SEMINARIO DE GRADUACIÓN

Trabajo de investigación desarrollado para optar por el grado de licenciatura en Ingeniería Informática con énfasis en redes y sistemas telemáticos

Seguridad y acceso a la información a través de una red Wireless en el Sistema Bancario Público Nacional

PROFESORA

Paula Brenes

ESTUDIANTE

Hazel Mariela Chacón Jiménez

Facultad de Ingeniería Informática

Resumen

En este trabajo se utilizó el enfoque cuantitativo debido a que se basó en un método de recolección de datos a través de una encuesta para contestar la siguiente pregunta: ¿Cómo acondicionar una red Wireless para los diferentes usuarios del Sistema Bancario Nacional, según políticas internacionales de acceso y autenticación? Se analizaron los datos por medio de estadísticas, se realizó una introducción, la revisión bibliográfica, Metodología, discusión y por último se generaron las conclusiones de dichos resultados. Con esta investigación se pretende beneficiar a las personas que deseen implementar más de un perfil en sus redes inalámbricas, con el fin de realizar una separación del tráfico de datos entre los empleados y los visitantes que utilizan la red Wireless de dicho Banco.

Además, se mencionan empresas a nivel internacional que poseen el conocimiento técnico y la experiencia para llevar a cabo dicho proyecto. También dentro de la investigación se tomó como referencia un documento de Cisco llamado "**Deployment Guide for Cisco Guest Access Using the Cisco Wireless Lan Controller**", el cual describe una metodología para implementar el manejo de una red inalámbrica para los visitantes (clientes, asesores entre otros). En él se describe paso a paso de cómo generar tiquetes para las personas que deseen accesar la red Wireless por periodos cortos, debido a que en el documento que se le entregará al usuario invitado se debe indicar el número de horas e incluso número de días si fuese el caso, que podrá disfrutar de la red Inalámbrica.

Introducción

Las Instituciones financieras como Bancos Públicos (conocidos como Bancos del Estado), utilizan diferentes tecnologías para accesar información, entre ellas las denominadas Redes inalámbricas la cual es conocida en inglés

como Wireless Network, está funciona a través de la conexión entre nodos sin necesidad de la existencia de cables entre ellos. Los Bancos del estado, necesitan este tipo de tecnología, con el fin de ser utilizada por sus funcionarios, miembros de la Junta Directiva General y visitantes (clientes, proveedores, contratistas, asesores entre otros). Requiere que existan diferentes formas de autenticación por parte de los usuarios, ya que no todas las personas son empleados de la Institución.

El inconveniente de hoy día, es que sólo existen dos tipos de modalidades para conectarse a la red Wireless en el sistema Bancario, uno de ellos es por medio de un usuario y un password (debe de ser digitado por un grupo de funcionarios autorizados por la institución) y el otro por medio de un Token (dispositivo que permite que la información sea encriptada). Esto para seguridad del usuario y de la institución Bancaria. La conexión debe realizarse tomando en cuenta lineamientos y metodologías internacionales, las cuales son establecidas por empresas u organismos reconocidos a nivel mundial, se desea que estos estándares se apliquen en la red inalámbrica del Sistema Bancario Nacional.

La idea principal de la investigación, es acondicionar una red Wireless para los diferentes usuarios del Sistema Bancario Nacional, según políticas internacionales de acceso y autenticación, en los siguientes perfiles:

Los funcionarios: Debe ser una red inalámbrica para que los empleados puedan tener acceso a sus aplicaciones internas, así como también la salida a Internet. El ingreso a ésta, se realizará por medio de certificados digitales, uno de ellos se instalará en la computadora del empleado y el otro es un dispositivo físico que se conectará al computador llamado Token, el cual le permitirá conectarse a la VPN del Banco (“Virtual Private Network” o red privada virtual), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada como Internet.

Miembros de la Junta Directiva: Esta modalidad, es para los altos Jerarcas de la Institución, quienes podrán accesar a Internet por medio un usuario y una clave de acceso, además se realizará un filtrado de cada una de las direcciones MAC (Mac Address, identificar de 48 bits, que corresponde de forma única con una Interfaz de red) de estas personas, con el fin de evitar problemas de conexión y a su vez restringe el uso de personas no autorizas a la red de Banco. Además, también podrán navegar dentro del sitio corporativo sin ningún inconveniente, utilizando el certificado de máquina llamado Token.

Teléfonos Inalámbricos (Voz sobre IP): Este perfil es exclusivo para altos ejecutivos del Banco, quienes utilizan teléfonos portátiles que se conectan a la red inalámbrica. Esto con el fin de que puedan trasladarse a las diferentes oficinas de la Institución sin ningún inconveniente y a su vez puedan ser localizados en cualquier área de la misma.

Para los visitantes (Guess): Este perfil tiene como finalidad dar a funcionarios de empresas proveedoras del Banco, aliados del negocio y visitantes especiales, acceso a Internet, ya sea para consultas o para establecer comunicación con sus respectivas empresas o instituciones. La red Inalámbrica para visitantes, no es una red interna del Banco, por lo tanto no está sometida a las políticas de seguridad y restricciones de navegación utilizadas por la Institución. La misma funcionará por medio de la generación de tiquetes (derecho de navegación) para los visitantes, el cual será entregado por un funcionario del Banco. El mismo le indicará al visitante la fecha y hora de inicio, la fecha y hora final, un usuario y un password para su conexión a la red inalámbrica. Queda bajo la responsabilidad de la persona, la utilización de la red y el Banco no se hará responsable por el daño o perdida de información que pueda sufrir un usuario por la utilización de esta red.

Con todo lo indicado anteriormente, le permitirá a la Institución poder tener una red Wireless para las diferentes necesidades de los usuarios, facilitando a los funcionarios del Banco, a los visitantes y a los altos Jerarcas de la institución

conectarse a internet de una forma segura, confiable y a su vez aplicando las políticas emitidas por organismos internacionales, para beneficios de todos.

Además, según un análisis realizado se identificó que hoy día ninguna institución financiera del Estado, maneja más de dos perfiles a nivel de redes inalámbricas. Es por esto, que este estudio busca la implementación de los perfiles mencionados en los párrafos anteriores. Para así, mejorar la funcionalidad de las redes inalámbricas establecidas en los Bancos del Estado.

Revisión Bibliografía

Actualmente, las empresas líderes se enfrentan con la provisión de acceso a la red para sus clientes, socios, proveedores, contratistas y otros visitantes. Este ingreso a la red ampliada permite una mayor productividad, una mejor colaboración y un mejor servicio, sin embargo, se requiere de políticas de acceso de invitados para hacer frente a un mayor uso de la red y los problemas de seguridad. Al implementar una solución de base amplia para la autenticación de las personas, las empresas pueden controlar el ingreso de red, eliminando su ad hoc (requerimiento de TI) usando seguridad y separando el tráfico de usuarios de manera segura por medio de recursos internos. (Cisco Systems, 2008)

La necesidad de acceso de invitados se ha desarrollado. Hoy en día, con computadoras portátiles, aplicaciones en red, y las líneas digitales de teléfono, la efectividad de una persona que está de visita es severamente limitada, sin acceso permanente a estas tecnologías. Estas redes están creadas para que sus clientes puedan acceder a Internet, y a su propia empresa sin poner en peligro la seguridad de la red de la empresa de acogida. Algunos de los requisitos técnicos es la completa integración en la red de la empresa y sus recursos, además la lógica de separación (segmentación) de tráfico de evaluación del tráfico interno de la empresa. También es necesario asegurar las conexiones VPN para los clientes

las redes corporativas donde es muy importante la autenticación y capacidades de entrada. (Cisco Systems, 2008)

En la actualidad, existen estándares para realizar la configuración y las conexiones a nivel inalámbrico. Uno de ellos se detalla a continuación:

Estándares IEEE

IEEE 802.11-2007: En este estándar se definen los requisitos específicos para conexión inalámbrica y control de acceso medio (MAC). El alcance de esta norma es definir un control Mac y a la capa física (PHY) especificando la conectividad inalámbrica para estaciones fijas, portátiles y móviles dentro de un área local. Este estándar también ofrece los organismos reguladores a manera de normalizar acceso a una o más bandas de frecuencia con el fin de que la comunicación de área local sea compatible para operar dentro ad hoc y las redes de infraestructuras, así como los aspectos de la movilidad STA (transición) en el plazo de dichas redes. (IEEE, 2007)

Además, permite el funcionamiento de un dispositivo IEEE 802.11, dentro de una red de área local inalámbrica (WLAN), con el fin de que puedan coexistir con la superposición de múltiples redes WLAN IEEE 802.11. A su vez, describe los requisitos y procedimientos para proporcionar confidencialidad de los datos de la información del usuario para que sean transferidos a través del medio inalámbrico y autenticación de los dispositivos IEEE 802.11. Para lo cual, se definen mecanismos para la selección de frecuencia dinámica (DFS) y de transmisión de control de potencia (TPC) que puede ser utilizado para satisfacer los requisitos reglamentarios para la operación en la banda de 5 GHz. (IEEE, 2007)

Actualmente existen regulaciones externas, en la cual describen la operación en las redes inalámbricas. Las mismas, se ejecutarán de conformidad

con esta norma y tanto las especificaciones como las definiciones que hacen referencia en él, están sujetas a los requisitos de certificación de equipos y de funcionamiento establecidos por organizaciones regionales y nacionales. En ella se establece los requisitos técnicos mínimos para interoperabilidad, en base a las regulaciones establecidas en el momento de que esta norma se publique. Estos regionales y regulaciones nacionales son objeto de revisión y no podrán ser sustituidos. (IEEE, 2007)

Casos de Empresas que ofrecen el servicio a nivel Internacional

SPC INTERNACIONAL, es una empresa proveedora de soluciones avanzadas en redes y telecomunicaciones, a nivel de Centroamérica con oficinas regionales en Guatemala, El Salvador, Honduras, Panamá y Costa Rica; enfocada en la satisfacción y cumplimiento de los objetivos de negocio de clientes, por medio del diseño, implementación y administración de sus servicios informáticos. Desarrolla e implementa soluciones Integrales eficientes, que mejoran notoriamente el rendimiento de los sistemas de información y comunicaciones. Actualmente funge como asesores externos y habilitadores en materia de seguridad informática, telecomunicaciones y conectividad para empresas privadas, el sector bancario e instituciones públicas. Esta empresa ha asesorado a Instituciones Bancarias del Estado, en la Planificación y ejecución de las redes inalámbricas incluyendo además la telefonía IP, con la que cuentan estas organizaciones financieras hoy día. (SPC INTERNACIONAL, 2009)

DESCA, Empresa líder facilitadora en tecnologías de información y Comunicaciones para Latinoamérica. Su objetivo es potenciar el desarrollo de empresas y entidades en la región, proveyéndolas con nuevas tecnologías y facilitando su aplicación en cuanto soporte técnico, adicionalmente tiene un completo portafolio de servicios y soluciones especializadas. Esta empresa tiene sede central en Miami, posee oficinas de ventas y soporte técnico en Argentina, Brasil, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras,

Nicaragua, México, Panamá y Venezuela. Esta Institución ha participado en la realización de Proyectos importantes relacionados con redes inalámbricas a nivel Internacional en Bancos de Centroamérica. (DESCA, 2011)

Datacyl, es una empresa ubicada en Europa (Castilla y León), dedicada a ofrecer servicios informáticos integrales, para lo cual recomienda la generación de tiquetes para la conexión de visitantes a la red inalámbrica. Dicha empresa recomienda la utilización de esta tecnología en empresas donde llegan clientes y requieren por alguna razón conectarse a Internet. El sistema que esta empresa propone es que los clientes pueden conectar sus propios equipos portátiles a internet de una forma fácil y sencilla mediante la generación de tickets, en la cual el cliente tendrá que solicitar en la recepción un ticket o bono con el número de horas que quiere poder disfrutar de la red wifi. Una vez haya transcurrido el tiempo del ticket o bono que solicitó el sistema cerrará la conexión del cliente a internet y éste no podrá volver a conectarse a menos que solicité otro derecho para la conexión a la red inalámbrica. (DATACYL, 2005)

Leyes en Costa Rica

Costa Rica posee dos leyes relacionadas con el área de Informática, la primera corresponde a la 8454 - "LEY DE CERTIFICADOS, FIRMAS DIGITALES Y DOCUMENTOS ELECTRÓNICOS", en la cual se expone sobre la gestión y conservación de documentos electrónicos, Firmas digitales, Certificados digitales (homologación, suspensión y revocación). También se habla sobre amonestaciones, multas y suspensiones a ejecutar en caso de incumplimiento. (LEY DE CERTIFICADOS, FIRMAS DIGITALES Y DOCUMENTOS ELECTRÓNICOS, 2005)

La segunda es la Ley No. 8148, la cual es creada para reprimir y sancionar los delitos Informáticos, según se indica en los siguientes artículos

"Artículo 196 bis.—Violación de comunicaciones electrónicas. Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos. La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos."

"Artículo 217 bis.—Fraude informático. Se impondrá pena de prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema."

"Artículo 229 bis.—Alteración de datos y sabotaje informático. Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accese, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora.

Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años de prisión. Si el programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años." (Asamblea Legislativa , 2001)

Además de los estándares establecidos a nivel internacional y las leyes nacionales citadas anteriormente, en las instituciones financieras del gobierno, se

crean procedimientos para accesar las redes Wireless. Uno de ellos se denomina **"Procedimiento para conexión a las redes Inalámbricas",** el consiste en seguir una serie de pasos con el fin de tener acceso a los servicios de la red interna de la institución de manera segura, considerado la autenticación, autorización y confidencialidad de los datos que viajan a través de la red. (Banco Nacional de Costa Rica, 2009).

Metodología

Se recurre al enfoque cuantitativo que utiliza la recolección y análisis de datos para contestar preguntas de investigación establecidas previamente, se confía en la medición numérica, el conteo y en el uso de la estadística para establecer con una mayor exactitud los patrones de comportamiento en una determinada comunidad. (Hernández, Fernández y Baptista, 2003)

La presente investigación tomó dicho enfoque debido a que se utilizó un método de recolección de datos a través de una encuesta, dado que se busca contestar la siguiente pregunta: ¿Cómo acondicionar una red Wireless para los diferentes usuarios del Sistema Bancario Nacional, según políticas internacionales de acceso y autenticación?. Ante esto, se analizaron los datos por medio de estadísticas con el programa Ms Excel®, para contestar la pregunta anteriormente expuesta, se realizó la discusión y las conclusiones de dichos resultados.

El cuestionario de la encuesta se divide en tres áreas, en la primera (general) se pregunta sobre características básicas de la red inalámbrica de la institución. En la segunda (seguridad) se investiga sobre si los usuarios realizan autenticaciones de diferentes tipos para ingresar a la red inalámbrica, como también la seguridad física existente. En la tercera (equipos), se consulta sobre los dispositivos que se utilizan en la institución, para un total de 19 preguntas.

La población a la que se le aplicó el cuestionario fue a los ingenieros (Informáticos y/o Electrónicos) que trabajan en el área de Tecnología en los Bancos del Estado, como lo son el Banco Nacional, El Banco Popular y El Banco de Costa Rica, las preguntas fueron entregadas a 55 profesionales que las contestaron en su totalidad, esto dio como resultado una muestra de 50 encuestas completas. La cantidad de empleados pertenecientes al área de Tecnología de los diferentes Bancos se divide aproximadamente de la siguiente manera 260 personas del Banco Nacional, 200 del Banco de Costa Rica y 80 del Banco Popular; para un total de 540 funcionarios, lo cual significa que existe un margen de error de aproximadamente de 13.2%. (Datum Internacional, 2011)

Las encuestas fueron enviadas vía correo electrónico, en un formato de Ms Word®, la muestra fue seleccionada a conveniencia, en el Banco Nacional: Redes e Infraestructura, Desarrollo de Aplicaciones, Arquitectura de Software y Hardware, Implantación de Sistemas y por último Producción (en este se encuentran los ambientes que interactúa con el usuario final). En el Banco de Costa Rica se entrevistó a los funcionarios de las siguientes Unidades: Servicios de Telecomunicaciones y a la de Control y Seguimiento de Proyectos. En lo respecta al Banco Popular, se encuestó únicamente al personal de Investigación Tecnológica quienes analizan y proponen las nuevas estructuras de la Institución a nivel de Redes y Sistemas. Es importante mencionar, que todas las personas entrevistadas son conscientes de que en el Banco donde laboran cuentan con una red inalámbrica, la cual es una pregunta filtro para el análisis de los datos y tener una base sólida para el desarrollo de la investigación.

Resultados

Es conveniente indicar que los datos obtenidos, procesados e interpretados en el siguiente análisis, son producto de la encuesta aplicada un 66% de los encuestados son profesionales con un grado académico de Bachillerato, un 22% son de Licenciatura y por último 12% tienen una Maestría. Además, un 46% poseen de 5 a 10 años de trabajar para la Institución, un 24% cuentan con más de 10 años, un 18% están entre 2 a 5 años y por último 12% son funcionarios que tienen de 0 a 2 años.

Tiempo de laborar y Grado académico

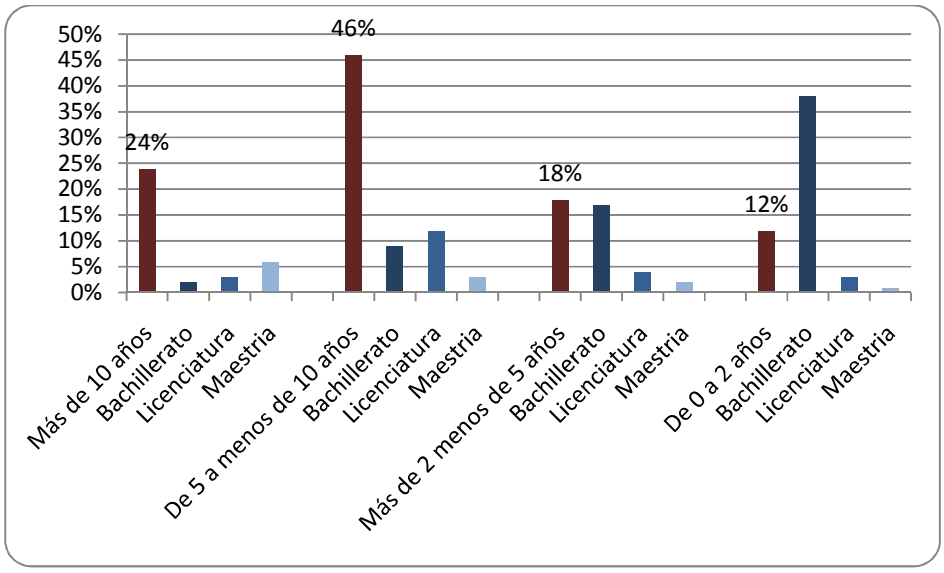

Gráfico No.1

También se analizó que de las personas encuestadas, un 64% trabajan en el área de Redes directamente y las otras 36% se desenvuelven en otras áreas de Tecnología. Este dato es muy importante debido a que se observó que las personas que laboran para redes directamente son las que tienen el conocimiento para responder las preguntar técnicas de la encuesta en cuanto a la seguridad de la Institución y los equipos que utiliza el Banco en su infraestructura física.

Unidad donde se desempeña

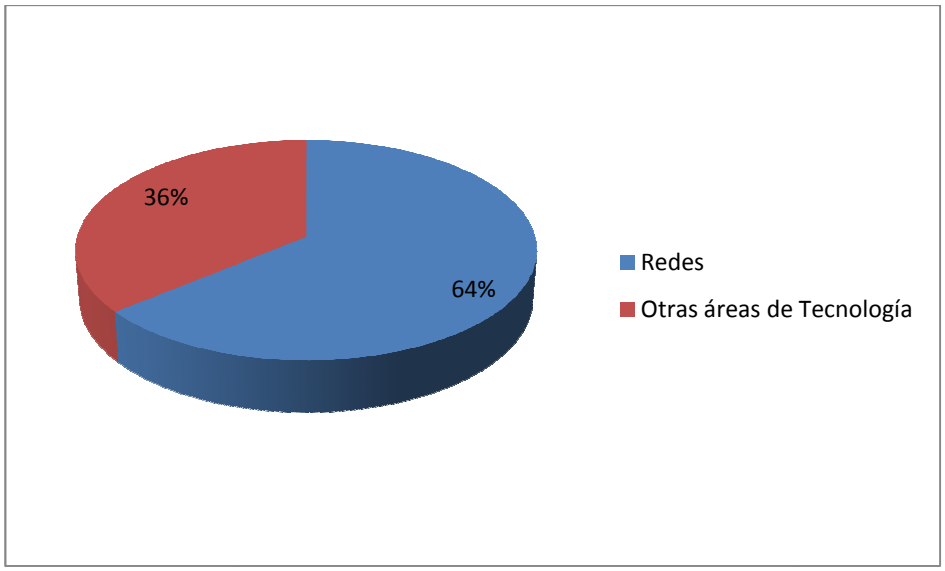

Gráfico No.2

Una de las preguntas claves de la encuesta fue, ¿Cuántos perfiles de redes inalámbricas tienen en la Institución en cual usted labora?, después de analizados los datos se concluyó que esa información es únicamente de conocimiento de los funcionarios que trabajan en redes, por cuanto un 34% indican que poseen 3 perfiles de redes inalámbricas, un 18% dice que tienen 2 perfiles, un 12% manifiestan que tienen 1 perfil y por último un 36% de la población lo desconocen. Esta pregunta de la encuesta es muy importante, ya que la misma va de la mano con nuestra investigación, por cuanto se está recomendando la creación de cuatro perfiles de redes a nivel Bancario, para así tener una separación más minuciosa de los datos que viajan por la red, lo cual asegura no mezclar el tráfico interno con el de los usuarios visitantes.

Perfiles de redes inalámbricas

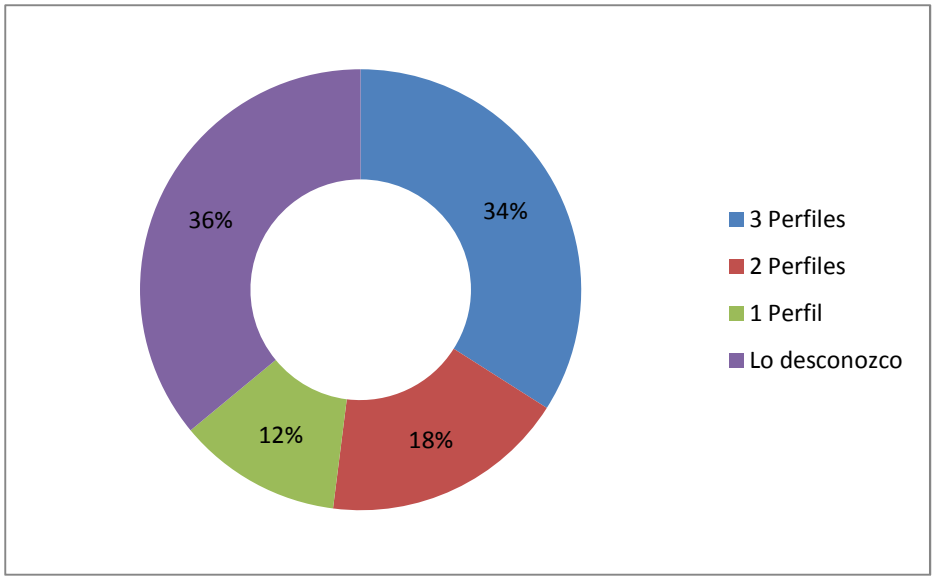

Gráfico No.3

En cuanto a las zonas o pisos que tienen red inalámbrica en las la Instituciones bancarias, se determinó que el 34% de la población indican en Junta Directiva y/o Gerencia y áreas específicas, 18% dicen que tienen solo en áreas específicas, un 12% manifiestan que solo en Junta Directiva y/o Gerencia, y por último 36% mencionan que lo desconocen. Por cuanto se observa que el servicio de redes inalámbricas para empleados y visitantes apenas está iniciando en los Banco del Estado.

Zonas o pisos donde existen redes inalámbricas

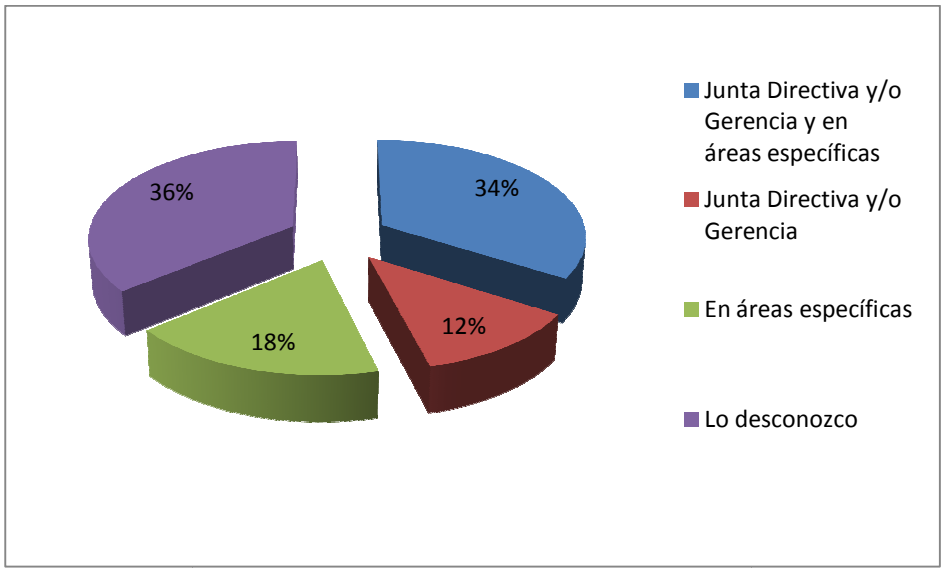

Gráfico No.4

Se consultó a los encuestados, que es lo más importante en una red inalámbrica en cuanto a los criterios de velocidad, seguridad, movilidad, escalabilidad, flexibilidad y adaptabilidad. El 72% de la población indicaron que la seguridad, un 24% seleccionaron Seguridad y Movilidad, un 4% mencionaron que Seguridad y Velocidad y por último el resto de los ítem no fue marcado por ningún encuestado. Como se podrá observar para todas las personas encuestadas la seguridad es muy importante en una red inalámbrica.

Criterios de Importancia en una red inalámbrica

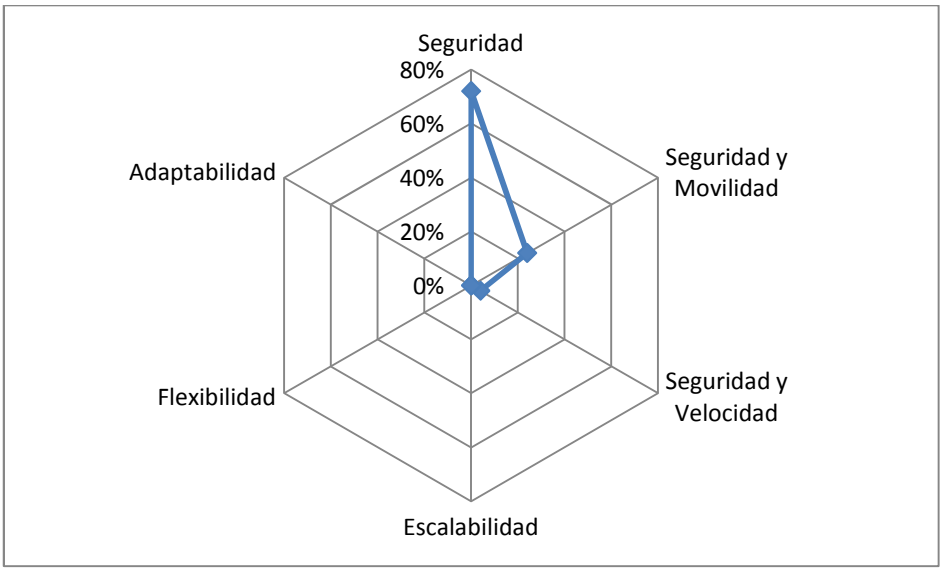

Gráfico No.5

Se investigó sobre el uso de los certificados (usuario y máquina), para conectarse a la red inalámbrica, los cuales permiten que la información viaje de manera encriptada. En cuanto a los resultados obtenidos, se indica que de los Bancos encuestados el 67% de la población indica que si lo usan, un 30% que no lo usan y por último un 3% que lo desconocen.

Certificado de Usuario y Certificado de Máquina

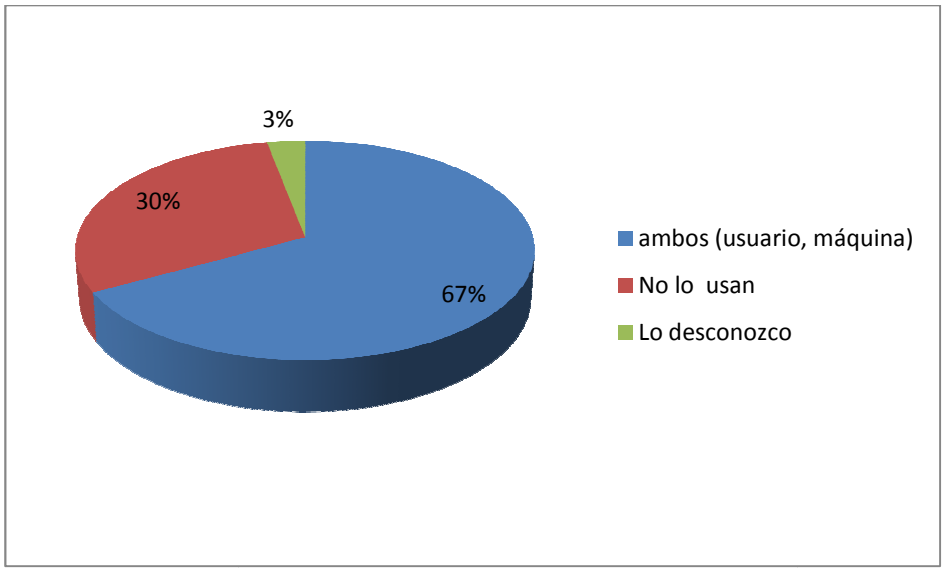

Gráfico No.6

Por último, en cuanto a los estándares utilizados por los Bancos, se indica según las encuestas realizadas que las tres instituciones utilizan todos los estándares a nivel internacional los cuales son 802.11a, 802.11b, 802.11g y el 802.11n.

Discusión

Después de haber analizado la información, se observó que actualmente los bancos consideran importante no sólo tener una red alámbrica si no también estar a la altura de muchas empresas en cuanto a nivel de tecnología y servicio. Es por esto, que los bancos estatales vieron la necesidad de facilitar a nuestros empleados, miembros de la Junta Directiva, clientes, proveedores entre otros, disponer de una red sin cables, ya que según la encuesta realizada en estas

instituciones financieras, todos cuentan con una red inalámbrica pero ninguno posee la segmentación de red que se propone en este documento. Es importante indicar que según conversación con miembros de los Bancos sería interesante poner en práctica lo que se propone en la presente investigación.

Para el 100% de las personas encuestadas la seguridad en una red inalámbrica es de suma importancia ya que el hecho de proponer varios perfiles en una red, da seguridad de no mezclar tráfico de información de empleados con los datos de los invitados. Siguiendo con el tema de seguridad, en la mayoría de los bancos aplican filtros en sus direcciones MAC (Mac Address), con el propósito de que si una persona externa averigua la clave de la red no pueda ingresar a la misma debido a que su dirección Mac no está configurada con los equipos de la red inalámbrica. Otro aspecto de seguridad es que en dos de los tres Bancos encuestados utilizan Certificado de Máquina y Certificado de Usuario (recomendado por Microsoft), el primero sirve para autenticar la estación o el dispositivo que se conecte a la red y el segundo funciona para verificar que la persona que se está conectando a la red sea efectivamente quien dice ser.

En cuanto a los estándares, se consultó a los encuestados, sobre cuáles aplican a sus empresas, según lo analizado, en los tres bancos aplican los establecidos por la IEEE (Organismo reconocido a nivel internacional). Estos consisten en especificar las velocidades de transmisión las cuales se realizan por señales infrarrojas, además utilizan el protocolo CSMA/CA (Múltiple acceso por detección de portadora evitando colisiones), el cual tiene como función el control de redes evitando colisiones entre los paquetes de datos debido a que comúnmente en redes inalámbricas, no se cuenta con un modo práctico para transmitir y recibir simultáneamente. Los servicios ofrecidos por este estándar son: el control y acceso a la seguridad, transmisión y distribución de los mensajes, el armado de las tramas y por último, el tiempo que dura la conexión.

Otro aspecto importante, es que en los tres Bancos aplican a lo que se conoce como Calidad de Servicio (Quality of Service, en inglés), esto es una tecnología que recomienda Cisco, la cual garantiza envió de información en un tiempo dado. Es importante para ciertas aplicaciones tales como la transmisión de datos, vídeo y voz, lo cual permite marcar los paquetes con el fin de darle prioridad a las transacciones que viajan por la red. También se indagó sobre si existe un Firewall entre la red alámbrica y la red inalámbrica para realizar la separación de datos, lo cual está siendo ejecutado solamente por uno de los tres bancos encuestados.

Referente a las topologías utilizadas en los bancos en su red inalámbrica dos de ellos utilizan la denominada múltiples puntos de acceso y “roaming”, este es utilizado para resolver problemas particulares de estructura, el diseñador de la red puede elegir usar un Punto de Extensión (EPs) para aumentar el número de puntos de acceso a la red. Los puntos de extensión funcionan como su nombre indica: extienden el rango de la red retransmitiendo las señales de un cliente a un punto de acceso o a otro punto de extensión. Los puntos de extensión pueden encadenarse para pasar mensajes entre un punto de acceso y clientes lejanos de modo que se construye un "puente" entre ambos. El otro Banco trabaja con la topología llamada cliente-punto de acceso, este es “concentrador” inalámbrico. El transmisor/receptor conecta entre sí los nodos de la red inalámbrica y normalmente también sirve de puente entre ellos y la red cableada. Un conjunto de puntos de acceso (coordinados) se pueden conectar unos con otros para crear una gran red inalámbrica. Desde el punto de vista de los clientes inalámbricos (como las computadoras portátiles o las estaciones móviles), un punto de acceso provee un cable virtual entre los clientes asociados. Este “cable inalámbrico” conecta tanto a los usuarios entre sí, como los clientes con la red cableada. Ambas topologías son recomendadas por Cisco.

En sección de equipos, se le consultó a los encuestados sobre los fabricantes que nos facilitan los dispositivos para redes inalámbricas se observó

que un 100% de los encuestados seleccionaron la marca Cisco, la cual es una empresa reconocida a nivel mundial en lo que a dispositivos y redes de Internet se refiere. Esta empresa se implica especialmente en el ámbito educacional. Enfoca su investigación a la aplicación de la tecnología en la educación y en más de una ocasión ha participado activamente para mejorar este ámbito.

Algunos de los dispositivos que utilizan los Bancos para conexión de sus redes inalámbricas son: routers, switches hubs, dispositivos de seguridad como Cortafuegos y Concentradores para VPN, Productos de Telefonía IP como teléfonos y el CallManager el cual es un software que administra toda la configuración de los teléfonos inalámbricos, Equipos para Redes de Área de Almacenamiento, Comunicaciones ópticas, Interfaces y módulos como también Sistemas de interoperabilidad.

Por último, todos los bancos utilizan un servidor AAA, para la autenticación a su red inalámbrica. Cuyas siglas significan autorización, autenticación y accounting (registro de logs), se utilizan para una mayor seguridad en el acceso dentro de una red inalámbrica. Este servidor es recomendado por Microsoft, para múltiples tareas en las Instituciones, entre ellas la indicada anteriormente. (Microsoft, 2011)

Conclusiones

Existen varios puntos importantes que mencionar después de analizada la información de las encuestas y lo recomendado por Cisco, IEEE y Microsoft, mediante sus páginas Web. En Primera, los resultados de trascendencia en esta investigación fue facilitado por personas especialistas en el área de Redes, debido a que la información solicitada en las encuestas la mayoría es muy técnica. Por lo

que, con esta selección se concluye que en los Bancos del Estado mantienen normas de seguridad en cuanto a la información, sin embargo el personal de otras dependencias ajenas a redes no conocen a fondo los rubros relacionados con la infraestructura y seguridad de las redes inalámbricas en la Institución.

En segunda, se determinó que ninguno de los tres Bancos (Banco Nacional, Banco de Costa Rica y Banco Popular) maneja más de tres perfiles en sus redes inalámbricas, lo cual es muy importante para la separación del tráfico y para la misma seguridad de la empresa. Actualmente Cisco, según el documento llamado "**Deployment Guide for Cisco Guest Access Using the Cisco Wireless Lan Controller**" indicado en la bibliografía de este documento, en el cual recomiendan una metodología para implementar el manejo de la red inalámbrica para los visitantes, con el propósito de hacer que la misma sea utilizada por los usuarios de las empresas (clientes, Proveedores, asesores, entre otros) únicamente cuando sea necesario, debido a que se generará un tiquete el cual va indicar el número de horas e incluso el número de días si fuese del caso, para poder disfrutar de la red Inalámbrica, por lo que se aconseja a los Bancos invertir en esta modalidad para seguridad de ellos y de los usuarios visitantes.

En tercera, se concluye que la seguridad en una red inalámbrica es importante para la población encuestada ya que todas las personas en cuanto a los criterios de velocidad, seguridad, movilidad, escalabilidad flexibilidad y adaptabilidad seleccionaron el ítem de seguridad. Además dos de los tres Bancos (Banco Nacional y Banco Popular) utilizan certificados de Usuario y Máquina (recomendado por Microsoft), lo cual permite que la información viaje encriptada para beneficio de ambas las partes.

Se conoce, que de la Población encuestada el 100 %, seleccionó a Cisco como un fabricante de confianza, con lo que deducimos que por su buena reputación a nivel internacional, las empresas hacen uso de sus productos (telecomunicaciones) y sigue sus recomendaciones por medio de las empresas Parther, las cuales dos de ellas se citan en la bibliografía de este documento.

Por último, según se observó, no existe a nivel de nuestro país una Ley, en la cual se especifiquen las sanciones a realizar si alguna persona ingresa a una red inalámbrica para visitantes (Guest), en una empresa determinada y se valga de técnicas informáticas para hacer daño a la institución aprovechándose de que existen debilidades en seguridad. Por lo que, a criterio sería importante retomar este tema, debido a que hoy día las comunicaciones Wireless están tomando cada vez más fuerza a nivel internacional.

Bibliografía

Asamblea Legislativa . (09 de 11 de 2001). *Ley no.8148 Delitos informaticos*. Recuperado el 18 de marzo de 2011, de http://www.pgr.go.cr/

Banco Nacional de Costa Rica. (2009). *Procedimiento para conexión de redes inalámbricas.* San José.

Cisco Systems. (1 de Febrero de 2008). *Deployment Guide for Cisco Gust Access Using the Cisco Wireless Lan Controller*. Recuperado el 18 de marzo de 2011, de http://www.cisco.com/en/US/docs/wireless/technology/guest_access/technical/reference/4.1/GAccess_41.html#wp1000402

DATACYL. (2005). *SOLUTIONS DATACYL*. Recuperado el 18 de marzo de 2011, de http://www.datacyl.com/

Datum Internacional. (2011). *Calculadora del margen de Error*. Recuperado el 24 de Marzo de 2011, de http://www.datum.com.pe/margendeerror.php

DESCA. (2011). *Desca, Enabling Technology, Empowering Business*. Recuperado el 18 de Marzo de 2011, de http://www.desca.com

IEEE. (12 de Junio de 2007). *LOCAL AND METROPOLITAN AREA NETWORK STANDARDS*. Recuperado el 18 de Marzo de 2011, de http://standards.ieee.org/getieee802/download/802.11-2007.pdf

LEY DE CERTIFICADOS, FIRMAS DIGITALES Y DOCUMENTOS ELECTRÓNICOS. (30 de agosto de 2005). Recuperado el 18 de marzo de 2011, de http://www.bccr.fi.cr/documentos/secretaria/archivos/Ley%208454-Ley%20de%20Firma%20Digital.pdf

Microsoft. (2011). Recuperado el 24 de marzo de 2011, de www.microsoft.com/.../directory/activedirectory/

Profesional, P. (2010). *Acerca de los conceptos competencia y competencia laboral*. Recuperado el 27 de 03 de 2010, de http://pedagogia-profesional.idoneos.com/index.php/Acerca_de_los_conceptos_competencia_y_competencia_laboral_Acerca_de_los_conceptos_competencia_y_competencia_laboral

SPC INTERNACIONAL. (2009). Recuperado el 18 de 03 de 2011, de http://www.spcinternacional.com/nuestraemp.html

Anexo

Cuestionario

El presente cuestionario forma parte de un estudio con el que la Universidad está llevando a cabo con el fin de conocer la opinión de los especialistas y no especialistas en redes, con el fin de determinar los perfiles existentes en una red Inalámbrica a nivel del Sistema Bancario Nacional. El cuestionario es fácil y rápido de completar: estimamos que usted deberá disponer de unos 5 minutos para responderlo.

Su participación en este estudio es voluntaria. Usted no tiene que darnos su nombre. Los resultados serán de uso estrictamente interno de ULACIT. Le solicitamos se sirva contestar de forma objetiva, pues nuestro propósito es contar con un diagnóstico de la carrera con miras a su continuo mejoramiento.

Instrucciones: Seleccione con "X" (equis) la(s) opción(es) que considere más acertada(s), según las Políticas utilizadas en la empresa para la cual usted trabaja. (Puede marcar más de una Opción, cuando lo considere).

Generales

1. *En el Banco donde usted labora cuenta con red inalámbrica?*
    a. *Si*
    b. *No*

2. *En cuales zonas o pisos tiene red inalámbrica la institución?*
    a. *En todo el Edificio*
    b. *Junta Directiva y/o Gerencia*
    c. *En áreas especificas*
    d. *Sitios remotos*
    e. *Otros*

3. *Cuantos perfiles de redes inalámbricas tienen?*
    a. *Uno*
    b. *Dos*
    c. *Tres*
    d. *Más de tres*
    e. *Lo desconozco*

4. *Qué topología utilizan en la red inalámbrica?*
    a. *Peer-to-Peer*
    b. *Cliente-punto de acceso*
    c. *Múltiples puntos de acceso y "roaming"*
    d. *Uso de un punto de extensión*
    e. *Utilización de antenas direccionales*
    f. *Lo desconozco*

5. *Para usted que es más importante en una red Inalámbrica?*
    a. *Velocidad*
    b. *Seguridad*
    c. *Movilidad*
    d. *Escalabilidad*
    e. *Flexibilidad*
    f. *Adaptabilidad*
    g. *Lo desconozco*

6. *Cuanto es el tiempo que tiene de trabajar para la Institución Bancaria*
    a. *0 a 2 años*
    b. *Más de 2 años y menos de 5*
    c. *De 5 a 10 años*
    d. *Más de 10 años*

7. *Su grado académico es el siguiente:*
    a. *Bachillerato*
    b. *Licenciatura*
    c. *Maestría*
    d. *Ninguno de los anteriores*

Seguridad

8. *Que método para implementar una buena seguridad implementan?*
    a. *Filtrado de direcciones Mac*
    b. *Web (Wired Equivalent Privacy)*
    c. *Las VPN*
    d. *El 802.X*
    e. *WPA (Wi-fe Protected Access)*
    f. *Lo desconozco*

9. *Utilizan certificados para proteger su red inalámbrica?*
    a. *Si*
    b. *No*

10. *Si su respuesta anterior es afirmativa. Cuales certificados utiliza?*
    a. *De máquina*
    b. *De Usuario*
    c. *Ambos*
    d. *No usamos*
    e. *Lo desconozco*

11. *Qué tipo de Autenticación utiliza el Access Point?*
    a. *Open System*
    b. *Shared Key*
    c. *Lo desconozco*

12. *Existe un firewall entre la red alámbrica e inalámbrica?*
    a. *Si*
    b. *No*
    c. *Lo desconozco*

13. *Aplica encriptación en su red inalámbrica?*
    a. *Si*
    b. *No*
    c. *Lo desconozco*

14. *Si su respuesta anterior es afirmativa. Cuales esquemas de encriptación / seguridad emplea su Institución?*
    a. *IPSEC*
    b. *SSH*

c. *SSL*
d. *LWAPP/CAPWAP*
e. *Lo desconozco*
f. *Ninguna*
g. *Otro _____*

15. *Utilizan Quality of Service (QoS) en su red?*
    a. *Si*
    b. *No*
    c. *Lo desconozco*

16. *Qué protocolos utilizan en la red inalámbrica?*
    a. *WEP*
    b. *WPA*
    c. *WPA2*
    d. *Lo desconozco*
    e. *Otro _____*

17. *Cuales estándares Soporta su red inalámbrica?*
    a. *802.11a*
    b. *802.11b*
    c. *802.11g*
    d. *802.11n*
    e. *Todos los anteriores*
    f. *Lo desconozco*

Equipos

18. *Qué fabricante le da más confianza?*
    a. *Cisco*
    b. *D-Link*
    c. *TP-Link*
    d. *Huavey*
    e. *Ninguno de los anteriores*
    f. *Otro _____*

19. *Utiliza un servidor AAA como servidor de autenticación?*
    a. *Si*
    b. *No*
    c. *Lo desconozco*