajo la óptica de COBIT 5.0, para la Clínica Internacional, en Perú, concluye que dicho modelo permitió elaborar el *business case* que justificara la implementación del Gobierno de TI en la organización, así como mapear las fases del ciclo de vida del Gobierno de TI según COBIT 5.0 para la empresa, elaborar la declaración de aplicabilidad de COBIT 5.0 para el enfoque de Seguridad de la Información dentro de la empresa, elaborar las políticas de Gobierno de TI a aplicarse dentro de la empresa “TO-BE”, evaluar el estado de los procesos habilitadores, correspondientes a los enfoques de Gobierno de TI que aplican en la empresa, su evolución y nivel de madurez.

Arévalo et al. (2015) relatan la aplicación de un sistema de gestión de seguridad de información bajo la ISO 27001. Los autores llegan a la conclusión de que en Ocaña, Colombia, la red empresarial se halla altamente atomizada, y es la microempresa su base esencial, nueve de cada diez empresas son microempresas y, por ende, esta es la plataforma para la generación de riqueza y empleo. Por ende, las microempresas representan el 96% del total de las empresas, mientras que las empresas medianas y pequeñas representan 3% y 1%, respectivamente, contexto que manifiesta su concentración en sectores de medio y bajo contenido tecnológico. Esta situación debe evaluarse en el momento de precisar una política organizacional que tenga en cuenta un sistema de gestión de seguridad de información.

Por su parte, Salamanca (2016) subraya la significación del diseño de un sistema de gestión de seguridad de la información, asentado en los estándares ISO/IEC 27002:2013, NIST SP800-12 e ITILv3. El autor exhorta su empleo para cumplir con los elementos requeridos para aminorar las falencias en la entidad en función del crecimiento de la empresa. Los resultados manifiestan una real presencia de posibilidades para superar las dificultades que inciden negativamente sobre la seguridad de la red en las entidades, así también se constató la ausencia de buenas prácticas que promovían el riesgo de la información.

5. Conclusiones

La seguridad de los SGSI está representando un papel determinante en el desarrollo de las Pyme al ser predecesoras del mejoramiento de la administración de la información y la calidad de la información que resulta en su desempeño organizacional.

El análisis de riesgo a nivel empresarial resulta un óptimo instrumento para crear programas de contingencia y continuidad de la organización, gracias a que facilita a las entidades reducir el riesgo y avalar el rendimiento de los sistemas informáticos. Cabe destacar que resulta improbable eliminar un riesgo totalmente, lo que se puede realizar con el empleo de metodologías es disminuirlo para que no cree ningún daño representativo al sistema informático de la empresa.

El componente que mayormente puede ayudar al mantenimiento y desarrollo de la competitividad de la empresa es la gestión de la calidad, según las condiciones actuales, o sea, inmersa en un proceso de transformación y apertura comercial. Este contexto presume un refuerzo de las condiciones competitivas, sobre todo para las empresas más retrasadas en esfuerzos de calidad o en modernización tecnológica.

Cada entidad debe estipular sus principales mecanismos de protección, para que puedan formar un crecimiento diario y a largo plazo, de esta manera poder instituir una estructura básica que constituya una ventaja. Los profesionales a cargo del manejo de TIC´S deben exponer la causa de la necesidad de obtener cada equipo, detallando el valor útil que va a poseer en la organización, para que de esta manera los directivos puedan tomar las medidas apropiadas para que no se presente filtración alguna de individuos externos o pérdida de datos.

Referencias bibliográficas

Abril, A., Pulido, J. y Bohada, J. A. (2013). Análisis de riesgos en seguridad de la información. Revista Ciencia, Innovación y Tecnología (RCIYT), 1, 39-53.

Álvarez, D., Buonaffina, R. y Zabala, S. (2014). Tecnologías de la Información y las Comunicaciones (TIC) para el Desarrollo Organizacional de la Policía del Estado Nueva Esparta (Preparación para el Cambio). Revista ESPACIOS Vol. 35 (Nº 13). Recuperado de https://www.revistaespacios.com/a14v35n13/14351307.html

Arévalo, J. G., Bayona, R. A. y Rico, D. W. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información. Tecnura, 19(46), 123-134.

Burgos, J. y Campo, P. G. (2009). Modelo Para Seguridad de la Información en TIC. Concepción, Chile: Universidad del Bío-Bío.

Dávalos, A. F. (2013). Auditoría de seguridad de información. Fides Et Ratio, 6(6). Recuperado de http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2013000100004

Lepage, D. E. (2014). Diseño de un modelo de Gobierno de TI con enfoque de seguridad de información para empresas prestadoras de servicios de salud bajo la óptica de COBIT 5.0 (tesis de grado). Pontificia Universidad Católica del Perú, Lima, Perú.

Martelo, R. J., Madera, J. E. y Betín, A. D. (2015). Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI). Información Tecnológica, 26(2), 129-134.

Martínez, K. J., Pacheco, J. y Zúñiga, I. (2009). Firewall – Linux: Una Solución De Seguridad Informática Para Pymes (Pequeñas Y Medianas Empresas). Revista UIS Ingenierías, 8(2), 155-165.

Medina, J. M, Lavín, J. y Pedraza, N. A. (2012). Seguridad en la administración y calidad de los datos de un sistema de información contable en el desempeño organizacional. Contaduría y Administración, 57(4), 11-34.

ORDAZ J., BENIGNI G., GERVASI O. y HORMAZABAL E. (2012) Openvas + Wireshark: Vulnerabilidad + Captura de Tráfico. *Revista Espacios*. Vol. 33 (Nº 2) Pág. 11. Recuperado de: http://www.revistaespacios.com/a12v33n02/12330261.html

Posso, J. y Barrios, M. (2014). Diseño de un modelo de control interno en la empresa prestadora de servicios hoteleros eco turísticos nativos activos Eco Hotel La Cocotera, que permitirá el mejoramiento de la información financiera (tesis de grado). Universidad de Cartagena, Cartagena de Indias, Colombia.

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.

---

1. Magíster en Educación Superior. Docente de la carrera de Sistemas de la Universidad Regional Autónoma de los Andes (UNIANDES). Santo Domingo. Email: us.silviomachuca@uniandes.edu.ec

2. Ingeniera en Sistemas. Graduada de la carrera de Sistemas de la Universidad Regional Autónoma de los Andes (UNIANDES). Santo Domingo. Email: ss.ingridparraga@uniandes.edu.ec

3. Magister en Ingeniería y Sistemas de Computación. Docente de la carrera de Sistemas de la Universidad Regional Autónoma de los Andes (UNIANDES). Santo Domingo. Email: us.rcarlossampedro@uniandes.edu.ec

4. Magister en Ingeniería y Sistemas de Computación. Docente de la carrera de Sistemas de la Universidad Regional Autónoma de los Andes (UNIANDES). Santo Domingo. Email: us.robertlalama@uniandes.edu.ec

---

Revista ESPACIOS. ISSN 0798 1015
Vol. 40 (Nº 28) Año 2019

[Índice]