UNIVERSIDAD TÉCNICA DE BABAHOYO FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA PRUEBA

PRÁCTICA PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN SISTEMAS

TEMA:

ESTUDIO DE LA INTERCONECTIVIDAD Y SEGURIDAD DE DATOS DEL GAD_MUNICIPAL DE BABA.

MARIA MERCEDES VERA MEJIA.

TUTORA:

ING. ANA DEL ROCIO FERNANDEZ TORREZ.

AÑO 2019

I.- INTRODUCCION

En el presente estudio de caso es una investigación de la interconectividad y seguridad de datos del GAD Municipal de Baba.

La interconectividad es la comunicación de dos o más redes conectadas entre sí. En la actualidad la seguridad e interconexión de datos van de la mano, se han implantado procedimientos y tecnologías de seguridad disponibles para proteger la integridad de los datos, pero no se puede afirmar que estén completamente a salvo de los intrusos. La seguridad de datos se enfoca en la protección de la infraestructura y de toda la información incluida en un ordenador. Se puede decir que las principales características de la seguridad de datos son: la integridad de los datos, la confidencialidad, disponibilidad.

La protección de datos es de vital importancia, ya que de ella depende la ejecución de las tareas de cada uno de los departamentos que conforman la institución, la cual debe ser siempre una información segura y factible, con lo cual se podrá agilizar los procesos, que en tiempo pasados no generaban confianza, ya que los mismo eran operados de forma manual por las personas encargadas en cada uno de los departamentos.

El GAD Municipal del Cantón Baba es uno de los cantones más antiguos de la Provincia de Los Ríos, se encuentra localizada al noroeste del Cantón Babahoyo, es una entidad que pertenece al sector público, con autonomía administrativa y financiera, que concentra su gestión en entregar a su población urbana y rural una adecuada planificación territorial; fomenta el desarrollo humano, comercial y social de manera integral; gestión en el ordenamiento del crecimiento urbanístico y rural; servicios básicos de calidad; oportuna ayuda social y fomento al turismo, educación, cultura, deportes y recreación; en un ambiente de respeto, colaboración y transparencia.

Esta institución está conformada por doce departamentos, entre los que tenemos; Alcaldía, Vicealcaldia , dirección de relaciones públicas, dirección de procuraduría sindica, dirección de administrativa, dirección financiera, secretaria general, dirección de obras públicas, dirección de desarrollo social y comunitario, dirección de planificación, unidad de asesoría, consejo de participación ciudadana y control social, teniendo en cuenta que no todos los departamentos están interconectados tecnológicamente, por lo cual no existe una comunicación eficaz y segura de la información que se genera en las unidades que conforman el GAD Baba.

La presente investigación está enfocada en determinar los distintos problemas de la interconectividad y la seguridad de datos, que se presentan por la indebida conexión de equipos no autorizados, y a las ves mal configuradas, y la compartición del ancho de banda dentro de la institución, y los distintos departamentos que se encuentran dentro del GAD Baba.

El caso de estudio se realizó siguiendo la sub-línea de investigación que se ubica en procesos de transmisión de datos y telecomunicaciones, la metodología utilizada fue la inductiva por cuanto nos conlleva a razonar, partiendo de una serie de observaciones particulares, que permiten la producción de leyes y conclusiones generales, para el desarrollo del caso de estudio de la interconectividad y seguridad de datos del GAD Municipal del cantón Baba.

Para la obtención de los resultados se utilizó como técnicas; entrevistas y observación los que proporcionaron una información exacta de los problemas que se suscitaban en la institución, por eso se pudo determinar la factibilidad del caso de estudio.

DESARROLLO

El Gobierno Autónomo Descentralizado Municipal del cantón Baba es una entidad de derecho público que goza de autonomía administrativa y financiera, siendo el nivel de gobierno a nivel del territorio cantonal, donde se encuentran las oficinas de los funcionarios: alcalde, concejales, Dirección Administrativa y demás dignidades que conforman el cuerpo principal de esta entidad pública.

Actualmente toda organización cuenta con una infraestructura de Red Informática y se las conoce como como Tecnología de la Información y Comunicación (TIC), es una rama que se descubre totalmente esencial en todo lo que se trata de redes, que está compuesto por varios elementos y equipos activos que cumple el objetivo de disponer el medio de transmisión y comunicación para de esta manera respaldar el correcto traslado de información.

Pero la infraestructura de red del cantón Baba a simple vista no cuenta con una infraestructura de red adecuada porque su instalación se encuentra en deterioro, además cuenta con una mala configuración de sus equipos y sobre todo la organización del cableado de la red está hecho un caos. (Pacheco, 2018)

En la presente investigación propone un estudio en la infraestructura de la red del GAD Municipal del Cantón Baba, con el objetivo de identificar las anomalías existentes tanto en las infraestructuras como en el soporte informático para dar una mayor calidad y realce a la Municipalidad del cantón.

En cualquier operación en la cual exista redes de computadoras, hay tres cuestiones importantes, primero, una red debe tener usuarios; segundo, los usuarios deben estar conectados entre sí de alguna manera, y tercero, todos los miembros de la red deben establecer

claramente la comunicación con cada uno de ellos para que pueda tener lugar una comunicación efectiva, para lograr la fluidez de la información. (Molina Ruiz, 2015)

La infraestructura de red debe servir a todas las peticiones que soliciten los usuarios que estén conectados en la red y esta debe cumplir los objeticos fundamentales de la seguridad de la información los cuales son la disponibilidad, la confiabilidad e integridad tanto de la infraestructura física de la red como la información que se gestiona en la misma.

Los sistemas informáticos que se utilizan para las entidades del sector público consideran que se deben tener todas las medidas de seguridad para precautelar la información generada y almacenada, en el presente documentos se analiza la seguridad de la red informática del Gobierno Autónomo Descentralizado Municipal del cantón Baba. (NARVÁEZ NARVÁEZ, 2019)

Como normas de aplicación dentro de la infraestructura de red, existen una serie de criterios que velan por nuestra seguridad e integridad, así como por inversiones y una serie de recomendaciones que, aunque no son de obligado cumplimiento se garantizan la independencia al estandarizar su uso.

El Soporte Informático que se trata de un servicio mediante el cual los especialistas en apoyo informático o expertos en digital le ofrecen asistencia técnica, soporte remoto ante algún problema y asesoramiento a los usuarios y organizaciones que trabajan cada día con las nuevas tecnologías. (Marín Martínez, Ramos, & & Diego)

Para la recolección de los datos necesarios para identificar el estado de la red del GAD de Baba se utiliza metodología la investigación cualitativa, donde se realizará un análisis de las características que establecen el estado de la red para determinar las medidas y protocolos de seguridad se usan en el en el GAD de Baba, usando como técnica a la entrevista, el cuestionario

como donde se desea obtener información más detallada sobre la infraestructura de red del municipio.

En la visita realizada al GAD Baba se logró observar la mala distribución de la red, ya que los cables se encuentran dispersos por doquier, ya que no existe una red estructurada, ni una correcta administración de los recursos tecnológicos disponibles en la institución. (***Ver Anexos. Ilustración 4***)

Esto conlleva a problemas en la interconectividad debido a que puede existir ruido en la transmisión de los datos, causando muchas veces que la información transmitida no llegue a su destino, por la mala ubicación del cableado que está expuesto a sufrir daños en el entorno, y que no se realicen buenas prácticas de seguridad informática para mantener una infraestructura tecnológica de transmisión de datos.

La seguridad informática establece principios que garantizan las buenas prácticas de mantener a la información confiable, integra y disponible, lo que conlleva un plus para la protección de los datos más importantes de la institución. Una información integra significa que esta se mantiene igual sin sufrir ninguna modificación durante su transmisión. La información confiable demuestra que esta es manejada solo por personas autorizadas y la información disponible es que esta esta accesible para poder utilizarla en cualquier momento. (Gargallo, 2018)

La topología que se utiliza en el Gobierno Autónomo Descentralizado Municipal del cantón Baba es de tipo de Árbol. La distribución de los equipos y terminales es determinada gracias a un switch, del cual salen ramificaciones de cable. El cableado que se utiliza es UTP categoría 5 y 6 su instalación no presenta canaletas, distribuido para las 12 terminales que cuentan con el sistema operativo Windows 7.

La seguridad de los datos informáticos en la actualidad es una constante preocupación en la institución, considerando que una entidad pública maneja información que es confidencial, como pueden ser los datos de los usuarios en el tema de recaudación catastral los cuales permiten ingresos a la administración municipal, el departamento Financiero y Contable, Talento Humano entre las dependencias con mayor riesgo de vulnerabilidad. (Mercado, Yengle, & Silva, 2018)

Con el paso del tiempo el internet se ha convertido en una herramienta necesaria de comunicación en todo el mundo, por cuanto la información está presente en la base de datos de una entidad debe está segura, accesible para usuarios autorizados y sobre todo integra, es por eso que se debe utilizar con los mecanismos y modelos de seguridad, porque existen muchos agentes ya sea naturales, voluntarios o error humano que pueden poner en riesgo dicha información. (López, 2017)

El internet está presente a escala mundial y se está haciendo presente en la mayoría de los trámites que se realizan actualmente en todo tipo de organizaciones. La necesidad de automatizar los procesos para mejorar la calidad de los servicios que ofrecen, viene de la mano con la implementación de las redes, pero esta implementación a establecer buenas prácticas y políticas de seguridad en cuanto a los equipos, datos y también a las personas.

En la actualidad cada vez las entidades del sector público y empresas privadas son más dependientes de la internet y de diversos sistemas de información, teniendo en cuenta que los datos que se tienen pertenecen a sus contribuyentes o usuarios y clientes que es muy importante para el desarrollo de sus actividades, lo cual genera mayor cantidad de riesgo y amenazas de ataques por medio de los diferentes instrumentos como los códigos maliciosos, la piratería informática y otras herramientas. (Ramos, 2019)

En el presente caso de estudio se establecieron cuatro fases para la recolección de la información necesaria para encontrar los puntos débiles que existen el en la red de datos del GAD de Baba.

- **En la fase 1**, se define el alcance del presente caso de estudio**.**
- **En la fase 2** se procede a identifica al equipamiento e infraestructura presente en el GAD de Baba.
- **En la fase 3** se procede a identifica las amenazas tanto físicas como lógicas presentes en la institución. Para este objetivo se utilizó la herramienta de libre para escaneo de red y detección de vulnerabilidades lógicas de la misma.
- **Fase 4** se analizan las amenazas encontradas. La infraestructura informática del GAD de Baba, no establece ni hace uso de ninguna ISO para la gestión de la seguridad. La infraestructura se encuentra en total abandono, en el cualquier momento podría sufrir un colapso en la infraestructura física.

Definir el alcance

El presente trabajo de investigación, sólo como objetico evaluar el estado de la red referente a la seguridad de los datos. No se realizarán modificaciones, ni configuraciones en la red presente en el GAD, debido a que el presente tiene como finalidad identificar, exponer, evaluar y recomendar las buenas prácticas de seguridad referentes a la transmisión de los datos y la infraestructura de la red. Tampoco tiene como objetivo gestionar la compra de nuevo equipos tecnológicos que sean necesarios para la organización.

Identificar los activos

Basada en la en la entrevista que se realizó a los encargados de los GAD de Baba y del departamento técnico se pudo constatar que existes los siguientes activos.

Dentro de los activos encontrados en la organización se pudieron clasificar en hardware y software e infraestructura.

En el hardware se pudo identificar los siguientes activos.

- Switch
- Router inalámbrico
- 5 computadoras Core 2duo con 2gb RAM
- 7 computadoras inter Core i3
- 2 servidores

En relación al software se pude identificar

- Sistema operativo Windows 7 original

En la infraestructura se pudo identificar que no existe una correcta instalación de la misma, puesto que el cableado no se encuentra estructurado, así como también se pudo observar el libre acceso de cualquier empleado del GAD de Baba acceder a conectar cables ajenos a los equipos presentes en la red. Los cables parecen telaraña, y es muy difícil distinguir el procedente de cada uno. Este problema atribuye a fallas que pueden ocurrir por mantener el cableado de una red de esa forma.

Identificar las amenazas

Se procedió a aplicar la herramienta Nmap tal para identificar las amenazas y vulnerabilidades que existen en la red del GAD de Baba.

Dentro de las amenazas encontradas en la organización, se encuentra en que la red no se encuentra acorde con los estándares de calidad establecidos para resguardar la información que circula por ese medio.

Dentro de las amenazas físicas, la incorrecta instalación de los componentes y equipos de red que la conforman. Existe una mala configuración en los cables.

Para determinar las amenazas lógicas se realizó un testeo con Nmap, para identificar las amenazas potenciales que existe en los equipos en su configuración.

Nmap, abreviatura de Network Mapper, es una herramienta gratuita de código abierto para el escaneo de vulnerabilidades y el descubrimiento de redes. Los administradores de red usan Nmap para identificar qué dispositivos se están ejecutando en sus sistemas, descubriendo los hosts que están disponibles y los servicios que ofrecen, encontrando puertos abiertos y detectando riesgos de seguridad. (Sosa, 2018)

El tráfico de la red es el término que se le da cuando los datos viajan de un punto a otro usando los medios de la red. Estos datos, en forma de paquetes recorren una ruta para ingresar a un sistema y para salir de él por medio de las tarjetas de red. Estos paquetes pueden ser tráfico de voz, o tráfico de archivos, a los cuales se pueden dar un tratamiento especial, para disfrutar un servicio de calidad. (Solarte, Rosero, & del Carmen Benavides, 2015)

Identificar vulnerabilidades

Se procedió a realizar el respetivo escaneo con la herramienta seleccionada. Con la autorización y supervisión del encargado de soporte tecnologías del GAD de Baba, se procedió a instalar la herramienta en uno de los equipos. Nmap monitorea hosts individuales, así como vastas redes que abarcan cientos de miles de dispositivos y multitud de subredes.

Nmap es extremadamente flexible, en el fondo es una herramienta de escaneo de puertos, que recopila información enviando paquetes sin formato a los puertos del sistema. Escucha las respuestas y determina si los puertos están abiertos, cerrados o filtrados de alguna manera, por ejemplo, mediante un firewall. Otros términos utilizados para el escaneo de puertos incluyen descubrimiento o enumeración de puertos.

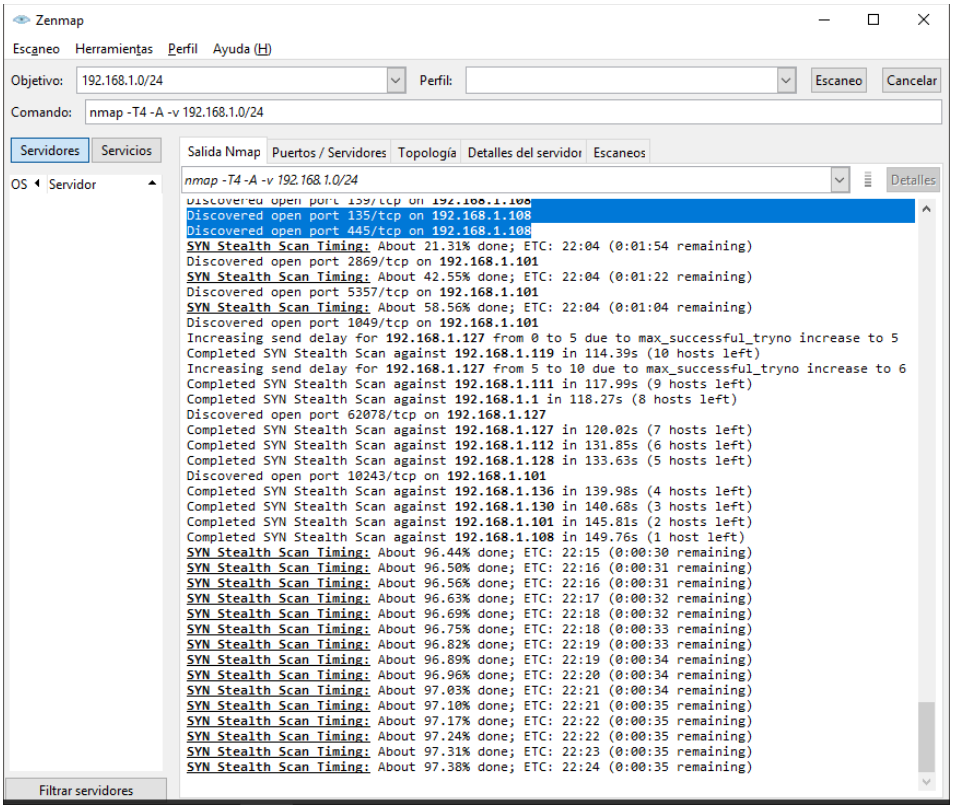

Gráfico 1. Escaneo con Nmap.

El proceso de escaneo tuvo un tiempo de duración de 30 minutos.

Evaluar de resultados

El nivel de los riesgos se reducirá con la aplicación de controles, de modo que el riesgo residual se pueda revaluar como admisible. Se analizan todos los activos y se evalúa las consecuencias mitigadas

Debido a problemas presentados de rendimiento en el servidor financieros e identificó que los recursos asignados de procesador y memoria eran insuficientes, por lo que se decidió cambiar de un ambiente virtual a un ambiente real, con contingencia de energía UPS, mitigando significativamente el riesgo y el impacto.

Los criterios por los cales Nmap evalúa a los las vulnerabilidad de la red es la siguiente:

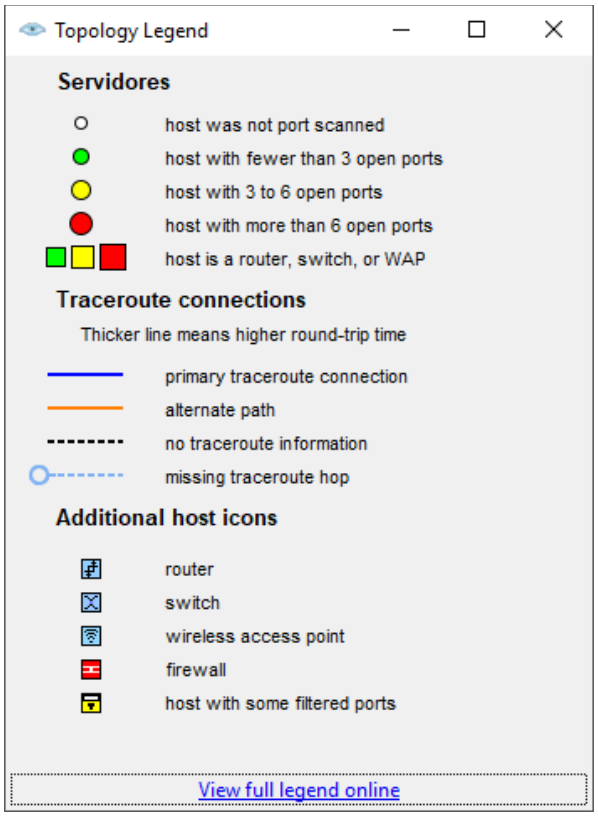

Gráfico 2. Criterios de evaluación.

Después del escaneo se obtuvieron los siguientes resultados:

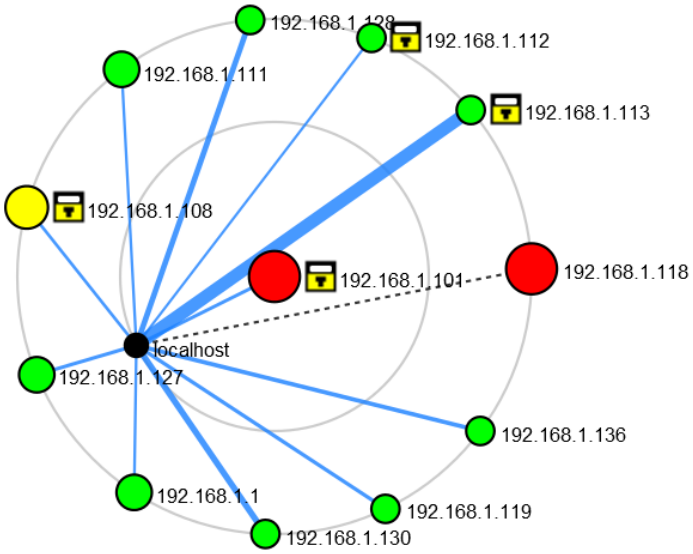

Gráfico 3. Resultados.

Como se puede observar hay dos equipos que tiene más de seis puertos abierto los cuales, presentan vulnerabilidades muy peligrosas, ya que tienen una configuración inadecuada, que si no se evalúan y se gestionan correctamente pueden ocasionar perdidas de datos o sufrir ataques informáticos inadecuados.

Basado en la entrevista se determinó que el GAD de Baba debe aplicar políticas y normas de seguridad informática en el departamento informático. Se han determinado las siguientes normas;

- Mejorar conocimiento de los empleados de la organización en seguridad de la información.
- Mejorar el control de activos sensibles e información
- Proporcionar un enfoque para la implementación de políticas de control
- Definir el acceso restringido de la red para que solo personal autorizado tenga acceso a ellos.

- Revisar periódicamente el estado de la red a través de escaneos para corregir errores en caso los haya

Se han identificado tres políticas de seguridad que está en análisis de aprobación, gestionada por la Gerencia de la Seguridad de la Información. En caso de aplicarse estas políticas, el GAD de BABA tendrá que adquirir equipamiento, reformar reglamentos y gestionar un programa de capacitación. Las políticas creadas son las siguientes:

- Diseñar políticas de control de acceso
- Definir políticas para evitar ataques de Denegación de Servicios
- Política de desvinculación de personal

Luego de implementada la política se realizó una nueva evaluación para determinar si la política ha sido de ayuda para mitigar los problemas encontrados a través de los escenarios planteados. En la siguiente tabla se indica la posición del riesgo detectada y se compara junto a la del riesgo residual.

La ISO (International Organization for Standardization), es una norma que tiene alcance a nivel mundial cuya finalidad es establecer estándares que normalicen diferentes procesos. Las Normas ISO permiten asegurar la calidad de los productos y servicios, mediante procesos estandarizados que conllevan a una mejora significativa en la producción y eficiencia.

La norma ISO 27001 se encuentra vigente desde el 2013, tiene como enfoque principal el Sistema de Gestión de la Seguridad de la Información (SGSI) estas sirven de guía para elaborar e implementar las políticas de seguridad.

La norma ISO 27001 se basa en el cumplimiento del SGSI, el mismo que se desarrolla considerando los principios de la seguridad como: confidencialidad, integridad y disponibilidad de la información, procurando con ello tener mayor confianza entre la entidad

y los usuarios, con el fin de que se garantice la seguridad de la información que posee la organización.

La ISO 27002 es una guía de buenas prácticas que describe los objetivos de control y los indicadores recomendables en cuanto a seguridad de la información. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Aunque no es certificable, su uso puede lograr grandes resultados para garantizar la seguridad de la información del Gad de Baba.

Uno de los objetivos de la ISO/27002, es el establecimiento de políticas de seguridad en la organización. El contenido de las políticas se basa en el contexto, la operación, la organización y la escritura para cumplir los objetivos. En este contexto el Gad de Baba, debe implementar políticas claras para garantizar la seguridad de los datos y de su infraestructura.

La seguridad física es otro objetivo de la norma ISO/27002, donde se establece que el establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles de protección para las instalaciones de procesamiento de información crítica o sensible de la organización, contra el acceso físico no autorizado.

Esta norma también, también tiene como objetivo establecer métricas para el control de accesos. Para impedir el acceso no autorizado a los sistemas de información se deberían implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información.

La implementación de buenas prácticas para la correcta gestión de los recursos informáticos de un sistema de información, conlleva a garantizar que la información viaje segura desde su origen hacia su destino. Entre los controles de la Norma ISO/27002 se han escogido los más óptimos según el modelo de gestión y los problemas encontrados en el GAD de Baba.

Bibliografía

Gargallo, L. (2018). La seguridad para los menores Internet. *Editorial UOC*.

ISO27000 Español. (2015). *El portal de ISO 27002 en Español*. Obtenido de Seguridad física y Ambiental: http://www.iso27000.es/iso27002_11.html

López, A. A. (2017). Seguridad en internet. . *PAAKAT: revista de tecnología y sociedad*, 6(11).

Marín Martínez, C. A., Ramos, L., & & Diego, J. (s.f.). (). Análisis y gestión de riesgos informáticos para la red LAN de la Gobernación del Meta. *2019*.

Mercado, J. G., Yengle, R. I., & Silva, M. T. (2018). Diseño y dimensionamiento de una red de datos convergente bajo una infraestructura de cableado estructurado para el campamento nuevo de la Mina Constancia. *PUEBLO CONTINENTE*, 29(2), 299-308.

Molina Ruiz, J. E. (2015). Propuesta de segmentación con redes virtuales y priorización del ancho de banda con QoS para la mejora del rendimiento y seguridad de la red LAN en la Empresa Editora El Comercio Planta Norte.

NARVÁEZ NARVÁEZ, Á. E. (2019). ANALISIS DE VULNERABILIDADES PARA LA RED LAN DE LA EMPRESA "HIDROMAG", BAJO LA METODOLOGIA "OSSTMM". *(Bachelor's thesis, Quito)*.

Pacheco, C. A. (2018). Vulnerabilidad del protocolo MySql en redes LAN bajo plataforma Linux., . *Télématique: Revista Electrónica de Estudios Telemáticos*, 8(1), 71-78.

Ramos, V. &. (2019). Diseño y desarrollo de una red LAN jerárquica y un prototipo de sistema web con módulos de: turnos, citas previas y seguridad perimetral de la red para la

Sociedad Ecuatoriana pro-rehabilitación de los lisiados . *Carrera de Ingeniería En Networking y Telecomunicaciones*.

Solarte, F. N., Rosero, E. R., & del Carmen Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica-ESPO*.

Sosa, C. &. (2018). Estudio de Amenazas y Vulnerabilidades en la Red de Comunicación del Departamento de Sistemas de la Universidad Técnica de Babahoyo . *(Bachelor's thesis, BABAHOYO)*.

CONCLUSIONES

El análisis con las metodologías que se propuso a la GAD dio como conclusión según las observaciones y aplicando la herramienta tal Nmap que existen muchos puertos inseguros en la institución no existen políticas adecuadas, además se la infraestructura no está completa en su totalidad, basado en un análisis de estándar internacional de seguridad en conectividad se pudo notar que no son aplicados en su totalidad por lo tanto esto ocasiona que no sea una red 100% adecuada para esta institución.

En cada departamento existen vulnerabilidades por no cumplir las normas ISO/IEC 27001, es decir que el cableado o tendido de red es realizado de forma empírica, con equipos no apropiados lo cual genera inconformidad en los usuarios y el personal que la labora en la entidad municipal.

Los backup de la información se consideran como un elemento primordial en la seguridad informática, en el Gad municipal esto se lo realiza de manera manual, es decir el funcionario visita cada uno de los departamentos para realizar dicho respaldo.

RECOMENDACIONES

Se propone la realización de una topología estable y establecer una nueva estructuración guiada y no guiada, con el uso de equipos de interconexión apropiados para mantener la red configurada y monitoreada acorde a los estándares antes mencionados.

Aplicar las normas ISO 27001 porque los beneficios comerciales de la certificación ISO 27001 son considerables. Los estándares no solo ayudan a garantizar que los riesgos de seguridad de una empresa se gestionen de manera rentable, sino que la adhesión a los estándares reconocidos envía un mensaje valioso e importante a los clientes y socios comerciales: este negocio hace las cosas de la manera correcta.

La ISO 27001 es invaluable para monitorear, revisar, mantener y mejorar el sistema de gestión de seguridad de la información de cualquier organización, sin duda, brindará a las organizaciones asociadas y a los clientes una mayor confianza en la forma en que interactúan con su negocio.

Por otra parte, también se recomienda hacer uso de la ISO 27002 ya su objetivo principal de es establecer pautas y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Esto también incluye la selección, implementación y gestión de controles, teniendo en cuenta los entornos de riesgo encontrados en una organización con tecnología informática.

La ISO 27002 proporciona cientos de controles potenciales y mecanismos de control que están diseñados para implementarse con la orientación proporcionada dentro de ISO 27001. Los controles sugeridos enumerados en la norma están destinados a abordar problemas específicos identificados durante una evaluación formal de riesgos. El estándar también está

destinado a proporcionar una guía para el desarrollo de estándares de seguridad y prácticas efectivas de administración de seguridad.

Incentivar a una cultura de seguridad informática a nivel los empleados de la Institución, es decir que se debe situar claves de acceso en cada una de las computadoras utilizadas en el GAD Baba, con lo cual si un funcionario abandona de forma momentáneamente el equipo el mismo no pueda ser utilizado por otra persona.

Como plan de mejora el departamento de Sistemas debe implementar un cronograma de renovación de claves para establecer un mayor rango de seguridad de la información.

Se debe tomar en cuenta que nunca existirá una seguridad total de la información, esto nos obliga a realizar una planificación de respaldo de la información que se encuentra en cada uno de los equipos que se poseen en la institución.

ANEXOS

FOTOGRÁFICAS VISITA AL GAD MUNICIPAL DE BABA

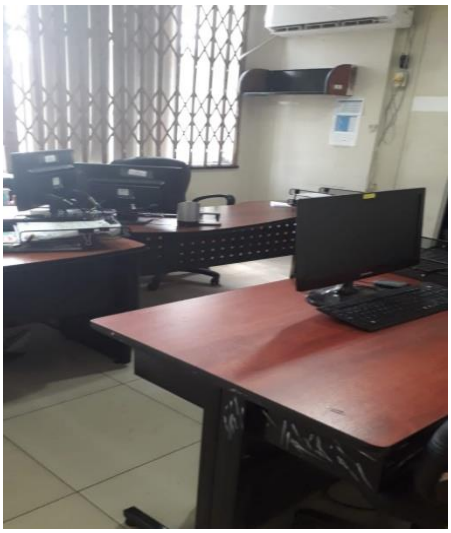

Ilustración 1: Dirección de relaciones publicas
Fuente: María Vera Mejía

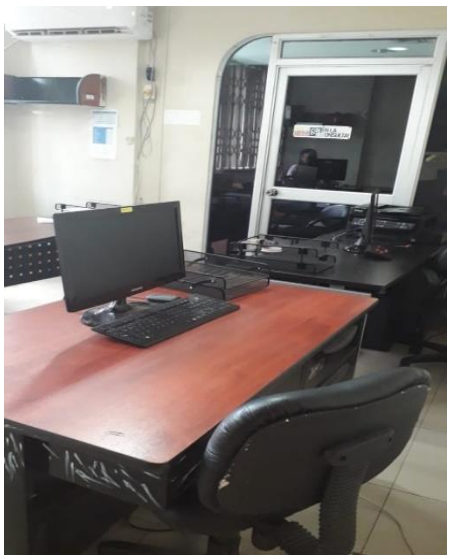

Ilustración 2:departamento de tesorería
Fuente: María Vera Mejía

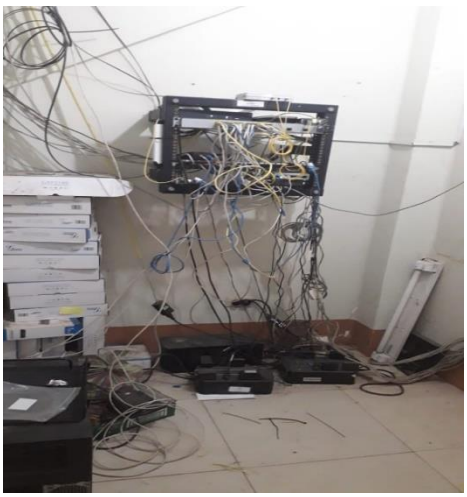

Ilustración 3: Departamento de sistemas
Fuente: María Vera Mejía.

Ilustración 4: Depart_sistema
Fuente: María Vera Mejía

FOTOS DE LA ENTREVISTA REALIZADA

Ilustración 5: Desarrollo Social
Fuente: María Vera Mejía

Ilustración 6: Dirección Financiera
Fuente: María Vera Mejía

Ilustración 7: Secretaria General
Fuente: María Vera Mejía

CUESTIONARIO PREGUNTAS PARA LA ENTREVISTA

¿Cuáles son los servidores implementados?

Actualmente existen dos servidores, los cuales permiten la comunicación entre los diferentes departamentos. Estos brindan servicio de impresión, comparten archivos por la red.

¿Cuál es el proveedor de servicios de internet?

Actualmente nuestro proveedor es CNT

¿Se está utilizando software adicional?

Ciertamente nos estamos adaptando aun, porque se ha realizado un cambio de administración y se está procediendo a resolver todos los problemas que hay actualmente en la red de a institución. En lo cuento al software más adelante se tiene estimado utilizar software más eficiente que el que se tiene actualmente.

¿Se está alquilando equipo adicional para atender la solicitud?

No, solo trabajamos con el equipo tecnológico que pertenece a la institución.

¿Se definieron usuarios de acuerdo a las políticas de la empresa?

No tenemos conocimientos, ya que la administración saliente no nos otorgó esa información.

¿Cuántos Switches, Patch panel, UPS, Hub, módems, y/o routers?

Tenemos un switch, un router inalámbrico, 7 computadoras core2duo con 2gb de RAM, 7 computadores Core i3 y dos servidores. Pero como puede usted observar todo está hecho un desastre, regado por todos lados, estamos trabajando para mejorar la condiciones de la red.

¿Qué categoría usan para el cableado? (5E o 6)

Hay una mezcla de los dos.

¿Cómo están organizados los servidores?

¿La red se encuentra segmentada?

No, simplemente se han repartido cables según el ámbito y oficina para el acceso de la misma.

¿Qué sistema operativo de red administra actualmente a la red?

Actualmente contamos con Windows server 2012 R2.

¿Qué esquema de direccionamiento llevan actualmente? (IPv4 o IPv6)

Actualmente constamos con IPV4/

¿Qué protocolos de red tienen actualmente configurados?

Aun estamos trabajando en eso, porque hemos planteado rediseñar toda la red y mejorar la calidad de la misma.