UNIVERSIDAD Rafael Belloso Chacín

Revista Electrónica de Estudios Telemáticos

TÉLÉMATIQUE

Sistema de gestión de seguridad en la red de área local para la Institución Educativa La Gloria, Departamento de La Guajira, Colombia

(Security management system in the local area network for La Gloria Educational Institution, Department of La Guajira, Colombia)

Dilia Bolaños
Universidad de la Guajira
dilianbol0811@hotmail.com

RESUMEN

El objetivo general de la investigación fue proponer un sistema de gestión de seguridad en la red de área local para la Institución Educativa La Gloria, departamento de La Guajira, Colombia. El análisis de la variable sistema de gestión de seguridad en la Red de Área Local (LAN) se sustentó en los criterios teóricos de Aguirre (2014), Castro (2015), entre otros. Desde el punto de vista metodológico, el estudio se desarrolló como una investigación centrada en el tipo denominado proyecto factible y de orden descriptivo, con un diseño no experimental, trasversal. Para la recolección de información se utilizó la técnica de encuesta para el primer objetivo de la investigación. En cuanto al instrumento se aplicó un cuestionario estructurado constituido por treinta (30) ítems, con cinco alternativas de respuestas; el mismo fue sometido a un proceso de confiabilidad mediante la aplicación de la fórmula Alfa de Cronbach, arrojando un resultado 0,912, considerándose altamente confiable para su aplicación. Asimismo, el instrumento fue sujeto a una validación mediante el juicio de cinco (5) expertos. De acuerdo con los resultados obtenidos, se evidenció la existencia de debilidades en el sistema de gestión de seguridad en la red LAN de la organización estudiada, referente al desaprovechamiento de algunos enlaces y conexiones en la infraestructura de la red actual. En consecuencia, se presentó el diseño de una propuesta orientada a fortalecer la competitividad, interoperabilidad y flexibilidad de las redes LAN, que permita brindar al usuario servicios de calidad, de manera que se mantenga actualizado en todo momento la dinámica del sistema de seguridad, pues dichas redes suelen ser sometidas a cambios constantes, propios del desarrollo tecnológico.

Palabras Claves: Gestión, Sistema, Seguridad, Red

ABSTRACT

The general objective of the research was to propose a security management system in the local area network for the La Gloria Educational Institution, Department of La Guajira, Colombia. The analysis of the variable security management system in LAN networks was based on the theoretical criteria of Aguirre, D. (2014), Castro, V. (2015), among others. From a methodological point of

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 17 Edición No 1 – Año 2018

view, the study was developed as an investigation focused on the type called feasible project and of a descriptive order, with a non-experimental, transversal design. For the collection of information, the survey technique was used for the first objective of the investigation. Regarding the instrument, a structured questionnaire consisting of thirty (30) items was applied, with five alternative responses; it was subjected to a reliability process by applying Cronbach's Alpha formula, yielding a result of 0.912, considering it highly reliable for its application. Likewise, the instrument was subject to validation through the judgment of five (5) experts. According to the results obtained, the existence of weaknesses in the security management system in the LAN network of the studied organization was evidenced, referring to the waste of some links and connections in the current network infrastructure. Consequently, the design of a proposal aimed at strengthening the competitiveness, interoperability and flexibility of LAN networks was presented, allowing the user to provide quality services, so that the dynamics of the security system are kept updated at all times, since These networks are usually subject to constant changes, typical of technological development.

Keywords: Management, System, Security, Network

INTRODUCCIÓN

En los últimos años, las redes de área local o local area network (LAN) constituyen uno de los avances informáticos más importantes, ya que permiten compartir recursos físicos o lógicos a los usuarios de un área determinada, como puede ser un centro de trabajo; razón por la cual, las instituciones a nivel mundial que contaban con una infraestructura informática, primero implementaban redes de área local donde los usuarios dentro de una misma localidad podían compartir documentos informáticos entre computadores. En este sentido, al utilizar las redes de área local se hace más fácil la gestión y seguridad de los equipos interconectados entre sí.

Resulta oportuno indicar que en países latinoamericanos como Chile, Brasil, Argentina y México, que se consideraban vanguardistas en este tema, las telecomunicaciones se realizaban principalmente desde entornos académicos, a través de las universidades e institutos de investigación, para luego incursionar en el mercado, tanto residencial como empresarial, englobando poco a poco los demás países del continente. De allí que, hoy día, los procesos dentro de las empresas dependan en gran parte de la informática y las telecomunicaciones.

Es preciso destacar, que dentro de una red LAN los problemas se presentan por el cableado y los conectores que enlazan las componentes de la red. Los medios físicos más utilizados son el cable de par trenzado, cable coaxial, fibra óptica, par de cables por su duración y mantenimiento, ya que siguiendo normas pueden influir en la seguridad de la red. De allí, la gran importancia de tener en consideración que para el buen funcionamiento de dichas redes, se deben establecer ciertas medidas de seguridad que no son más que los lineamientos establecidos para control de la vulnerabilidad de las redes.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 17 Edición No 1 – Año 2018

A este respecto, las prevenciones están preestablecidas en el mundo por lo cual se utilizan de igual forma en todas las redes, no solo para proteger la información, sino también para agilizar la productividad, protegiendo así, tanto los equipos como los componentes lógicos, contra daños y alteraciones en la configuración de los mismos, que pudieran ser accidentales o intencionales, proveniente de agentes externos así como agentes internos. En este sentido, Delgado (2014) indica que la seguridad debe estar orientada a mecanismos estrictos que deben ser aplicados en la infraestructura tecnológica preparando la misma; el hecho de que no esté preparada implica vulnerabilidad tecnológica y amenazas de inseguridad, lo cual, impide determinar los niveles de seguridad en sus redes y establecer las políticas que garanticen la confiabilidad e integridad de la información.

De lo anterior se desprende que, para el buen funcionamiento de las redes, se deben establecer ciertas medidas de seguridad, que no son más que los lineamientos establecidos para controlar la vulnerabilidad de las mismas. En el caso del Departamento de Informática de la Institución Educativa La Gloria, departamento de La Guajira (Colombia), se pudo conocer que constantemente surgen complicaciones con el funcionamiento de la red, entre las cuales se mencionaron insuficiente control de acceso, mal manejo de la red, poca capacidad de almacenamiento de la información y la lentitud en cuanto a la velocidad de procesamiento de la información, que incide negativamente en su correcto funcionamiento.

De la misma manera, los informantes manifestaron que dentro de la institución existe falta de conocimiento para el manejo y control de la información, ya que los administradores de la red poseen debilidades que se deben a diversos factores; por una parte no están familiarizados con los mecanismos de seguridad que se encuentran en el sistema, y por otra, el acceso de personas no autorizadas al sistema genera descontrol, lo cual trae como consecuencias que se puedan ver afectadas las operaciones en ella.

Asimismo, los sujetos entrevistados mencionaron que es necesario analizar las políticas de seguridad, las cuales deberían estar acordes con las actividades de la entidad; a su vez, en la estructura no se puede identificar con exactitud la seguridad o inseguridad de la plataforma por su incapacidad para detectar fallas, así como sus vulnerabilidades y las posibles amenazas de seguridad; todo esto obedece a que la red no se encuentra segmentada adecuadamente y por ende cada área no cuenta con las medidas de resguardo de la información.

Tomando en consideración lo anteriormente planteado, se puede establecer que de continuar presentándose esta situación dentro de la institución educativa objeto de estudio, donde la accesibilidad a la red se establece sin llevar un control adecuado de los elementos de seguridad que atenúen las vulnerabilidades existentes en cuanto al acceso no autorizado, podrían sobrevenir incidentes que pudieran afectar la infraestructura informática en relación con sus recursos, total o parcialmente, trayendo como consecuencia que se irrumpa directamente cada una de las operaciones de la entidad que dependen de dichas actividades.

Finalmente, se puede mencionar que de continuar la ausencia de medidas de seguridad, la red seguiría expuesta al hurto de información por parte de los usuarios no autorizados, lo que pudiera derivar en resultados inadecuados por el mal uso de

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 17 Edición No 1 – Año 2018

la misma; por lo tanto, sería difícil determinar y establecer políticas que garanticen la confiabilidad e integridad de la información.

OBJETIVO

Proponer un Sistema de Gestión de Seguridad en la Red de Área Local para la Institución Educativa La Gloria, departamento de la Guajira, Colombia.

METODOLOGÍA

La presente investigación se considera de tipo descriptivo con base en la teoría de Hernández, Fernández y Baptista (2014), ya que su propósito fue recolectar información directamente de las personas, abarcando los elementos claves para finalmente proponer un sistema de gestión de seguridad en la red de área local para la Institución Educativa La Gloria, en el departamento de La Guajira, Colombia. Así mismo, la presente investigación se enmarca dentro del tipo proyecto factible, dado que se pretende elaborar una propuesta para dar solución a la problemática de la Institución Educativa La Gloria. Según UPEL (2016) éste tipo de estudio "consiste en la investigación, elaboración y desarrollo de una propuesta de un modelo operativo viable para solucionar problemas, requerimientos o necesidades de organizaciones o grupos sociales.

Con relación al diseño de la investigación, en este estudio se hizo referencia al planteamiento de una serie de actividades sucesivas y organizadas, las cuales debieron adaptarse a las particularidades de la investigación; las mismas indicaron los pasos y pruebas aplicadas, así como las técnicas utilizadas para recolectar y analizar los datos que se recogieron directamente en el lugar de los hechos Landeau (2012), es decir, en la Institución Educativa La Gloria, en el departamento de La Guajira colombiana. Bajo este esquema de trabajo se materializaron los objetivos específicos de la investigación, cabe decir, mediante la realización de las actividades que permitieron recolectar los datos requeridos directamente de la fuente primaria representada por la ya mencionada Institución.

De igual manera, el presente trabajo se ubica dentro del diseño no experimental, por cuanto se centró en proponer un sistema de gestión de seguridad en la red de área local para la Institución Educativa La Gloria, describiendo y analizando sus características, sin ejercer manipulación alguna sobre las variables. Asimismo, esta investigación se ubica dentro del tipo transversal o transeccional, debido a que la información se recolectó en un momento único, lo cual permitió obtenerla directamente (Hernández et al., 2014).

Con respecto a la población, esta estuvo conformada por cinco (5) personas que laboran en las áreas de tecnología y que dan soporte a toda la infraestructura tecnológica de la Institución Educativa La Gloria quienes son los únicos sujetos que manejan la información en la parte de informática y tecnológica. Para efectos de esta investigación, el número de unidades informantes se consideró por su cantidad como finita, y por su función como accesible al presente estudio.

Para realizar el análisis de los resultados obtenidos a través de las respuestas arrojadas por el cuestionario aplicado, se diseñó un baremo que facilitó la

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 17 Edición No 1 – Año 2018

interpretación y comparación de la información tabulada con los rangos de medición, para determinar el nivel de cumplimiento de los cinco (5) sujetos que conformaron la población; también su clasificación o categorización. Al respecto, Hernández et al. (2014) definen el termino medición como el proceso de vincular conceptos abstractos con indicadores empíricos, el cual se realiza mediante un plan explícito y organizado para clasificar (y con frecuencia cuantificar) los datos disponibles (los indicadores), en términos del concepto que el investigador tenga en mente.

Es preciso indicar, que el instrumento aplicado dio respuesta al primer objetivo de la investigación, es decir, fue el punto de partida de la misma ya que permitió determinar las necesidades de la institución y con base en esa información, establecer parámetros para realizar la posterior propuesta de un diseño para el sistema de gestión de seguridad de la Institución Educativa La Gloria, departamento de La Guajira, Colombia.

Cabe destacar, que la validez del instrumento se obtuvo mediante el proceso de validación de contenido, el cual consistió en la evaluación del instrumento por parte de cinco (5) expertos en el área, que reunieron las condiciones para valorarlo equilibradamente. Para ello se les facilitó un ejemplar del cuestionario, el cuadro de operacionalización de la variable y un formato para evaluar el contenido; también se suministró la tabla de construcción de ítems del cuestionario a ser aplicado a los profesionales en informática, redes y telemática relacionados con el sistema de gestión de seguridad en la red de área local para la Institución Educativa La Gloria, La Guajira, Colombia".

Para el análisis e interpretación la información recolectada a través de la aplicación del instrumento, se estimó conveniente la categorización y la tabulación de los datos mediante el uso de frecuencias estadísticas descriptivas. Se efectuó el análisis en función de los resultados obtenidos a través del instrumento de investigación elaborado con la matriz de la variable y a través de una hoja de cálculo de Microsoft Office Excel y el cual fue aplicado a la población del estudio constituida por los profesionales en informática, redes y telemática relacionados con el sistema de gestión de seguridad en la red de área local para la Institución Educativa La Gloria, La Guajira, Colombia.

RESULTADOS

Con la finalidad de analizar los resultados obtenidos, se utilizó la estadística descriptiva para la primera fase de la investigación donde se determinó la moda, mediana y media aritmética de los datos agrupados por cada indicador; asimismo, para determinar la tendencia del comportamiento de dichos indicadores, se calculó la dispersión de los datos mediante la desviación estándar.

Por último, los resultados se compararon con las bases teóricas para detectar las coincidencias y contradicciones entre la información obtenida y la postura de los teóricos, de manera que se pueda cumplir con los objetivos planteados en la investigación. Los cálculos estadísticos se presentaron considerando la variable Sistema de Gestión de Seguridad, con sus dimensiones e indicadores, los cuales quedaron evidenciados de forma detallada en tablas.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 17 Edición No 1 – Año 2018

Situación actual en la red local de la Institución Educativa La Gloria en el departamento de La Guajira, Colombia

Tabla 1
Indicador: Estructura Organizacional

Ítems	Alternativas de respuestas												Promedio de Ponderación (MEDIA)
	SIEMPRE		CASI SIEMPRE		ALGUNAS VECES		CASI NUNCA		NUNCA		TOTAL		
	Fa	Fr	Fa	Fr	Fa	Fr	Fa	Fr	Fa	Fr	Fa	Fr	
1. La institución define la responsabilidad del personal de acuerdo a sus funciones.	0	0,00	1	20,00	3	60,00	1	20,00	0	0,00	5	100,00	3,00
2. La institución distribuye las tareas que hay que hacer.	0	0,00	2	40,00	3	60,00	0	0,00	0	0,00	5	100,00	3,40
3. La institución cuenta con una estructura organizacional en pro de laborar con eficiencia en los diferentes departamentos de trabajo.	0	0,00	1	20,00	3	60,00	1	20,00	0	0,00	5	100,00	3,00
Total	0	0,00	4	80,00	9	180,00	2	40,00	0	0,00	15	100,00	9,40
Tendencia	0	0,00	1	26,67	3	60,00	1	13,33	0	0,00	5	100,00	3,13
Media: 3,13													

Fuente: Elaboración propia (2016)

De acuerdo con la tabla 1, se reflejan los resultados para el indicador estructura organizacional, donde 60,00% de los sujetos consultados manifestaron que algunas veces la institución define la responsabilidad del personal de acuerdo a sus funciones. Seguidamente, 26,67% expresaron casi siempre cuenta con una estructura organizacional en pro de laborar con eficiencia en los diferentes departamentos de trabajo, 9,63% casi nunca. Mientras que siempre y nunca no tuvieron respuesta.

A este respecto, la investigadora considera que la estructura organizacional la tienen presente y definida donde se evidencia que la institución distribuye las tareas que hay que realizar en el caso particular en la Institución Educativa La Gloria, en el departamento de La Guajira, Colombia, según las funciones que cada departamento o áreas donde están asignadas las responsabilidades junto con la definición de los cargos de los empleados.

Los resultados arrojaron un valor de media de 3,13, que corresponde a la categoría moderada, lo cual indica, que las evidencias encontradas medianamente presentan similitud con la teoría expuesta por Delgado (2014) en este paso se definen quienes serán los responsables, cuales tareas hay que hacer, quien las hace, como se agrupan, quien rinde cuentas a quien y donde se forman las decisiones, por lo cual puede afirmarse, que es la distribución formal de los empleados dentro de una organización como las tareas puedan distribuirse tanto con eficacia, como eficiencia entre los diferentes departamentos de trabajo.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 17 Edición No 1 – Año 2018

Tabla 2
Indicador: Políticas de Seguridad

Ítems	Alternativas de respuestas												Promedio de Ponderación (MEDIA)
	SIEMPRE		CASI SIEMPRE		ALGUNAS VECES		CASI NUNCA		NUNCA		TOTAL		
	Fa	Fr	Fa	Fr	Fa	Fr	Fa	Fr	Fa	Fr	Fa	Fr	
4. Las políticas de seguridad comprenden un conjunto de objetivos para la institución.	0	0,00	0	0,00	5	100,00	0	0,00	0	0,00	5	100,00	3,00
5. La institución establece políticas de seguridad en la redes LAN.	0	0,00	0	0,00	4	80,00	1	20,00	0	0,00	5	100,00	2,80
6. Se implementan reglas de comportamiento de usuarios en la institución, como requerimiento para la gestión de Sistema garantizando la seguridad en las redes.	0	0,00	0	0,00	2	40,00	3	60,00	0	0,00	5	100,00	2,40
Total	0	0,00	0	0,00	11	220,00	4	80,00	0	0,00	15	100,00	8,20
Media	0,00	0,00	0,00	0,00	3,67	73,33	1,33	26,67	0,00	0,00	5	100,00	2,73
Media: 2,73													

Fuente: Elaboración propia (2016)

Seguidamente, en la tabla 2, se evidencia que 73,33% de los encuestados, manifestaron que algunas veces Las políticas de seguridad comprenden un conjunto de objetivos para la institución. Estos fueron apoyados por 26,67% quienes indicaron que casi nunca la institución establece políticas de seguridad en la redes LAN. Mientras casi siempre, nunca y siempre no tuvieron ponderación.

A este respecto, la investigadora infiere --según los resultados arrojados-- que las políticas de seguridad son de gran relevancia dentro de cualquier institución toda vez que las mismas resguardan la información de dicho organismo, en este caso de estudio en la Institución Educativa La Gloria, del Departamento de la Guajira en Colombia. Es preciso mencionar, que se presentan situaciones donde no se implementan reglas de comportamiento de usuarios en la institución como requerimiento para la gestión de sistema, lo que trae como consecuencia que no se garantiza la seguridad en las redes, evidenciándose debilidad en este sentido.

Ahora bien, los resultados obtenidos arrojaron un valor para la media de 2,73, correspondiente a la categoría moderada de acuerdo al baremo de interpretación de la media. Estos resultados muestran mediana concordancia con la teoría expuesta por Delgado (2014), quien afirma que las políticas de seguridad comprenden un conjunto de objetivos para la institución; son reglas de comportamiento de usuarios y administradores, así como requerimientos para la gestión de sistemas que garanticen la seguridad en redes de forma colectiva.

Tabla 3
Indicador: Confiabilidad

Ítems	Alternativas de respuestas					Promedio de Ponderación (MEDIA)
	SIEMPRE	CASI SIEMPRE	ALGUNAS VECES	CASI NUNCA	NUNCA	TOTAL

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 17 Edición No 1 – Año 2018

	Fa	Fr	Fa	Fr	Fa	Fr	Fa	Fr	Fa	Fr	Fa	Fr	
7. La institución dentro de sus premisas, para el acceso a los datos establece que solo pueden ingresar el personal autorizado.	0	0,00	1	20,00	1	20,00	3	60,00	0	0,00	5	100,00	2,60
8. La institución diseña planes de seguridad en la red, en base a la confiabilidad de la misma.	0	0,00	0	0,00	2	40,00	3	60,00	0	0,00	5	100,00	2,40
9. La institución aplica normativas protegiendo de accesos no permitidos.	0	0,00	1	20,00	1	20,00	3	60,00	0	0,00	5	100,00	2,60
Total	0	0,00	2	40,00	4	80,00	9	180,00	0	0,00	15	100,00	7,60
Tendencia	0,00	0,00	0,67	13,33	1,33	26,67	3,00	60,00	0,00	0,00	5	100,00	2,53
Media: 2,53													

Fuente: Elaboración propia (2016)

Para el indicador confiabilidad, en la tabla 3 se observó que 60,00% de los entrevistados comentaron que la institución casi nunca establece dentro de sus premisas para el acceso a los datos, que solo puede ingresar el personal autorizado. Seguidamente, el 26,67% mencionaron que algunas veces diseñan planes de seguridad en la red, con base en la confiabilidad de la misma. Y el 13,33% expresó que casi siempre se aplican normativas protegiendo de accesos no permitidos. Mientras que siempre y nunca no tuvieron respuestas.

A este respecto, la investigadora considera que dentro de la Institución Educativa La Gloria, se observa una debilidad con relación a la confiabilidad, producto de no tener reglas ni políticas de seguridad, toda vez que no establecen como norma que solo puede ingresar el personal autorizado para el acceso a los datos, situación por la cual el sistema de seguridad es vulnerado. La media para este indicador arrojó un valor de 2,53, indicando poca presencia de confiabilidad, lo cual difiere con lo expresado por los autores Barker y Morris (2013), la confiabilidad solo autoriza a individuos/sistemas los cuales pueden ver información confidencial o clasificada. De igual manera, también implica que las personas no autorizadas no deben tener ningún tipo de acceso a los datos.

Tabla 4
Indicador: Integridad

Ítems	**Alternativas de respuestas**												**Promedio de Ponderación (MEDIA)**
	SIEMPRE		**CASI SIEMPRE**		**ALGUNAS VECES**		**CASI NUNCA**		**NUNCA**		**TOTAL**		
	Fa	Fr	Fa	Fr	Fa	Fr	Fa	Fr	Fa	Fr	Fa	Fr	
10. La institución tiene como objetivo evitar alteraciones de los datos de la red.	0	0,00	1	20,00	3	60,00	1	20,00	0	0,00	5	100,00	3,00
11. La institución realiza auditorias que permita detectar si los datos han perdido su integridad.	0	0,00	1	20,00	0	0,00	4	80,00	0	0,00	5	100,00	2,40

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 17 Edición No 1 – Año 2018

12. Dentro de la institución, los usuarios cuentan con el conocimiento para operar los mecanismos que aseguren la integridad de los datos.	0	0,00	0	0,00	2	40,00	3	60,00	0	0,00	5	100,00	2,40
Total	0	0,00	2	40,00	5	100,00	8	160,00	0	0,00	15	100,00	7,80
Media	0,00	0,00	0,67	13,33	1,67	33,33	2,67	53,33	0,00	0,00	5	100,00	2,60
Media: 2,60													

Fuente: Elaboración propia (2016)

Para el indicador integridad, en la tabla 4 se observó que 53,33% de los entrevistados comentaron que casi nunca la institución realiza auditorias que permitan detectar si los datos han perdido su integridad. Seguidamente, el 33,33% mencionó que algunas veces la institución tiene como objetivo evitar alteraciones de los datos de la red., 13,33% expresó que casi siempre se da. Las alternativas siempre y nunca no tuvieron ponderación porcentual.

Para la investigadora, según los resultados arrojados, la integridad está amenazada de cualquier riesgo de pérdida de información, dado que los usuarios no cuentan con el conocimiento para operar los mecanismos que aseguren la integridad de los datos. Por ello, es preciso realizar periódicamente auditorías al sistema a fin de proteger todos los datos allí guardados, que son de vital importancia para la Institución Educativa La Gloria ubicada en el Departamento de La Guajira, Colombia.

La media para este indicador arrojó un valor de 2,60, indicando poca presencia del mismo, este resultado difiere con lo expresado por Aguirre y Palacios (2014) la integridad tiene como objetivo evitar la alteración de los datos sin que sea detectado, por lo cual, no se puede modificar la información excepto con las credenciales apropiadas, en este caso se refiere a la legitimidad de modificar la información, por lo que debe haber un registro o log que permita auditar tales cambios.

Tabla 5
Indicador: Disponibilidad de activos

Ítems	**Alternativas de respuestas**												**Promedio de Ponderación (MEDIA)**
	SIEMPRE		**CASI SIEMPRE**		**ALGUNAS VECES**		**CASI NUNCA**		**NUNCA**		**TOTAL**		
	Fa	Fr	Fa	Fr	Fa	Fr	Fa	Fr	Fa	Fr	Fa	Fr	
13. La institución asegura los activos identificándolos para una mejor disponibilidad.	0	0,00	0	0,00	1	20,00	4	80,00	0	0,00	5	100,00	2,20
14. La institución garantiza la disponibilidad de los activos en caso de presentarse alguna contingencia.	0	0,00	0	0,00	4	80,00	0	0,00	1	20,00	5	100,00	2,60
15. Se resguarda una copia de seguridad de los archivos existentes en otro sitio fuera de las premisas de la institución.	0	0,00	0	0,00	3	60,00	2	40,00	0	0,00	5	100,00	2,60

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 17 Edición No 1 – Año 2018

	Total	0	0,00	0	0,00	8	160,00	6	120,00	1	20,00	15	100,00	7,40
	Tendencia	0	0,00	0	0,00	3	53,33	2	40,00	0	6,67	5	100,00	2,47
							Media: 2,47							

Fuente: Propia (2016)

En la tabla 5, se muestran los resultados en función del indicador disponibilidad de los activos, donde se observó que los sujetos entrevistados manifestaron que algunas veces la institución garantiza la disponibilidad de los activos en caso de presentarse alguna contingencia con un 53,33%, mientras el 40,00% respondieron casi nunca la institución asegura los activos identificándolos para una mejor disponibilidad., por su parte dijeron nunca se resguarda una copia de seguridad de los archivos existentes en otro sitio fuera de las premisas de la institución con un porcentaje fue de 6,67%, siempre y nunca no tuvo respuesta.

Ante los resultados arrojados la investigadora infiere que la disponibilidad de los activos está en peligro en la institución educativa La Gloria del municipio Manaure del Departamento de La Guajira – Colombia, debido a que no se encuentran disponibles al momento de necesitarlos, así como tampoco están identificados para su posterior utilización, trayendo como consecuencia que se vulnere la información, la cual es vital en un sistema de seguridad.

Estos resultados arrojaron una media de 2,47 lo que refleja poca presencia en el manejo del indicador referido. Lo cual discrepa del planteamiento de Aguirre y Palacios (2014) indica que el primer paso para asegurar los activos es clasificarlos, además de identificarlos y los mismos se encuentren reconocidos, debido a que la presencia de los activos facilita el funcionamiento de la empresa u organización y la consecución de sus objetivos. Al hacer un estudio de los activos existentes hay que tener en cuenta la relación que guardan entre ellos y la influencia que se ejercen; cómo afectaría en uno de ellos un daño ocurrido a otro.

Tabla 6
Dimensión: Situación actual

Alternativas de respuestas													
Indicadores	**SIEMPRE**		**CASI SIEMPRE**		**ALGUNAS VECES**		**CASI NUNCA**		**NUNCA**		**TOTAL**		**Promedio de Ponderación de la Media**
	Fa	Fr	Fa	Fr	Fa	Fr	Fa	Fr	Fa	Fr	Fa	Fr	
Estructura Organizativa	0	0,00	1	26,67	3	60,00	1	13,33	0	0,00	5	100	3,13
Políticas de Seguridad	0	0,00	0	0,00	4	73,33	1	26,67	0	0,00	5	100	2,73
Confiabilidad	0	0,00	1	13,33	1	26,67	3	60,00	0	0,00	5	100	2,53
Integridad	0	0,00	1	13,33	2	33,33	3	53,33	0	0,00	5	100	2,60
Disponibilidad de los activos	0	0,00	0	0,00	3	53,33	2	40,00	0	6,67	5	100	2,47
TOTAL	0	0,00	3	53,33	10	193,33	8	153,33	0	0,00	20	400	11,00
Tendencia	0	0,00	1	13,33	2	48,33	2	38,33	0	0,00	5	100	2,75

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 17 Edición No 1 – Año 2018

Media: 2,75

Fuente: Elaboración propia (2016)

Ahora bien, en la tabla 6 se observan los promedios generales para los indicadores que conforman la dimensión Situación actual, donde el valor de media para la misma fue de 2,75 indicando estar moderadamente presente, con tendencia a poco presente, de acuerdo con el baremo de interpretación de la media propuesta. Ante los resultados obtenidos, se infiere que la situación actual con respecto al sistema de seguridad, debe desarrollar políticas de seguridad que les garantice confiabilidad e integridad de la información, en virtud de que los mismos no tienen políticas ni normas que les obligue a proteger la información en las redes.

Así mismo tiende a destacarse la estructura organizacional donde se tienen fijadas las responsabilidades de cada cargo y las funciones que deben cumplir, en cuanto a las políticas de seguridad se ubicó en 2,73 de promedio de la media. De igual manera se encuentra con menor valoración la integridad con 2,60, la confiabilidad en 2,53 y la disponibilidad con 2,47 encontrándose los últimos tres indicadores no presente según el baremo de la media, dentro del sistema de seguridad de la institución educativa, razón por la cual debe proponerse un sistema de gestión de seguridad.

Este resultado difiere medianamente con lo planteado por Castro (2015) señalan que hay dos partes en un sistema de gestión de seguridad informática; la primera parte, la seguridad de la información, la cual puede ser definida como una preservación de la confidencialidad, integridad, disponibilidad de los activos de información; y la otra son los sistemas de gestión, que son las actividades coordinadas para gobernar y controlar una organización.

Por otra parte, con respecto a la situación actual, estos resultados están concordancia con Delgado (2014), quien sostiene que los procedimientos y tecnologías que se establezcan en la organización, implican por lo general los siguientes tres conceptos básicos: Confidencialidad, Integridad y Disponibilidad (CID), proporcionando una protección adecuada de los recursos de red. De acuerdo con los resultados, se pudo evidenciar la existencia de un serio problema de seguridad en las redes de la institución universitaria de estudio, desde el punto de vista organizacional, políticas, normas y procedimientos. Así mismo, que no se tiene sistemas de control de registro de los usuarios.

Requerimientos funcionales dentro de la gestión de la red del área local para la Institución Educativa La Gloria, municipio Manaure del Departamento de La Guajira – Colombia

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 los 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; en consecuencia, el conocimiento de cada área de trabajo permite revisar periódicamente los registros o logs del sistema para determinar el grado de utilización de los servicios por parte de usuarios y

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 17 Edición No 1 – Año 2018

operadores autorizados, alertas sobre fallas del sistemas. Existen diversos tipos de activos descritos por un conjunto de elementos que determinan sus características propias, tal como se muestra en el cuadro; toda esta información se estructura con base en la observación directa realizada por el investigador.

Cuadro 1
Tipos de activo

Tipos de activos	Descripción
Datos/información	Bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, disposiciones relativas a sistemas de emergencia para la reposición de información pérdida. Software o aplicación.
Software o aplicación	Software de aplicación, software de sistemas, herramientas de desarrollo y sistemas de información, aplicaciones de servidores entre otros.
Hardware	Equipos de oficina (PC, portátiles, video Beam, impresoras, servidores, dispositivos móviles, entre otros).
Red	Dispositivos de conectividad de redes (router, swicth, concentradores, entre otros), red local, internet, red telefónica
Instalación	Cableado estructurado, instalaciones eléctricas.
Personal	Personal informático (administradores, webmaster, desarrolladores, entre otros), usuarios finales y personal técnico.

Fuente: Elaboración propia (2016)

De acuerdo con el contenido del cuadro anterior, cada activo mantiene su privacidad mediante la aplicación de medidas de seguridad que eviten la captura, apropiación y divulgación de los mismos, por y hacia entes externos a la organización. Cada usuario de la red LAN, debe ser responsable de resguardar la privacidad de su contraseña para evitar comprometer la vulnerabilidad de otras cuentas y recursos.

De hecho, ante cualquier situación irregular se debe identificar la fuente de amenazas, acerca de los intrusos que irrumpen en la red, incluyendo la intervención de usuarios internos en la captura y apropiación indebida de la información resguardada en la red. En este caso, es necesaria la elaboración de planes de contingencia y seguridad de una red LAN, para involucrar o concienciar a todos los usuarios y administradores de sistemas en los temas de seguridad e implicaciones legales del uso de la misma.

Según Carrasquero y Pérez (2016), 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. Por otro lado, reducir los riesgos de error humano, robo, fraude y utilización abusiva de

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 17 Edición No 1 – Año 2018

los equipamientos. Desde la vinculación del personal, se deben tener controles que permitan verificar la idoneidad e identidad, ética profesional y conducta. Los términos y condiciones de trabajo deben establecer la responsabilidad del personal, por la seguridad de los activos de información, que van más allá de la finalización de la relación laboral o contractual, por lo que se debe firmar un acuerdo de confidencialidad que tengan acceso a la información.

A su vez, indican que dentro de este contexto la valoración de los riesgos ayuda a focalizarlos derechos de acceso del usuario, sean debidamente solicitados y aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. Por lo cual, las identidades del usuario y los derechos de acceso se mantienen en un repositorio de datos centralizados. Por ende, se logra la autenticación y habilitación a los derechos de acceso. En el cuadro siguiente se muestran los niveles de riesgo en los que incurre cada activo. Para esto se tiene en cuenta el nivel de importancia asignado a cada uno y los factores de riesgo asociados.

Cuadro 2:
Identificación de Riesgos

Causas	Riesgo	Descripción	Consecuencias Potenciales
Equipos insuficientes y algunos obsoletos.	Incumplimiento en la generación de respuestas a los usuarios	No se generan las respuestas dentro de los términos legales	Sanciones Demandas.
No se realizan las actualizaciones de hardware y software.			
Proceso manual, que puede generar registros erróneos o falta de registros, Información desactualizada			
Desconocimiento de la normatividad Aplicada, Resistencia al Cambio, Desmotivación.	Generación de respuestas inadecuadas o erróneas a los usuarios.	Respuestas sin la competencia técnica o no acorde a lo requerido.	Pérdida de imagen y alto Nivel de quejas por parte de los Fallas en el usuarios
Fallas en el usuario seguimiento a los procedimientos del proceso.			

Fuente: Barker y Morris (2013)

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. (Carrasquero, E. Pérez, L.2016

Cabe resaltar, que la selección y luego la implementación de controles de seguridad debe ser enfocada a la protección de los activos señalados en el cuadro, a objeto de garantizar la política de seguridad de la organización con respecto a la gestión del sistema de redes LAN. Al respecto, es importante señalar algunos controles que permiten verificar el uso de claves de seguridad, tales como: cambio

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 17 Edición No 1 – Año 2018

de claves de seguridad cada cierto periodo, reporte de incidencias al responsable del departamento, aplicación de medidas de solución a las incidencias reportadas y reprogramación de los controles de seguridad defectuosos.

En cuanto, a los tipos de controles a aplicar, cabe resaltar los siguientes: efectuar un análisis de riesgos para valorar los activos y así adecuar las políticas a la realidad de la organización; establecer el alcance y definir las violaciones a las políticas; comunicar a todo el personal involucrado sobre el desarrollo de las políticas de seguridad; identificar quién tiene la autoridad para tomar decisiones en cada departamento; monitorear periódicamente los procedimientos y operaciones en la organización; detallar explícita y concretamente el alcance de las políticas, con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad.

Tal como se puede evidenciar la selección de objetivos de control y controles es determinante para el efectivo funcionamiento de las redes LAN por cuanto permite tomar las acciones correctivas correspondientes en el momento indicado y proteger la seguridad de los recursos humanos y equipos, la ambiental y la gestión de comunicaciones a nivel intra y extra organizacional. A continuación se presenta el cuadro

Cuadro 3

Tipos de control

Controles de Gestión	Políticas claras aplicadas Seguimiento al plan estratégico y operativo Indicadores de gestión Tableros de control Seguimiento a cronograma Evaluación del desempeño Informes de gestión Monitoreo de riesgos
Controles Operativos	Conciliaciones Consecutivos Verificación de firmas Listas de chequeo Registro controlado Segregación de funciones Niveles de autorización Custodia apropiada Procedimientos formales aplicados Seguridad física Contingencias y respaldo Personal capacitado Aseguramiento y calidad
Controles Legales	Normas claras y aplicadas Control de términos

Fuente: Barker y Morris (2013)

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 17 Edición No 1 – Año 2018

Sistema de gestión de seguridad en la red de área local para la Institución Educativa La Gloria, municipio Manaure del Departamento de La Guajira, Colombia

Para monitorear los servidores instalados, se toma en cuenta la estructura de los elementos de la estación; ya que para analizar los datos, interfaz de usuario, solicitudes del usuario, peticiones de monitoreo, control a los elementos remotos y base de datos con información de la Base de Información Gestionada (Management Information Base [MIBS]), los elementos de red son gestionados por el Protocolo Simple de Administración de Red (SNMP). Esta investigación se inclina a la utilización de sistemas de monitoreo y sistemas de gestión que están basados en el modelo de gestión SNMP por que posee una estructura de la Información gestionada (SMI) basada en TCP/IP, capacidad de comunicación gestor a gestor y seguridad en los accesos a datos complejos no soportados por SNMP. También permite un acceso más eficiente a los datos que sí soportan SNMP, e incorpora un nivel de seguridad de cifrado con clave pública y firma digital.

Por lo cual, se hace propuesta de paquetes para el manejo de la gestión de seguridad y servidores de nombres de dominio (DNS) tales como Microsoft Security Assessment Tool 4.0, que es una aplicación de evaluación de riesgos diseñada para proporcionar información y recomendaciones sobre las mejores prácticas para la seguridad dentro de una infraestructura de tecnología de la información (TI). Así mismo, la herramienta emplea un enfoque holístico para medir su postura de seguridad al cubrir temas de personas, procesos y tecnología.

A su vez, para complementar el trabajo que realiza la primera aplicación, se propone el uso de Microsoft Baseline Security Analyzer 2.3 (for IT Professionals) que proporciona un método optimizado para identificar las actualizaciones de seguridad faltantes y las configuraciones incorrectas de seguridad comunes, además, corrige problemas menores informados por los clientes, busca actualizaciones de seguridad, acumulaciones y servicios faltantes y actualiza paquetes con las tecnologías de actualización de Microsoft para evaluar las actualizaciones de seguridad que faltan.

Ahora bien, se deben contemplar los puntos de ataque para los servidores DNS, por lo cual es recomendable configurar la raíz solo a los servidores internos y no de internet. También surgen problemas respecto a la caché, ya que server 2012 configurado como DNS, almacena los resultados de sus consultas antes de enviar la respuesta al servidor que ha realizado la consulta. Esto quiere decir, que si la memoria caché es “contaminada” de alguna forma con lugares web maliciosos, estos pueden ser reenviados a los distintos usuarios. Por tanto, se debe procurar configurar el servidor DNS para evitar esta “contaminación”. La distribución de DNS debe ser doble por si falla uno de los dos, y con una IP fija para que exista la correcta denegación de zonas por servidores específicos. Para estos casos, deben crearse directivas de firewall y bloqueos de usuario internos externo que se conecten a servidores que no estén bajo a las pautas de seguridad de la empresa.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 17 Edición No 1 – Año 2018

Gestión y Seguridad en servidores de Correo electrónico

En el área administrativa de la institución, el servicio de correo electrónico es un servicio de mucha necesidad, ya que los usuarios intercambian información a diario con otros usuarios o el mundo exterior. Así mismo, el servicio de correo electrónico es un servicio vulnerable debido a la recepción de mensajes no deseados, por ello se busca proteger la institución de cualquier amenaza que pueda llegar o ser enviada por esta vía y promover las comunicaciones corporativas mediante el uso de este servicio.

Es importante destacar, que los sistemas de correo electrónico son vulnerables, sobre todo a la protección de la información contenida en los mensajes, preservación de la privacidad y seguridad de la data de la institución, por lo cual es recomendable tener implantado un servidor en un centro de datos, ya que se puede gestionar y administrar de manera segura la información y en control de los datos que circulan a través de los correos.

Además de esto, es imprescindible contar con diferentes medios que limiten el acceso a los servidores, contando con herramientas que controlen un acceso seguro a los usuarios, y que permitan mitigar ataques de seguridad, como inundaciones de correo, spam o ataques de denegación de servicio, donde hMailServer se promueve como uno de los mejores gestores de correo a nivel del protocolo para transferencia simple de correo (SMTP o POP). Cabe indicar que hMailServer es un servidor de correo electrónico gratuito y de código abierto para Microsoft Windows, ejecutándose como un servicio de Windows e incluye herramientas de administración para la gestión y respaldo de los mensajes, tiene soporte para los protocolos de correo electrónico IMAP , POP3 y SMTP, y puede utilizar motores de bases de datos externas como MySQL, MS SQL o PostgreSQL, o un motor interno MS SQL para almacenar datos de configuración e índice.

Una de las medidas de seguridad que tiene hMailServer es que los usuarios pueden autenticarse tanto contra el sistema local de usuario hMailServer como contra un Active Directory externo. hMailServer ofrece una serie de diferentes mecanismos AntiSpam: Lista negra de DNS basada en host (DNSBL), Lista negra de DNS basada en URL (SURBL) e Integración de soporte para ClamWin / ClamAV.

Para ejecutar cualquier escáner de virus de línea de comando, otro mecanismo de seguridad es un antivirus implantado desde un servidor que permita de manera remota la revisión, actualización, mantenimiento y limpieza, tanto del sistema como de la base de datos de los mensajes de los usuarios; para ello, ESET Secure Business, ya que tiene como característica fundamental para este tipo de servidores, el control antispam, además posee un filtro adicional de protección para las distintas capas de red y para los grupos de trabajo, también protege de sitios antiphishing, malware, gusanos**,** rootkits y spyware.

Gestión y Seguridad en servidores de Antivirus

Los paquetes Business Edition agregan ESET Remote Administrator, lo que permite la implementación y administración del servidor, la duplicación de las

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 17 Edición No 1 – Año 2018

actualizaciones de la base de firmas de amenazas y la capacidad de instalar en los sistemas operativos Microsoft Windows Server. También funciona como consola de administración central ya que maneja protocolos de detección de equipos de red; este paquete ofrece la posibilidad de administrar de manera remota, bajo protocolos de administración de red (SNMP), centralizando los programas en la red corporativa de la empresa o institución donde sean instalados.

Una de las mayores amenazas a la información, son los virus informáticos, así como el malware (software malicioso) en general. Dentro de la categoría de malware consideramos todo aquel software que no es capaz de infectar otros archivos, como si lo hacen los virus tradicionales, y que, pese a ello, pueden traer problemas a una computadora o red, como el spyware, hardware, los troyanos, etc.

Gestión y Seguridad en servidores WEB

Los servidores web tienen que estar protegidos frente a cualquier tipo de amenazas, tienen que estar preparados para ser el primer punto de entrada a cualquier compañía, ya que estos ataques se producen como consecuencia de una mala configuración del servidor o un mal diseño del mismo, así como de fallos de programación derivados de los ajustados Service Level Agreement (SLA) al que se enfrentan los desarrolladores de los portales web.

Para ello, los administradores deben contar con herramientas de seguridad dedicadas exclusivamente a la securización de estos servidores. En el mercado existen herramientas diseñadas para proteger servidores web, dispositivos de seguridad capaces de ofrecer multitud de funcionalidades que, sin lugar a dudas, serán de gran utilidad a la hora de proteger el entorno web. Estos dispositivos son capaces de realizar funciones que van desde firewall de aplicación web (Web Application Firewall -WAF-), aceleración de las propias aplicaciones, balanceo de carga entre los servidores e IPS.

Son muchas las posibilidades que ofrecen este tipo de herramientas, que cada vez más se están imponiendo en las compañías con el fin de proteger la parte más importante de la empresa de cara al exterior. Entre los beneficios que ofrecen este tipo de dispositivos, se pueden destacar la detección de intrusos al sistema, denegación de acceso por firewall ya sea por un puerto específico o por una IP fija asignada.

Para proteger la red administrativa de la institución se utilizó un firewall de hardware, ya que un firewall basado en software se centra en una posición de red posterior a un enrutador, lo cual la hace ineficiente. Una manera de hacer la red mucho más segura, es implementando un firewall basado en hardware porque se encuentran directamente detrás de su enrutador, por lo que cada paquete de datos proveniente de Internet debe pasar a través de su controlador de acceso antes de aterrizar en cualquiera de sus unidades internas.

Gestión y Seguridad en servidores de Base de Datos

El manejo de la información es de gran importancia para el crecimiento de las empresas, ya que el acceso a los datos es de carácter crítico, debido a la necesidad

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 17 Edición No 1 – Año 2018

de integrar la información de múltiples fuentes de datos, a menudo por parte de terceros para la toma de decisiones, captación de tendencias, minimización de riesgos y análisis de opiniones. Es por ello, que administrar una base de datos no es solo agregar, modificar, borrar o buscar una información, administrar una BBDD es garantizar la integridad, disponibilidad y calidad de los datos y diagnosticar el nivel de seguridad de la información de acuerdo con las normas internacionales y el objeto de negocio. Para ello, el administrador de un Servidor de Base de datos debe:

- Conocer la arquitectura de la base de datos.
- Conocer los privilegios de los usuarios y dependencias.
- Conocer los protocolos de administración y configuración del sistema manejador de base de datos (smbd), orientados al mantenimiento preventivo, correctivo para mantener la calidad del servicio.
- Tener un manual de procedimiento para la gestión de incidentes
- Tener planes de contingencia para la gestión del riesgo
- Tener políticas para la seguridad de la base de datos
- Estar capacitado con estudios técnicos de herramientas la administración y mantenimiento de una BBDD. Para que un administrador de Base de Datos pueda tener una buena administración del servicio de BBDD, debe contar con un sistema gestor de BBDD (SGBD), que permiten el almacenamiento, modificación y extracción de la información en una base de datos, además de proporcionar herramientas para añadir, borrar, modificar y analizar los datos.

Además, estos sistemas también proporcionan métodos para mantener la integridad de los datos, para administrar el acceso de usuarios a los datos y para recuperar la información si el sistema se corrompe. Permiten presentar la información de la base de datos en variados formatos. La mayoría incluyen un generador de informes. También pueden incluir un módulo gráfico que permita presentar la información con gráficos y tablas. Un SGBD permite controlar el acceso a los datos, asegurar su integridad, gestionar el acceso concurrente a ellos, recuperar los datos tras un fallo del sistema y hacer copias de seguridad. Las bases de datos y los sistemas para su gestión son esenciales para cualquier organización.

Gestión y Seguridad en servidores de Aplicaciones

Diseño y desarrollo Colaborativo. Ultimus proporciona un entorno de usuario que equipos de TI y de Negocios permite monitorear, gestionar y actualizar los equipos para diseñar y desarrollar sus procesos.

Rápida automatización. Ultimus BPM utiliza un enfoque de "código libre" en diseño de procesos y permite integrar rápidamente el proceso a los sistemas existentes utilizando herramientas de arrastrar y soltar.

Visibilidad y control completo. Ultimus proporciona un conjunto completo de reportes, como medio de monitoreo de actividad interactiva que permite la gestión para medir la efectividad del proceso respecto a los indicadores clave de rendimiento y efectividad.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 17 Edición No 1 – Año 2018

Agilidad para manejar excepciones y cambios. GUI de Ultimus BPM Gestor de Reportes de BPM. Otra ventaja que BPM brinda a un servidor de aplicaciones, es la gran variedad de soluciones que ayudan a optimizar y acelerar el servidor de aplicaciones para mejorar el rendimiento, tales como:

- Web Application Accelerator (WAA). Es un servicio basado en la nube que permite a las empresas distribuir aplicaciones basadas en la web de manera rentable, rápida, fiable y segura.
- Alta. Es una plataforma de controlador de distribución de aplicaciones que permite a las empresas superar los desafíos relacionados con la distribución de aplicaciones a través de TCP/IP.
- Global Traffic Management. Aplica un enfoque centrado en el APPServer que respecta al equilibrio de carga global, ofreciendo una alta disponibilidad y capacidad de respuesta ante las solicitudes de los usuarios.

Gestión de Servidor de Respaldo

En el equipo servidor tendrá que ser implantado sistemas de Dominios (DNS Alternativo)para poder generar respaldo de los diferentes sistemas como medida de contingencia ante la falla de algún equipo y pueda funcionar como servidor de respaldo y que pueda realizar respaldo de manera remota con la asistencia de los sistemas instalados en los servidores mencionados anteriormente; para ello, estos equipos deben estar configurados con el direccionamiento de la red de servidores para que puedan tener conexión directa con los equipos de servicios. El equipo a utilizar es un HP proliant DL380p de Octava Generación G8, con múltiples capacidades de procesamiento y múltiples bancos de memorias y discos SAS con controladores de energía eléctrica permitiendo que al haber fallos eléctricos, se reduce el 50 % del consumo eléctrico, aumentando el tiempo de uso del equipo.

Conclusiones

Finalizada esta investigación, la cual buscó proponer un sistema de gestión de la seguridad de la información para redes en medianas empresas, se presentan a continuación las conclusiones obtenidas de acuerdo a cada uno de los objetivos específicos:

En relación al primero, el cual trata de diagnosticar la situación actual, se tuvo que la institución objeto de estudio, no cuenta con una situación actual acorde con el cumplimiento de las políticas de seguridad de la información, y a su vez presenta carencias en lo que respecta a las evaluaciones de riesgos informáticos, ya que se desconocen las vulnerabilidades que poseen los sistemas de computación de la empresa, sin observar prácticas cónsonas de sus usuarios con respecto al manual de seguridad de la información.

Con respecto al segundo objetivo específico, el cual trata de identificar los parámetros de la gestión de la seguridad de la información, la empresa cumple en llevar a cabo tales parámetros, sin embargo, se observó un rendimiento bajo en la confidencialidad al no poseer los usuarios conocimiento de funciones para la

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 17 Edición No 1 – Año 2018

encriptación de datos, así como un rendimiento moderado en el conocimiento del manejo de la información que garantice la integridad de los datos.

Referente al tercer objetivo, sobre diseñar la estructura de seguridad en redes LAN), se pudo focalizar que el diseño de mecanismos de seguridad en la red LAN propuesto tiene como finalidad mejorar la accesibilidad a la información y fuerza bruta en la información manejada a través de la red LAN.

Finalmente al cuarto objetivo, con respecto a determinar la factibilidad de un sistema de gestión de seguridad en redes LAN, con base a los resultados obtenidos se logró la construcción de una propuesta de un sistema de gestión de seguridad en redes LAN, que permita la creación de las condiciones apropiadas para que el desarrollo de los servicios informáticos estén privilegiados por mecanismos de competitividad, interoperabilidad, flexibilidad, al usuario.

Referencias Bibliográficas

Aguirre, D. y Palacios, J. (2014). *Evaluación Técnica de Seguridades del Datacenter del Municipio de Quito según las Normas ISO/IEC 27001:2005 SGSIE ISO/IEC 27002:2005.* Universidad de las Fuerzas Armadas ESPE. Sangolqui, Ecuador.

Aguirre, D. (2014). Diseño de un Sistema de Gestión de Seguridad de Información para Servicios Postales del Perú S.A*. Sistema de Bibliotecas de la Pontificia Universidad Católica del Perú.* Ciudad de Lima, Perú. ISSN: 2310-8894.

Barker, K. y Morris, S. (2013). *CCNA Security 640-554 Official Cert Guide. Cisco Press.* Indianápolis, Indiana, E.E.U.U. Recuperado de: https://fdocuments.in/document/ccna-security-640-554.html

Castro, V. (2015). *Sistema de Gestión de Seguridad para una Red LAN en Empresas de Servicios Públicos*. (Tesis de Maestría). Universidad Privada Dr. Rafael Belloso Chacín. Maracaibo, Venezuela.

Carrasquero, E. y Pérez, L. (2016). Sistema de gestión de seguridad en redes LAN. *Télématique,* 15(2), p.p. 133

Delgado, A. (2014), *Sistema de gestión de seguridad en Redes LAN para la Universidad Nacional Abierta.* (Tesis de Maestría). Universidad Privada Dr. Rafael Belloso Chacín. Venezuela.

Hernández, R., Fernández, C. y Baptista, L. (2014). *Metodología de la investigación.* México: McGraw-Hill Education.

Landeau, R. (2012). *Metodología y Nuevas Tecnologías*. Venezuela: Editorial Alfa.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 17 Edición No 1 – Año 2018

Manual de trabajo y especialidad, maestría y tesis doctoral UPEL. (2016). Recuperado de: https://bibliotecavirtualupel.blogspot.com/2016/09/manual-de-trabajo-de-grado-de.html

Melean, R. (2014). *Sistema de Gestión de Seguridad en Redes LAN para la Universidad Nacional Experimental Rafael María Baralt*. (Tesis de Maestría). Universidad Privada Dr. Rafael Belloso Chacín. Maracaibo, Venezuela.

Depósito Legal: PPX200002ZU2142 / ISSN:1856-4194. Volumen 17 Edición No 1 – Año 2018