FECHA	8–FEBRERO–2011

NÚMERO RAE	
PROGRAMA	Ingeniería de Sistemas

AUTOR (ES)	PULIDO, Andrea; RINCON, Paulo y VELASQUEZ, Oscar
TÍTULO	Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá.

PALABRAS CLAVES	Seguridad de la información, red SOHO, norma 17799, norma 27001, Infraestructura, aplicaciones, operaciones, personal, política de seguridad, controles de seguridad.

DESCRIPCIÓN	A causa del creciente uso de Internet, más empresas aceptan que sus clientes, empleados, socios y proveedores ingresen a sus sistemas de información. Adicionalmente, por el estilo de vida migratorio que existe en la actualidad, donde los empleados acceden remotamente a los sistemas de información, se les pide a estos llevar consigo información fuera de la empresa. Por consiguiente, es de vital importancia conocer ¿qué recursos necesitan ser protegidos en las empresas? con el fin de tener control sobre la información, ¿qué personal ingresa al sistema? y ¿cuáles son sus permisos en éste? No solo deben emplearse soluciones técnicas, sino también, deben hacer énfasis en la capacitación y toma de conciencia por parte del usuario sobre la seguridad de la información, además de la aplicación de medidas claramente definidas. Las medidas que se adopten para la seguridad de la información pueden también producir molestias a los usuarios. A menudo, las reglas y los procedimientos se tornan cada vez más difíciles de cumplir e implementar cuando crece la red. Por tanto, la seguridad de la información debe garantizar que los usuarios hagan uso adecuado de ella. Además, deben identificarse las principales vulnerabilidades para conocer y deducir el camino del atacante. La intención de este proyecto es proponer políticas y controles de seguridad de la información, así como dar una visión general de los posibles atractivos de los atacantes, clasificarlos y dar una percepción de las vulnerabilidades de los sistemas de información para saber cuál es la forma más apropiada para reducir el riesgo de ataques e intrusiones. Este proyecto proviene de un macro-proyecto realizado en la Universidad San Buenaventura en el semillero de NEOBYTE, el cual dividió las empresas por sectores tal como lo divide la Cámara de Comercio de Bogotá. Con base en esto, el proyecto se centra en el diseño de políticas y controles para las empresas del sector transporte con redes SOHO en Bogotá.

FUENTES BIBLIOGRÁFICAS	• Norma Técnica Colombiana NTC – ISO/IEC 17799, Tecnología de la Información, ICONTEC, 2006 • Norma Técnica Colombiana NTC – ISO/IEC 27001, Tecnología de la Información, ICONTEC, 2006 • Organization for Economic Cooperation and Development (OEDC) Guidelines for Security of Information Systems. 1992. • SWANSON et al. (1996) National Institute of Standard and Technology (NIST). General Principles for Information Systems Security Policies. • CHAPMAN, B y ZWICKY, E.(1997) Construya Firewalls para Internet. O'Really. Edición en Español por McGraw Hill. • BAYUK, J. (1997) Security through process management. Price Waterhouse, LLP. • WILSON, M (1996) Marketing and Implementing Computer Security. NIST. • CERRACEDO, G Justo. "Seguridad en redes telemáticas". Mac Graw Hill. 2004 • COMER Douglas E. "Redes de Computadores, Internet e interredes". Prenticel Hall. Primera edición. 1998. • MENDES, Alvarado, Iván. "PROYECTO SEGURIDAD INFORMÁTICA PARA LAS REDES DE DATOS SOHO EN LA PEQUEÑA EMPRESA DE BOGOTÁ". • STALLINGS, William, "fundamentos de seguridad en redes aplicaciones y estándares". Prentice Hall .2006 • MARCELO RODAJO , "Piratas Cibernéticos" editorial: RA-MA 2003 • CARRACEDO GALLARDO,JUSTO "Seguridad en redes telemáticas", editorial Mac Graw Hill. • Ing. Ramírez-David http://www.fortinet.com/ 16 de noviembre de 2008 12:45 • http://www.monografías.com, La Informática y Su Impacto Social, 16 de noviembre de 2008 13:30 • http://www2.vo.lu/homepages/phahn/humor/hacker30.txt 23 de noviembre de 2008 12:30 • http://www.informaticajuridica.com/legislacion/colombia.asp 23 de mayo de 2009 14:00 • http://eva.utpl.edu.ec/openutpl/ocw/mod/glossary/view.php?id=153&mode=date 11 de febrero de 2009 17.00 • http://www.inegi.gob.mx/inegi/contenidos/espanol/ciberhabitat/museo/cerquita/redes/seguridad/intro.htm 14 de febrero de 2009 14:00 • http://www.unal.edu.co/seguridad/legislacion.htm 16 de agosto de 2009 13:00

NÚMERO RAE	
PROGRAMA	Ingeniería de Sistemas

CONTENIDOS	Los objetivos propuestos para nuestro proyecto son: *Identificar las principales vulnerabilidades en los sistemas de información en las pequeñas empresas con redes SOHO en el sector transporte de Bogotá. *Analizar la información obtenida de las empresas, para la adecuada categorización de las vulnerabilidades, teniendo en cuenta la Norma NTC-ISO/IEC 27001 - 17799. *Plantear las políticas necesarias para la seguridad de la información en las pequeñas empresas con redes SOHO en el sector transporte de Bogotá. *Definir controles que garanticen la seguridad de la información en las pequeñas empresas con redes SOHO en el sector transporte de Bogotá. Para cumplir a cabalidad con estos objetivos, seguimos los siguientes pasos: • **Asignación del sector transporte por parte del semillero de investigación NEOBYTE**. Según la Cámara de Comercio de Bogotá las empresas se dividen por sectores. Así mismo, el semillero de investigación NEOBYTE de la universidad de San Buenaventura Bogotá asigno a sus integrantes estos sectores para desarrollar una investigación sobre las vulnerabilidades que tienen las pequeñas empresas con respecto a su información almacenada digitalmente. Para el presente proyecto fue asignado el sector transporte. • **Sectorización de empresas y llamada de presentación por parte de los estudiantes de la universidad San Buenaventura. a las empresas previamente seleccionadas.** De un total de 258 empresas resulto una muestra de 100. (Ver anexo C del documento de tesis) Al realizar las llamadas y en el caso de tener respuesta a esta, se tomó como base un libreto de presentación suministrado por el semillero de investigación NEOBYTE. (Ver anexo D del documento de tesis). En la verificación de datos comerciales de las empresas se pudo encontrar que muchas ya no se encontraban activas, el número telefónico no correspondía a la empresa o no estaban interesados en participar de la investigación (Ver Tabla 11 del documento de tesis).

- **Visita y aplicación de encuestas sobre los niveles de seguridad que tienen las empresas que aceptaron participar en la investigación.**

Se procedió a visitar a las 16 empresas, a aplicar una encuesta, recibir sugerencias de los encuestados y motivarlos para que protejan sus sistemas de información adecuadamente.

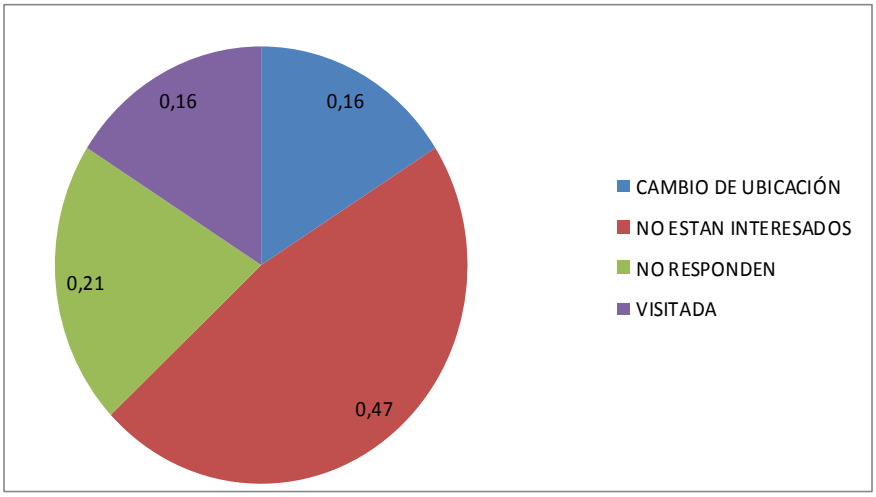
- **Tabulación de resultados**.

Después de haber visitado todas las empresas se hizo la recopilación y consolidación de la información obtenida, posteriormente se realizó la tabulación y la generación de los informes sobre los resultados obtenidos.

Ilustración 4 Llamada a empresas.

RESULTADO LLAMADA	N. EMPRESAS	%
CAMBIO DE UBICACIÓN	16	0,16
NO ESTAN INTERESADOS	47	0,47
NO RESPONDEN	21	0,21
VISITADA	16	0,16

TOTAL EMPRESAS LLAMADAS	**100**



- **Análisis de Vulnerabilidades con respecto a los informes obtenidos en las encuestas.**

De acuerdo con las respuestas obtenidas en la evaluación de riesgos aplicada durante la encuesta, las medidas de defensa se calificaron de la siguiente forma. Infraestructura, aplicaciones y operaciones. Con base en la información obtenida se identificaron las falencias en cuanto a la seguridad de la información de las empresas.

- **Selección de los dominios aplicables a las empresas y sus necesidades.**

Basados en la norma NTC-ISO 17799 y en el análisis de vulnerabilidades se definieron los dominios aplicables a las empresas del sector transporte y de este modo se clasificaron las áreas que se cubrieron con las políticas de seguridad.

- **Plantear las políticas de seguridad más apropiadas para las empresas.**

Con los dominios ya puntualizados, se plantearon las políticas de seguridad apoyadas en las especificaciones dadas por la norma NTC-ISO 17799 de tal modo que se cubrió la gran mayoría de vulnerabilidades encontradas en el análisis.

- **Definición de controles**

Después de analizar las vulnerabilidades y formular políticas, se propusieron controles que van a permitir reducir riesgos y generar mayor confiabilidad.
Para aumentar los niveles de seguridad se recomendaron controles adaptativos con el fin de reducir amenazas, errores o ataques, tanto en ubicaciones físicas como lógicas. Se utilizó como referencia el manual de cableado estructurado. (Ver anexo E del documento de tesis).

NÚMERO RAE	
PROGRAMA	Ingeniería de Sistemas

METODOLOGÍA

LÍNEA DE INVESTIGACIÓN DE USB/ SUBLÍNEA DE FACULTAD / CAMPO TEMÁTICO DEL PROGRAMA

Desde el punto de vista de la Facultad de Ingeniería de la Universidad de San Buenaventura sede Bogotá y siguiendo las directrices del consejo de investigación Bonaventuriano para proyectos de este tipo, la Línea de investigación es: “Tecnologías actuales y sociedad”, la Sub-línea es: “Sistemas de información y comunicación” y el campo temático hace referencia a: “Redes de Computadores”.

POBLACIÓN Y MUESTRA

Se tomó una población de doscientos cincuenta y ocho (258) pequeñas empresas del sector TRANSPORTE registradas en la cámara de comercio de Bogotá. Dejando una muestra representativa de cien (100) de estas, de las cuales solo participaron del proyecto dieciséis 16 empresas.

HIPÓTESIS

Con el fin reducir los riesgos de ataques y amenazas a los que se encuentran expuesta las pequeñas y medianas empresas con redes SOHO en el sector transporte de Bogotá, se plantea un manual estableciendo políticas y controles basados en Normas para la seguridad de la información.

VARIABLES

Variables Independientes

- Sector de trasporte en las pequeñas y medianas empresas en Bogotá.
- Usuarios que se encuentran ingresando a la información.

Variables Dependientes

- Sistemas de seguridad de la información.
- Políticas y controles para la seguridad de la información.

CONCLUSIONES	• Proteger la información es una tarea cada vez más compleja para las empresas. • Se ha observado que el riesgo que las empresas corren frente a las amenazas de seguridad es serio, debido a la poca importancia que se dá a este tópico y a la falta de conocimiento que estas tienen sobre el tema de seguridad de la información. • Para disminuir los riesgos que se corren frente a la seguridad las empresas solo tienen en cuenta la Tecnología y no los procesos ni el persona • El éxito de un plan para mitigar los riesgos queda en manos de los usuarios. • Las empresas del sector transporte no toman la seguridad de la información como parte de la organización empresarial y si como un proceso aislado. • La seguridad de la información es un agente importante dentro de las empresas y como tal se debe plantear mecanismos y/o estrategias que garanticen la integridad de dicha información. • En general las empresas no implementan ningún tipo de seguridad en el perímetro de la red. No hay escudo protector contra intrusos, existen carencias severas en el punto donde la red interna de las pequeñas empresas se conecta con el exterior. • Las empresas con redes SOHO no emplean procedimientos estrictos de autenticación de usuarios administradores, locales y de acceso remoto. Por tal motivo, intrusos pueden acceder fácilmente y sin autorización a la red mediante ataques locales o remotos. • En las empresas analizadas no se garantiza la integridad y confidencialidad de los datos, la pérdida o el robo de estos afectan negativamente tanto los ingresos de las empresas como su reputación. • En Colombia la seguridad de la información es muy escasa, en muy pocas empresas se preocupan por proteger adecuadamente su información.

DISEÑO DE POLÍTICAS Y CONTROLES PARA LA SEGURIDAD DE LA INFORMACIÓN EN PEQUEÑAS EMPRESAS CON REDES SOHO EN EL SECTOR TRANSPORTE DE BOGOTÁ.

ANDREA MARCELA PULIDO CHADID
PAULO CÉSAR RINCÓN ALBARRACÍN
OSCAR MAURICIO VELÁSQUEZ ACOSTA

UNIVERSIDAD DE SAN BUENAVENTURA
FACULTAD DE INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
BOGOTÁ
2010

DISEÑO DE POLÍTICAS Y CONTROLES PARA LA SEGURIDAD DE LA INFORMACIÓN EN PEQUEÑAS EMPRESAS CON REDES SOHO EN EL SECTOR TRANSPORTE DE BOGOTÁ.

ANDREA MARCELA PULIDO CHADID
PAULO CÉSAR RINCÓN ALBARRACÍN
OSCAR MAURICIO VELÁSQUEZ ACOSTA

Trabajo de grado como requisito para optar por el título de Ingeniería de Sistemas

UNIVERSIDAD DE SAN BUENAVENTURA
FACULTAD DE INGENIERÍA
PROGRAMA INGENIERÍA DE SISTEMAS
BOGOTÁ
2010

CONTENIDO

INTRODUCCIÓN 4
1. PLANTEAMIENTO DEL PROBLEMA 5
1.1. ANTECEDENTES 5
1.2. DESCRIPCIÓN Y FORMULACIÓN DEL PROBLEMA 7
1.3. JUSTIFICACIÓN 8
1.4. OBJETIVOS DE LA INVESTIGACIÓN 9
1.4.1. Objetivo General. 9
1.4.2. Objetivos Específicos. 9
1.5. ALCANCES Y LIMITACIONES DEL PROYECTO 10
1.5.1. Alcances. 10
1.5.2. Limitaciones. 10
2. LÍNEA DE INVESTIGACIÓN DE USB/ SUBLÍNEA DE FACULTAD / CAMPO TEMÁTICO DEL PROGRAMA 11
3. METODOLOGÍA 12
3.1. ENFOQUE DE LA INVESTIGACIÓN 12
4. MARCO DE REFERENCIA 13
4.1. MARCO TEÓRICO – CONCEPTUAL 13
4.1.1. La información como parte primordial de las organizaciones 13
4.2. MARCO LEGAL O NORMATIVO 21
5. DESARROLLO INGENIERIL 24
5.1. RECOLECCIÓN Y ANÁLISIS DE LA INFORMACIÓN 24
5.2. ANÁLISIS DE VULNERABILIDADES 24
5.2.1. Infraestructura 25
5.2.2. Aplicaciones 27
5.2.3. Personal y operaciones 29
5.3. DOMINIOS 32
5.4. POLÍTICAS 33
5.4.1. Política de Seguridad. 33
5.4.2. Seguridad Organizacional. 33
5.4.3. Administración de Activos de Información. 35
5.4.4. Seguridad del Recurso Humano. 36
5.4.5. Seguridad Física y Ambiental. 36

5.4.6. Administración de comunicaciones y operaciones. 38
5.4.7. Control de Acceso. 39
5.4.8. Mantenimiento y desarrollo de sistemas de información. 40
5.4.9. Administración de Incidentes de Seguridad. 40
5.4.10. Administración de la continuidad del negocio 40
5.5. CONTROLES 41
5.5.1. Controles de infraestructura 41
5.5.2. Controles de aplicaciones 48
5.5.3. Controles de personal 49
5.5.4. Controles de operaciones 51
6. PRESENTACIÓN Y ANÁLISIS DE RESULTADOS. 52
7. CONCLUSIONES 55
8. RECOMENDACIONES 56
9. BIBLIOGRAFÍA 57
GLOSARIO 59
ANEXOS 65

LISTA DE TABLAS

Tabla 1 Defensa perimetral. 25
Tabla 2 Autenticación. 26
Tabla 3 Gestión y control. 27
Tabla 4 Implementación y uso. 28
Tabla 5 Diseño de aplicaciones. 28
Tabla 6 Almacenamiento y comunicaciones de datos. 29
Tabla 7 Requisitos y evaluaciones. 30
Tabla 8 Directiva y procedimientos. 30
Tabla 9 Formación y conocimiento. 31
Tabla 10 Vulnerabilidades por secciones. 31

LISTA DE ILUSTRACIONES

Ilustración 1 RED SOHO 17
Ilustración 2 Conexión enrutada 18
Ilustración 3 Conexión Traducida..... 19
Ilustración 4 Llamada a empresas. 53

INTRODUCCIÓN

A causa del creciente uso de Internet, más empresas aceptan que sus clientes, empleados, socios y proveedores ingresen a sus sistemas de información. Adicionalmente, por el estilo de vida migratorio que existe en la actualidad, donde los empleados acceden remotamente a los sistemas de información, se les pide a estos llevar consigo información fuera de la empresa. Por consiguiente, es de vital importancia conocer ¿qué recursos necesitan ser protegidos en las empresas? con el fin de tener control sobre la información, ¿qué personal ingresa al sistema? y ¿cuáles son sus permisos en éste?

No solo deben emplearse soluciones técnicas, sino también, deben hacer énfasis en la capacitación y toma de conciencia por parte del usuario sobre la seguridad de la información, además de la aplicación de medidas claramente definidas.

Las medidas que se adopten para la seguridad de la información pueden también producir molestias a los usuarios. A menudo, las reglas y los procedimientos se tornan cada vez más difíciles de cumplir e implementar cuando crece la red. Por tanto, la seguridad de la información debe garantizar que los usuarios hagan uso adecuado de ella. Además, deben identificarse las principales vulnerabilidades para conocer y deducir el camino del atacante. La intención de este proyecto es proponer políticas y controles de seguridad de la información, así como dar una visión general de los posibles atractivos de los atacantes, clasificarlos y dar una percepción de las vulnerabilidades de los sistemas de información para saber cuál es la forma más apropiada para reducir el riesgo de ataques e intrusiones.

Este proyecto proviene de un macro-proyecto realizado en la Universidad San Buenaventura en el semillero de NEOBYTE, el cual dividió las empresas por sectores tal como lo divide la Cámara de Comercio de Bogotá.

Con base en esto, el proyecto se centra en el diseño de políticas y controles para las empresas del sector transporte con redes SOHO en Bogotá.

1. PLANTEAMIENTO DEL PROBLEMA

1.1. ANTECEDENTES

"*Los datos son para las organizaciones lo que significa el corazón para el cuerpo humano*"[1]. A partir de este enunciado se podría decir que la información es el bien más preciado de una empresa, ya que en esta se apoyan todos los negocios existentes, alrededor se rigen o se basan todos los procesos que se llevan a cabo, la información resulta ser todo, por lo tanto, mantenerla segura y protegerla de extraños resulta ser de vital importancia en el ámbito laboral.

Haciendo un poco de historia, durante los primeros años de la era informática, los ataques a sistemas requerían pocos conocimientos técnicos. Por un lado, los ataques realizados desde el interior de la red se basaban en la alteración de permisos para modificar la información del sistema. Generalmente los ataques están enfocados en explotar vulnerabilidades tanto en el diseño de las redes TCP/IP como en la configuración y operación de los sistemas informáticos que conforman las redes conectadas a Internet. Hoy en día cualquier usuario con una conexión a Internet tiene acceso a numerosas aplicaciones para realizar estos ataques y peor aun las instrucciones necesarias para ejecutarlos.

"Sólo hay dos cosas infinitas: el universo y la estupidez humana; y no estoy seguro de la primera", Albert Einstein. Por lo que según esta frase da a entender que gran parte de la seguridad depende de los individuos y no tanto del equipo o sistema, sin embargo para comprender mejor como lograr un sistema seguro, instituciones como la Asociación Colombiana de Ingenieros de Sistemas (ACIS) y la Universidad de Valle de Atemajac (UNIVA) han realizado investigaciones[2] en los diferentes sectores productivos del país, analizando demografía, presupuestos, fallas de Seguridad, políticas de seguridad, herramientas y prácticas de seguridad. Algunas de las conclusiones fueron:

- En Colombia, para trabajar en el área de seguridad informática, la industria exige como requisito, tener más de dos años de experiencia en este campo.

- Certificaciones tales como; CISSP *(CertifiedInformationSystems Security Professional)*, CISA *(CertifiedInformationSystems Auditor*) y CISM *(CertifiedInformation Security Management*), son las más reconocidas a la hora de considerar un proyecto de seguridad de la información.

- Las redes y sus componentes son aquellas con mayor inversión en seguridad de la información.

[1]Ing. Santos, Guillermo http://www.acis.org.co/fileadmin/Revista_106/02-entrevistal.pdf[hora 12:20 pm Día 16/11./08]

[2]http://www.acis.org.co/fileadmin/Revista_110/05investigacion1.pdf

- Las cifras en 2009 muestran a los antivirus, las contraseñas, los firewalls de *software* y *hardware* como los mecanismos de seguridad más utilizados para evitar ataques.

- La inexistencia de políticas de seguridad y la falta de tiempo, no deben ser una excusa. La inversión en seguridad es costosa, pero los robos y ataques pueden serlo mucho más.

- Los resultados sugieren que en Colombia el ISO 27001, y las Guías del NIST (*NationalInstitute of Standards and Technology)* son el estándar para las buenas prácticas en el área de seguridad de la información o en los departamentos de tecnología informática.

- Son motivadores de la inversión en seguridad: la continuidad de negocio, el cumplimiento de regulaciones y normativas internas y externas, así como la protección de la reputación de la empresa. Así mismo, se manifiesta la necesidad de adelantar al menos un ejercicio anual de análisis de riesgos como soporte a los temas de seguridad y procesos de negocio.

El Ingeniero Edwin Antonio Ochoa presento a la ACIS unos consejos[3] de cómo proteger la pequeña y mediana empresa, también aclara que estas recomendaciones son un mínimo respecto a la seguridad de la información.

- Es necesario conocer cómo se encuentran conectados los dispositivos entre sí.

- Asigne claves seguras en los equipos de red (Routers y Firewalls)

- Se deben tener copias actualizadas de los datos importantes en lugares externos a la organización.

- Asigne los permisos necesarios de acceso a la información.

- Use antivirus y anti-spam actualizados.

- Use estaciones de alimentación ininterrumpida (UPS[4]).

"*Tenga en cuenta que estas recomendaciones sólo son un mínimo con respecto a la seguridad informática, muchos hackers, crackers y empleados deshonestos*

[3] htp://acishost.acis.org.co/fileadmin/Revista_105/EAOchoa.pdf [hora 12:20 pm Día 29/11/2010]

[4] ***UninterruptiblePowerSupply*,** Sistema de Potencia Ininterrumpida, es un dispositivo que gracias a sus baterías, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos que tenga conectados.

están al acecho todos los días, además de los desastres. Proteja su información y su organización[5]".

Fortinet es una compañía dedicada a desarrollar software y hardware que protege los sistemas de información de ataques e intrusiones. Desarrolló Fortigate[6], una suite de seguridad de alto desempeño, confiable y de administración sencilla e intuitiva, su costo varía desde 800 hasta 50 mil dólares dependiendo del desempeño, flexibilidad, escalabilidad y servicios que preste el producto. Este valor aunque es relativamente pequeño para empresas multinacionales, es excesivo para una pequeña empresa en Colombia, por lo que estas se encuentran vulnerables la mayor parte del tiempo.

"El proyecto que se encuentra en curso y que pretende realizar una investigación aplicada acerca de analizar, diseñar y desarrollar políticas, estrategias y mecanismos de control y de seguridad que garanticen la protección de la información almacenada en bases de datos y la transmisión en las redes SOHO (*Small Office/Home Office*) de la pequeña empresa en la ciudad de Bogotá"[7], es un proyecto de investigación de la Universidad de San Buenaventura sede Bogotá, en donde se realizó una selección de pequeñas empresas por sectores que poseen redes SOHO, para así verificar el estado de las empresas y responder al interrogante, ¿qué tan seguras son las pequeñas empresas en Bogotá y qué se puede aportar para que esa seguridad en la información sea mayor y de menor costo?

Existen también algunas publicaciones realizadas por ACIS y CISCO SYSTEMS donde muestran algunos índices sobre la seguridad de la información (ver Anexo A y Anexo B).

1.2. DESCRIPCIÓN Y FORMULACIÓN DEL PROBLEMA

En el mundo tecnológico específicamente en el área de TI (Tecnologías de Información), las compañías se han preocupado por mantenerse al día en las diferentes tendencias del mercado para ser competitivos, dejando un poco de lado el concepto de la seguridad de la información; sin embargo, los requerimientos legales aplicables a algunos sectores y experiencias no gratas, han generado un cambio sustancial en la atención de temas como la definición de políticas y procedimientos al respecto.

La seguridad de la información ha logrado pasar de solo herramientas de *software*, que neutralicen el acceso ilegal y los ataques a los sistemas de información, hacia

[5] IBID

[6] http://www.fortinet.com/products/fortigate/ [hora 03:25 pm Día 27/11/2010]

[7] MENDEZ, Alvarado, Iván. "Proyecto seguridad informática para las redes de datos SOHO en la pequeña empresa de Bogotá". Universidad de San Buenaventura. Bogotá. Pg. 5

modelos de gestión de la seguridad de la información en el que prima lo dinámico sobre lo estacional.

Para lograr niveles adecuados de seguridad se requiere de las disciplinas que tengan un impacto en el logro de este cometido, teniendo siempre presente que un sistema de gestión no garantiza la desaparición de los riesgos que se ciernen con mayor intensidad sobre la información. Esto permite tener una base clara que sirva para implementar y mantener plataformas funcionales y seguras.

Las pequeñas y medianas empresas del sector de transporte en Bogotá, no poseen buenos niveles de seguridad en la información, por lo tanto se plantea ¿Cuáles son las políticas de seguridad y qué controles se deben aplicar para las pequeñas empresas del sector transporte con redes SOHO en Bogotá?

1.3. JUSTIFICACIÓN

En Colombia al igual que en muchos países las empresas, y las personas, aún no se han concientizado de todos aquellos peligros que se encuentran en el área de la informática. En los últimos tiempos esta área ha venido creciendo de tal forma que la información guardada dentro de las computadoras son más susceptibles a ataques de los llamados "Hackers y Crackers" los cuales aprovechan vulnerabilidades en la seguridad y por ende es posible que ellos plagien o roben información valiosa.

"*Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que puede lograrse por medios técnicos es limitada y debe ser respaldada por una gestión y procedimientos adecuados. La identificación de los controles que deben implementarse requiere una cuidadosa planificación y atención a todos los detalles. La administración de la seguridad de la información, exige, como mínimo, la participación de todos los empleados de la organización. También puede requerir la participación de proveedores, clientes y accionistas. Asimismo, puede requerirse el asesoramiento experto de organizaciones externas. Los controles de seguridad de la información resultan considerablemente más económicos y eficaces si se incorporan en la etapa de especificación de requerimientos y diseño."*[8]

El punto de partida para la gestión de la seguridad de la información dentro de una organización se encuentra en la política de seguridad[9] que se formule. Como parte integral de un Sistema de Gestión de Seguridad de la Información (SGSI), un manual de normas y políticas de seguridad, trata de definir; ¿Qué?, ¿Por qué?, ¿De qué? y ¿Cómo? se debe proteger la información. Estos engloban una serie

[8]Norma Técnica Colombiana NTC – ISO/IEC 17799, Tecnología de la Información, ICONTEC, 2006

[9] Política de Seguridad: Documento escrito que describe, cómo la organización puede protegerse de mejor manera de distintas amenazas, esta incluye una lista de pasos a seguir en caso que ocurran ciertos eventos vinculados a la seguridad.

de objetivos, estableciendo los mecanismos necesarios para lograr un nivel de seguridad adecuado a las necesidades establecidas dentro de la institución. Estos documentos tratan a su vez de ser el medio de interpretación de la seguridad para toda la organización.

En el nuevo plan nacional de tecnologías de la información y la comunicación[10] se establece que Colombia debe estar en capacidad de ofrecer competitividad como país, por esta razón se pretende crear resultados e iniciativas que permitan contribuir al desarrollo tecnológico de las pequeñas empresas, con el fin de mejorar el desarrollo económico y social en Colombia.

Para ofrecer esta competitividad como país lo primero que se debe hacer es proporcionar sistemas más seguros y confiables, en donde sea difícil vulnerar la seguridad de la información.

Las políticas y controles que se utilizan en grandes empresas son adquiridas a un gran costo. Las pequeñas empresas no tienen los recursos necesarios para poder adquirirlos, por lo que poseen una mayor vulnerabilidad de ataques tanto del exterior como del interior de la organización.

Este estudio técnico que establece normas, políticas y controles de seguridad de la información en el sector de transporte de las pequeñas empresas con redes SOHO en Bogotá, surge de la necesidad de que estas empresas adquieran una protección para su información que pueda estar almacenada en bases de datos o sea transmitida mediante redes de comunicación.

1.4. OBJETIVOS DE LA INVESTIGACIÓN

1.4.1. Objetivo general. Diseñar políticas y controles de seguridad de la información para ser aplicadas en pequeñas empresas con redes SOHO en el sector transporte de Bogotá.

1.4.2. Objetivos específicos. Identificar las principales vulnerabilidades en los sistemas de información en las pequeñas empresas con redes SOHO en el sector transporte de Bogotá.

Analizar la información obtenida de las empresas, para la adecuada categorización de las vulnerabilidades, teniendo en cuenta la Norma NTC-ISO/IEC 27001 - 17799.

[10]Las Tecnologías de la Información y las Comunicaciones (TIC), son el conjunto de herramientas, equipos, programas informáticos, aplicaciones, redes y medios, quepermiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes. http://www.slideshare.net/karencardozo/ley-de-tics

Plantear las políticas necesarias para la seguridad de la información en las pequeñas empresas con redes SOHO en el sector transporte de Bogotá.

Definir controles que garanticen la seguridad de la información en las pequeñas empresas con redes SOHO en el sector transporte de Bogotá.

1.5. ALCANCES Y LIMITACIONES DEL PROYECTO

1.5.1. Alcances. Se realizará un documento guía donde se definan políticas y controles (adaptativos y administrativos) de seguridad de la información para pequeñas empresas con redes SOHO en el sector transporte de Bogotá.

Se considerarán controles a nivel físico, lógico y administrativo.

Solo se aplicarán encuestas en aquellas empresas que deseen participar.

1.5.2. Limitaciones. El proyecto solo genera políticas y controles, las cuales pretenden garantizar la seguridad de la información, cuando éstas sean aplicadas.

Solo se incluirán en la investigación pequeñas empresas con redes SOHO en el sector transporte de Bogotá.

La base de datos proporcionada por la cámara de comercio de Bogotá es del año 2008, por ende, las empresas pueden haber cambiado de localización física o no renovaron el Registro Mercantil (inactivas).

La solución de diseño de las políticas y controles se orienta únicamente a redes guiadas.

2. LÍNEA DE INVESTIGACIÓN DE USB/ SUBLÍNEA DE FACULTAD / CAMPO TEMÁTICO DEL PROGRAMA

Desde el punto de vista de la Facultad de Ingeniería de la Universidad de San Buenaventura sede Bogotá y siguiendo lasdirectrices del consejo de investigación Bonaventuriano para proyectos de este tipo, la Línea de investigación es:“Tecnologías actuales y sociedad”, la Sub-líneaes: “Sistemas de información y comunicación” y el campo temático hace referencia a: “Redes de Computadores”.

3. METODOLOGÍA

3.1. ENFOQUE DE LA INVESTIGACIÓN

Considerando que el proyecto desarrollado por el grupo de trabajo para optar al título de Ingeniero de Sistemas se enmarca en el proyecto "DISEÑO E IMPLEMENTACIÓN DE ESTRATEGIAS Y MECANISMOS DE CONTROL PARA LA SEGURIDAD DE LA INFORMACIÓN EN LAS REDES DE DATOS SOHO DE LA PEQUEÑA EMPRESA DE BOGOTÁ" aprobado por el Consejo de Investigación Bonaventuriano (CIB), inicialmente en la convocatoria de 2008 y posteriormente en la convocatoria 2011, el enfoque de la investigación es de tipo descriptivo- cuantitativo.

Teniendo en cuenta los objetivos planteados, el enfoque descriptivo que toma el proyecto se debe a los diagnósticos que se hacen a partir de la información recolectada y analizada, de tal forma que se pueda "asociar y desarrollar nuevas estrategias y mecanismos de seguridad que satisfagan las necesidades de la pequeña empresa"[11], en el sector transporte de Bogotá. El enfoque cuantitativo corresponde a una muestra aleatoria de 16 empresas del sector transporte de Bogotá, que se encuentren registradas en la Cámara de Comercio de Bogotá, donde se van a aplicar las encuestasde investigación considerando la siguiente población:

"Los administradores de red y sistemas de información y/o jefes de departamentos de tecnología o directores de centros de cómputo por ser los directos responsables de determinar en las redes de comunicación de datos, la disponibilidad, la utilización, el rendimiento y la gestión de sus recursos"[12].

Se sabe que la muestra para la investigación dentro de un proyecto se puede recolectar de varias maneras: "estratificada, por conveniencia y aleatoriamente"[13]. Para el actual proyecto se tomará una ***muestra aleatoria*** en la ciudad de Bogotá, con el objetivo de considerar solo las empresas vigentes, con información real y actualizada dentro de los registros que maneja la Cámara de Comercio de Bogotá, teniendo en cuenta el estudio realizado por el Decano de la Escuela de Negocios y Ciencias Empresariales de la Universidad Sergio Arboleda de Bogotá en el 2005 titulado "Situación y necesidades de la pequeña empresa"[14], donde el 63% de las pequeñas empresasse encuentran geográficamente situadas en la ciudad de Bogotá.

[11] MENDEZ, Alvarado Iván. Diseño e implementación de estrategias y mecanismos de control para la seguridad de la información en las redes de datos SOHO de la pequeña empresa de Bogotá. Pág. 4
[12] IBID
[13] IBID
[14] www.usergioarboleda.edu.co/civilizar/revista9/SITUACION_NECESIDAD_PEQUENA_MEDIANA_EMPRESA.pdf

4. MARCO DE REFERENCIA

4.1. MARCO TEÓRICO – CONCEPTUAL

4.1.1. La información como parte primordial de las organizaciones. Se ha reconocido desde hace algunos años la importancia de relacionar la administración de los principales recursos con la informática, y cuando se habla de informática generalmente se piensa en nuevas tecnologías, aplicaciones, hardware, nuevas formas de tratar y procesar la información de tal manera que ésta sea más consistente, pero no se tenía en cuenta la base para llegar a la informática o sus elementos; se desconocía que la información es la parte esencial de la informática.[15]

Las organizaciones han visto actualmente a la ***información*** como uno de sus principales recursos. Las entidades encargadas de tomar decisiones comprenden ahora que no se debe tomar la información sólo como un subproducto de la administración empresarial, sino que simultáneamente sirve de retroalimentación a los negocios, siendo un factor determinante en el éxito o el fracaso de los mismos. La información debe ser orientada por las organizaciones de la misma manera como se administran los demás recursos existentes, de una forma clara, organizada, correcta y eficiente, de tal forma que se maximice la utilidad que posee ésta. Los individuos que administran deben entender que hay costos relacionados con la producción, distribución, seguridad, almacenamiento y recuperación de la información que se maneja dentro de las organizaciones. Se debe comprender que ésta información tiene un valor económico, y que su uso logra mejoras importantes que les permite ser más eficientes y competitivas. Los usos y/o procesos que se realizan con la información deben ser evaluados y respaldados por una agrupación de componentes interrelacionados llamados ***sistemas de información*** **(*SI*)**, dentro de los cuales interactúan los siguientes aspectos: El recurso humano, los datos o información fuente, actividades, técnicas de trabajo, los procedimiento de políticas y reglas de operación, recursos informáticos y de telecomunicaciones y recursos físicos en general.

Un SI realiza cuatro actividades básicas:

- **Entrada de la información (INPUT)**: Técnica mediante la cual el sistema obtiene los datos que necesita para el procesamiento de la información, por medio de teclados, código de barras, medios magnéticos, etc.

[15]SALAZAR, Jacqueline Lam. La Informática y Su Impacto Social, Universidad de Pinar del Río "HnosSaíz Montes de Oca". Cuba.

- **Almacenamiento de la información**: Tarea con mayor importancia que se realiza, puesto que a través de ella el sistema puede recordar la información empleada (modificada, eliminada, agregada, etc.) en procesos anteriores.

- **Procesamiento de la información**: Propiedad del sistema que posibilita la transformación de la información para luego ser utilizada para generar proyecciones, por los tomadores de decisiones, con los datos obtenidos en el procesamiento y volver más eficiente y competitivo un negocio.

- **Salida de la información (OUTPUT)**: Método por el cual se saca la información procesada, esto mediante impresiones, medios magnéticos, videos, etc.

El manejo adecuado de los SI es un reto muy grande e importante para los gerentes organizacionales, puesto que al transformarse hacia el terreno de la información se corre el riesgo del fracaso, debido a las amenazas del mercado y la incapacidad de competir. De tal modo las tareas de los SI representan:

• Un departamento dentro de la organización, que va a ser tan importante funcionalmente para el éxito de la empresa como las que las áreas de contabilidad, marketing, administración de recursos humanos, etc., desempeñan.

• Un apoyo importante tanto para el buen desempeño operacional, productivo y moral del empleado, como satisfacción del servicio reflejado en el cliente.

• Un componente esencial en la producción y prestación de servicios arrolladores que dan a las organizaciones ventajas fundamentales y valiosas en el mercado.

Seguridad de la información

Como se evidencia anteriormente los SI son de vital importancia en la empresa por consiguiente su componente principal (información) debe estar debidamente protegido,**"***La seguridad de la información tiene como fin garantizar la continuidad comercial, minimizar el daño al mismo y maximizar el retorno sobre las inversiones y las oportunidades**.***

La información puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

La seguridad de la información se define aquí como la preservación de las siguientes características:

a) ***confidencialidad****: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella.*

b) ***integridad****: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.*

c) ***disponibilidad****: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera.*

Política de seguridad

La seguridad de la información se logra implementando un conjunto adecuado de controles que abarcan, prácticas, procedimientos, estructuras organizacionales, funciones del software"[16]y un documento en el cual se expresa el compromiso de la gerencia de la organización con la seguridad de la información, este contiene la definición de la seguridad de la información bajo el punto de vista de la empresa. Este documento debe ser enriquecido y compatibilizado con otras políticas dependientes de ésta, objetivos de seguridad y procedimientos. Debe estar fácilmente accesible de forma que los empleados estén al tanto de su existencia y entiendan su contenido.

La política de seguridad puede ser también un documento único o inserto en un manual de seguridad. Se debe designar un propietario que será el responsable de su mantenimiento y su actualización a cualquier cambio que se requiera.

El desarrollo de una política de seguridad se divide en tres pasos o etapas:

El primer paso en la fase de desarrollo de una política es la planificación, la investigación y la redacción de la política o, tomado todo junto, la creación. La creación de una política implica identificar por qué se necesita la política, por ejemplo, requerimientos legales, regulaciones técnicas, contractuales u operacionales; determinar el alcance y la aplicabilidad de la política, los roles y las responsabilidades inherentes a la aplicación de la política y garantizar la factibilidad de su implementación. La creación de una política también incluye la investigación para determinar los requerimientos organizacionales para desarrollar las políticas, es decir, que autoridades deben aprobarla, con quién se debe coordinar el desarrollo y estándares del formato de redacción, y la investigación de las mejores prácticas en la industria para su aplicabilidad a las necesidades organizacionales actuales. De esta etapa se tendrá como resultado

[16]Instituto Argentino de Normalización – Esquema 1 de Norma IRAM-ISO IEC 17799 Tecnología de la Información.

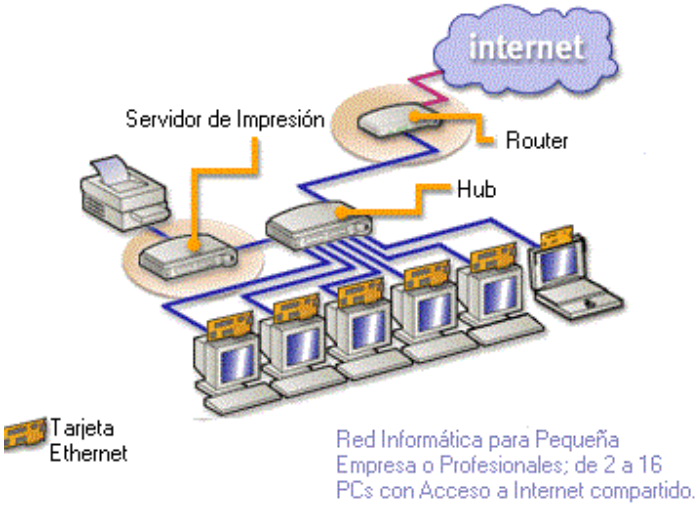
la documentación de la política de acuerdo con los procedimientos y estándares de la organización, al igual que la coordinación con entidades internas y externas que la política afectará, para obtener información y su aceptación. En general, la creación de una política es la función más fácil de entender en el ciclo de vida de desarrollo de una política.
La revisión de la política es la segunda etapa en la fase. Una vez la documentación de la política ha sido creada y la coordinación inicial ha sido iniciada, esta debe ser remitida a un grupo (o un individuo) independiente para su evaluación antes de su aprobación final. Hay varios beneficios de la revisión independiente: una política más viable a través del escrutinio de individuos que tienen una perspectiva diferente o más vasta que la persona que redactó la política; apoyo más amplio para la política a través de un incremento en el número de involucrados; aumento de credibilidad en la política gracias a la información recibida de diferentes especialistas del grupo de revisión. Propio de esta etapa es la presentación de la política a los revisores, ya sea de manera formal o informal, exponiendo cualquier punto que puede ser importante para la revisión, explicando su objetivo, el contexto y los beneficios potenciales de la política y justificando por qué es necesaria. Como parte de esta función, se espera que el creador de la política recopile los comentarios y las recomendaciones para realizar cambios en la política y efectuar todos los ajustes y las revisiones necesarias para obtener una versión final de la política lista para la aprobación por las directivas.

El paso final en la fase de desarrollo de la política es la aprobación. El objetivo de esta etapa es obtener el apoyo de la administración de la organización, a través de la firma de una persona ubicada en una posición de autoridad.

La aprobación permite iniciar la implementación de la política. Requiere que el proponente de la política haga una selección adecuada de la autoridad de aprobación, que coordine con dicho funcionario, presente las recomendaciones emitidas durante la etapa de revisión yhaga el esfuerzo para que sea aceptada por la administración. Puede ocurrir que por incertidumbre de la autoridad de aprobación sea necesaria una aprobación temporal. Estos pasos sugeridos anteriormente sirven tanto para empresas grandes como para las empresas clasificadas para este proyecto, es decir empresas con redes SOHO.

Red SOHO (*Small Office, Home Office*);
Hace referencia a los negocios que poseen de 1 a 16equipos de computo con accesos a internet compartido (ver Ilustración 1) y se aplica para denominar a los aparatos destinados a un uso profesional pero que, a diferencia de otros modelos, no están pensados para asumir un gran volumen de trabajo.

Ilustración 1 RED SOHO



Fuente: Panafonic.com

Existen dos clases o métodos de conexión en una red SOHO a internet:

- **Conexión enrutada**

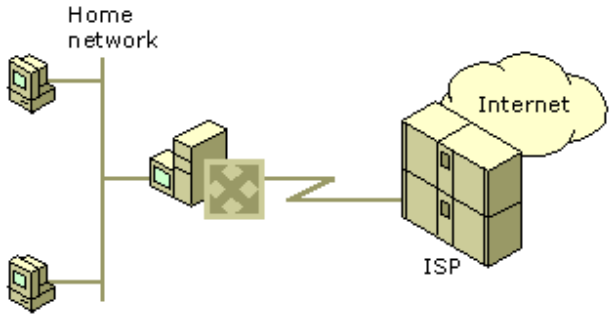
"En una conexión enrutada, el servidor que ejecuta Enrutamiento y acceso remoto funciona como un enrutador IP que reenvía paquetes entre los hosts SOHO y los hosts de Internet.

Una red SOHO tiene las siguientes características:

- *Un segmento de red.*
- *Un único protocolo: TCP/IP.*
- *Conexiones de marcado a petición o de vínculo dedicado con el proveedor de servicios Internet (ISP).*

En la siguiente ilustración se muestra un ejemplo de una red SOHO.

Ilustración 2 Conexión enrutada



Fuente: Microsoft.com

El servidor que ejecuta Enrutamiento y acceso remoto está configurado con un adaptador de red para los medios que se utilizan en la red doméstica (por ejemplo, Ethernet) y un adaptador ISDN (RDSI) o un módem analógico. Puede utilizar una línea concedida u otra tecnología de conexión permanente, como xDSL y módems por cable, pero en este escenario se describe la configuración más usual, que utiliza un vínculo de acceso telefónico con un ISP local."[17]

- **Conexión traducida**

"En una conexión traducida, el servidor que ejecuta Enrutamiento y acceso remoto y NAT funciona como traductor de direcciones de red, un enrutador IP que traduce las direcciones de los paquetes reenviados entre los hosts SOHO y los hosts de Internet. La configuración de red se simplifica con el uso del protocolo de enrutamiento de Traducción de direcciones de red (NAT, Network AddressTranslation), que proporciona servicios de traducción de direcciones de red, de direccionamiento y de resolución de nombres para equipos de red SOHO.

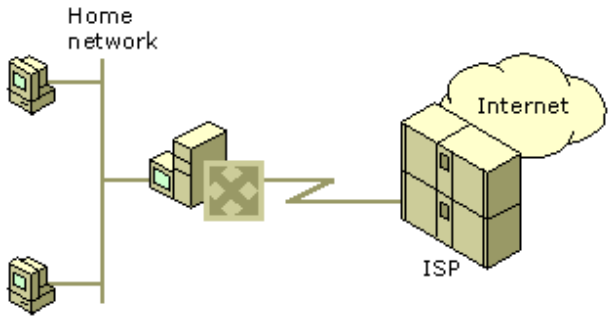
Una red SOHO tiene las siguientes características:

- *Un segmento de red.*
- *Un único protocolo: TCP/IP.*
- *Conexiones de marcado a petición o de vínculo dedicado con el proveedor de servicios Internet (ISP).*

En la siguiente ilustración se muestra un ejemplo de una red SOHO.

[17] http://technet.microsoft.com/es-es/library/cc736774(WS.10).aspx[11/28/2010 6:51 p.m.]

Ilustración 3 Conexión Traducida



Fuente: Microsoft.com

El servidor que ejecuta el servicio Enrutamiento y acceso remoto está configurado con un adaptador de red para los medios que se utilizan en la red doméstica (por ejemplo, Ethernet) y un adaptador ISDN (RDSI) o un módem analógico. Puede utilizar una línea concedida u otra tecnología de conexión permanente, como xDSL y módems por cable, pero en este escenario se describe la configuración más usual que utiliza un vínculo de acceso telefónico a un ISP local."[18]

Como se observa,para que ocurra el proceso de intercambiar la información, los PC's deben estar cerca geográficamente, lo que hace que los usuarios que manejan la información se conozcan más y exista mayor confianza entre ellos, siendo realmente un riesgo alto para las redes SOHO y a la vez una ventaja para los intrusos que desean acceder a la información. Por eso, se debe prestar mayor atención en cuanto a su protección, con dispositivos que permitan un mayor control en el acceso.

Sistemas biométricos

Los sistemas biométricos permiten el reconocimiento del individuo mediante una característica personal, que es reconocida o verificada de manera automatizada.

La tecnología biométrica ha permitido identificar con mayor precisión a un individuo para así poder obtener mayor confiabilidad a la hora de validar su identidad.

Cifrado o encriptación

Las redes se diseñan normalmente para impedir el acceso no autorizado a datos confidenciales desde fuera de la intranet de la empresa mediante el cifrado o encriptación de la información. Esta técnica hace referencia al "proceso para volver ilegible información considera importante. La información una vez

[18] http://technet.microsoft.com/es-es/library/cc780147(WS.10).aspx [11/28/2010 6:56 p.m.]

encriptada sólo puede leerse aplicándole una clave"[19]. Sin embargo, la mayor parte de las redes manejan las comunicaciones entre los hosts de la red interna como texto sin formato. Con acceso físico a la red y un analizador de protocolos, un usuario no autorizado puede obtener fácilmente datos privados.

IPSec
se encarga de laautenticación de los equipos y el cifradode los datos para su transmisión entre hosts en una red, intranet o extranet, incluidas las comunicaciones entre estaciones de trabajo y servidores, y entre servidores. El objetivo principal de IPSec es proporcionar protección a los paquetes IP. IPSec está basado en un modelo de seguridad de extremo a extremo, lo que significa que los únicos hosts que tienen que conocer la protección de IPSec son el que envía y el que recibe. Cada equipo controla la seguridad por sí mismo en su extremo, bajo la hipótesis de que el medio por el que se establece la comunicación no es seguro.

Otro medio para garantizar la seguridad de la información son losdetectores de patrones de escritura como lo es la firma digital.

Firma digital
Es una firma electrónica que puede ser utilizada para autenticar la identidad de quien envía un mensaje o quien firma un documento, y hace posible garantizar que el contenido original de un mensaje o documento ha sido enviado sin modificaciones. Las firmas digitales se pueden transmitir fácilmente, no pueden ser imitadas por alguien más, y se pueden marcar con sello de hora y fecha automáticamente. La habilidad para garantizar que el mensaje original firmado llegue en su totalidad, también significa que el emisor del mensaje no lo puede repudiar (negar que lo envió) posteriormente. Una firma digital se puede utilizar con cualquier tipo de mensaje, cifrado o no, solo para que el receptor tenga certeza sobre la identidad del emisor y que el mensaje llegó intacto.

Además de asegurar los accesos a la información, se debe poner un filtro que controle el paso de información de una red a otra (conexión con el exterior), para evitar que intrusos tengan acceso a información confidencial. Esta protección puede ser implementada mediante un dispositivo de Hardware o Software, llamado **firewall**.

Muchas de las amenazas relacionadas con la perdida de información, como virus, gusanos y ataques combinados, explotan vulnerabilidades tales como puertos abiertos para entrar en las redes.

Un **Puerto abierto** es aquel por donde un programa puede transmitir información bien sea entrante o saliente. Por lo tanto solo se debe tener abiertos los

[19] http://www.alegsa.com.ar/Dic/encriptaci%C3%B3n.php [11/29/2010 10:06 p.m.]

puertosque se necesitan. Si no se cuenta con un firewall una red estará expuesta a cualquier tipo de ataque.

4.2. MARCO LEGAL O NORMATIVO

En Colombia no existe mucha legislación acerca de la in ningún control A continuación se nombran algunasleyes que la regulan.

Decreto 460 de 16 de marzo de 1995. Reglamento del Registro Nacional de Derechos de Autor.

Decreto nº 1360, de 23 de junio de 1989, donde se reglamenta el Registro de los programas de computador.

Ninguna persona puede modificar o copiar un programa de computador hecho por otra persona a menos de que el autor lo permita.

Decreto 1747 de 11 de septiembre de 2000, por el cual se reglamenta parcialmente la Ley 527 certificados y firmas digitales.

En éste decreto se reglamenta que cada sitio debe tener su certificado de legalidad y quedebe cumplir con todas la normas establecidas.

La norma ISO/IEC 17799:2000 considera la organización como una totalidad y tiene en consideración todos los posibles aspectos que se pueden ver afectados ante los posibles incidentes que puedan producirse. Esta norma se estructura en 11 dominios y cada uno de ellos hace referencia a un aspecto de la seguridad de la organización. Lo citados dominios son:

- Política de seguridad.
- Aspectos organizativos para la seguridad.
- Clasificación y control de activos.
- Seguridad del personal.
- Seguridad física y del entorno.
- Gestión de comunicaciones y operaciones.
- Control de accesos.
- Desarrollo y mantenimiento de sistemas.
- Gestión de incidentes.

- Gestión de continuidad del negocio.
- Conformidad legal.

Por medio de estos dominios se conoce la empresa en su totalidad, y se comienzan a resaltar los objetivos de control y los controles que se deben tener en cuenta a la hora de formular políticas de seguridad.

Se debe tener en cuenta que la norma maneja:

- Organización de la seguridad de la información y organización interna: se gestiona la seguridad de la información dentro de la organización.
- Coordinación de la seguridad de la información: toda actividad que se realice en seguridad de información debe ser coordinada por un representante.
- Asignación de responsabilidades a la seguridad de la información: se deben definir claramente las responsabilidades en cuando a la seguridad de la información.
- Proceso de autorización para los servicios de procesamiento de la información: se debe definir y limitar un proceso de autorización de la dirección para los nuevos servicios de procesamiento de información.
- Acuerdos sobre confidencialidad: Se deberían identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de ni divulgación.
- Contacto con las autoridades: se deberán mantener contactos apropiados con autoridades pertinentes.
- Organización Externa: mantener la seguridad de la información y de los servicios de procesamiento de información de la organización, y a las cuales se pueden acceder externamente.
- Identificación de riesgos: identificar los riesgos para la información y los servicios de procesamiento de la información de la organización a los procesos del negocio que involucran partes externas e implementar los controles apropiados antes de autorizar el acceso.
- Abordaje de seguridad en cuanto a los clientes: todos los requisitos de seguridad identificados se deben abordar antes de dar acceso a algún cliente a los activos de la organización
- Abordaje de seguridad en cuanto a las terceras partes: se deben considerar todos los requerimientos antes de realizar acuerdos con terceras partes.

El estándar para la seguridad de la información ISO/IEC 27001 agrupa en 11 áreas o dominios todo el conjunto de acciones, documentos, procedimientos y

medidas técnicas adoptadas para garantizar que cada amenaza, identificada y valorada con un cierto riesgo, sea minimizada.

En el actual proyecto y basados en las normas ISO/IEC 17799 e ISO/IEC 27001 se van a manejar 9 dominios de los 11 y partiendo de estos generar políticas y controles adecuados para las empresas con redes SOHO del sector transporte de Bogotá.

- Política de Seguridad
- Seguridad Organizacional
- Administración de Activos de Información:
- Seguridad del Recurso Humano
- Seguridad Física y Ambiental
- Administración de comunicaciones y operaciones
- Control de Acceso
- Adquisición mantenimiento y desarrollo de sistemas de información
- Administración de la continuidad del negocio

Ley No. 1273[20] enero 2009 “De la protección de la información y de los datos”.

Esta ley crea nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.

Esta ley plasmó como delitos una serie de conductas relacionadas con el manejo de datos personales, ya que es de gran importancia que las empresas se protejan jurídicamente para evitar transgresiones en alguno de estos tipos penales.

En relación con los atentados informáticos, la ley contempla que los avances tecnológicos y el uso de los mismos para apropiarse indebidamente del patrimonio de terceros como lo son la clonación de tarjetas, alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante el manejo de programas y afectación de los cajeros, entre otras, son conductas cada vez más usuales en todas partes.

[20] http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html

5. DESARROLLO INGENIERIL

Para contrarrestar los problemas de vulnerabilidad en la información almacenada, el desarrollo ingenieril se realizó considerando las siguientes etapas o fases:

- Recolección y análisis de la información.
- Selección de los dominios más apropiados para la seguridad de la información propuestos en el estándar ISO/IEC 17799 e ISO/IEC 27001.
- Definición de políticas de seguridad de la información en cada dominio.
- Definición de controles según las políticas obtenidas.

A continuación se presenta el desarrollo de cada una de las etapas o fases mencionadas anteriormente:

5.1. RECOLECCIÓN Y ANÁLISIS DE LA INFORMACIÓN

Para realizar la recolección de información y poder determinar las debilidades que presentan los sistemas de información en las pequeñas empresas del sector de transporte con redes SOHO en Bogotá; se diseñó una encuesta como instrumento para evaluar y diagnosticar las vulnerabilidades.

El instrumento consta de seis partes a saber: seguridad física, hardware, software, transmisión de datos, organización y administración de la red y archivos. Por cada ítem mencionado se plantearon un promedio de 10 preguntas.

En el anexo F Se aprecia por cada etapa o fase, la cantidad y el porcentaje de respuestas SI, NO y N/A (No aplica) por cada empresa encuestada.

5.2. ANÁLISIS DE VULNERABILIDADES

El análisis de vulnerabilidades ha sido diseñado para ayudar a identificar y abordar riesgos de seguridad para la información en las redes SOHO, analizando la cultura del personal, los procesos que realiza cada usuario y la tecnología (software y hardware) de las empresas en el sector transporte de Bogotá.

Los resultados de este análisis condujeron a la realización de un documento que incluye los controles y políticas de seguridad que una empresa debe implementar para garantizar la seguridad de la información. (Ver manual en ANEXO I)

Para la realización del análisis de vulnerabilidades se tuvo en cuenta el estudio por empresa (ANEXO G) y a partir de este, se obtuvieron unos porcentajes que definen el grado de seguridad de la información en todas las empresas que

participaron en la investigación. Durante el análisis se conformaron tres secciones que son; Infraestructura, Aplicaciones y personal y operaciones.

5.2.1. Infraestructura. La seguridad en la infraestructura se refiere a la forma como debe funcionar la red, a los procesos comerciales que se deben implantar, a cómo se configuran y se utilizan los hosts, a como se deben configurar y utilizar los host y a las actividades de gestión y mantenimiento que se debe realizar.

Una seguridad efectiva de la infraestructura, ayuda a mejorar significativamente aspectos como la defensa de la red, las reacciones a incidentes, la disponibilidad de la red y el análisis de fallos. Al establecer un diseño de la infraestructura que todos puedan comprender y seguir, se podrá identificar las áreas de riesgo y desarrollar métodos para reducir las amenazas.

Esta parte de la evaluación revisa los procedimientos de alto nivel que las empresas siguen actualmente para reducir el riesgo, enfocándose en las siguientes áreas de seguridad: Defensa del perímetro, Autentificación, Gestión y control.

En la Tabla No 1. Se aprecia en porcentajes, el estado general (parte superior, primera fila, color verde) y especifico (demás filas) de la seguridad de la información para la primera área de seguridad de la sección relacionada con la Infraestructura (defensa del perímetro[21]).

Las siguientes convenciones serán utilizadas para todas las tablas del análisis de vulnerabilidades y representan el estado actual de la seguridad de la información en las empresas con respecto a las prácticas recomendadas por las normas.

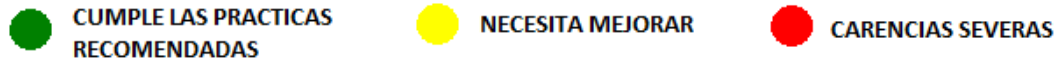


Tabla 1 Defensa perimetral.

Defensa del perímetro	19.5 %	12.5 %	77.6 %
Reglas y filtros de cortafuegos	12.5 %	0 %	87.5 %
Antivirus - Equipos de escritorio	93.7 %	0 %	6.25 %
Antivirus – Servidores	43.7 %	0 %	56.2%

[21] Se debe entender como Defensa del perímetro a: Cortafuegos, antivirus, acceso remoto, segmentación.

Acceso remoto	0 %	0 %	100 %
Segmentación	0 %	0 %	100 %
Sistema de detección de intrusiones.	0 %	12.5 %	87.5 %

Defensa perimetral

De acuerdo con la norma ISO/IEC 27001 con respecto a la seguridad perimetral y según los datos recogidos, 15 de las 16 empresas (93.75%) afirman que protegen sus equipos de escritorio con antivirus actualizado, siendo el único ítem que cumple con las mejores prácticas recomendadas por la norma.

Se observa también un alto porcentaje (87.5%) de carencias severas en cuanto a la creación de reglas y filtros de firewalls. En una de las empresas que participaron en la investigación fue posible montar un firewall en Linux y a través de reglas creadas en éste, mostrar como negar o conceder permisos a los PC de una red interna para que pueda navegar en Internet, el ejercicio esta descrito en el anexo H.

Por tanto se deduce que las empresas no poseen seguridad en el perímetro de la red (77.6% no cumplen con las prácticas recomendadas); no hay escudo protector contra intrusos, existen carencias severas en la parte donde la red interna de las pequeñas empresasconecta con el exterior.

Autenticación

Se debe entender como autenticación, a las directivas de contraseña que permiten que un usuario pueda acceder a los procesos que se corren en red.

La tabla No 2. Muestra los resultados del análisis elaborado en la parte relacionada con la autenticación.

Tabla 2 Autenticación.

Autenticación	**3.9 %**	**14.8 %**	**81.2 %**
Usuarios administrativos	0 %	6.25 %	93.7 %
Usuarios internos	0 %	18.7 %	81.2 %
Usuarios de acceso remoto	0 %	12.5 %	87.5 %
Directivas de contraseñas	0 %	18.7 %	81.2%
Directivas de contraseñas-Cuenta de administrador	18.75 %	0 %	81.2 %

Directivas de contraseñas-Cuenta de usuario	12.5 %	0 %	87.5 %
Directivas de contraseñas-Cuenta de acceso remoto	0 %	0 %	100 %
Cuentas inactivas	0 %	62.5 %	37.5 %

Como puede observarse en la tabla anterior (Tabla No 3), las empresas con redes SOHO no poseen procedimientos estrictos de autenticación el 81.2% del total de empresas tienen carencias severas, por tal motivo, intrusos pueden acceder fácilmente y sin autorización a la red mediante ataques locales o remotos.

Gestión y control

Se debe entender como Gestión y control todo lo relaciondo con el manejo y la administración de los archivos de registro. En seguida se presentan los resultados.

Tabla 3 Gestión y control.

Gestión y control	**0 %**	**6.25 %**	**93.7 %**
Informes sobre incidentes y respuesta	0 %	0 %	100 %
Creación segura	0 %	0 %	100 %
Seguridad física	0 %	18.7 %	81.2 %

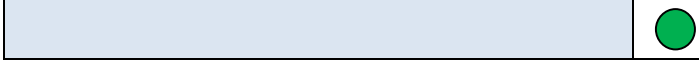
Tal y como se observa en la tabla No. 3, 93.7% de las empresas no cumple con las prácticas recomendadas en cuanto a gestión y control se refiere. No existe supervisión ni registros adecuados para mantener y analizar los entornos informáticos (81.2%). Ni siquiera, después de sufrir un ataque habrá un informe de análisis del incidente (100% carencias).

5.2.2. Aplicaciones. El objetivo de este análisis es valorar las aplicaciones instaladas y diseñadas desde el punto de vista de la seguridad, disponibilidad, continuidad e integridad. La evaluación revisa los procedimientos que una empresa sigue para reducir los riesgos, centrándose en las siguientes áreas de seguridad: Implementación y uso, Diseño de aplicaciones, Almacenamiento y comunicaciones de datos.

Implementación y uso

La siguiente tabla (tabla No 4) muestra los resultados de análisis para el área de seguridad: implementación y uso en la sección de aplicaciones. Se debe entender como Implementación y uso a: Los mecanismos que mejoren la disponibilidad.

Tabla 4 Implementación y uso.

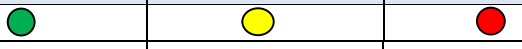
Implementación y uso	0 %	15.6 %	84.3 %
			
Equilibrio de carga	0 %	0 %	100 %
Clústeres	0 %	0 %	100 %
Aplicación y recuperación de datos	0 %	0 %	100 %
Fabricante de software independiente (ISV)	0 %	6.25 %	93.7 %
Desarrollado internamente	0 %	87.5 %	12.5 %
Vulnerabilidades	0 %	0 %	100 %

Al observar la tabla No. 4 es posible apreciar que una buena porción (87.5%) de las empresas desarrolla internamente las aplicaciones, pero necesitan mejorar en este aspecto. La mayoría de carencias (84.3%) se encuentran al momento de instalar y utilizar las aplicaciones, ya que no es tarea fácil asegurar la disponibilidad de esas aplicaciones y de los servidores en los que estas se ejecutan. Esto puede deberse a la falta de mantenimiento continuo para asegurar que los errores de seguridad se corrigen y que no se introducen nuevas vulnerabilidades en el entorno.

Diseño de aplicaciones

Se debe entender como Diseño de aplicaciones a: La autenticación, control de acceso, gestión de actualizaciones, validación de datos de entrada, registros y auditorias.Analizando el área de seguridad de diseño de aplicaciones en la sección aplicaciones, se obtienen los siguientes valores.

Tabla 5 Diseño de aplicaciones.

Diseño de aplicaciones	3.1 %	4.1 %	92.7 %
			
Autenticación	0 %	12.5 %	87.5 %
Directivas de contraseñas	0 %	12.5 %	87.5 %
Autorización y control de acceso	12.5 %	0 %	87.5 %
Registro	6.25 %	0 %	93.7 %
Validación de datos de entrada	0 %	0 %	100 %
Metodologías de desarrollo de seguridad de software	0 %	0 %	100 %

Al observar las respuestas de la tabla No. 5, lo primero que llama la atención es el elevado grado de carencias severas (92.7%), de donde se deduce que un diseño que no aborda adecuadamente los mecanismos de seguridad como la autenticación, la autorización, y la validación de datos podría permitir que los atacantes aprovechen las vulnerabilidades de seguridad en las empresas para acceder a información confidencial.

Almacenamiento y comunicaciones de datos

Se debe entender como Almacenamiento y comunicaciones de datos al cifrado, transferencia de datos y acceso restrictivo. Los resultados se aprecian en la siguiente tabla:

Tabla 6 Almacenamiento y comunicaciones de datos.

Almacenamiento y comunicaciones de datos	**0 %**	**0 %**	**100 %**
Cifrado	0 %	0 %	100 %
Cifrado – Algoritmo	0 %	0 %	100 %

Al observar la tabla No. 6 se aprecia que en absolutamente todas las empresas (100%) analizadas tienen carencias severas. No se garantiza la integridad y confidencialidad de los datos.

La pérdida o el robo de datos puede afectar negativamente tanto a los ingresos de las empresas como su reputación. Es importante comprender como las aplicaciones controlan y protegen los datos críticos.

5.2.3. Personal y operaciones. Esta sección revisa aquellos procesos de empresa que regulan las directivas de seguridad corporativa, los procesos relacionados con los recursos humanos, así como la formación y la divulgación de las políticas y controles para seguridad de la información entre los empleados. El área de análisis del personal también se centra en la seguridad; ya que relaciona las tareas diarias operativas y las definiciones de roles y revisa los procedimientos de alto nivel que una empresa puede seguir para ayudarle a reducir los riesgos en cuanto a la información que manejan los empleados, centrándose en las siguientes áreas de seguridad del personal: Requisitos y evaluaciones, Directiva y procedimientos, Formación y conocimiento

Requisitos y evaluaciones

Se debe entender como Requisitos y evaluaciones a la planificación y evaluaciones de terceros. La tabla que describe el área de seguridad de requisitos y evaluaciones en la sección Personal es la siguiente:

Tabla 7 Requisitos y evaluaciones.

Requisitos y evaluaciones	3.1 %	3.1 %	93.7 %
Requisitos de seguridad	0 %	0 %	100 %
Evaluaciones de seguridad	6.25 %	6.25 %	87.5 %

Según la tabla No. 7, se deduce que para las empresas, la mayor dificultad radica en la falta de comprender los requisitos de seguridad por parte de los encargados de la toma de decisiones (100%), para que las decisiones comerciales y técnicas adoptadas aumenten la seguridad. En muchos casos los encargados se contradicen entre sí. En la tabla también se puede apreciar la falta de evaluaciones periódicas (87.5%), las cuales pueden ayudar a la empresa a revisar, valorar e identificar las posibles mejoras

Directivas y procedimientos

Se debe entender como Directivas y procedimientos a: Las directivas de recursos humanos y relaciones con terceros. La tabla 8 contiene los resultados correspondientes.

Tabla 8 Directiva y procedimientos.

Directiva y procedimientos	47.9 %	6.25 %	45.8 %
Comprobaciones del historial personal	68.7 %	0 %	31.2 %
Directiva de recursos humanos	75 %	0 %	25 %
Relaciones con terceros	0 %	18.7 %	81.2 %

Como puede notarse en la tabla inmediatamente anterior (tabla No. 8), existe una mayor aproximación a cumplir con las practicas recomendadas en lo referente a los procedimientos para contratar aspirantes y finalizar sus contratos (Comprobaciones del historial personal 47.9% y Directiva de recursos humanos 75%); lo que resulta muy importante a la hora de proteger a la empresa contra

empleados sin escrúpulos o descontentos. Por medio de la tabla podemos también percibir que la relación con terceros necesita mejorar muchísimo (81.2%). Los procedimientos claros y prácticos en la gestión de las relaciones con los fabricantes y socios pueden ayudarle a minimizar el nivel de riesgos al que se expone la empresa.

Formación y conocimiento

Se debe entender como Formación y conocimiento a la divulgación de medidas de seguridad.

Tabla 9 Formación y conocimiento.

Formación y conocimiento	**9.3 %**	**3.1 %**	**87.5 %**
Conocimiento de seguridad	0 %	0 %	100 %
Formación sobre seguridad	18.7 %	6.25 %	75 %

En la tabla No. 9 se puede estimar que la falta de conocimiento (100%) y formación (75%) de los empleados de las empresas es insuficiente. Los empleados deben recibir formación para que sean conscientes de cómo las medidas de seguridad afectan sus actividades diarias, para no exponer a la empresa a mayores riegos.

Las encuestas realizadas muestran un claro predominio de carencias severas en todas las secciones definidas para el análisis. A continuación se presenta una tabla que tiene como objetivo mostrar en ella los valores porcentuales de las vulnerabilidades en las secciones de: Infraestructura, Aplicaciones y Personal del total de empresas del sector transporte de Bogotá que participaron en la investigación.

Tabla 10 Vulnerabilidades por secciones.

Secciones			
Infraestructura	9.8 %	12.5 %	77.6 %
Aplicaciones	1.3 %	8.4 %	90 %
Personal y operaciones	24.1 %	4.46 %	71.4 %

En la tabla No. 10 se observa que el mayor porcentaje de carencias severas se encuentra en la sección de Aplicaciones (90%) y el menor en la sección Personal y operaciones. Según las normas ISO 17799 e ISO 27001 la seguridad de la información debe incluir todas las áreas de la empresa pero principalmente se debe tener en cuenta el personal por ser el eslabón más difícil de asegurar.

Las falencias por cada una de las empresas pueden verse en el anexo G.

5.3. DOMINIOS

En el actual proyecto y basados en las normas ISO/IEC 17799 e ISO/IEC 27001 se van a manejar 9 dominios de los 11 que incluye esta norma y partiendo de estos se generaran políticas y controles adecuados para las empresas con redes SOHO del sector transporte de Bogotá.

5.3.1. Política de Seguridad. Dirigir, aprobar e informar de forma adecuadaal personal implicado el manual y dar soporte a la gestión de la seguridad de la información.

5.3.2. Seguridad Organizacional. Gestionar la seguridad de la información dentro de la organización, mantener la seguridad de los activos accedidos por terceros, aún si la responsabilidad de su proceso pasa a otra organización teniendo en cuenta que la seguridad no es sólo un aspecto técnico.

5.3.3. Administración de Activos de Información. Mantener y asegurar un nivel de protección adecuada de acuerdo a su criticidad sobre los activos de la información de la organización.

5.3.4. Seguridad del Recurso Humano. Asegurar que los usuarios se concienticen de las amenazas y riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y los servicios, minimizando los daños provocados por incidencias de seguridad y por el mal funcionamiento, para controlarlos y aprender de ellos.

5.3.5. Seguridad Física y Ambiental. Prevenir las exposiciones a riesgo como incendios, robos de información y de recursos de tratamiento de información, evitando accesos no autorizados, daños e interferencias contra los locales y la información de la organización.

5.3.6. Administración de comunicaciones y operaciones. Minimizar el riesgo de fallos en los sistemas, protegiendo la integridad del software, la disponibilidad de los servicios de tratamiento de la información y comunicación, y proteger las redes y su infraestructura de apoyo.

5.3.7. Control de Acceso. Controlar los accesos a la información, evitando accesos no autorizados a los sistemas de información, servicios de red y ordenadores.

5.3.8. Adquisición mantenimiento y desarrollo de sistemas de información. Proteger la confidencialidad, autenticidad e integridad de losdatos, para garantizar que los sistemas de información se encuentren protegidos.

5.3.9. Administración de la continuidad del negocio. Aprobar y revisar periódicamente planes de contingencia para evitar la interrupción de actividades del negocio y proteger sus procesos críticos frente grandes fallos o desastres.

5.4. POLÍTICAS

Teniendo en cuenta el análisis de vulnerabilidades y los dominios que maneja la Norma ISO/IEC 27001 y la ISO/IEC 17799 en este documento se definen las políticas más relevantes a partir de las necesidades de la pequeña y mediana empresa en el Sector transporte de Bogotá**.**

Para mayor información ver anexo I donde se encuentra el manual con todas las políticas de seguridad de la Información diseñadas.

5.4.1. Política de Seguridad. Estas políticas de seguridad les brindaran a las pequeñas empresas del sector transporte de Bogotá una mayor protección en la información y protección de las herramientas tecnológicas de la organización, de tal modo que sean una guía de implementación, en la cual se habrá tenido en cuenta los resultados de las encuestas aplicadas y analizadas previamente, para así conocer cuáles son las principales deficiencias en la organización y cómo prevenir a costos alcanzables para las pequeñas empresas.
Estas políticas de seguridad abarcan los posibles cambios que la organización pueda sufrir, como mejoramiento de las instalaciones, incremento de personal e incremento en las herramientas informáticas entre otros.

5.4.2. Seguridad Organizacional. Los servicios informáticos de la Red Organizacional dentro de una PYME del Sector Transporte de Bogotá son de uso exclusivo de la misma, para las gestiones administrativas, técnicas y de orden laboral, cualquier cambio en el uso de los servicios debe ser expresado y adecuado como política de seguridad en este documento.

- **Funciones y Responsabilidades Del Área De Seguridad Organizacional**

a) El área de Seguridad Organizacional, es la encargada de establecer, mantener y administrar una arquitectura de seguridad para la PYME del Sector Transporte de Bogotá y facilitar la incorporación de prácticas de seguridad de la información en todas las dependencias.

b) El área de Seguridad Organizacional debe estar ubicada organizacionalmente de manera que tenga autonomía e independencia frente a las demás áreas de tecnología tales como: soporte, diseño y desarrollo, entre otras.

- **Funciones De Control**

a) Contar con mecanismos de monitoreo con el fin de detectar oportunamente procedimientos inseguros para los Sistemas Operacionales, Aplicativos, Datos y Redes.

b) El Área de Seguridad Organizacional, es responsable por la revisión continua de las Políticas de seguridad de la información por lo menos una vez al año.

- **Jefe de seguridad de la información**

a) Se debe crear una Autoridad de Nivel Superior que integra el Comité de Seguridad. Bajo su administración están la aceptación y seguimiento de las políticas y normativa de seguridad en concordancia con las autoridades de nivel superior.

b) El jefe principal de la seguridad de la información debe claramente especificar, por escrito, la asignación de las responsabilidades de la propiedad de la información para las bases de datos, los archivos maestros y otras recopilaciones de información compartidas y debe designar a las personas con derecho a acceder a dichas recopilaciones en nombre de los Propietarios.

- **Coordinación de la seguridad**

a) Efectuar estudios de análisis de riesgos en seguridad de la información para identificar oportunamente los eventos o situaciones de fallos en los accesos o en el manejo de la información presentados en la PYME del Sector Transporte en Bogotá, estableciendo planes de acción que incluyan controles para contrarrestarlos y reducir el riesgo a un nivel aceptable.

b) Dar soporte y apoyo a las investigaciones sobre violaciones a la seguridad de los sistemas en apoyo al área de Seguridad no Tecnológica (Física) y presentar los informes respectivos a la Dirección de la Organización.

- **Seguridad con Terceros**

a) No debe otorgarse identificador de usuario ni privilegios para utilizar los computadores o los sistemas de comunicación de la PYME del Sector

Transporte de Bogotá a las personas que no sean empleados, a contratistas o consultores, a menos que se obtenga la autorización escrita del gerente del área.

b) El acceso de terceros a cualquier información interna de la PYME del Sector Transporte de Bogotá se concede sólo demostrando la necesidad de conocerla y cuando tal divulgación este expresamente autorizada por la gerencia de la Empresa.

- **Responsabilidad por la información**

a) El jefe o administrador de cada área dentro de la Red Organizacional de la PYME del Sector Transporte en Bogotá, es el único responsable de las actividades procedentes de las acciones que se lleven a cabo en su área.

b) La responsabilidad de especificar controles de información apropiados por parte del Propietario de la información no debe ser delegada a proveedores de servicios fuera de la PYME del Sector Transporte en Bogotá.

5.4.3. Administración de Activos de Información. Cada uno de los activosdebe tener un dueño, "propietario" o una persona delegada para la custodia, mantenimiento y controles adecuados en el manejo de la información, con el fin de tener buen manejo de la misma, basada en la organización.

- **Inventario de Activos**

a) Se debe elaborar y actualizar constantemente un inventario con todos los activos previamente identificados por su importancia.

b) En caso de desastre la información debe estar completa. El inventario deberá incluir los siguientes ítems; tipo de activo, formato, ubicación, información de soporte, licencias y valor para el negocio.

- **Clasificación de la información**

a) Al momento de clasificar la información debe hacerse en términos de su valor, requisitos legales, sensibilidad e importancia en la empresa.

b) Hacer y efectuar un conjunto de procedimientos para el etiquetado y manejo de la información de acuerdo con el esquema de clasificación utilizado por la empresa, comprendiendo los activos de información en formatos físico y electrónico.

5.4.4. Seguridad del Recurso Humano. Dar a conocer a los candidatos al trabajo durante el proceso previo a su contratación las responsabilidades y funciones para disminuir los riesgos o para evitar el inadecuado uso de la infraestructura.

- **Responsabilidades de los usuarios**

a) El área de contratación de recursos humanos deberá realizar estudios sobre antecedentes de los aspirantes a algún cargo dentro de la organización según los requisitos de la empresa, clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.

b) Se debe firmar un acuerdo de confidencialidad o de no divulgación en caso que el empleado o usuario tenga acceso a información sensible. antes de que este utilice los servicios de procesamiento de información.

- **Entrenamiento**

a) Brindar educación y formación continua a los empleados para que respondan con su función de trabajo correctamente.

b) Establecer un proceso disciplinario para los empleados que han cometido alguna violación de seguridad de la empresa, corroborando la infracción cometida para así tomar la decisión pertinente dependiendo de la gravedad. En los casos más graves de mala conducta este proceso deberá permitir el retiro instantáneo de las funciones al empleado y si es necesario su expulsión de la empresa.

5.4.5. Seguridad Física y Ambiental. Las instalaciones donde las pequeñas empresas del sector transporte de Bogotá se encuentran ubicadas, deberán cumplir con ciertos requisitos para así garantizar la seguridad física y lógica de la organización, ya que la mayor parte de las amenazas ambientales y externas no se pueden controlar por parte de la organización, por lo que se deben definir medidas de seguridad para evitar catástrofes o incidentes en la organización, tales como la pérdida total o parcial de la información o de las herramientas tecnológicas utilizadas para preservar dicho bien.

- **Controles de acceso perimetral**

a) Las entradas a las instalaciones deberán contar con un sistema de vigilancia privada y controles de accesos mediante identificación de usuarios (empleados y visitantes), permitiendo así el control de quién entra y quién sale de las instalaciones de la organización.

b) Deberán ser instalados sistemas de detección de intrusos, como sensores de robo en ventanas, puertas y otros accesos físicos que tenga la organización.

- **Controles ambientales**

Los controles ambientales serán aquellos que protejan a la organización de desastres causados por el medio ambiente; como desastres naturales o desastres provocados por el hombre que alteren el medio ambiente.

a) Toda oficina o área de trabajo debe poseer entre sus inventarios, herramientas (extintores, alarmas contra incendios, lámpara de emergencia), necesarias para proteger los recursos tecnológicos y la información.

b) Las instalaciones de las áreas de trabajo deben contar con una estación de alimentación ininterrumpida o UPS para evitar la pérdida de información.

- **Mantenimiento**

a) Las herramientas tecnológicas deberán entrar a mantenimiento durante ciertos intervalos de tiempo previamente establecidos por el proveedor de estos.

b) Cuando el equipo es programado para mantenimiento deberá notificarse con anticipación al usuario para que este pueda realizar un backup de todos sus archivos, evitando así perdida de información. Si la información es sensible y el mantenimiento del equipo va a ser realizado fuera de las instalaciones de la organización,se deberá realizar una copiade la información antes de que el equipo de cómputo sea sacado de la organización.

.

- **Centro de Cómputo**

La seguridad en un centro de cómputo se refiere a la protección del hardware, y del software. Algunas medidas de seguridad de un centro de cómputo son:

a) Debe darse una buena capacitación a los operadores del centro de cómputo para que estos sean capaces de resolver problemas para evitar que haya fallas en el procesamiento de la información.

b) Evitar introducir alimentos al centro de cómputo, tales como líquidos, para impedir que puedan derramarsesobre las máquinas, lo cual afectaría seriamente los equipos.

5.4.6. Administración de comunicaciones y operaciones. La administración de comunicaciones tiene como función gestionar y garantizar que las instalaciones donde se procese la información sean seguras. Para esto se debe asignar ciertas responsabilidades que garanticen el correcto funcionamiento de las comunicaciones de la organización.Estas responsabilidades incluyen desarrollo de instrucciones operativas y procesamientos apropiados para poder obtener una buena respuesta a incidentes.

Es necesario implementar una separación de obligaciones cuando sea necesario, ya que por medio de este procedimiento es posible reducir el riesgo de negligencias en el uso del sistema.

- **Documentación operativa**

a) Se debe preparar documentos sobre mantenimiento de las herramientas tecnológicas, indicando la clase de mantenimiento y la fecha estimada de la realización del procedimiento.

b) Es necesario mantener una documentación sobre cualquier cambio, eliminación o creación en los procesos operativos para así poder llevar un seguimiento de quien realizo los cambios o quien, creo o elimino dichos procesos.

- **Separación de ambientes**

Consiste en que no toda la información debe estar centralizada, ya que esta práctica se presta para manipulación indebida, alteración y robo de información.

a) Se deben separar los rolesy funciones de los administradores de la información a fin de mejorar el control y disminuir el riesgo de mal uso accidental o deliberado del sistema.

Las pequeñas empresasdel Sector Transporte de Bogotá pueden encontrar este método de control difícil de cumplir debido al costo que representa la contratación de personal adicional. El principio debe aplicarse en la medida de lo posible.

- **Servicios de red**

La administración de servicios de red tiene como objetivo proteger la información que está siendo utilizada a través de esta.

a) Se deben fijar responsabilidades y procedimientos en la administración de los equipos de red.

b) Los servicios que presta el proveedor de internet deben ser controlados y estar sometidos a un acuerdo a nivel de servicio para fijar todas las estipulaciones necesarias en dicho acuerdo.

- **Backups**

El Backup es un método para proteger la información de la empresa de tal forma que si alguno de los equipos de la empresa sufre daño, robo o algún tipo de catástrofe, esta no pierda información vital.Por lo que permite contar con una copia de respaldo. Garantizando disponibilidad en la información.

Se deben establecer procedimientos para la realización de las copias de seguridad:

a) La frecuencia con la cual se realizan las copias de seguridad deberán ser establecidas por la organización.Esta frecuencia dependerá de la cantidad de información que necesita resguardar y de su importancia.

b) Estas copias de seguridad deberían ser almacenadas en un lugar remoto, ya que si se almacena en el mismo lugar, se corre el riesgo de perder el riesgo de perder información en forma definitiva debido a desastres como incendios, robos, inundaciones, etc.

5.4.7. Control de Acceso.

- **Administración de usuarios**

Debe asegurar los accesos a usuarios autorizados y prevenir el acceso la información protegida.

a) El usuario solo podrá acceder a información o programas a los cuales tenga permisos de acceso y modificación.

b) Debe existir un documento donde se indique las condiciones de acceso de los usuarios a la información de la organización.

- **Controles de acceso de red**

a) El servicio de red solo debe proporcionarse a los usuarios de la organización.

b) La dirección debe controlar los procedimientos de cómo se protegen los accesos a la red.

5.4.8. Mantenimiento y desarrollo de sistemas de información. El objetivo de las políticas presentadas en este ítem, es garantizar que la seguridad se encuentre incorporada en todos los sistemas de información de la organización.
El diseño e implementación de los procesos del aplicativo o servicio pueden ser cruciales para la seguridad. Las necesidades en seguridad deberán ser identificados, justificados y aprobados en la fase de requerimientos.

- **Requerimientos de seguridad**

a) Todos los requerimientos de seguridad que fueron previamente aprobados deberán ser agregados en la etapa de implementación del aplicativo.

- **Administración de la vulnerabilidad técnica**

La administración de vulnerabilidades técnicas trata de reducir riesgos, esta debe ser puesta en ejecución de una manera sistemática, y repetible de forma que se vea la eficacia de la misma. Estas consideraciones deben incluir los sistemas operativos así como los aplicativos que están en uso.

a) Se deben definir y establecer responsabilidades para la administración de las vulnerabilidades técnicas, incluyendo la supervisión de estas y la evaluación de riesgos y parches.

b) Si la organización identifica una vulnerabilidad técnica potencial, se debe identificar los riesgos asociados y las acciones que se tomarán.

5.4.9. Administración de Incidentes de Seguridad. Una vez que un incidente ha sido reportado se debe comenzar con un proceso de mejora y cambio, para luego dar una pronta solución a dicho incidente.

a) Deben existir procedimientos o planes de contingencia para los incidentes mencionados anteriormente (Reporte de Incidentes y eventos de seguridad).

b) El procedimiento para la recuperación de violaciones de seguridad, corrección de fallas o incidentes debe ser informado formalmente al consejo de seguridad informática.

5.4.10. Administración de la continuidad del negocio. La administración de la continuidad del negocio permite contrarrestar las interrupciones dentro de los sistemas de información y las herramientas tecnológicas de tal forma que la organización no se vea afectada con fallas o desastres.

- **Planeación del Plan de Continuidad del Negocio**

a) Se deben identificar los recursos disponibles (recursos financieros, organizacionales, técnicos, y ambientales) para saber cómo clasificarlos y suadecuada respuesta al incidente presentado.

b) Se debe asegurar la protección del personal y de las instalaciones.

5.5. CONTROLES

Los controles fueron definidos con base a las normas ISO 27001 y 17799 y las vulnerabilidades encontradas en las empresas encuestadas.
Estos controles fueron diseñados con el fin de reducir riesgos, ataques o cualquier posible amenaza que sufran los datos y así garantizar la integridad, disponibilidad y confiabilidad de la información.

5.5.1. Controles de infraestructura. Permitirán a las organizaciones tener una adecuada protección en la defensa del perímetro, en la autenticación y en la gestión y el control.

5.5.1.1. Segmentación

- Utilice segmentos para impedir el acceso a extranets específicas por parte de fabricantes, socios o clientes.
- Cada segmento externo de la red debe permitir que sólo se encamine determinado tráfico hacia los hosts y puertos concretos de aplicaciones que proporcionan servicios a los clientes.
- Asegúrese de que existan controles de red que permitan sólo el acceso necesario para cada conexión de terceros.
- Limite el acceso a los servicios de red suministrados, así como el acceso entre los segmentos de red.

5.5.1.2. Red SOHO

- Se debe configurar el protocolo TCP/IP en el servidor y el acceso remoto a la interfaz de la red. Se debe contar con la dirección IP, con la máscara de subred y la dirección del servidor DNS,parámetros suministrados por el proveedor de servicios de internet.
- Es necesario determinar cómo van a obtener las direcciones IP los equipos de la red.

- Se deben registrar y resolver nombres NetBIOS de los equipos en la red.
- Si su sistema operativo es Windows; utilice el comando **nslookup** con el fin de comprobar que se puede resolver nombres DNS. Utilice el comando **ping** para probar que TCP/IP está instalado y funciona correctamente.
- Considere instalar sistemas de detección de intrusiones basados en red o host, para así detectar o notificar cualquier ataque que se produzca.
- Se debe realizar un escaneo de puertos periódicamente, con el fin de identificar que puertos se encuentran abiertos y mediantequé servicio o aplicación.
- Se deben cerrar todos aquellos puertos que no se estén usando por aplicaciones o servicios permitidos por el comité de seguridad de la organización.

5.5.1.3. Reglas y filtros del firewall

- Los firewalls son un mecanismo de primera línea de defensa y se deben colocar en todas las ubicaciones de borde de red. Las reglas implementadas en los firewalls deben ser muy restrictivas y establecerse host a host y servicio a servicio.
- Se debe utilizar un dispositivo para controlar el acceso al nivel de red como un firewall, con una configuración que controle el tráfico. Se deben usar filtros de entrada y de salida para evitar el acceso no autorizado a los servicios.
- Realice un análisis de las reglas del firewall para así hacer cambios si estas lo requieren.
- El firewall debe estar establecido con una posición de denegación predeterminada, permitiendo únicamente el tráfico necesario.

5.5.1.4. Acceso remoto

- Limite el acceso de los usuarios que tienen permiso de acceder remotamente de acuerdo a su nivel de permisos, también límite el tiempo de permanencia.
- Utilice conectividad sitio-a-sitio basada en la tecnología IPSEC. Configure listas de acceso a redes y de usuario para limitar el acceso a los recursos corporativos necesarios.

5.5.1.5. Antivirus

- Piense en utilizar una solución antivirus al principio en los servidores de archivos importantes y, a continuación, en los servidores de correo, de base de datos y de red.

- Considere además utilizar la solución antivirus en los equipos de escritorio y portátiles.

5.5.1.6. Seguridad física

La seguridad física es uno de los aspectos más importantes que se debe tener en cuenta a la hora de diseñar un sistema informático. A de pesar que la información sea la más segura en cuanto a ataques externos, la seguridad será nula si no se tienen medidas de control, en caso de tener que enfrentar un desastre. De esta manera se dice que la seguridad física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención o contramedidas ante amenazas a los recursos e información confidencial[22], refiriéndose a los controles y mecanismos que se deben implementar dentro y cerca de los centros informáticos para proteger tanto el hardware como los medios de almacenamiento de la información, de esta forma las empresas de transporte protegen de manera básica la información que poseen.

- Desastres

Este tipo de seguridad se focaliza en cubrir las amenazas ocasionadas por el hombre y la naturaleza a las unidades físicas donde se almacena la información. Las principales amenazas que se observan son:

- Desastres naturales, incendios accidentales, tormentas e inundaciones.
- Disturbios, sabotajes internos y externos deliberados.

Con el fin de brindar oportunamente una serie de acciones para prevenir, reducir, recuperar y corregir los diferentes riesgos, a continuación se consideran los peligros más importantes que pueden ocurrir en los centros informáticos.

[22]http://www.rediris.es/cert/doc/unixsec/node7.html. Seguridad física de los sistemas, hora 8:30 am Día 20/NOV/2009

- Incendios

El fuego es una de las principales amenazas contra la información, ya que puede destruir en pocos minutos una computadora arruinando y eliminando fácilmente los archivos de información y el software.

Desafortunadamente los sistemas anti-fuego muchas veces pueden ocasionar más daño a los sistemas electrónicos que el mismo incendio.

Los diferentes factores que se deben tener en cuenta para prevenir un incendio son los siguientes:

- El local donde se encuentra el centro informático no debe ser combustible o inflamable.
- El área no debe ubicarse cerca a lugares donde fabriquen, almacenen o procesen materiales inflamables, explosivos.
- Las paredes se deben fabricar de materiales incombustibles y extenderse desde el suelo hasta el techo.
- Se debe construir sobre el piso real un piso falso con materiales incombustibles y resistentes al fuego.
- No se debe fumar en esta área.
- Los muebles y cestas para los papeles no deben ser de materiales plásticos e inflamables, preferiblemente metálicos.
- El centro de cómputo y de almacenamiento debe ser impermeable.

- Inundaciones

Las inundaciones son las mayores causas de pérdidas de información y daños en los centros de cómputo. Para evitar esto, se deben colocar pisos falsos con una altura mayor que la del piso original del centro de cómputo.También se debe construir techos impermeables para evitar el paso de agua del nivel superior.

- Instalaciones eléctricas

  Los centros de cómputo deben tener medidas de seguridad industrial en cuanto a redes eléctricas se trata. Por lo tanto se debe tener un especialista que evalúe riesgos particulares y aplique las soluciones de acuerdo a las normas.

- Controles de acceso

Utilizar controles de acceso permite tener un registro sobre quien ingresa o sale de la empresa, con el fin de brindar una mayor seguridad en la información.

- Uso de vigilancia privada - control de acceso de personas

  Para tener un control de acceso de las personas que entran y salen de la empresa se sugiere contratar un servicio de vigilancia. Este servicio deberá realizar las siguientes inspecciones a personas que entran a la empresa:

  Si es un empleado se recomienda el uso de credenciales con foto, y cargo, con el fin de efectuar un control en el ingreso y salida del personal.
  Desventajas: cuando las credenciales son validadas mediante códigos de barra u otro método es posible que estas sean robadas o clonadas, permitiendo que cualquier persona no autorizada ingrese a las instalaciones de la empresa.

  Si es un visitante se recomienda que éste llene un formulario donde ingrese sus datos personales, motivo de visita, lugar al cual se dirige y se lleve un registro de la hora de ingreso y salida de este. A su vez se aconseja pedir un documento de identificación validando nombre y foto y reemplazarlo con una credencial de visitante. Cuando este salga de las instalaciones obtendrá de vuelta su documento y entregara la credencial de visitante.

  Además de esto se debe anunciar al visitante al sector de la empresa donde va para obtener autorización de ingreso correspondiente.

- Control de acceso de vehículos

  Como se habla de empresas de transporte, el número de vehículos que ingresan a estas es grande. Por esto los vehículos que pertenecen a la empresa deben estar debidamente listados en una base de datos relacionando allí el dueño del vehículo y el conductor. Se deberá tener un registro de horarios de ingreso y salida así como realizar una inspección del contenido del vehículo.

  Los vehículos que no pertenezcan a la empresa deben portar una tarjeta de permiso para ingresar y se deben registrar en una base de datos donde este la

información tanto del vehículo como del conductor y así mismo controlar la hora de ingreso y de salida, como también el contenido del baúl del vehículo.

- Uso de sistemas biométricos

La tecnología biométrica permite identificar con mayor precisión a un individuo para así poder obtener mayor confiabilidad a la hora de validar su identidad.

Esta tecnología permite eliminar o restarle importancia a una credencial de identificación al momento de validar la identidad al ingresar a la empresa.

Los costos de administración de la tecnología biométrica son más económicos que los costos de administración y mantenimiento de las credenciales, ya que solo se debe contar con alguien que los limpie y que verifique su correcto funcionamiento. Otra persona estará encargada de actualizar la base de datos. La mayor ventaja de esta tecnología es que las características biométricas de una persona, son intransferibles a otras.

El sistema más sencillo y económico de utilizar es la verificación de patrones mediante huellas dactilares.

- Verificación de huella dactilar

Esta verificación se basa en el principio de que no existen dos huellas dactilares iguales. Las huellas digitales poseen diferentes arcos, ángulos bucles y remolinos, llamados crestas papilares. Estas crestas son analizadas para así obtener la información de la persona y compararla contra la base de datos para así identificar plenamente a la persona.

Actualmente la identificación mediante el sistema biométrico de verificación de huella dactilar es el más usado, ya que este es de bajo costo y se consigue fácilmente. El costo aproximado de estos aparatos es de $ 180000 pesos colombianos.

- Circuito cerrado de televisión

Permite visualizar las instalaciones de la empresa en tiempo real mientras estén bajo la constante vigilancia de personal calificado. De esta forma se tiene pleno conocimiento de quien utiliza o entra a los distintos sectores de la empresa. Estas cámaras cuentan con un sistema de control contra sabotaje de manera que si existe algún corte de luz, o se produce algún daño, se enviara una señal a la central para que se realice la acción correspondiente.

- Detectores pasivos sin alimentación

Existen unos sensores que son capaces de detectar incendios, robos o intrusiones. Estos son instalados por compañías de seguridad especializadas. Cuando algún cambio es detectado por los sensores, se activa un sistema de alarma, el cual envía una señal a la central y este, dependiendo del tipo de señal avisa a los bomberos o a la policía.

5.5.1.7. Usuarios administrativos.

- Considere tener cuentas separadas para las actividades administrativas o de gestión y asegúrese de que las credenciales administrativas se modifican con frecuencia.
- Cambie las contraseñas básicas por contraseñas que sean alfanuméricas, que incluyan mayúsculas y minúsculas, que tenga al menos un carácter especial y una longitud mínima de 8 caracteres.

5.5.1.8. Directivas de contraseñas.

- Las cuentas administrativas deben tener mayor protección. con algunas lleve registros y monitoree todas las autenticaciones, correctas o incorrectas.

- Utilice logs para almacenar los intentos de conexión fallidos por mal ingreso de usuario y contraseña, y permita que los administradores del sistema reciban alertas sobre estas anomalías.

5.5.1.9. Cuentas inactivas.

- Visite con regularidad los sitios de fabricantes y otros proveedores de soluciones de seguridad para buscar avisos de ataques recientes y brotes de virus. Realice auditorías regularmente para comprobar que los usuarios remotos actualizan sus sistemas.

5.5.1.10. Usuarios internos.

- Piense en poner en práctica controles de contraseñas complejas para todos los usuarios, con independencia de su nivel de acceso. Una contraseña se considera compleja si cumple con los criterios de ser alfanumérica, que incluya mayúsculas y minúsculas, caracteres especiales y tener una longitud mínima de 8 caracteres.

5.5.1.11. Usuarios de acceso remoto.

- Piense en poner en práctica controles de contraseñas complejas para todos los usuarios de acceso remoto, sin importar si el acceso se concede a través de tecnologías telefónicas o vpn

5.5.2. Controles de aplicaciones. Permitirán a las organizaciones tener una adecuada protección en todo lo relacionado con las aplicaciones; su implementación y uso, el diseño de estas y la autenticación.

5.5.2.1. Almacenamiento

La restricción mediante controles de acceso se pueden implementar en:

- Sistemas operativos
- Programas específicos
- Bases de datos
- Sistemas de seguridad específica

Algunas de las posibles formas para poder controlar los accesos son:

- Mediante sistemas biométricos, como lo es el lector de huellas.
- Mediante contraseñas que solo conoce el usuario o pines asignados al mismo.
- Mediante detector de patrones de escritura como lo es la firma digital.

Se necesita una buena administración de los permisos de acceso para que estos surtan efecto y logren ejercer su control sobre los archivos. Para esto se debe tener en cuenta unos consejos para el buen funcionamiento, creación y asignación de permisos de acceso, de usuario y de aplicación.

Debe existir un proceso de solicitud de permiso del usuario al administrador del sistema de la empresa, el cual, debe ser el encargado de verificarlos y de borrar usuarios no existentes. La habilitación de permisos debe provenir de la autorización de un superior, en donde especifique a qué información puede acceder.

Deben existir unas revisiones periódicas sobre las cuentas de usuarios y sus permisos. Se deben generar auditorias para verificar cual es el estado de la seguridad en la empresa.

Se debe realizar un monitoreo constante para así detectar intrusiones o actividades no autorizadas, de tal modo que se tenga una alta confiabilidad de la información que fluye dentro de la organización.

5.5.2.2. Desarrollado por un proveedor de software independiente

- Cuando aparezca una actualización de la aplicación, pruébela completamente antes de utilizarla.
- Consiga la documentación para reforzar los conocimientos sobre la aplicación. Si existe revise las configuraciones de la aplicación.

5.5.2.3. Directivas de contraseñas

- Utilice registros para las autenticaciones fallidas. Éstos deberán enviar alertas a los administradores de los sistemas.Coloque contraseñas fuertes en todas las aplicaciones.
- Utilice directivas de bloqueo de cuentas para las aplicaciones principales de su empresa.

5.5.2.4. Autenticación

- Piense en poner en práctica controles de contraseñas complejas para todas las cuentas de las aplicaciones importantes.

5.5.2.5. Autorización y control de acceso

- Visite regularmente los sitios web de las aplicaciones y busque todas las actualizaciones disponibles en seguridad.

5.5.3. Controles de personal. Se encargara de establecer lineamientos para que los directivos de la organización, tengan control sobre el personal que trabaja en esta.

5.5.3.1. Relaciones con terceros

- El personal interno deberá otorgar permisos a terceros dependiendo de lo que vaya a trabajar en los equipos de cómputo, tomando en cuenta restricciones de hora, de día y de acceso a información entre otros.

5.5.3.2. Roles

Se debe tener en cuenta, que un rol debe llevar permisos como:

- **Escritura**: en donde el usuario puede modificar la información.
- **Lectura**: el usuario solo puede leer la información pero no posee la capacidad de modificarla.
- **Ejecución**: en donde el usuario tiene o no permisos de utilizar programas.
- **Borrado**: en donde el usuario tiene los permisos para borrar archivos.Debe existir un control, de cuáles son los archivos que va a borrar.

5.5.3.3. Requisitos de seguridad.

- La asignación de niveles de importancia a cada componente de la infraestructura informática permite que la mayoría de los recursos se apliquen a aquéllos equipos establecidos como los más críticos y que los sistemas que son menos críticos reciban menos recursos. Como consecuencia, se aplican con mayor eficacia los escasos recursos de seguridad en aquellos sistemas que los necesitan más.

5.5.3.4. Evaluaciones de seguridad.

- Primero deberá evaluar internamente su infraestructura, el estado de su red, y el de sus aplicaciones. Al tener los resultados de las evaluaciones utilícelos para realizar procesos de mejora.

5.5.3.5. Formación sobre seguridad

- La formación basada en roles y el aprendizaje continuo garantizan que todos los empleados entiendan qué se espera de ellos y cómo deben satisfacer esas expectativas. Siga ofreciendo formación en todos los niveles de la empresa y en todos los aspectos de seguridad que exigen el desempeño de los distintos cargos.

5.5.3.6. Comprobaciones del historial personal

- Asegúrese de comprobar el historial del personal donde incluya una evaluación del historial laboral, la formación y los antecedentes penales del aspirante.

5.5.3.7. Directiva de recursos humanos

- Revise a menudo el procedimiento para los empleados que dejan la empresa de forma hostil, asegúrese de dejar record en su hoja de vida.

5.5.4. Controles de operaciones. Se encarga de proporcionar controles en el área de administración de continuidad del negocio y de prevenir perdida de información vital para la organización.

5.5.4.1. Copias de seguridad y recuperación

- Documente como se realiza el proceso de copia de seguridad y recuperación para los sistemas críticos para la continuidad empresarial.

- Pruebe el proceso de copia de seguridad y restauración frecuentemente para garantizar que todos los componentes (hardware y software) funcionen adecuadamente.

5.5.4.2. Dispositivos de copia de seguridad

- Tenga en cuenta que los dispositivos de copias de seguridad asi como los backups, se encuentren en un lugar protegido y en lo posible en otra instalación diferente a la empresa.

5.5.4.3. Eliminación de datos

- Los procesos de eliminación de datos en los servidores se deben hacer mediante permisos especiales y solo lo podrá hacer un administrador de tecnología, teniendo autorización previa del gerente de la empresa e internamente llevar un registro de quien borro los datos.

6. PRESENTACIÓN Y ANÁLISIS DE RESULTADOS.

- **Asignación del sector transporte por parte del semillero de investigación NEOBYTE**.

Según la Cámara de Comercio de Bogotá las empresas se dividen por sectores. Así mismo, el semillero de investigación NEOBYTE de la universidad de San Buenaventura Bogotá asigno a sus integrantes estos sectores para desarrollar una investigación sobre las vulnerabilidades que tienen las pequeñas empresas con respecto a su información almacenada digitalmente. Para el presente proyecto fue asignado el sector transporte.

- **Sectorización de empresas y llamada de presentación por parte de los estudiantes de la universidad San Buenaventura. a las empresas previamente seleccionadas.**

De un total de 258 empresas resulto una muestra de 100. (Ver anexo C)
Al realizar las llamadas y en el caso de tener respuesta a esta, se tomó como base un libreto de presentación suministrado por el semillero de investigación NEOBYTE. (Ver anexo D).
En la verificación de datos comerciales de las empresas se pudo encontrar que muchas ya no se encontraban activas, el número telefónico no correspondía a la empresa o no estaban interesados en participar de la investigación (Ver Tabla 11).

- **Visita y aplicación de encuestas sobre los niveles de seguridad que tienen las empresas que aceptaron participar en la investigación.**

Se procedió a visitar a las 16 empresas, a aplicar una encuesta, recibir sugerencias de los encuestados y motivarlos para que protejan sus sistemas de información adecuadamente.

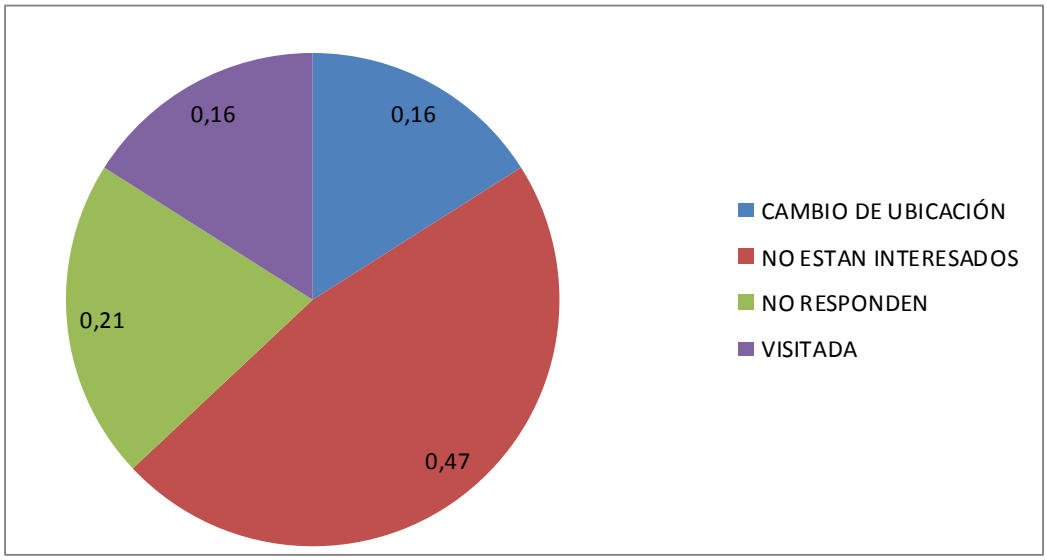
- **Tabulación de resultados**.

Después de haber visitado todas las empresas se hizo la recopilación y consolidación de la información obtenida, posteriormente se realizó la tabulación y la generación de los informes sobre los resultados obtenidos.

Ilustración 4 Llamada a empresas.

RESULTADO LLAMADA	N. EMPRESAS	%
CAMBIO DE UBICACIÓN	16	0,16
NO ESTAN INTERESADOS	47	0,47
NO RESPONDEN	21	0,21
VISITADA	16	0,16

TOTAL EMPRESAS LLAMADAS	100



- **Análisis de Vulnerabilidades con respecto a los informes obtenidos en las encuestas.**

De acuerdo con las respuestas obtenidas en la evaluación de riesgos aplicada durante la encuesta, las medidas de defensa se calificaron de la siguiente forma. Infraestructura, aplicaciones y operaciones.Con base en la información obtenida se identificaron las falencias en cuanto a la seguridad de la información de las empresas.

- **Selección de los dominios aplicables a las empresas y sus necesidades.**

Basados en la norma NTC-ISO 17799 y en el análisis de vulnerabilidades se definieron los dominios aplicables a las empresas del sector transporte y de este modo se clasificaron las áreas que se cubrieron con las políticas de seguridad.

- **Plantear las políticas de seguridad más apropiadas para las empresas.**

Con los dominios ya puntualizados, se plantearon las políticas de seguridad apoyadas en las especificaciones dadas por la norma NTC-ISO 17799 de tal modo que se cubrió la gran mayoría de vulnerabilidades encontradas en el análisis.

- **Definición de controles**

Después de analizar las vulnerabilidades y formular políticas, se propusieron controles que van a permitir reducir riesgos y generar mayor confiabilidad.

Para aumentar los niveles de seguridad se recomendaron controles adaptativos con el fin de reducir amenazas, errores o ataques,tanto en ubicaciones físicas como lógicas. Se utilizó como referencia el manual de cableado estructurado. (Ver anexo E).

6. CONCLUSIONES

- Proteger la información es una tarea cada vez más compleja para las empresas.

- Se ha observado que el riesgo que las empresas corren frente a las amenazas de seguridad es serio, debido a la poca importancia que se dá a este tópico y a la falta de conocimiento que estas tienen sobre el tema de seguridad de la información.

- Para disminuir los riesgos que se corren frente a la seguridad las empresas solo tienen en cuenta la Tecnología y no los procesos ni el persona

- El éxito de un plan para mitigar los riesgos queda en manos de los usuarios.

- Las empresas del sector transporte no toman la seguridad de la información como parte de la organización empresarial y si como un proceso aislado.

- La seguridad de la información es un agente importante dentro de las empresas y como tal se debe plantear mecanismos y/o estrategias que garanticen la integridad de dicha información.

- En general las empresas no implementan ningún tipo de seguridad en el perímetro de la red. No hay escudo protector contra intrusos, existen carencias severas en el punto donde la red interna de las pequeñas empresas se conecta con el exterior.

- Las empresas con redes SOHO no emplean procedimientos estrictos de autenticación de usuarios administradores, locales y de acceso remoto. Por tal motivo, intrusos pueden acceder fácilmente y sin autorización a la red mediante ataques locales o remotos.

- En las empresas analizadas no se garantiza la integridad y confidencialidad de los datos, la pérdida o el robo de estos afectan negativamente tanto los ingresos de las empresas como su reputación.

- En Colombia la seguridad de la información es muy escasa, en muy pocas empresas se preocupan por proteger adecuadamente su información.

7. RECOMENDACIONES

Las siguientes recomendaciones forman parte de las principales actividades que se deben tener en cuenta al llevar a cabo un proyecto similar al actual:

- Definir dentro del grupo de trabajo, un líder que coordine todo el proceso para la recolección de la información.
- Tener una sólo vocero oficial, que proporcione información acerca de las labores que debe cumplir cada miembro del grupo y que frente a las Directivas de la Universidad o Institución sea quien represente al grupo de trabajo.
- Buscar todas las facilidades para que los miembros del grupo de trabajo tengan acceso a toda la información sobre las empresas de sector que van a analizar.
- Verificar con un tiempo considerable la información comercial de las empresas, ante las entidades correspondientes (Cámaras de Comercio, SENA), para no perder tiempo en el momento de realizar visitas de campo o llamadas telefónicas.
- Pedir citas para realizar las visitas de campo.
- Pedir a la Universidad o Institución, las cartas de presentación correspondientes, para que en el momento de la visita de campo el estudiante sea atendido por la empresa.
- Tener preparados, todos los documentos (Encuestas, checklist, etc.) y llevar consigo preferiblemente una grabadora de sonido (pequeña) en el momento de tener la entrevista con la persona responsable de la seguridad de la información.
- El manejo de la información suministrada por las empresas debe ser de absoluta confidencialidad.
- Se deben generar las políticas y los controles, apoyados en los responsables de la seguridad de la información.

Siguiendo estas recomendaciones, se puede disminuir los tiempos para cumplir los objetivos planteados en un proyecto como el actual.

8. BIBLIOGRAFÍA

- BAYUK, J. Security through process management. Price Waterhouse, LLP. 1997.
- CARRACEDO Gallardo,Justo “Seguridad en redes telemáticas”, editorial Mac Graw Hill. 2004.
- CHAPMAN, B y ZWICKY, E.(1997) Construya Firewalls para Internet. O’Really. Edición en Español por McGraw Hill.
- COMER Douglas E. “Redes de Computadores, Internet e interredes”. Prenticel Hall. Primera edición. 1998.
- GRATTON, Pierre, “ Protección informática” editorial Trillas 1998.
- http://www.monografías.com, La Informática y Su Impacto Social, [16 de noviembre de 2008 13:30].
- http://www2.vo.lu/homepages/phahn/humor/hacker30.txt [23 de noviembre de 2008 12:30].
- http://www.informatica-juridica.com/legislacion/colombia.asp[23 de mayo de 2009 14:00].
- http://eva.utpl.edu.ec/openutpl/ocw/mod/glossary/view.php?id=153&mode=date [11 de febrero de 2009 17.00].
- http://www.inegi.gob.mx/inegi/contenidos/espanol/ciberhabitat/museo/cerquita/redes/seguridad/intro.htm[14 de febrero de 2009 14:00].
- http://www.unal.edu.co/seguridad/legislacion.htm[16 de agosto de 2009 13:00].
- http://blog.kalvinman.com/hackers/delitos-informaticos-en-colombia-ley-proteccion-de-la-informacion-y-de-los-datos/[15 noviembre de 2009 20:00].
- http://www.microsoft.com/spain/empresas/legal/informatica_forense.mspx [13 de enero de 2010 14:00].
- Ing. Guillermo –Santos http://www.acis.org.co/fileadmin/Revista_106/02-entrevistal.pdf [16 de noviembre de 2008 12:30].
- Ing. Ramírez-David http://www.fortinet.com/ [16 de noviembre de 2008 12:45].
- MENDES, Alvarado, Iván. “Proyecto seguridad informática para las redes de datos SOHO en la pequeña empresa de Bogotá".
- MARCELO RODAJO , “Piratas Cibernéticos” editorial: RA-MA 2003.
- Norma Técnica Colombiana NTC – ISO/IEC 17799, Tecnología de la Información, ICONTEC, 2006.
- Norma Técnica Colombiana NTC – ISO/IEC 27001, Tecnología de la Información, ICONTEC, 2006.

- Organization for Economic Cooperation and Development (OEDC) Guidelines for Security of Information Systems. 1992.
- STALLINGS, William, “fundamentos de seguridad en redes aplicaciones y estándares”. Prentice Hall .2006.
- SWANSON et al. (1996) National Institute of Standard and Technology (NIST). General Principles for Information Systems Security Policies.
- WILSON, M (1996) Marketing and Implementing Computer Security. NIST.

GLOSARIO

ACCESO: acción mediante la cual un usuario entra en un determinado recurso, (local, sistema de información, equipo informático, red…)

ACIS (Asociación Colombiana de Ingenieros de Sistemas): organización sin ánimo de lucro que agrupa a más de 1500 profesionales en el área de sistemas. Es el gremio de los Ingenieros de Sistemas participante en el desarrollo nacional.

ACTIVO: los activos son los recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección. Ejemplos de activos pueden ser los servidores de datos, las aplicaciones informáticas o los expedientes en papel.

ACTUALIZACIÓN:es el término que se utiliza para identificar los diferentes tipos de paquetes que pueden hacer que un sistema esté al día y/o incluya nuevas funcionalidades.

ADMINISTRADOR: persona que se encarga de todas las tareas de mantenimiento de un sistema informático. Tiene acceso total y sin restricciones al mismo.

AMENAZA: evento que puede producir un daño en el sistema de información.

ANTIVIRUS: software para la detección y prevención de virus.

AUDITORÍA:proceso de obtención y análisis de evidencias a fin de su evaluación y la elaboración de un informe acerca de la fiabilidad de los registros analizados.

AUTENTICACIÓN: proceso mediante el cual se comprueba la identidad de un usuario.

AUTORIZACIÓN: derecho otorgado a un individuo autenticado o proceso para utilizar el sistema de información y la información que éste contiene.

BACKUP: copia de seguridad que se realiza con el fin de mantener los datos de forma segura.

CERTIFICACIONESCISSP(CertifiedInformationSystems Security Professional), **CISA** (CertifiedInformationSystems Auditor) y **CISM** (CertifiedInformation Security Management): son la más valoradas por el mercado a la hora de considerar un proyecto de seguridad de la información.

CERTIFICADODIGITAL: sistema de acreditación que contiene información de un usuario o servidor, para la verificación de su identidad en el sistema de información.

CÓDIGO MALICIOSO (MALWARE): hardware, software o firmware que es intencionalmente introducido en un sistema de información con un fin malicioso o no autorizado, (virus, troyanos, gusanos, rootkit…).

COMUNICACIONES: transmisión y recepción de información que se realiza entre dos o más equipos o soportes de un sistema de información.

CONFIDENCIALIDAD: políticas y normas para garantizar que los datos no sean comunicados incorrectamente ni a personal no autorizado.

CONTRASEÑA: cadena de caracteres que un usuario o servicio utiliza para verificar su identidad frente a un equipo, soporte o sistema de información.

CONTROL DE ACCESO: mecanismo que en función de la identificación ya autentificada permite acceder a datos o recursos de un sistema de información, dejando un registro de dicho acceso.

CONTROLES FÍSICOS: medidas de seguridad que vigilan y registran accesos físicos a un sistema de información.

CONTROLES LÓGICOS: conjunto de principios y normas que vigilan y registran los accesos a datos, procesos e información.

DATOS DE CARÁCTER PERSONAL: cualquier información concerniente a personas físicas que las identifique o las haga identificables.

DISPONIBILIDAD: garantizar que los recursos estén disponibles cuando se necesiten.

DIVULGACIÓN: la exposición de información a terceros que no tienen acceso a ella.

DOCUMENTO DE SEGURIDAD: documento que contiene las medidas de seguridad aplicadas por la empresa, para proteger los datos de carácter personal de accesos no autorizados.

ENCRIPTACIÓN: proceso mediante el cual la información es codificada para evitar el acceso a la misma por terceros no autorizados.

ENTORNO: conjunto de elementos que rodean el sistema de información de una empresa sin formar parte del mismo.

EVIDENCIA: prueba que demuestra de forma clara, manifiesta y perceptible un hecho.

FIREWALL: conjunto de hardware y software cuya función es proteger un sitio privado conectado a una red (local, intranet, Internet…) contra accesos no autorizados.

GESTIÓN: proceso mediante el cual se obtiene, despliega o utiliza una variedad de recursos básicos para apoyar los objetivos del proceso.

HACKER: experto informático especialista en entrar en sistemas ajenos sin permiso.

INCIDENCIA: cualquier anomalía que afecte o pueda afectar a la seguridad de los datos del sistema de información de la empresa.

INFORMACIÓN: conjunto de datos que al relacionarse adquieren sentido o un valor de contexto o de cambio.

INFORMACIÓN CONFIDENCIAL: conjunto de datos relativos a la empresa que pueda comprometer sus procesos clave. También se refiere a los datos especialmente protegidos(Ideología, religión, afiliación sindical, creencias, origen racial o étnico, salud o vida sexual).

INTEGRIDAD: seguridad de que una información no ha sido alterada.

INTERNET: conjunto de equipos y redes conectados a nivel mundial para el intercambio de información.

ISO (International OrganizationforStandarization): organización voluntaria, no gubernamental, cuyos miembros han desarrollado estándares para las naciones participantes. Uno de sus comités se ocupa de los sistemas de información.

ISO 17799: código de Buenas Prácticas de Seguridad de la Información.

ISO/IEC 27001 (*Informationtechnology - Security techniques - Informationsecuritymanagementsystems - Requirements*): el estándar para la seguridad de la información fue aprobado y publicado como estándar internacional en octubre de 2005 por ISO. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) .

LEY 1273 DE 2009: modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

LINUX: sistema operativo de la familia UNIX. El proyecto original pertenece a LinusTorvalds

MAC (Media Access Control): control de acceso al medio. La inferior de las dos subcapas de la capa de enlace de datos definida por IEEE. La subcapa MAC administra el acceso a medios compartidos.

PERFIL DE USUARIO: definición de las competencias, niveles de acceso y responsabilidades asignadas a un usuario para el desempeño de sus funciones.

PERMISO: reglas para regular qué usuarios pueden obtener acceso y de qué manera a los distintos recursos del sistema de información.

PIRATA INFORMÁTICO: persona que copia software, con derecho de autor, ilegalmente sin que medie el permiso expreso del desarrollador. No confundir con el termino Hacker.

POLÍTICA DE SEGURIDAD:documento escrito que describe, cómo la organización puede protegerse de mejor manera de distintas amenazas, esta incluye una lista de pasos a seguir en caso que ocurran ciertos eventos vinculados a la seguridad.

PRIVACIDAD: el control sobre el uso, comunicación y distribución de la información.

PRIVILEGIOS: derechos del usuario para utilizar los distintos activos del sistema de información.

PROCESO: conjunto de actividades o eventos que se realizan o suceden con un determinado fin.

PROXY: entidad que, a fin de lograr mayor eficiencia, esencialmente suple otra entidad.

RECURSO: cualquier componente de un sistema de información.

RED LOCAL: el término red local incluye tanto el hardware como el software necesario para la interconexión de varios ordenadores y periféricos con el objeto de intercambiar recursos e información.

REGISTRO (LOG): documento que recoge evidencias objetivas de las actividades efectuadas o de los resultados obtenidos en un proceso.

RIESGO: probabilidad de obtener un resultado desfavorable como resultado de la exposición a un evento especifico.

ROUTER: dispositivo de capa de red que utiliza una o más métricas para determinar la ruta óptima por la que se enviara el tráfico de la red. Los Routers envían paquetes de una red a otra en base a la información de capa de red. Ocasionalmente llamado Gateway.

SEGURIDAD: disciplina, técnicas y herramientas diseñadas para ayudar a proteger la confidencialidad, integridad y disponibilidad de información y sistemas.

SERVER (Servidor): maquina que ofrece servicios a otras dentro de una red. También llamado Host.

SISTEMAS BIOMÉTRICOS: la Biometría, es una tecnología basada en reconocimiento de características físicas e intransferibles de una persona.

SISTEMA DE INFORMACIÓN: conjunto de elementos, ordenadamente relacionados entre sí que aporta a la organización las directrices de manejo de la información para el cumplimiento de sus fines.

SOFTWARE: conjunto de programas y aplicaciones para el manejo de información en el sistema empresarial.

SOPORTE: objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.

SPAM: correo electrónico que se recibe sin haberlo solicitado (llamados “e-mail basura”). Un envio masivo de Spam puede provocar un colapso en el sistema que los recibe, en este caso se les denomina MailBombing.

SSID (**S**ervice**S**et **ID**entifier): es un nombre incluido en todos los paquetes de una red inalámbrica (Wi-Fi) para identificarlos como parte de esa red.

SWITCH: dispositivo que opera en la capa de enlace del modelo OSI. Dispositivo electrónico o mecánico que permite establecer una conexión cuando resulte necesario y terminarla cuando no haya sesión alguna que soportar.

TERCEROS: personas que no forman parte de la organización.

TIC (Las Tecnologías de la Información y las Comunicaciones): son el conjunto de herramientas, equipos, programas informáticos, aplicaciones, redes y medios, que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes.

TRATAMIENTO DE DATOS: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

USERNAME(Usuario): nombre único que identifica a un usuario, y es utilizado como medio de identificación ante un sistema.

VPN(Virtual Private Network): es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

VULNERABILIDAD: probabilidad de que una amenaza afecte a un activo causando un daño.

WEB SITES(Sitio Web): sistema dedicado al intercambio de información On-Line.

WEP (WiredEquivalentPrivacy): "Privacidad Equivalente a Cableado", es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite

Windows: sistema operativo grafico de la empresa Microsoft.

WPA (Wi-Fi Protected Access): es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo.

ANEXOS

ANEXO A

Revista ACIS
SISTEMAS Rastreando la inseguridad
No. 101 Julio-Septiembre 2007

ESTADISTICAS
Encuesta-análisis a través de la página Web dispuesta por la Asociación Colombiana de Ingenieros de Sistemas - ACIS

Nota: en 2006 el número de personas participantes no fue estadísticamente significativo y por lo tanto, no se presentaron los resultados de la encuesta.

POLÍTICAS DE SEGURIDAD
ESTADO ACTUAL DE LAS POLÍTICAS DE SEGURIDAD

	2002 %	2003 %	2004 %	2005 %	2007 %
No se tienen políticas de seguridad definidas	25	27.5	28.8	23	27.9
Actualmente se encuentran en desarrollo	48.1	49	46.8	44	43.5
Política formal, escrita, documentada e informada a todo el personal.	26.9	23.5	24.4	33	28.6

Comentarios Generales:
El 71.4% de las empresas en Colombia no cuentan con una política de seguridad definida de manera formal o se encuentran en desarrollo. Esta cifra muestra que si bien se ha avanzado en temas de tecnologías de seguridad de la información, las políticas sobre el tema siguen relegadas y como un asunto que debe desarrollar el área de tecnología. Esta divergencia entre lo tecnológico y lo estratégico muestra como el tema de seguridad no hace parte del negocio de las organizaciones y solo es considerado crítico cuando un evento infortunado ocurre.

PRINCIPAL OBSTÁCULO PARA DESARROLLAR UNA ADECUADA SEGURIDAD

	2002 %	2003 %	2004 %	2005 %	2007 %
Inexistencia de la política de seguridad.	20	22.7	17.0	16	36.1
Falta de tiempo.	17.1	14	23.5	18	32.7
Falta de formación técnica.	12.1	16.3	8.5	7	26.5
Falta de apoyo directivo.	13.6	15.1	18.3	23	34
Falta de colaboración entre áreas/departamentos.	12.1	14.5	9.8	13	28.6
Complejidad tecnológica.	12.9	6.4	7.8	9	16.3
Poco entendimiento de la seguridad informática	12.1	11	15.0	14	29.9
Otro: Asignación presupuestal, falta de recurso humano, cultura de la empresa.	-	-	-	-	8.8

Comentarios Generales:
La inexistencia de una política de seguridad de la información, la falta de tiempo y el poco entendimiento de la seguridad informática se manifiestan como los rubros mas sobresalientes. Estas cifras hablan del limitado entendimiento de la seguridad de la información en el contexto de negocio y de la poca creatividad de los profesionales de la seguridad para vender a distinción de la seguridad y el día a día de la operación de los mecanismos de seguridad. La gestión de la seguridad de la información entendida más allá del PHVA (Planear, Hacer, Verificar y Actuar) del ISO 27001 es regular, adaptar y aprender de la inseguridad, como la fuente misma de la protección de los negocios de la organización.

La inexistencia de políticas de seguridad y la falta de tiempo, no pueden ser excusas para no gestionar la seguridad. La inversión en seguridad es costosa, pero la materialización de inseguridad puede serlo mucho más.

ANEXO B

Comunicado de Prensa
Redacción Virtual – Cisco Systems
http://www.ciscoredaccionvirtual.com/redaccion/comunicados/ver_comunicados.asp?Id=1498

Colombia Debe Mejorar en Seguridad Informática

Cisco lanzó su primer Índice de Seguridad, una evaluación de la percepción del estado de la seguridad informática en Latinoamérica

Colombia obtuvo 62 puntos, lo que ubica al país por debajo del promedio regional.
Bogotá, Colombia, 23 de Julio de 2008 – Cisco dio a conocer hoy los resultados del primer Índice de Seguridad de Cisco, un punto de referencia sobre la manera como las empresas de la región evalúan su seguridad informática. El Índice de Seguridad ubicó a Colombia por debajo del promedio de Latinoamérica, con un puntaje de 62.
El promedio regional es de 64 puntos, lo cual muestra que aún cuando las empresas están implementando políticas de Seguridad de la Información, aún queda mucho por recorrer para alcanzar mejores estándares.

El valor del Índice de Seguridad puede ir de 0 a 100. Una puntuación máxima (100) representa el más alto nivel de implementación y compromiso con lo que podrían considerarse las mejores prácticas en cuanto a políticas de seguridad de la información. Un puntaje de 0 refleja un alejamiento total de adherencia a las prácticas generalmente aceptadas de protección y defensa contra las amenazas en las organizaciones.

El puntaje del Índice obtenido por cada país fue el siguiente:

País	Puntaje
Colombia	62
Argentina	62
Brasil	63
Venezuela	64
Chile	64
México	66

El Índice de Seguridad de Cisco fue elaborado por la consultora independiente KaaganResearchAssociates y está basado en 600 encuestas a gerentes de Tecnologías de la Información de Argentina, Brasil, Chile, Colombia, México y Venezuela.

Uno de los aspectos en los cuales Colombia parece tener más problemas que los demás países es la implementación de procesos por parte de las organizaciones, con el fin de proteger la Seguridad de la Información para garantizar la continuidad del negocio. El 41% de los encuestados manifestaron que la alta gerencia da una "importancia moderada" a la seguridad de la información

Esto se relaciona con el hecho que en el país tan solo el 35% de las empresas entrevistadas afirmaron que sus políticas de Seguridad de la Información son aprobadas a nivel de Junta Directiva, lo cual revela que las empresas no reconocen la seguridad de la información como un aspecto estratégico para el negocio.

"*El Índice de Seguridad Cisco nos ayuda a conocer cuál es la percepción y preparación de las empresas en Colombia y la región para establecer puntos de referencia y una guía hacia las mejores prácticas*", dijo Fernando Rodríguez, Gerente de Ingeniería para sector Empresas, Pequeñas empresas y Gobierno de Cisco Colombia.

"*Colombia, con un puntaje de 62 indica que aún hay mucho para mejorar respecto a cómo las compañías formulan y gestionan sus políticas de seguridad y sistemas*".

Hallazgos del estudio:

- El 35% de los entrevistados Colombianos están "muy confiados" en cuanto a la protección frente a amenazas externas en sus organizaciones. Con este resultado el país se ubica entre el grupo más confiado frente a este tipo de amenazas. Venezuela (26%) y Brasil (28%) obtuvieron los porcentajes más bajos.
- Solo el 16% de los Colombianos entrevistados están "muy confiados" en la protección de la información frente a amenazas internas. Colombia obtuvo el segundo porcentaje más bajo siguiendo a Brasil que alcanzó el 15%.
- La mayoría de los representantes de las áreas TI de todos los países sondeados consideran que los ataques de virus y gusanos son una amenaza realmente seria a su Seguridad Informática. Los colombianos mostraron niveles altos de preocupación: el 65% lo considera entre "extremadamente" y "muy" serio.

- El 49% de los Gerentes TI en Colombia califican como "extremadamente serio" y "muy serio" el Spyware y el Malware. Con este resultado Colombia se ubica como el país menos preocupado frente a ese nivel de amenaza. Chile resultó ser el país con mayor porcentaje de preocupación con un 70% de las respuestas entre "extremadamente serio" y "muy serio".
- Los colombianos encuestados son quienes ocupan el segundo lugar de la región (por detrás de los brasileños, con el 65%) en cuanto a preocupación acerca de la capacidad del crimen organizado para comprometer la Seguridad de la Información. Un 62% de los colombianos dijeron estar al menos "bastante" preocupados al respecto.
- Colombia es el país que mayores niveles de aflicción mostró en América Latina en cuanto a las amenazas a la información que representa el terrorismo, con el 48% de los entrevistados entre "muy preocupados" y "algo preocupados" por el tema.
- Colombia tiene el porcentaje más alto de uso en cuanto a control de accesos basado en roles, con el 95% de implementación. Lo sigue México, con el 91%.
- Un 50% de las organizaciones colombianas realizan mediciones formales sobre los costos de su Seguridad de la Información. El primer lugar lo ocupa Chile, con el 59%, mientras que las organizaciones brasileñas son las menos propensas a incorporar métricas de costos, con el 30% de los casos.
- Aún cuando la autenticación biométrica no es usada en la mayoría de las organizaciones de América Latina, Colombia es el país que muestra la más baja penetración (21%), junto con las organizaciones brasileras (20%).

"*En Cisco estamos trabajando para entregar a las organizaciones soluciones de seguridad que satisfagan las necesidades de nuestros clientes corporativos alrededor de la seguridad y el cumplimiento de políticas. Por ello hemos evolucionado nuestro concepto de Red Autodefensiva hacia un enfoque de sistemas más amplio, fortaleciendo así de manera integral la protección de las redes y de la diversidad de puntos finales, aplicaciones y contenidos que las utilizan*", concluyó Fernando Rodríguez.

ANEXO C

LISTADO DE EMPRESAS LLAMADAS

RESPUESTA	RAZON SOCIAL	TELEFONO	BARRIO
CAMBIO DE UBICACIÓN	MENDEZ DE HENAO OMAIRA	3704099	PALOQUEMAO
CAMBIO DE UBICACIÓN	TORRES TELLEZ HUGO EDUARDO	3750226	RICAURTE
CAMBIO DE UBICACIÓN	OMH TRANSPORTES LTDA	2016428	RICAURTE
CAMBIO DE UBICACIÓN	CARRILLO GIL DORIS ROSALBA	6746687	BRITALIA
CAMBIO DE UBICACIÓN	TRANSPORTES COMPUTAXI S.A.	6256552	PRADO VERANIEGO
CAMBIO DE UBICACIÓN	4 CARGO LTDA	6155716	PRADO VERANIEGO NORTE
CAMBIO DE UBICACIÓN	RINCON CASTILLO OMAR JOSUE	6782462	SAN JOSE DE BAVARIA
CAMBIO DE UBICACIÓN	TRANSPORTES EXPRESO CUNDINAMARCA LTDA. Y CIA. S.C.A.	6210878	LA CASTELLANA
CAMBIO DE UBICACIÓN	MEJIA BARON LUIS MARIA	6105139	POLO CLUB
CAMBIO DE UBICACIÓN	LIMA TRANSPORTES S A	6114570	POLO CLUB
CAMBIO DE UBICACIÓN	SASO S A	5300623	ANTIGUO COUNTRY
CAMBIO DE UBICACIÓN	EQUIMAC S A	6167858	CHICO NORTE II
CAMBIO DE UBICACIÓN	IDEANDINA S A	2960977	CHICO NORTE II
CAMBIO DE UBICACIÓN	COLUMBUS INTERNATIONAL FREIGHT FORWARDERS LTDA	4139641	SAN JOSE FONTIBON
CAMBIO DE UBICACIÓN	SOCIEDAD TRANSPORTADORA MIXTA URBANA DE BOGOTA SOTRANSMIUR S.A.	4075011	ALCALA

CAMBIO DE UBICACIÓN	LINEAS ESCOTUR S.A.	3141631	MUEQUETA
NO ESTAN INTERESADOS	GAS CORDILLERA SA E S P	3476680	CHAPINERO CENTRAL
NO ESTAN INTERESADOS	INVERSIONES ALBARRACIN GOMEZ ALBAGE LIMITADA	2017769	
NO ESTAN INTERESADOS	SARMIENTO RAMIREZ RICHAR ALFREDO	2774447	LA ESTANZUELA
NO ESTAN INTERESADOS	PABON ROJAS JULIETHE PATRICIA	2846404	PALOQUEMAO
NO ESTAN INTERESADOS	TRANSPORTES ESPECIALES DE BOGOTA S A	2748106	CANODROMO
NO ESTAN INTERESADOS	COMPANIA DE CARGA MOVITRANSPORTES LIMITADA	2265978	CLUB LOS LAGARTOS
NO ESTAN INTERESADOS	TRANSPORTADORA INTERCARIBE LTDA	4836667	GUACANI
NO ESTAN INTERESADOS	INDUSTRIAS URBA LTDA	6760720	JULIO FLOREZ
NO ESTAN INTERESADOS	POVEDA DIAZ ROBERTO	4214027	MONACO
NO ESTAN INTERESADOS	LIMO CAR S LIMITADA	4835252	NIZA
NO ESTAN INTERESADOS	CAR TAXIS S A	6275777	PRADO PINZON
NO ESTAN INTERESADOS	LIDERES EN TRANSPORTES ESPECIALES S A LIDERTRANS S A	2451366	LA SOLEDAD
NO ESTAN INTERESADOS	GRUPO D R J S A	2850656	LA SOLEDAD
NO ESTAN INTERESADOS	COMPANIA DE TRANSPORTE ESPECIAL FENIX EXPREX LTDA	3401699	PALERMO
NO ESTAN INTERESADOS	DIEMAR LTDA	2223695	PABLO VI
NO ESTAN INTERESADOS	TRANSPORTE NUEVO RUMBO LTDA	2684516	QUINTA PAREDES
NO ESTAN INTERESADOS	SERVIPESADOS LTDA	5708333	QUINTA PAREDES

NO ESTAN INTERESADOS	CARS TURISMO LTDA	3350339	QUINTA PAREDES
NO ESTAN INTERESADOS	ADMINISTRACION Y TRANSPORTES ESPECIALES E U EMPRESA UNIPERSONAL	2682088	QUINTA PAREDES
NO ESTAN INTERESADOS	CAPITAL TRAFFIC S A	3408384	QUINTA PAREDES
NO ESTAN INTERESADOS	INTEGRACION DE TRANSPORTADORES COLOMBIANOS DE SERVICIO ESPECIAL LTDA CON SI	2563939	LA CASTELLANA
NO ESTAN INTERESADOS	MULTIMODAL LOGISTIC AGENCY LTDA PUDIENDOSE UTILIZAR LA SIGLA MLA	6915811	LA CASTELLANA
NO ESTAN INTERESADOS	SPEEDWAY EXPRESS DE COLOMBIA LIMITADA	6132108	LOS ANDES
NO ESTAN INTERESADOS	TRANSPORTES SIBARIA S A CON SIGLA TRANSIBARIA S A	6110352	CHICO
NO ESTAN INTERESADOS	NOVATOS TOURS LIMITADA NOVATOURS	2861355	CHICO NORTE II
NO ESTAN INTERESADOS	LOGISTICS CARGO S A	6218408	CHICO NORTE II
NO ESTAN INTERESADOS	TRANSPORTES SERVIFRIO S A	6353671	CHICO NORTE III
NO ESTAN INTERESADOS	AGENCIA DE VIAJES VILLA DE LEIVA S A	3212020	EL NOGAL
NO ESTAN INTERESADOS	T.L.I SA	4135489	AEROPUERTO EL DORADO
NO ESTAN INTERESADOS	AEROCHARTER CARGA LTDA	4148055	AEROPUERTO EL DORADO
NO ESTAN INTERESADOS	NACIONAL DE AVIACION LTDA	4820682	AEROPUERTO EL DORADO
NO ESTAN INTERESADOS	GLOBAL SERVICE AVIATION LIMITADA	4135429	AEROPUERTO EL DORADO
NO ESTAN INTERESADOS	INTERNATIONAL TRADING CARGO LTDA	4139390	SAN JOSE FONTIBON

NO ESTAN INTERESADOS	CARGOCOL LIMITADA BROKERS & FORWARDERS	4134195	SAN JOSE FONTIBON
NO ESTAN INTERESADOS	COMPANIA DE PROPIETARIOS DEL TRANSPORTE S A COPROTRANS S A	4075005	ALCALA
NO ESTAN INTERESADOS	TRANSPORTES DINAGAS LIMITADA	5978430	CIUDAD SALITRE
NO ESTAN INTERESADOS	TRANSPORTES EURO S A	6090391	SIETE DE AGOSTO
NO ESTAN INTERESADOS	GARCIA GUERRA GERMAN GABRIEL	2114509	MUEQUETA
NO ESTAN INTERESADOS	SERVITTUR S A	2486246	NORTE
NO ESTAN INTERESADOS	INTERNATIONAL TRANSPORT SERVICES LTDA	4042904	SAN JOSE FONTIBON
NO ESTAN INTERESADOS	COMERCIALIZADORA Y TRANSPORTADORA SAN JOSE LTDA	3365739	LA CATEDRAL
NO ESTAN INTERESADOS	VUELOS CHARTER DE AMERICA LTDA.	4135075	LAS AGUAS
NO ESTAN INTERESADOS	CIFUENTES CASTRILLON MARINO	6276477	COUNTRY CLUB
NO ESTAN INTERESADOS	MERCADEO Y SERVICIOS SOCIEDAD ANONIMA MESER S A	2746283	LA CAROLINA
NO ESTAN INTERESADOS	BPM SECURITY LTDA	2167150	PLENITUD
NO ESTAN INTERESADOS	BARON HERMANOS & COMPANIA LIMITADA	6700753	RINCON DEL NORTE
NO RESPONDEN	CITYTRANS S A	3116255	JORGE ELIECER GAITAN
NO RESPONDEN	TRANSPORTES ALEX LTDA	2447165	USATAMA
NO RESPONDEN	TRANSPORTES ESPECIALES EMMANUEL S A	6760200	CASA BLANCA
NO RESPONDEN	BLANCO CARLOS ALBERTO	2269938	SANTA HELENA I
NO RESPONDEN	TRANSPORTES FEDA LTDA	6278500	VICTORIA NORTE

NO RESPONDEN	AMBULANCIAS Y SERVICIOS MEDICOS S.A.	2359377	EL CAMPIN	
NO RESPONDEN	HELICSA LIMITADA	2576241	CHICO NORTE	
NO RESPONDEN	SERVICIOS INDUSTRIALES PETROLEROS SERINPETROL LTDA	6235956	CHICO NORTE	
NO RESPONDEN	TRANSPORTUARIA LTDA	6162031	CHICO NORTE	
NO RESPONDEN	ACARREOS LOS GUADUALES S.A.	6553945	CHICO NORTE II	
NO RESPONDEN	TRANSPORTES GLAMAR LIMITADA	6352714	CHICO NORTE III	
NO RESPONDEN	VENSECAR INTERNACIONAL C A SUCURSAL COLOMBIA	4138150	AEROPUERTO EL DORADO	
NO RESPONDEN	GIANNINI BASTIANI GIOVANNI	5619260	LA CATEDRAL	
NO RESPONDEN	AIR CHARTER LIMITED	6092334	LAS AGUAS	
NO RESPONDEN	SERVITRANSMAQUINAS LTDA	3131712	BELLAVISTA	
NO RESPONDEN	TRANSPORTES ESCOLARES GAMES LIMITADA	6763666	LA CALLEJA	
NO RESPONDEN	TRANSPORTES CAMOA S A	6148563	LA CAROLINA	
NO RESPONDEN	CORREDOR CELY LUIS ALBERTO	2582138	LOS CEDROS	
NO RESPONDEN	POVEDA SALAZAR ROBERTO BELARMINO	6721163	LOS CEDROS	
NO RESPONDEN	MINAS Y CANTERAS LIMITADA	6290187	SANTA BARBARA ORIENTAL	
NO RESPONDEN	SERVICIO INTEGRAL EN TRANSPORTE DE CARGA S A	5225149	SANTA BARBARA ORIENTAL	
NO RESPONDEN	SERVICIO AEREO REGIONAL SAER LTDA	4139095	CHAPINERO NORTE	
EMPRESAS VISITADAS				
VISITADA	SERVIMILENIUM LTDA	6491670	MAZUREN	C.C. MazurénL-

				261
VISITADA	INGEOSTUDIOS S P LTDA	6018946	MONACO	Calle 66 # 11-39
VISITADA	SMART LTDA	5280192	SAN CRISTOBAL	Cll 163 # 51-95 Casa 61
VISITADA	PATRICIA DE LEIVA Y CIA LTDA. SIGLA TRANSPAL LTDA	2531195	MARLY	CRA 11 No 40-21
VISITADA	SANCHEZ MORALES JOSE ALBERTO	2018417	URBANIZACION CORDOBA NIZA	CRA 34A No 3C-63
VISITADA	ROBAYO MURCIA ABEL	5708333	QUINTA PAREDES	CLL 21 No 42C-53
VISITADA	UNICARGO DE COLOMBIA S A	6916070	ANTIGUO COUNTRY	Cra19 A # 84-14
VISITADA	COLORA LIMITADA	6218904	CHICO NORTE	Cr 14 # 94A-61 Of 403
VISITADA	VICTORIA LINE COLOMBIA LTDA	6162021	CHICO NORTE	Cr 11 A No.94-76 Of.304
VISITADA	LA METROPOLITANA DE TRANSPORTE	4150888	FONTIBON	Av 22 # 120-50
VISITADA	CARPA INTERNACIONAL	4703713	SAN RAFAEL	Cr 54D No. 135-06 Torre I Of 302
VISITADA	AVIASERVICE S.A.	414 74 44	AEROPUERTO EL DORADO	
VISITADA	PANAMERICANA LTDA	6912158	CASTELLANA	Kra 32 # 91-87
VISITADA	SOPRO USAQUEN S A	6773139	LOS CERROS DE SANTA CRIS	Av 7a # 160A - 45
VISITADA	DOLPHIN EXPRESS VIAJES Y TURISMO	6096892	SAN CRISTOBAL	Cl 161 # 14-45
VISITADA	EXPRESO VIAJES Y TURISMO	593 4949	ANTIGUO COUNTRY	Cl 85 # 19A-24

ANEXO D

LIBRETO PARA LAS PEQUEÑAS EMPRESAS

Llama a la empresa y cuando le contesten, pregunta: Buenos días o buenas tardes me contestan de la empresa XXXXX, si le contestan de la empresa a la que se está llamando, si la respuesta es afirmativa pase a el saludo, sino pregunte si ellos saben el teléfono para poderlos contactar, sino pregunte si es otra nueva empresa y registre los datos en la hoja de Excel.

ESTUDIANTE: ***Saludo*** Buenos días o buenas tardes, Mi nombre es (XXXXXX), soy auxiliar de investigación del programa de Ingeniería de Sistema de la USB. La Universidad como ente educativo a nivel superior y a través de su función de investigación y proyección social está desarrollando un proyecto de interés social centrado en la seguridad informática para la pequeña empresa de Bogotá; el objetivo de proyecto es contribuir a resolver el problema de la seguridad de la información.

Inicialmente necesitamos su valiosa colaboración para confirmar información comercial de su empresa: nombre del representante legal, correo electrónico, teléfonos fijos, fax y todos los datos que se encuentran en la base de datos. (Si le preguntan para qué necesitan esa información ud responde que para poder enviarle información completa del proyecto y hacerle una visita formal)

Una vez le confirmen los datos el estudiante, pregunta si le pueden comunicar con el encargado del área de sistemas, para hacerle dos preguntas:

Estudiante: Saluda, se presenta de nuevo con el saludo propuesto en el segundo párrafo y luego: Podría Usted indicarme si la empresa posee red y cuantos usuarios exactamente, están conectados a la red? Si la persona sabe le contesta o usted le dice: Podría comunicarme con alguien que me suministre esa información. Si le pasa a otra persona usted vuelve y saluda: (buenos días o buenas tardes), mi nombre es XXXXXX, soy auxiliar de investigación de la Universidad de san Buenaventura de la Facultad de Ingeniería, y estamos trabajando un proyecto de investigación en seguridad informática para pequeñas empresas de Bogotá y nos gustaría saber si ustedes poseen red y cuantos usuarios exactamente se conectan en red.

Despedida:(Si la empresa posee red y posee hasta 20 usuarios conectados en red), Muchas gracias por su colaboración y su empresa por poseer estas características, estará incluida en nuestra investigación y que en los próximos días le estarán enviando un correo o se hará una llamada, para confirmar una visita de la universidad, en donde se le hará unas preguntas sobre seguridad informática.

Despedida:(Si la empresa no cumple con ambas características), Muchas gracias por su colaboración, pero su empresa por no cumplir con estas características no quedará incluida en esta fase del proyecto, pero será tenida en cuenta para una próxima oportunidad.

Al final le dice: muchas gracias por la atención, que tenga un felíz día o una felíz tarde y hasta una próxima oportunidad.

ANEXO E

NORMAS PARA CABLEADO ESTRUCTURADO

Al ser el cableado estructurado un conjunto de cables y conectores, sus componentes, diseño y técnicas de instalación deben cumplir con una norma no da servicio a cualquier tipo de red local de datos, voz y otros sistemas de comunicaciones, sin la necesidad de recurrir a un único proveedor de equipos y programas.

De tal manera que los sistemas de cableado estructurado se instalan de acuerdo a la norma para cableado para telecomunicaciones, EIA/TIA/568-A, emitida en Estados Unidos por la Asociación de la industria de telecomunicaciones, junto con la asociación de la industria electrónica.

EIA/TIA568-A
Estándar ANSI/TIA/EIA-568-A de Alambrado de Telecomunicaciones para Edificios Comerciales. El propósito de esta norma es permitir la planeación e instalación de cableado de edificios con muy poco conocimiento de los productos de telecomunicaciones que serán instalados con posterioridad.

ANSI/EIA/TIA emiten una serie de normas que complementan la 568-A, que es la norma general de cableado:

· Estándar ANSI/TIA/EIA-569-A de Rutas y Espacios de Telecomunicaciones para Edificios Comerciales. Define la infraestructura del cableado de telecomunicaciones, a través de tubería, registros, pozos, trincheras, canal, entre otros, para su buen funcionamiento y desarrollo del futuro.

· EIA/TIA 570, establece el cableado de uso residencial y de pequeños negocios.

· Estándar ANSI/TIA/EIA-606 de Administración para la Infraestructura de Telecomunicaciones de Edificios Comerciales.

· EIA/TIA 607, define al sistema de tierra física y el de alimentación bajo las cuales se deberán de operar y proteger los elementos del sistema estructurado.

Las normas EIA/TIA fueron creadas como norma de industria en un país, pero se ha empleado como norma internacional por ser de las primeras en crearse. ISO/IEC 11801, es otra norma internacional.

Las normas ofrecen muchas recomendaciones y evitan problemas en la instalación del mismo, pero básicamente protegen la inversión del cliente.
Elementos principales de un cableado estructurado El Cableado estructurado, es un sistema de cableado capaz de integrar tanto a los servicios de voz, datos y vídeo, como los sistemas de control y automatización de un edificio bajo una plataforma estandarizada y abierta. El

cableado estructurado tiende a estandarizar los sistemas de transmisión de información al integrar diferentes medios para soportar toda clase de tráfico, controlar los procesos y sistemas de administración de un edificio.

1. Cableado Horizontal: El cableado horizontal incorpora el sistema de cableado que se extiende desde la salida de área de trabajo de telecomunicaciones (WorkAreaOutlet, WAO) hasta el cuarto de telecomunicaciones.

2. Cableado del Backbone: El propósito del cableado del backbone es proporcionar interconexiones entre cuartos de entrada de servicios de edificio, cuartos de equipo y cuartos de telecomunicaciones. El cableado del backbone incluye la conexión vertical entre pisos en edificios de varios pisos. El cableado del backbone incluye medios de transmisión (cable), puntos principales e intermedios de conexión cruzada y terminaciones mecánicas.

3. Cuarto de Telecomunicaciones: Un cuarto de telecomunicaciones es el área en un edificio utilizada para el uso exclusivo de equipo asociado con el sistema de cableado de telecomunicaciones. El espacio del cuarto de comunicaciones no debe ser compartido con instalaciones eléctricas que no sean de telecomunicaciones. El cuarto de telecomunicaciones debe ser capaz de albergar equipo de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado. El diseño de cuartos de telecomunicaciones debe considerar, además de voz y datos, la incorporación de otros sistemas de información del edificio tales como televisión por cable (CATV), alarmas, seguridad, audio y otros sistemas de telecomunicaciones. Todo edificio debe contar con al menos un cuarto de telecomunicaciones o cuarto de equipo. No hay un límite máximo en la cantidad de cuartos de telecomunicaciones que puedan haber en un edificio.

4. Cuarto de Equipo: El cuarto de equipo es un espacio centralizado de uso específico para equipo de telecomunicaciones tal como central telefónica, equipo de cómputo y/o conmutador de video. Varias o todas las funciones de un cuarto de telecomunicaciones pueden ser proporcionadas por un cuarto de equipo. Los cuartos de equipo se consideran distintos de los cuartos de telecomunicaciones por la naturaleza, costo, tamaño y/o complejidad del equipo que contienen. Los cuartos de equipo incluyen espacio de trabajo para personal de telecomunicaciones. Todo edificio debe contener un cuarto de telecomunicaciones o un cuarto de equipo. Los requerimientos del cuarto de equipo se especifican en los estándares ANSI/TIA/EIA-568-A y ANSI/TIA/EIA-569.
5. Cuarto de Entrada de Servicios: El cuarto de entrada de servicios consiste en la entrada de los servicios de telecomunicaciones al edificio, incluyendo el punto de entrada a través de la pared y continuando hasta el cuarto o espacio de entrada. El cuarto de entrada puede incorporar el "backbone" que

conecta a otros edificios en situaciones de campus. Los requerimientos de los cuartos de entrada se especifican en los estándares ANSI/TIA/EIA-568-A y ANSI/TIA/EIA-569.

6. Sistema de Puesta a Tierra y Puenteado: El sistema de puesta a tierra y puenteado establecido en el estándar ANSI/TIA/EIA-607 es un componente importante de cualquier sistema de cableado estructurado moderno.

ANEXO F

UNIVERSIDAD DE SANBUENAVENTURA SEDE BOGOTÁ

FACULTAD DE INGENIERÍA PROGRAMA DE INGENIERÍA DE SISTEMAS					**PROYECTO DE GRADO: SEGURIDAD DE LA INFORMACIÓN EN LAS EMPRESAS DE TRANSPORTE DE BOGOTA**			
INSTRUMENTO DE EVALUACIÓN Y DIAGNÓSTICO EN SEGURIDAD INFORMÁTICA PARA LA PEQUEÑA EMPRESA EN BOGOTÁ								
RESULTADOS DE LAS ENCUESTAS								
SEGURIDAD FISICA								
		CANTIDAD				**PORCENTUAL**		
	CONTROLES	SI #	NO #	NA #		SI %	NO %	NA %
1	¿Posee su empresa mecanismos para la prevención de robo de equipos de cómputo?	7	8	1		43,8	50	6,25
2	¿Posee guardias de seguridad que revisen la identidad de las personas al ingresar a la empresa?	8	8	0		50	50	0
3	¿La empresa cuenta con alarma contra robos, incendios, o desastres naturales?	4	12	0		25	75	0
4	¿Los paquetes que salen de la empresa son revisados?	3	12	1		18,8	75	6,25
5	¿La empresa cuenta con algún tipo de identificación para el personal que trabaja en las instalaciones?	4	12	0		25	75	0
6	¿Cuenta la empresa con algún sistema de identificación de visitantes?	4	11	1		25	68,8	6,25
7	¿La empresa lleva el control de los vehículos que entran y salen de sus instalaciones?	1	14	1		6,25	87,5	6,25
8	¿Tiene la empresa cámaras de vigilancia en sus instalaciones?	4	12	0		25	75	0
9	¿Sus empleados saben qué hacer en caso de incendios, terremotos?	1	13	2		6,25	81,3	12,5
10	¿Poseen manuales de prevención para evitar el daño o	0	15	1		0	93,8	6,25

	pérdida de sus equipos de cómputo?						
11	En caso de desastres naturales sabe cómo proteger su información	0	15	1	0	93,8	6,25
HARDWARE							
CONTROLES		SI #	NO #	NA #	SI %	NO %	NA %
1	¿La Red se accede por medio de algún PC Portátil?	11	5	0	68,8	31,3	0
2	¿Tiene Terminales con acceso a internet para Uso Público?	1	15	0	6,25	93,8	0
3	¿Se realiza periódicamente evaluación de los equipos de cómputo?	12	4	0	75	25	0
4	¿La empresa cuenta con un diseño físico de hardware para el control de la seguridad de la información?	1	15	0	6,25	93,8	0
5	¿Para la seguridad de los datos la empresa dispone de dos o más máquinas servidores?	2	14	0	12,5	87,5	0
6	¿Durante el año en curso ha tenido casos de fraude o violaciones físicas de seguridad tuvieron lugar en su empresa?	2	12	2	12,5	75	12,5
7	¿Existen equipos informáticos para el filtrado de contenido en su red?	3	12	1	18,8	75	6,25
8	¿La empresa se expone a riesgos por los hábitos de uso de internet por parte de sus empleados?	12	3	1	75	18,8	6,25
9	¿Considera usted que la información de su empresa está segura?	3	12	1	18,8	75	6,25
10	¿Se ha presentado perdida de información por desastres naturales?	0	16	0	0	100	0
11	¿Ud. restringe el acceso a internet por medio de puertos?	1	10	5	6,25	62,5	31,3
12	¿Ud. restringe el acceso a internet por dirección origen/destino (MAC o	0	15	1	0	93,8	6,25

	Dirección física)?							
13	¿Las conexiones a los servidores de su red son fiables?	3	8	5		18,8	50	31,3
14	¿Su empresa cuenta con un mantenimiento de hardware adecuado por parte de técnicos autorizados?	3	5	7		20	33,3	46,7
SOFTWARE								
CONTROLES		SI #	NO #	NA #		SI %	NO %	NA %
1	¿El sistema operativo de las estaciones de trabajo es actualizado?	14	1	1		87,5	6,25	6,25
2	¿Se ha configurado un Servidor Web?	4	12	0		25	75	0
3	¿Se tiene instalado un Servidor de Correo Electrónico?	4	12	0		25	75	0
4	¿Se ha optado por un Servidor de Backup?	3	13	0		18,75	81,25	0
5	¿La Empresa dispone de Acceso a Internet?	15	1	0		93,75	6,25	0
6	¿Disponen de un Servidor de Base de Datos?	5	10	1		31,25	62,5	6,25
7	¿Se tiene configurado un Servidor de Aplicaciones?	4	12	0		25	75	0
8	¿Se trabaja con un Servidor de Firewall?	3	13	0		18,75	81,25	0
9	¿Poseen un Servidor de Comunicaciones?	1	15	0		6,25	93,75	0
10	¿La empresa cuenta con un Sitio WEB?	6	10	0		37,5	62,5	0
11	¿La Entidad cuenta con directivas internas para controlar virus informáticos?	6	10	0		37,5	62,5	0
12	¿Tiene procedimientos de control de los cambios que se realizan en el software, el sistema operativo de Servidores y Estaciones de Trabajo?	1	15	0		6,25	93,75	0
13	¿Tienen mecanismos de protección cuando se desarrolla	1	15	0		6,25	93,75	0

	software por parte de personal ajeno a la Empresa?						
14	¿Tienen identificada la normatividad legal a la que pueda sujetarse el Software que usan en la Red?	1	15	0	6,25	93,75	0
15	Se tienen mecanismos de Seguridad como Control de Accesos (Passport)	13	3	0	81,25	18,75	0
16	Existen mecanismos de Encriptación de Datos?	2	14	0	12,5	87,5	0
17	¿Disponen de Software Antivirus actualizado?	16	0	0	100	0	0
18	¿La empresa cuenta con un Sistema de Prevención y detección de intrusos?	7	8	1	43,75	50	6,25
19	¿Se hace uso de los Certificados Digitales?	3	10	3	18,75	62,5	18,75
20	¿La empresa trabaja con Redes Privadas Virtuales?	6	9	1	37,5	56,25	6,25
21	¿Dispone de algún análisis de vulnerabilidades del software?	0	16	0	0	100	0
TRANSMISION DE DATOS							
CONTROLES		SI #	NO #	NA #	SI %	NO %	NA %
1	¿Los equipos que salen y entran a la Empresa tienen mecanismos de seguridad de la información que utilizan?	6	9	1	37,5	56,25	6,25
2	¿Tienen establecidos controles en la Red de Datos contra Software malicioso?	4	8	4	25	50	25
3	¿Tienen un registro de fallas sobre la Transmisión de Datos?	1	13	2	6,25	81,25	12,5
4	¿Tienen información referida a la red de datos, como direcciones IP de cada máquina?	6	6	4	37,5	37,5	25
5	¿Tienen establecidos controles de Seguridad para el Sistema de Correo Electrónico?	6	6	4	37,5	37,5	25
6	¿Tienen políticas de control de acceso a los Sistemas	4	8	4	25	50	25

	informáticos de los Usuarios de la Red de Datos?							
7	¿Tienen políticas de Uso, de los Servicios de la Red de Datos?	4	8	4		25	50	25
8	¿Se cuenta con mecanismos de Seguridad para encriptación de las Comunicaciones?	3	9	4		18,75	56,25	25
ORGANIZACIÓN Y ADMINISTRACIÓN DE LA RED CONTROLES								
CONTROLES		SI #	NO #	NA #		SI %	NO %	NA %
1	¿La empresa cuenta con un cuarto de equipos que funcione como un centro de datos o de cómputo?	6	10	0		37,5	62,5	0
2	¿El cuarto de equipos posee seguridad por accesos?	3	8	5		18,75	50	31,25
3	¿El cuarto de equipos y centro de datos cumple con estándares nacionales y/o internacionales para su funcionamiento?	2	7	7		12,5	43,75	43,75
4	¿Actualmente aplican estrategias de política y seguridad para la información y en las redes?	1	15	0		6,25	93,75	0
5	¿En caso de responder a la pregunta anterior No: Han diseñado o proyectan diseñar políticas de seguridad para el tratamiento de la información y la red de datos?	1	13	1		6,667	86,67	6,667
6	¿Realizan evaluaciones y actualizaciones periódicas de las políticas de seguridad?	3	10	3		18,75	62,5	18,75
7	¿Tiene su empresa una persona asignada para las labores exclusivas de la seguridad informática?	4	12	0		25	75	0
8	¿Están preparados los usuarios para reportar los incidentes de seguridad de los sistemas de información?	3	13	0		18,75	81,25	0
9	¿Tienen mecanismos de	4	12	0		25	75	0

	seguridad de la información?							
10	¿Tiene políticas de uso de los servicios de la red de datos?	5	11	0		31,25	68,75	0
11	¿Existen políticas del control de acceso a la información de los usuarios que usan computadores portátiles?	4	12	0		25	75	0
12	¿La empresa tiene acuerdos con el personal sobre la confidencialidad de la información?	10	6	0		62,5	37,5	0
13	¿El presupuesto global de informática de su organización, incluye aspectos de seguridad de la información?	3	13	0		18,75	81,25	0
14	¿La empresa posee presupuesto para la seguridad informática?	4	12	0		25	75	0
15	¿El gasto de su organización en cuanto a la seguridad informática está centrado en la protección de la red?	4	11	1		25	68,75	6,25
ARCHIVOS								
CONTROLES		SI #	NO #	NA #		SI %	NO %	NA %
1	Posee Ud. control de los archivos que son retirados de su empresa	2	14	0		12,5	87,5	0
2	Los usuarios poseen permisos para acceder a todos los archivos	8	8	0		50	50	0
3	Protege Ud. con contraseña los archivos más importantes de su empresa	10	6	0		62,5	37,5	0
4	Tiene Ud. creado una lista de roles y permiso para acceso	4	11	0		26,67	73,33	0
5	Controla usted el ingreso a los archivos por medio de horarios de trabajo.	3	13	0		18,75	81,25	0
6	Realiza usted backups de los archivos de sus estaciones de trabajo	8	8	0		50	50	0

	Diariamente	0	0	0		0	0	0
	Semanalmente	0	0	0		0	0	0
	Mensualmente	4	0	0		100	0	0
	Otros	4	0	0		100	0	0
7	Posee usted la información de quien puede realizar cambios en archivos de la empresa	5	7	4		31,25	43,75	25

ANEXO G

FALENCIAS POR CADA UNA DE LAS EMPRESAS

AVIASERVICE SA

Infraestructura	
Defensa del perímetro	
Reglas y filtros de cortafuegos	
Antivirus	
Antivirus - Equipos de escritorio	
Antivirus - Servidores	
Acceso remoto	
Segmentación	
Sistema de detección de intrusiones (IDS)	
Inalámbrico	
Autenticación	
Usuarios administrativos	
Usuarios internos	
Usuarios de acceso remoto	
Directivas de contraseñas	
Directivas de contraseñas-Cuenta de administrador	
Directivas de contraseñas-Cuenta de usuario	
Directivas de contraseñas-Cuenta de acceso remoto	
Cuentas inactivas	
Gestión y control	
Informes sobre incidentes y respuesta	
Creación segura	
Seguridad física	

Aplicaciones	
Implementación y uso	
Equilibrio de carga	
Clústeres	
Aplicación y recuperación de datos	
Fabricante de software independiente (ISV)	
Desarrollado internamente	
Vulnerabilidades	
Diseño de aplicaciones	
Autenticación	
Directivas de contraseñas	
Autorización y control de acceso	
Registro	
Validación de datos de entrada	
Metodologías de desarrollo de seguridad de software	
Almacenamiento y comunicaciones de datos	

Operaciones	
Entorno	
Host de gestión	
Host de gestión-Servidores	
Host de gestión - Dispositivos de red	
Directiva de seguridad	
Clasificación de datos	
Eliminación de datos	
Protocolos y servicios	
Uso aceptable	
Gestión de cuentas de usuarios	
Regulación	
Directiva de seguridad	
Gestión de actualizaciones y revisiones	
Documentación de la red	
Flujo de datos de la aplicación	
Gestión de actualizaciones	
Gestión de cambios y configuración	
Copias de seguridad y recuperación	
Archivos de registro	
Planificación de recuperación ante desastres y reanudación de negocio	
Copias de seguridad	
Dispositivos de copia de seguridad	
Copias de seguridad y restauración	

Personal	
Requisitos y evaluaciones	
Requisitos de seguridad	
Evaluaciones de seguridad	
Directiva y procedimientos	
Comprobaciones del historial personal	
Directiva de recursos humanos	
Relaciones con terceros	
Formación y conocimiento	
Conocimiento de seguridad	
Formación sobre seguridad	

CARPA INTERNATIONAL

Infraestructura	
Defensa del perímetro	
Reglas y filtros de cortafuegos	
Antivirus	
Antivirus - Equipos de escritorio	
Antivirus - Servidores	
Acceso remoto	
Segmentación	
Sistema de detección de intrusiones (IDS)	
Inalámbrico	
Autenticación	
Usuarios administrativos	
Usuarios internos	
Usuarios de acceso remoto	
Directivas de contraseñas	
Directivas de contraseñas-Cuenta de administrador	
Directivas de contraseñas-Cuenta de usuario	
Directivas de contraseñas-Cuenta de acceso remoto	
Cuentas inactivas	
Gestión y control	
Informes sobre incidentes y respuesta	
Creación segura	
Seguridad física	

Aplicaciones	
Implementación y uso	
Equilibrio de carga	
Clústeres	
Aplicación y recuperación de datos	
Fabricante de software independiente (ISV)	
Desarrollado internamente	
Vulnerabilidades	
Diseño de aplicaciones	
Autenticación	
Directivas de contraseñas	
Autorización y control de acceso	
Registro	
Validación de datos de entrada	
Metodologías de desarrollo de seguridad de software	
Almacenamiento y comunicaciones de datos	

Operaciones	
Entorno	
Host de gestión	
Host de gestión-Servidores	
Host de gestión - Dispositivos de red	
Directiva de seguridad	
Clasificación de datos	
Eliminación de datos	
Protocolos y servicios	
Uso aceptable	
Gestión de cuentas de usuarios	
Regulación	
Directiva de seguridad	
Gestión de actualizaciones y revisiones	
Documentación de la red	
Flujo de datos de la aplicación	
Gestión de actualizaciones	
Gestión de cambios y configuración	
Copias de seguridad y recuperación	
Archivos de registro	
Planificación de recuperación ante desastres y reanudación de negocio	
Copias de seguridad	
Dispositivos de copia de seguridad	
Copias de seguridad y restauración	

Personal	
Requisitos y evaluaciones	
Requisitos de seguridad	
Evaluaciones de seguridad	
Directiva y procedimientos	
Comprobaciones del historial personal	
Directiva de recursos humanos	
Relaciones con terceros	
Formación y conocimiento	
Conocimiento de seguridad	
Formación sobre seguridad	

COLORA LIMITADA

Infraestructura	
Defensa del perímetro	
Reglas y filtros de cortafuegos	
Antivirus	
Antivirus - Equipos de escritorio	
Antivirus - Servidores	
Acceso remoto	
Segmentación	
Sistema de detección de intrusiones (IDS)	
Inalámbrico	
Autenticación	
Usuarios administrativos	
Usuarios internos	
Usuarios de acceso remoto	
Directivas de contraseñas	
Directivas de contraseñas-Cuenta de administrador	
Directivas de contraseñas-Cuenta de usuario	
Directivas de contraseñas-Cuenta de acceso remoto	
Cuentas inactivas	
Gestión y control	
Informes sobre incidentes y respuesta	
Creación segura	
Seguridad física	

Aplicaciones	
Implementación y uso	
Equilibrio de carga	
Clústeres	
Aplicación y recuperación de datos	
Fabricante de software independiente (ISV)	
Desarrollado internamente	
Vulnerabilidades	
Diseño de aplicaciones	
Autenticación	
Directivas de contraseñas	
Autorización y control de acceso	
Registro	
Validación de datos de entrada	
Metodologías de desarrollo de seguridad de software	
Almacenamiento y comunicaciones de datos	
Cifrado	
Cifrado - Algoritmo	

Operaciones	
Entorno	
Host de gestión	
Host de gestión-Servidores	
Host de gestión - Dispositivos de red	
Directiva de seguridad	
Clasificación de datos	
Eliminación de datos	
Protocolos y servicios	
Uso aceptable	
Gestión de cuentas de usuarios	
Regulación	
Directiva de seguridad	
Gestión de actualizaciones y revisiones	
Documentación de la red	
Flujo de datos de la aplicación	
Gestión de actualizaciones	
Gestión de cambios y configuración	
Copias de seguridad y recuperación	
Archivos de registro	
Planificación de recuperación ante desastres y reanudación de negocio	
Copias de seguridad	
Dispositivos de copia de seguridad	
Copias de seguridad y restauración	

Personal	
Requisitos y evaluaciones	
Requisitos de seguridad	
Evaluaciones de seguridad	
Directiva y procedimientos	
Comprobaciones del historial personal	
Directiva de recursos humanos	
Relaciones con terceros	
Formación y conocimiento	
Conocimiento de seguridad	
Formación sobre seguridad	

DOLPHIN EXPRESS VIAJES Y TURISMO

Infraestructura	
Defensa del perímetro	
Reglas y filtros de cortafuegos	
Antivirus	
Antivirus - Equipos de escritorio	
Antivirus - Servidores	
Acceso remoto	
Segmentación	
Sistema de detección de intrusiones (IDS)	
Inalámbrico	
Autenticación	
Usuarios administrativos	
Usuarios internos	
Usuarios de acceso remoto	
Directivas de contraseñas	
Directivas de contraseñas-Cuenta de administrador	
Directivas de contraseñas-Cuenta de usuario	
Directivas de contraseñas-Cuenta de acceso remoto	
Cuentas inactivas	
Gestión y control	
Informes sobre incidentes y respuesta	
Creación segura	
Seguridad física	

Aplicaciones	
Implementación y uso	
Equilibrio de carga	
Clústeres	
Aplicación y recuperación de datos	
Fabricante de software independiente (ISV)	
Desarrollado internamente	
Vulnerabilidades	
Diseño de aplicaciones	
Autenticación	
Directivas de contraseñas	
Autorización y control de acceso	
Registro	
Validación de datos de entrada	
Metodologías de desarrollo de seguridad de software	
Almacenamiento y comunicaciones de datos	
Cifrado	
Cifrado - Algoritmo	

Operaciones	
Entorno	
Host de gestión	
Host de gestión-Servidores	
Host de gestión - Dispositivos de red	
Directiva de seguridad	
Clasificación de datos	
Eliminación de datos	
Protocolos y servicios	
Uso aceptable	
Gestión de cuentas de usuarios	
Regulación	
Directiva de seguridad	
Gestión de actualizaciones y revisiones	
Documentación de la red	
Flujo de datos de la aplicación	
Gestión de actualizaciones	
Gestión de cambios y configuración	
Copias de seguridad y recuperación	
Archivos de registro	
Planificación de recuperación ante desastres y reanudación de negocio	
Copias de seguridad	
Dispositivos de copia de seguridad	
Copias de seguridad y restauración	

Personal	
Requisitos y evaluaciones	
Requisitos de seguridad	
Evaluaciones de seguridad	
Directiva y procedimientos	
Comprobaciones del historial personal	
Directiva de recursos humanos	
Relaciones con terceros	
Formación y conocimiento	
Conocimiento de seguridad	
Formación sobre seguridad	

EXPRESO VIAJES Y TURISMO

Infraestructura	
Defensa del perímetro	
Reglas y filtros de cortafuegos	
Antivirus	
Antivirus - Equipos de escritorio	
Antivirus - Servidores	
Acceso remoto	
Segmentación	
Sistema de detección de intrusiones (IDS)	
Inalámbrico	
Autenticación	
Usuarios administrativos	
Usuarios internos	
Usuarios de acceso remoto	
Directivas de contraseñas	
Directivas de contraseñas-Cuenta de administrador	
Directivas de contraseñas-Cuenta de usuario	
Directivas de contraseñas-Cuenta de acceso remoto	
Cuentas inactivas	
Gestión y control	
Informes sobre incidentes y respuesta	
Creación segura	
Seguridad física	

Aplicaciones	
Implementación y uso	
Equilibrio de carga	
Clústeres	
Aplicación y recuperación de datos	
Fabricante de software independiente (ISV)	
Desarrollado internamente	
Vulnerabilidades	
Diseño de aplicaciones	
Autenticación	
Directivas de contraseñas	
Autorización y control de acceso	
Registro	
Validación de datos de entrada	
Metodologías de desarrollo de seguridad de software	
Almacenamiento y comunicaciones de datos	
Cifrado	
Cifrado - Algoritmo	

Operaciones	
Entorno	
Host de gestión	
Host de gestión-Servidores	
Host de gestión - Dispositivos de red	
Directiva de seguridad	
Clasificación de datos	
Eliminación de datos	
Protocolos y servicios	
Uso aceptable	
Gestión de cuentas de usuarios	
Regulación	
Directiva de seguridad	
Gestión de actualizaciones y revisiones	
Documentación de la red	
Flujo de datos de la aplicación	
Gestión de actualizaciones	
Gestión de cambios y configuración	
Copias de seguridad y recuperación	
Archivos de registro	
Planificación de recuperación ante desastres y reanudación de negocio	
Copias de seguridad	
Dispositivos de copia de seguridad	
Copias de seguridad y restauración	

Personal	
Requisitos y evaluaciones	
Requisitos de seguridad	
Evaluaciones de seguridad	
Directiva y procedimientos	
Comprobaciones del historial personal	
Directiva de recursos humanos	
Relaciones con terceros	
Formación y conocimiento	
Conocimiento de seguridad	
Formación sobre seguridad	

FLOTA USAQUEN

Infraestructura	
Defensa del perímetro	
Reglas y filtros de cortafuegos	
Antivirus	
Antivirus - Equipos de escritorio	
Antivirus - Servidores	
Acceso remoto	
Segmentación	
Sistema de detección de intrusiones (IDS)	
Inalámbrico	
Autenticación	
Usuarios administrativos	
Usuarios internos	
Usuarios de acceso remoto	
Directivas de contraseñas	
Directivas de contraseñas-Cuenta de administrador	
Directivas de contraseñas-Cuenta de usuario	
Directivas de contraseñas-Cuenta de acceso remoto	
Cuentas inactivas	
Gestión y control	
Informes sobre incidentes y respuesta	
Creación segura	
Seguridad física	

Aplicaciones	
Implementación y uso	
Equilibrio de carga	
Clústeres	
Aplicación y recuperación de datos	
Fabricante de software independiente (ISV)	
Desarrollado internamente	
Vulnerabilidades	
Diseño de aplicaciones	
Autenticación	
Directivas de contraseñas	
Autorización y control de acceso	
Registro	
Validación de datos de entrada	
Metodologías de desarrollo de seguridad de software	
Almacenamiento y comunicaciones de datos	
Cifrado	
Cifrado - Algoritmo	

Operaciones	
Entorno	
Host de gestión	
Host de gestión-Servidores	
Host de gestión - Dispositivos de red	
Directiva de seguridad	
Clasificación de datos	
Eliminación de datos	
Protocolos y servicios	
Uso aceptable	
Gestión de cuentas de usuarios	
Regulación	
Directiva de seguridad	
Gestión de actualizaciones y revisiones	
Documentación de la red	
Flujo de datos de la aplicación	
Gestión de actualizaciones	
Gestión de cambios y configuración	
Copias de seguridad y recuperación	
Archivos de registro	
Planificación de recuperación ante desastres y reanudación de negocio	
Copias de seguridad	
Dispositivos de copia de seguridad	
Copias de seguridad y restauración	

Personal	
Requisitos y evaluaciones	
Requisitos de seguridad	
Evaluaciones de seguridad	
Directiva y procedimientos	
Comprobaciones del historial personal	
Directiva de recursos humanos	
Relaciones con terceros	
Formación y conocimiento	
Conocimiento de seguridad	
Formación sobre seguridad	

INGEOSTUDIOS SA

Infraestructura	
Defensa del perímetro	
Reglas y filtros de cortafuegos	
Antivirus	
Antivirus - Equipos de escritorio	
Antivirus - Servidores	
Acceso remoto	
Segmentación	
Sistema de detección de intrusiones (IDS)	
Inalámbrico	
Autenticación	
Usuarios administrativos	
Usuarios internos	
Usuarios de acceso remoto	
Directivas de contraseñas	
Directivas de contraseñas-Cuenta de administrador	
Directivas de contraseñas-Cuenta de usuario	
Directivas de contraseñas-Cuenta de acceso remoto	
Cuentas inactivas	
Gestión y control	
Informes sobre incidentes y respuesta	
Creación segura	
Seguridad física	

Aplicaciones	
Implementación y uso	
Equilibrio de carga	
Clústeres	
Aplicación y recuperación de datos	
Fabricante de software independiente (ISV)	
Desarrollado internamente	
Vulnerabilidades	
Diseño de aplicaciones	
Autenticación	
Directivas de contraseñas	
Autorización y control de acceso	
Registro	
Validación de datos de entrada	
Metodologías de desarrollo de seguridad de software	
Almacenamiento y comunicaciones de datos	
Cifrado	
Cifrado - Algoritmo	

Operaciones	
Entorno	
Host de gestión	
Host de gestión-Servidores	
Host de gestión - Dispositivos de red	
Directiva de seguridad	
Clasificación de datos	
Eliminación de datos	
Protocolos y servicios	
Uso aceptable	
Gestión de cuentas de usuarios	
Regulación	
Directiva de seguridad	
Gestión de actualizaciones y revisiones	
Documentación de la red	
Flujo de datos de la aplicación	
Gestión de actualizaciones	
Gestión de cambios y configuración	
Copias de seguridad y recuperación	
Archivos de registro	
Planificación de recuperación ante desastres y reanudación de negocio	
Copias de seguridad	
Dispositivos de copia de seguridad	
Copias de seguridad y restauración	

Personal	
Requisitos y evaluaciones	
Requisitos de seguridad	
Evaluaciones de seguridad	
Directiva y procedimientos	
Comprobaciones del historial personal	
Directiva de recursos humanos	
Relaciones con terceros	
Formación y conocimiento	
Conocimiento de seguridad	
Formación sobre seguridad	

COMPAÑÍA METROPOLITANA DE TRANSPORTE

Infraestructura	
Defensa del perímetro	
Reglas y filtros de cortafuegos	
Antivirus	
Antivirus - Equipos de escritorio	
Antivirus - Servidores	
Acceso remoto	
Segmentación	
Sistema de detección de intrusiones (IDS)	
Inalámbrico	
Autenticación	
Usuarios administrativos	
Usuarios internos	
Usuarios de acceso remoto	
Directivas de contraseñas	
Directivas de contraseñas-Cuenta de administrador	
Directivas de contraseñas-Cuenta de usuario	
Directivas de contraseñas-Cuenta de acceso remoto	
Cuentas inactivas	
Gestión y control	
Informes sobre incidentes y respuesta	
Creación segura	
Seguridad física	

Aplicaciones	
Implementación y uso	
Equilibrio de carga	
Clústeres	
Aplicación y recuperación de datos	
Fabricante de software independiente (ISV)	
Desarrollado internamente	
Vulnerabilidades	
Diseño de aplicaciones	
Autenticación	
Directivas de contraseñas	
Autorización y control de acceso	
Registro	
Validación de datos de entrada	
Metodologías de desarrollo de seguridad de software	
Almacenamiento y comunicaciones de datos	
Cifrado	
Cifrado - Algoritmo	

Operaciones	
Entorno	
Host de gestión	
Host de gestión-Servidores	
Host de gestión - Dispositivos de red	
Directiva de seguridad	
Clasificación de datos	
Eliminación de datos	
Protocolos y servicios	
Uso aceptable	
Gestión de cuentas de usuarios	
Regulación	
Directiva de seguridad	
Gestión de actualizaciones y revisiones	
Documentación de la red	
Flujo de datos de la aplicación	
Gestión de actualizaciones	
Gestión de cambios y configuración	
Copias de seguridad y recuperación	
Archivos de registro	
Planificación de recuperación ante desastres y reanudación de negocio	
Copias de seguridad	
Dispositivos de copia de seguridad	
Copias de seguridad y restauración	

Personal	
Requisitos y evaluaciones	
Requisitos de seguridad	
Evaluaciones de seguridad	
Directiva y procedimientos	
Comprobaciones del historial personal	
Directiva de recursos humanos	
Relaciones con terceros	
Formación y conocimiento	
Conocimiento de seguridad	
Formación sobre seguridad	

PANAMERICANA LTDA

Infraestructura	
Defensa del perímetro	
Reglas y filtros de cortafuegos	
Antivirus	
Antivirus - Equipos de escritorio	
Antivirus - Servidores	
Acceso remoto	
Segmentación	
Sistema de detección de intrusiones (IDS)	
Inalámbrico	
Autenticación	
Usuarios administrativos	
Usuarios internos	
Usuarios de acceso remoto	
Directivas de contraseñas	
Directivas de contraseñas-Cuenta de administrador	
Directivas de contraseñas-Cuenta de usuario	
Directivas de contraseñas-Cuenta de acceso remoto	
Cuentas inactivas	
Gestión y control	
Informes sobre incidentes y respuesta	
Creación segura	
Seguridad física	

Aplicaciones	
Implementación y uso	
Equilibrio de carga	
Clústeres	
Aplicación y recuperación de datos	
Fabricante de software independiente (ISV)	
Desarrollado internamente	
Vulnerabilidades	
Diseño de aplicaciones	
Autenticación	
Directivas de contraseñas	
Autorización y control de acceso	
Registro	
Validación de datos de entrada	
Metodologías de desarrollo de seguridad de software	
Almacenamiento y comunicaciones de datos	
Cifrado	
Cifrado - Algoritmo	

Operaciones	
Entorno	
Host de gestión	
Host de gestión-Servidores	
Host de gestión - Dispositivos de red	
Directiva de seguridad	
Clasificación de datos	
Eliminación de datos	
Protocolos y servicios	
Uso aceptable	
Gestión de cuentas de usuarios	
Regulación	
Directiva de seguridad	
Gestión de actualizaciones y revisiones	
Documentación de la red	
Flujo de datos de la aplicación	
Gestión de actualizaciones	
Gestión de cambios y configuración	
Copias de seguridad y recuperación	
Archivos de registro	
Planificación de recuperación ante desastres y reanudación de negocio	
Copias de seguridad	
Dispositivos de copia de seguridad	
Copias de seguridad y restauración	

Personal	
Requisitos y evaluaciones	
Requisitos de seguridad	
Evaluaciones de seguridad	
Directiva y procedimientos	
Comprobaciones del historial personal	
Directiva de recursos humanos	
Relaciones con terceros	
Formación y conocimiento	
Conocimiento de seguridad	
Formación sobre seguridad	

TRANSVAL LTDA

Infraestructura	
Defensa del perímetro	
Reglas y filtros de cortafuegos	
Antivirus	
Antivirus - Equipos de escritorio	
Antivirus - Servidores	
Acceso remoto	
Segmentación	
Sistema de detección de intrusiones (IDS)	
Inalámbrico	
Autenticación	
Usuarios administrativos	
Usuarios internos	
Usuarios de acceso remoto	
Directivas de contraseñas	
Directivas de contraseñas-Cuenta de administrador	
Directivas de contraseñas-Cuenta de usuario	
Directivas de contraseñas-Cuenta de acceso remoto	
Cuentas inactivas	
Gestión y control	
Informes sobre incidentes y respuesta	
Creación segura	
Seguridad física	

Aplicaciones	
Implementación y uso	
Equilibrio de carga	
Clústeres	
Aplicación y recuperación de datos	
Fabricante de software independiente (ISV)	
Desarrollado internamente	
Vulnerabilidades	
Diseño de aplicaciones	
Autenticación	
Directivas de contraseñas	
Autorización y control de acceso	
Registro	
Validación de datos de entrada	
Metodologías de desarrollo de seguridad de software	
Almacenamiento y comunicaciones de datos	
Cifrado	
Cifrado - Algoritmo	

Operaciones	
Entorno	
Host de gestión	
Host de gestión-Servidores	
Host de gestión - Dispositivos de red	
Directiva de seguridad	
Clasificación de datos	
Eliminación de datos	
Protocolos y servicios	
Uso aceptable	
Gestión de cuentas de usuarios	
Regulación	
Directiva de seguridad	
Gestión de actualizaciones y revisiones	
Documentación de la red	
Flujo de datos de la aplicación	
Gestión de actualizaciones	
Gestión de cambios y configuración	
Copias de seguridad y recuperación	
Archivos de registro	
Planificación de recuperación ante desastres y reanudación de negocio	
Copias de seguridad	
Dispositivos de copia de seguridad	
Copias de seguridad y restauración	

Personal	
Requisitos y evaluaciones	
Requisitos de seguridad	
Evaluaciones de seguridad	
Directiva y procedimientos	
Comprobaciones del historial personal	
Directiva de recursos humanos	
Relaciones con terceros	
Formación y conocimiento	
Conocimiento de seguridad	
Formación sobre seguridad	

ROBAYO MURCIA ABEL

Infraestructura	
Defensa del perímetro	
Reglas y filtros de cortafuegos	
Antivirus	
Antivirus - Equipos de escritorio	
Antivirus - Servidores	
Acceso remoto	
Segmentación	
Sistema de detección de intrusiones (IDS)	
Inalámbrico	
Autenticación	
Usuarios administrativos	
Usuarios internos	
Usuarios de acceso remoto	
Directivas de contraseñas	
Directivas de contraseñas-Cuenta de administrador	
Directivas de contraseñas-Cuenta de usuario	
Directivas de contraseñas-Cuenta de acceso remoto	
Cuentas inactivas	
Gestión y control	
Informes sobre incidentes y respuesta	
Creación segura	
Seguridad física	

Aplicaciones	
Implementación y uso	
Equilibrio de carga	
Clústeres	
Aplicación y recuperación de datos	
Fabricante de software independiente (ISV)	
Desarrollado internamente	
Vulnerabilidades	
Diseño de aplicaciones	
Autenticación	
Directivas de contraseñas	
Autorización y control de acceso	
Registro	
Validación de datos de entrada	
Metodologías de desarrollo de seguridad de software	
Almacenamiento y comunicaciones de datos	
Cifrado	
Cifrado - Algoritmo	

Operaciones	
Entorno	
Host de gestión	
Host de gestión-Servidores	
Host de gestión - Dispositivos de red	
Directiva de seguridad	
Clasificación de datos	
Eliminación de datos	
Protocolos y servicios	
Uso aceptable	
Gestión de cuentas de usuarios	
Regulación	
Directiva de seguridad	
Gestión de actualizaciones y revisiones	
Documentación de la red	
Flujo de datos de la aplicación	
Gestión de actualizaciones	
Gestión de cambios y configuración	
Copias de seguridad y recuperación	
Archivos de registro	
Planificación de recuperación ante desastres y reanudación de negocio	
Copias de seguridad	
Dispositivos de copia de seguridad	
Copias de seguridad y restauración	

Personal	
Requisitos y evaluaciones	
Requisitos de seguridad	
Evaluaciones de seguridad	
Directiva y procedimientos	
Comprobaciones del historial personal	
Directiva de recursos humanos	
Relaciones con terceros	
Formación y conocimiento	
Conocimiento de seguridad	
Formación sobre seguridad	

SANCHEZ MORALES

Infraestructura	
Defensa del perímetro	
Reglas y filtros de cortafuegos	
Antivirus	
Antivirus - Equipos de escritorio	
Antivirus - Servidores	
Acceso remoto	
Segmentación	
Sistema de detección de intrusiones (IDS)	
Inalámbrico	
Autenticación	
Usuarios administrativos	
Usuarios internos	
Usuarios de acceso remoto	
Directivas de contraseñas	
Directivas de contraseñas-Cuenta de administrador	
Directivas de contraseñas-Cuenta de usuario	
Directivas de contraseñas-Cuenta de acceso remoto	
Cuentas inactivas	
Gestión y control	
Informes sobre incidentes y respuesta	
Creación segura	
Seguridad física	

Aplicaciones	
Implementación y uso	
Equilibrio de carga	
Clústeres	
Aplicación y recuperación de datos	
Fabricante de software independiente (ISV)	
Desarrollado internamente	
Vulnerabilidades	
Diseño de aplicaciones	
Autenticación	
Directivas de contraseñas	
Autorización y control de acceso	
Registro	
Validación de datos de entrada	
Metodologías de desarrollo de seguridad de software	
Almacenamiento y comunicaciones de datos	
Cifrado	
Cifrado - Algoritmo	

Operaciones	
Entorno	
Host de gestión	
Host de gestión-Servidores	
Host de gestión - Dispositivos de red	
Directiva de seguridad	
Clasificación de datos	
Eliminación de datos	
Protocolos y servicios	
Uso aceptable	
Gestión de cuentas de usuarios	
Regulación	
Directiva de seguridad	
Gestión de actualizaciones y revisiones	
Documentación de la red	
Flujo de datos de la aplicación	
Gestión de actualizaciones	
Gestión de cambios y configuración	
Copias de seguridad y recuperación	
Archivos de registro	
Planificación de recuperación ante desastres y reanudación de negocio	
Copias de seguridad	
Dispositivos de copia de seguridad	
Copias de seguridad y restauración	

Personal	
Requisitos y evaluaciones	
Requisitos de seguridad	
Evaluaciones de seguridad	
Directiva y procedimientos	
Comprobaciones del historial personal	
Directiva de recursos humanos	
Relaciones con terceros	
Formación y conocimiento	
Conocimiento de seguridad	
Formación sobre seguridad	

Infraestructura	
Defensa del perímetro	
Reglas y filtros de cortafuegos	
Antivirus	
Antivirus - Equipos de escritorio	
Antivirus - Servidores	
Acceso remoto	
Segmentación	
Sistema de detección de intrusiones (IDS)	
Inalámbrico	
Autenticación	
Usuarios administrativos	
Usuarios internos	
Usuarios de acceso remoto	
Directivas de contraseñas	
Directivas de contraseñas-Cuenta de administrador	
Directivas de contraseñas-Cuenta de usuario	
Directivas de contraseñas-Cuenta de acceso remoto	
Cuentas inactivas	
Gestión y control	
Informes sobre incidentes y respuesta	
Creación segura	
Seguridad física	

Aplicaciones	
Implementación y uso	
Equilibrio de carga	
Clústeres	
Aplicación y recuperación de datos	
Fabricante de software independiente (ISV)	
Desarrollado internamente	
Vulnerabilidades	
Diseño de aplicaciones	
Autenticación	
Directivas de contraseñas	
Autorización y control de acceso	
Registro	
Validación de datos de entrada	
Metodologías de desarrollo de seguridad de software	
Almacenamiento y comunicaciones de datos	
Cifrado	
Cifrado - Algoritmo	

Operaciones	
Entorno	
Host de gestión	
Host de gestión-Servidores	
Host de gestión - Dispositivos de red	
Directiva de seguridad	
Clasificación de datos	
Eliminación de datos	
Protocolos y servicios	
Uso aceptable	
Gestión de cuentas de usuarios	
Regulación	
Directiva de seguridad	
Gestión de actualizaciones y revisiones	
Documentación de la red	
Flujo de datos de la aplicación	
Gestión de actualizaciones	
Gestión de cambios y configuración	
Copias de seguridad y recuperación	
Archivos de registro	
Planificación de recuperación ante desastres y reanudación de negocio	
Copias de seguridad	
Dispositivos de copia de seguridad	
Copias de seguridad y restauración	

Personal	
Requisitos y evaluaciones	
Requisitos de seguridad	
Evaluaciones de seguridad	
Directiva y procedimientos	
Comprobaciones del historial personal	
Directiva de recursos humanos	
Relaciones con terceros	
Formación y conocimiento	
Conocimiento de seguridad	
Formación sobre seguridad	

SMART LTDA

Infraestructura	
Defensa del perímetro	
Reglas y filtros de cortafuegos	
Antivirus	
Antivirus - Equipos de escritorio	
Antivirus - Servidores	
Acceso remoto	
Segmentación	
Sistema de detección de intrusiones (IDS)	
Inalámbrico	
Autenticación	
Usuarios administrativos	
Usuarios internos	
Usuarios de acceso remoto	
Directivas de contraseñas	
Directivas de contraseñas-Cuenta de administrador	
Directivas de contraseñas-Cuenta de usuario	
Directivas de contraseñas-Cuenta de acceso remoto	
Cuentas inactivas	
Gestión y control	
Informes sobre incidentes y respuesta	
Creación segura	
Seguridad física	

Aplicaciones	
Implementación y uso	
Equilibrio de carga	
Clústeres	
Aplicación y recuperación de datos	
Fabricante de software independiente (ISV)	
Desarrollado internamente	
Vulnerabilidades	
Diseño de aplicaciones	
Autenticación	
Directivas de contraseñas	
Autorización y control de acceso	
Registro	
Validación de datos de entrada	
Metodologías de desarrollo de seguridad de software	
Almacenamiento y comunicaciones de datos	
Cifrado	
Cifrado - Algoritmo	

Operaciones	
Entorno	
Host de gestión	
Host de gestión-Servidores	
Host de gestión - Dispositivos de red	
Directiva de seguridad	
Clasificación de datos	
Eliminación de datos	
Protocolos y servicios	
Uso aceptable	
Gestión de cuentas de usuarios	
Regulación	
Directiva de seguridad	
Gestión de actualizaciones y revisiones	
Documentación de la red	
Flujo de datos de la aplicación	
Gestión de actualizaciones	
Gestión de cambios y configuración	
Copias de seguridad y recuperación	
Archivos de registro	
Planificación de recuperación ante desastres y reanudación de negocio	
Copias de seguridad	
Dispositivos de copia de seguridad	
Copias de seguridad y restauración	

Personal	
Requisitos y evaluaciones	
Requisitos de seguridad	
Evaluaciones de seguridad	
Directiva y procedimientos	
Comprobaciones del historial personal	
Directiva de recursos humanos	
Relaciones con terceros	
Formación y conocimiento	
Conocimiento de seguridad	
Formación sobre seguridad	

SOPRO USAQUEN

Infraestructura	
Defensa del perímetro	
Reglas y filtros de cortafuegos	
Antivirus	
Antivirus - Equipos de escritorio	
Antivirus - Servidores	
Acceso remoto	
Segmentación	
Sistema de detección de intrusiones (IDS)	
Inalámbrico	
Autenticación	
Usuarios administrativos	
Usuarios internos	
Usuarios de acceso remoto	
Directivas de contraseñas	
Directivas de contraseñas-Cuenta de administrador	
Directivas de contraseñas-Cuenta de usuario	
Directivas de contraseñas-Cuenta de acceso remoto	
Cuentas inactivas	
Gestión y control	
Informes sobre incidentes y respuesta	
Creación segura	
Seguridad física	

Aplicaciones	
Implementación y uso	
Equilibrio de carga	
Clústeres	
Aplicación y recuperación de datos	
Fabricante de software independiente (ISV)	
Desarrollado internamente	
Vulnerabilidades	
Diseño de aplicaciones	
Autenticación	
Directivas de contraseñas	
Autorización y control de acceso	
Registro	
Validación de datos de entrada	
Metodologías de desarrollo de seguridad de software	
Almacenamiento y comunicaciones de datos	
Cifrado	
Cifrado - Algoritmo	

Operaciones	
Entorno	
Host de gestión	
Host de gestión-Servidores	
Host de gestión - Dispositivos de red	
Directiva de seguridad	
Clasificación de datos	
Eliminación de datos	
Protocolos y servicios	
Uso aceptable	
Gestión de cuentas de usuarios	
Regulación	
Directiva de seguridad	
Gestión de actualizaciones y revisiones	
Documentación de la red	
Flujo de datos de la aplicación	
Gestión de actualizaciones	
Gestión de cambios y configuración	
Copias de seguridad y recuperación	
Archivos de registro	
Planificación de recuperación ante desastres y reanudación de negocio	
Copias de seguridad	
Dispositivos de copia de seguridad	
Copias de seguridad y restauración	

Personal	
Requisitos y evaluaciones	
Requisitos de seguridad	
Evaluaciones de seguridad	
Directiva y procedimientos	
Comprobaciones del historial personal	
Directiva de recursos humanos	
Relaciones con terceros	
Formación y conocimiento	
Conocimiento de seguridad	
Formación sobre seguridad	

VICTORIA LINE DE COLOMBIA

Infraestructura	
Defensa del perímetro	
Reglas y filtros de cortafuegos	
Antivirus	
Antivirus - Equipos de escritorio	
Antivirus - Servidores	
Acceso remoto	
Segmentación	
Sistema de detección de intrusiones (IDS)	
Inalámbrico	
Autenticación	
Usuarios administrativos	
Usuarios internos	
Usuarios de acceso remoto	
Directivas de contraseñas	
Directivas de contraseñas-Cuenta de administrador	
Directivas de contraseñas-Cuenta de usuario	
Directivas de contraseñas-Cuenta de acceso remoto	
Cuentas inactivas	
Gestión y control	
Informes sobre incidentes y respuesta	
Creación segura	
Seguridad física	

Aplicaciones	
Implementación y uso	
Equilibrio de carga	
Clústeres	
Aplicación y recuperación de datos	
Fabricante de software independiente (ISV)	
Desarrollado internamente	
Vulnerabilidades	
Diseño de aplicaciones	
Autenticación	
Directivas de contraseñas	
Autorización y control de acceso	
Registro	
Validación de datos de entrada	
Metodologías de desarrollo de seguridad de software	
Almacenamiento y comunicaciones de datos	
Cifrado	
Cifrado - Algoritmo	

Operaciones	
Entorno	
Host de gestión	
Host de gestión-Servidores	
Host de gestión - Dispositivos de red	
Directiva de seguridad	
Clasificación de datos	
Eliminación de datos	
Protocolos y servicios	
Uso aceptable	
Gestión de cuentas de usuarios	
Regulación	
Directiva de seguridad	
Gestión de actualizaciones y revisiones	
Documentación de la red	
Flujo de datos de la aplicación	
Gestión de actualizaciones	
Gestión de cambios y configuración	
Copias de seguridad y recuperación	
Archivos de registro	
Planificación de recuperación ante desastres y reanudación de negocio	
Copias de seguridad	
Dispositivos de copia de seguridad	
Copias de seguridad y restauración	

Personal	
Requisitos y evaluaciones	
Requisitos de seguridad	
Evaluaciones de seguridad	
Directiva y procedimientos	
Comprobaciones del historial personal	
Directiva de recursos humanos	
Relaciones con terceros	
Formación y conocimiento	
Conocimiento de seguridad	
Formación sobre seguridad	

ANEXO H

“MONTAR UN FIREWALL EN LINUX BASADO EN IPTABLES POR MEDIO DE WEBMIN”

El objetivo del ejercicio es mostrar como negar o conceder permisos a los PC de una red interna para que pueda navegar en Internet haciendo tráfico por el Firewall que se va a configurar.

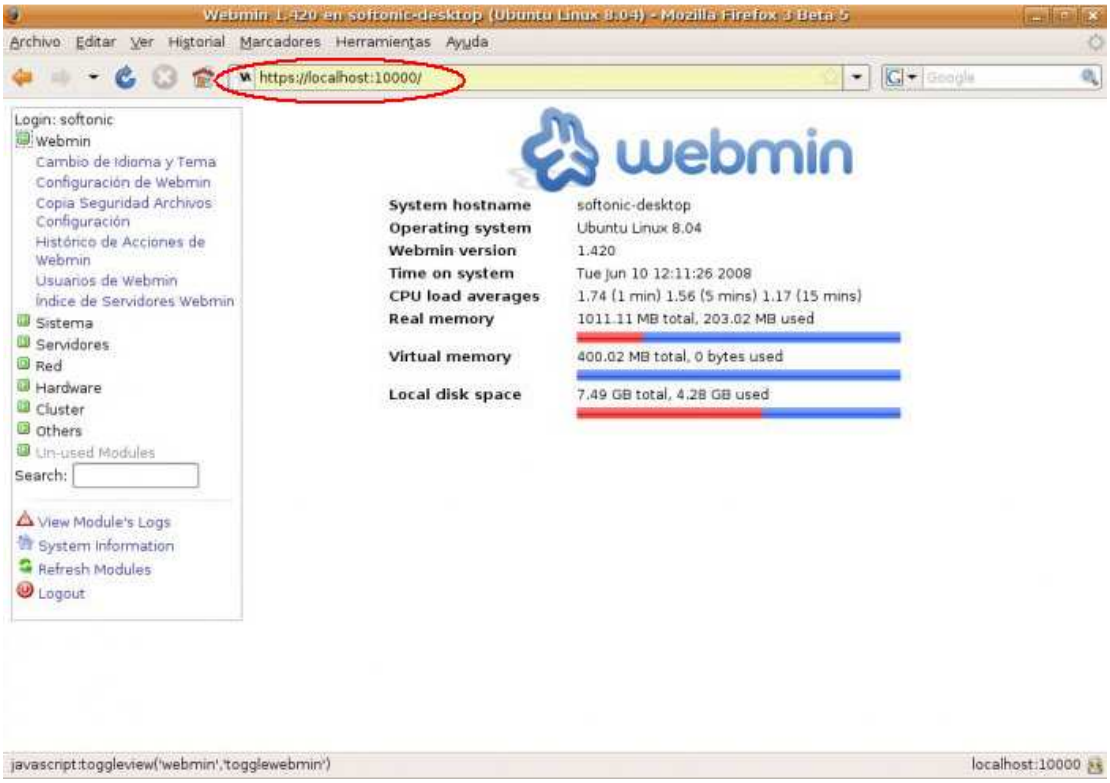
1 La herramienta grafica que se utilizará para este ejercicio es Webmin; se procede a descargar.

Webmin es una interfaz web para administrar y configurar un sistema Unix usando cualquier navegador que soporte tablas, formularios y Java para el módulo de administración de archivos.

Consta de un simple servidor web y un sinfín de scripts Perl y no usa módulos externos. Con Webmin se podrá configurar infinidad de opciones, como cuentas de usuarios, el servidor Apache y DNS, los comandos programados, el arranque y apagado del PC, instalación de nuevos paquetes, copia de seguridad del sistema, el cortafuegos, gestión de impresora, grabadora y GRUB, y un largo etcétera.

Webmin es una de las mejores maneras de administrar un sistema tanto remota como localmente.

2. Despues de instalado, se ingresa a la aplicación



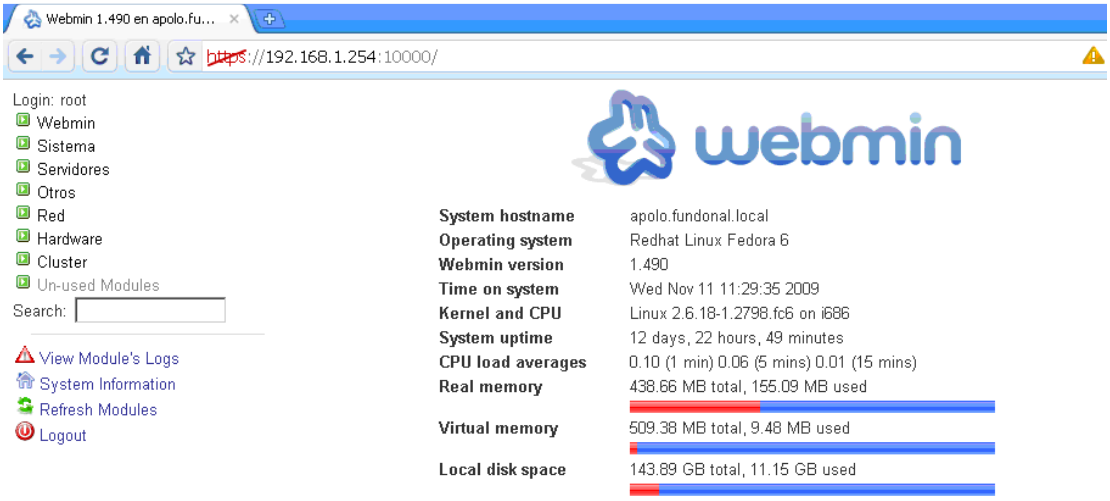
iptables es el nombre de la herramienta de espacio de usuario mediante la cual el administrador puede definir políticas de filtrado del tráfico que circula por la red.

iptables permite al administrador del sistema definir reglas acerca de qué hacer con los paquetes de red. Las reglas se agrupan en *cadenas*: cada cadena es una lista ordenada de reglas. Las cadenas se agrupan en *tablas*: cada tabla está asociada con un tipo diferente de procesamiento de paquetes.

Cada regla especifica qué paquetes la cumplen (*match*) y un *destino* que indica qué hacer con el paquete si éste cumple la regla. Cada paquete de red que llega a una computadora o que se envía desde una computadora recorre por lo menos una cadena y cada regla de esa cadena se comprueba con el paquete. Si la regla cumple con el datagrama, el recorrido se detiene y el destino de la regla dicta lo que se debe hacer con el paquete. Si el paquete alcanza el fin de una cadena predefinida sin haberse correspondido con ninguna regla de la cadena, la *política* de destino de la cadena dicta qué hacer con el paquete. Si el paquete alcanza el fin de una cadena definida por el usuario sin haber cumplido ninguna regla de la cadena o si la cadena definida por el usuario está vacía, el recorrido continúa en la cadena que hizo la llamada (lo que se denomina *implicit target RETURN* o RETORNO de destino implícito). Solo las cadenas predefinidas tienen políticas.

En *iptables*, las reglas se agrupan en cadenas. Una cadena es un conjunto de reglas para paquetes IP, que determinan lo que se debe hacer con ellos. Cada regla puede desechar el paquete de la cadena (cortocircuito), con lo cual otras cadenas no serán consideradas. Una cadena puede contener un enlace a otra cadena: si el paquete pasa a través de esa cadena entera o si cumple una regla de destino de retorno, va a continuar en la primera cadena. No hay un limite respecto de cuán anidadas pueden estar las cadenas. Hay tres cadenas básicas (*INPUT*, *OUTPUT* y *FORWARD*: ENTRADA, SALIDA y REENVÍO) y el usuario puede crear tantas como desee. Una regla puede ser simplemente un puntero a una cadena.

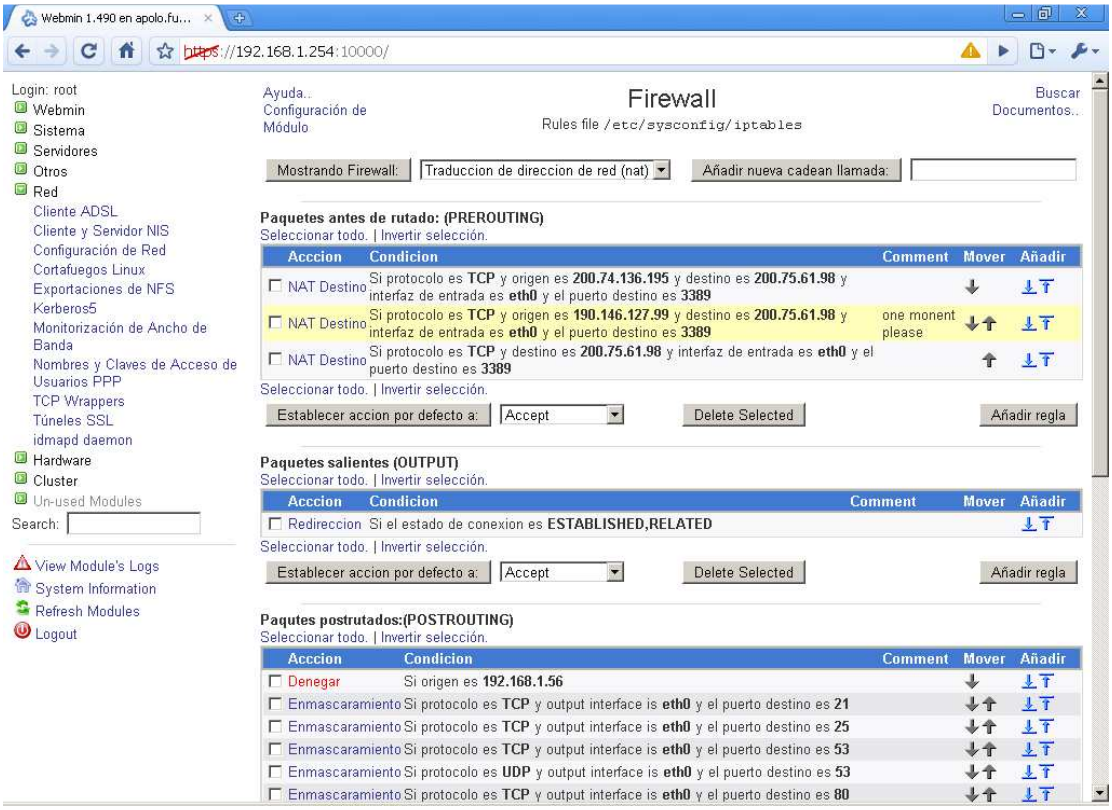
PAGINA DE INICIO



3.En red – cortafuegos linux – en donde dice mostrando firewall colocar traduccion de direccion de red (nat)

Si se lee la documentación sobre las tres tablas que hay (NAT, MANGLE y FILTER), se puede apreciar que solo sirve la tabla NAT.

Por eso se entraa esa tabla. Las otras dos tablas tienen funcionalidades que se salen del alcance del ejercicio; Como por ejemplo controlar las conexiones que tienen como destino el propio Firewall, conexiones para administración, etc.



nattable (*Tabla de traducción de direcciones de red*) — Esta tabla es la responsable de configurar las reglas de reescritura de direcciones o de puertos de los paquetes. El primer paquete en cualquier conexión pasa a través de esta tabla; los veredictos determinan como van a reescribirse todos los paquetes de esa conexión. Contiene las siguientes cadenas redefinidas:

- *PREROUTING chain* (Cadena de PRERUTEO) — Los paquetes entrantes pasan a través de esta cadena antes de que se consulte la

tabla de ruteo local, principalmente para DNAT (*destination*-NAT o traducción de direcciones de red de destino).

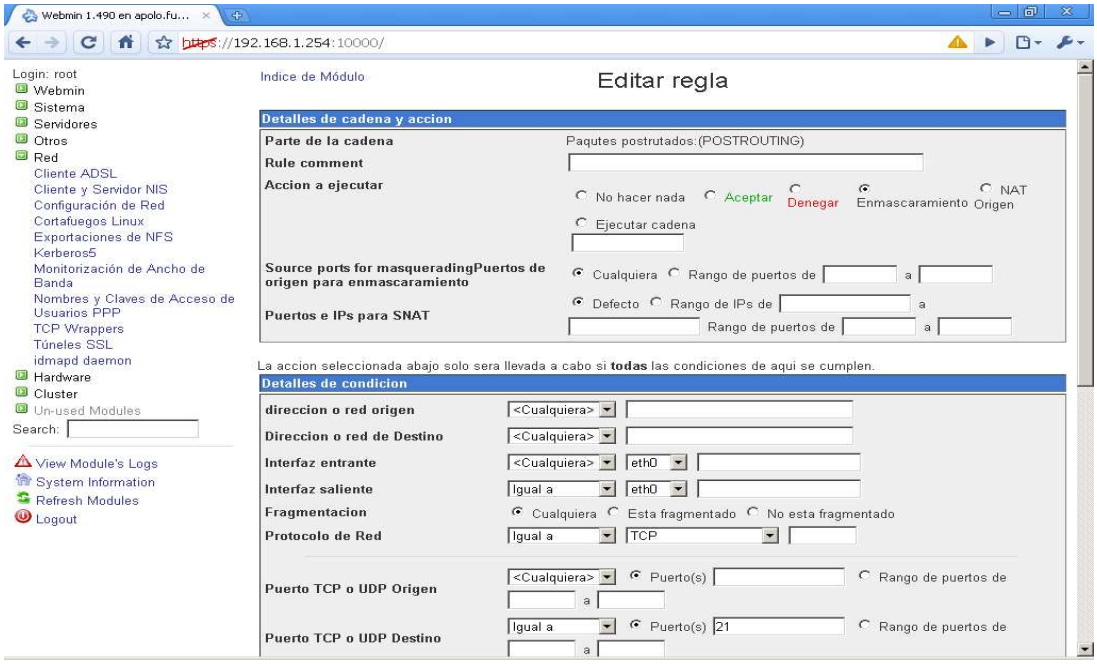
- *POSTROUTING chain* (Cadena de POSRUTEO) — Los paquetes salientes pasan por esta cadena después de haberse tomado la decisión del ruteo, principalmente para SNAT (*source*-NAT o traducción de direcciones de red de origen)
- *OUTPUT chain* (Cadena de SALIDA) — Permite hacer un DNAT limitado en paquetes generados localmente

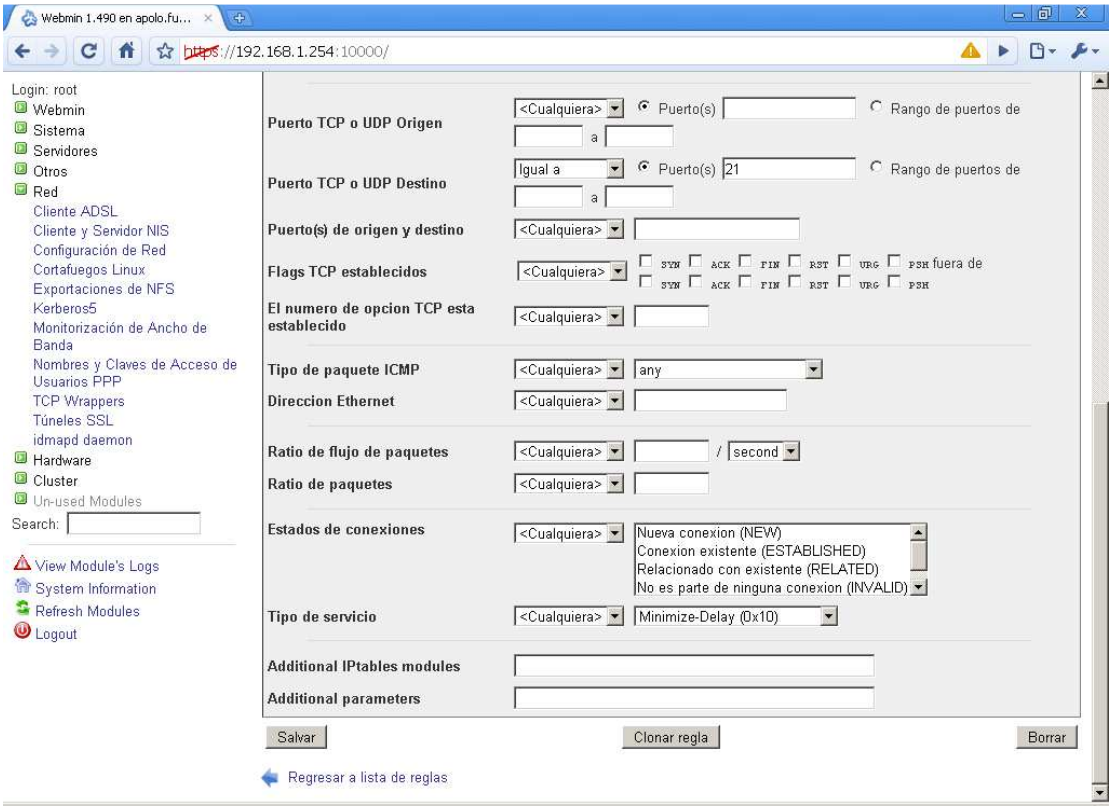
Para configurar una regla, se debe tener conocimiento del tráfico que se debe permitir.

Por ejemplo, el protocolo de transporte que utiliza (TCP, UDP, ICMP), el puerto TCP o UDP que utiliza (si aplica), ICMP no usa puertos, en su lugar usa tipo de trafico ICMP.

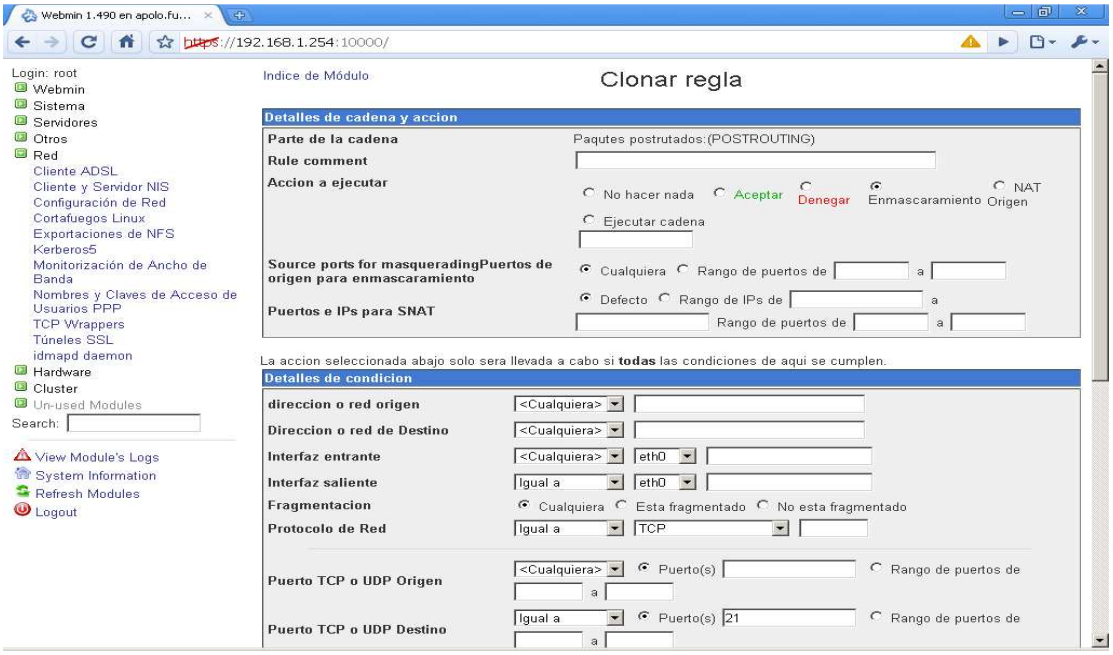
Si se desea filtrar el tráfico a nivel de IP y no a nivel de red, se debe saber a qué direcciones IP se debe permitir que tráfico.

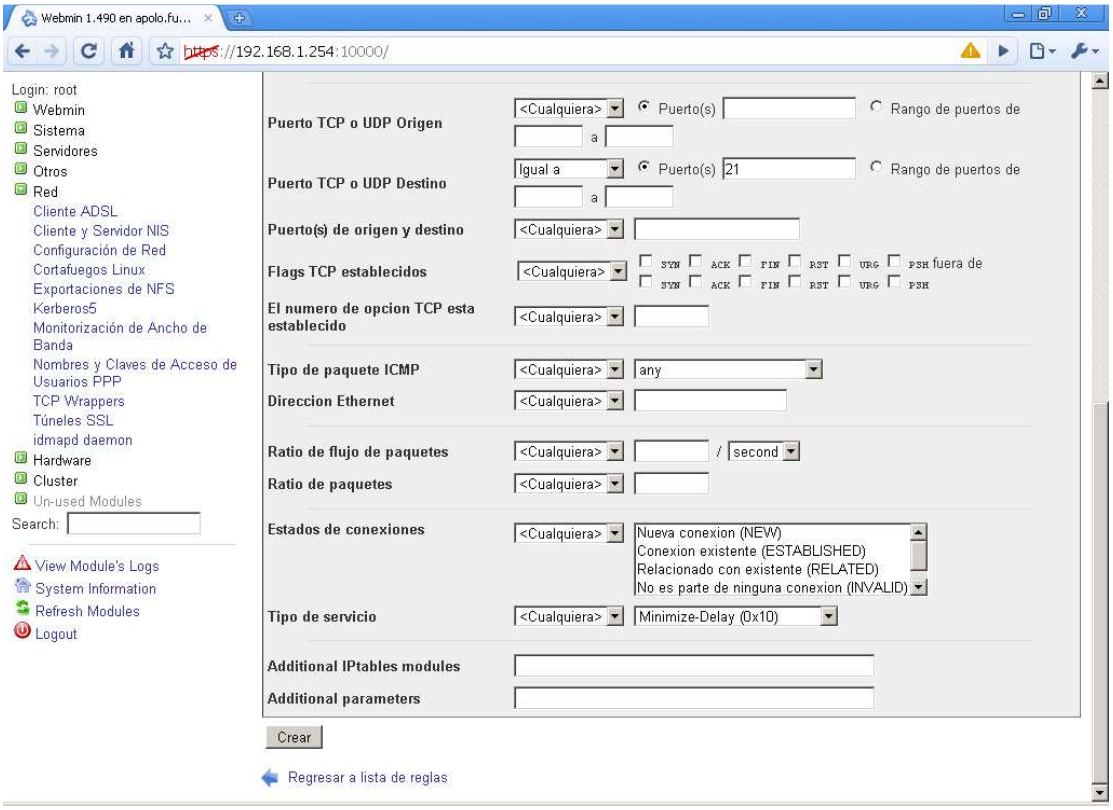
4. En la grafica del ejemplo se puede ver unas reglas ya configuradas *(donde dice paquetes postrutados(POSTROUTING))* " Si la dirección de origen es tal y el protocolo es tal y el puerto de destino es tal, entonces se Acepta, o se rechaza el paquete"Ingrese en una de estas.





5. Oprimir “clonar regla”





6. Hacer los cambios que considere necesarios,*(permitir a tal pc acceder a Internet por tal puerto)* crear y listo.