EVALUACIÓN E IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA EN LA ALCALDÍA DE SANTIAGO DE CALI

IVERT FERNANDO ANDRADE POTES
ERICH ESTRADA CORREA
DEBRAY RODRÍGUEZ URBANO

UNIVERSIDAD AUTÓNOMA DE OCCIDENTE
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE ELECTRÓNICA
PROGRAMA INGENIERIA ELECTRONICA
SANTIAGO DE CALI
2006

EVALUACIÓN E IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA EN LA ALCALDÍA DE SANTIAGO DE CALI

IVERT FERNANDO ANDRADE POTES
ERICH ESTRADA CORREA
DEBRAY RODRÍGUEZ URBANO

Pasantia para optar
Al titulo de Ingeniero Electrónico

Directores
Ing. GILBER CORRALES RUBIANO
Asesor de Informática y Telemática
Alcaldía de Santiago de Cali
ALEXANDER GARCÍA DÁVALOS
Msc. En Ciencias Computacionales
Departamento de Ciencias de la Información
Universidad Autónoma de Occidente

UNIVERSIDAD AUTÓNOMA DE OCCIDENTE
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE ELECTRÓNICA
PROGRAMA INGENIERIA ELECTRONICA
SANTIAGO DE CALI
2006

Nota de aceptación:

Trabajo aprobado por el comité de grado en cumplimiento a los requisitos exigidos por la Universidad Autónoma de Occidente para optar al titulo de ingeniero electrónico.

Ing. WILMAN FRANCO

_____

Jurado

Santiago de Cali, 20 de septiembre de 2006

AGRADECIMIENTOS

Expresamos sinceros agradecimientos a los Ingenieros ERMILSON DÍAZ y ALEXANDER GARCÍA DÁVALOS por colaborar en la realización de esta pasantía como coordinadores en la Alcaldía y la Universidad, por sus aportes para al buen desarrollo de la misma. Igualmente, al Ing. GILBER CORRALES por permitirnos realizar este proyecto en la Alcaldía municipal, entidad importante para la ciudad de Cali; agradecer a la Universidad Autónoma de Occidente por albergarnos todo este tiempo y permitirnos mejorar día a día y principalmente, a nuestras familias por tolerarnos, comprendernos y apoyarnos, sin ellos nunca podríamos haber culminado nuestros sueños.

Finalmente a Dios por darnos la vida y el conocimiento para poder sortear todas las dificultades pasadas, presentes y futuras.

CONTENIDO

Pág.

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

RESUMEN

La información constituye un activo que, como todos los demás activos comerciales importantes, es valioso para toda organización; por eso, es necesario protegerlo de una manera apropiada. La seguridad de la información protege la información contra amenazas muy diversas, para asegurar la continuidad de las actividades de la empresa, minimizar el perjuicio que puede ser causado y maximizar el rendimiento del capital invertido y las posibilidades de negocios. El Proyecto “Evaluación e Implementación de Políticas de Seguridad Informática en la Alcaldía de Santiago de Cali”, consistió en tres etapas: recopilar documentación referente a Auditoria Informática tanto a nivel interno como externo, realizar muestreo, análisis, y pruebas de vulnerabilidad de las diferentes dependencias que componen la Alcaldía, y al final entregar un documento de políticas de seguridad informática, en el cual está estipulado qué comportamiento deben tener los usuarios, encargados y administradores, en cuanto al acceso y al manejo de la información en la red. Si esto se cumple, se podría lograr certificar por medio de la norma ISO 17799 a la Alcaldía como una entidad con un alto nivel de seguridad. La etapa de investigación se baso en la revisar los documentos que posee la Oficina de Informática y Telemática de la Alcaldía de Santiago de Cali, en cuanto al funcionamiento y estructura de la red de telecomunicaciones de dicha entidad; a demás de examinar otros documentos que brindan información acerca de auditoria informática y la norma ISO 17799. En la segunda fase se realizó una encuesta que cubrió aspectos relacionados con la seguridad informática, y abarco tanto encargados de red como usuarios. En la etapa siguiente se analizaron los resultados arrojados por la encuesta, y se evaluó la seguridad de los equipos que hacen parte de la red de telecomunicaciones. Para la fase final, conociendo el comportamiento de los usuarios, el rendimiento de los equipos y su nivel de seguridad se procedió a redactar un documento que sirva como carta de navegación en cuanto al manejo de la información en la entidad.

INTRODUCCIÓN

Desde la aparición de los primeros equipos de computo alrededor del año 1940 (los cuales eran aparatos electromecánicos de gran tamaño) hasta nuestros días, la computadora ha sufrido grandes cambios gracias al aporte de muchas personas entre ellas Walter Houser Brattain, John Bardeen y William Bradford Shockley de Laboratorios Bell, los cuales desarrollaron el transistor de estado sólido, sin el cual no se hubiera podido reducir el tamaño de las computadoras. Luego vino el circuito integrado, el cual contenía algunos miles o millones de transistores en su interior, y así sucesivamente se sumaron una colección de inventos y se aplicaron una serie de modificaciones para llegar a la computadora de hoy. Las computadoras tienen muchos usos en la actualidad; pero el mayor potencial que poseen y el que más interesa en este proyecto, es la posibilidad de utilizar todas sus características de procesamiento y almacenamiento en una red de computadores.

Una red no solo son dos o más computadores conectados mediante un cable para compartir archivos, es mucho más, es la agrupación de protocolos, electrónica, personas y demás relaciones para utilizar una gran diversidad de servicios. Por otro lado, en estos momentos Internet es la mayor agrupación de computadores interconectados por todo el mundo.

Al evolucionar los computadores y las redes de interconexión de los mismos, también se ve la necesidad de “evolucionar” la seguridad informática, para evitar la perdida de información o corrupción de la misma por parte de personas no autorizadas.

El tema de seguridad informática, es unos de los temas más importantes a tratar a la hora de implementar algún tipo de red y proveer algún tipo de servicio a un grupo de usuarios. Se debe tener en cuenta que no existe una red cien por ciento segura, pero si se puede acercar bastante.

Para poder implementar una red segura, se debe contar con muchas variables, entre ellas: los usuarios que van acceder a la red, el medio, los servicios, equipos, los encargados. Para esto existen modelos de implementación de redes seguras, los cuales proveen una estructura metodológica para realizar una auditoria del estado de la red, evaluando el comportamiento de los usuarios y de los encargados de sistemas, revisando los servicios que se van a prestar y evaluando las políticas implementadas en el hardware (routers, firewalls, proxys y servidores), de esta manera, se le indica a la empresa o institución cómo se encuentra, qué vulnerabilidades posee, y qué acciones debe realizar para mejorar.

El presente informe trata principalmente de indicar como se desarrolló el Proyecto "Evaluación e Implementación de Políticas de Seguridad Informática en la Alcaldía de Santiago de Cali", mostrando los pasos en la obtención de documentación, muestreo y análisis de las diferentes dependencias que componen la Alcaldía, para al final entregar un documento de políticas de seguridad informática, en el cual está estipulado qué comportamiento deben tener los usuarios, encargados y administradores, en cuanto al acceso y al manejo de la información en la red. Si esto se cumple, se podría lograr certificar por medio de la norma ISO 17799 a la Alcaldía como una entidad con un alto nivel de seguridad.

1. PLANTEAMIENTO DEL PROBLEMA

En la actualidad, la torre donde funciona la Alcaldía de Santiago de Cali cuenta con una gran cantidad de cableado entre sus pisos, que idealmente debería corresponder a redes que pueden ser tanto de voz como de datos, pero debido a su expansión desordenada, ni siquiera los mismos ingenieros de la Alcaldía al observar éstos cables, saben de donde viene ni para donde va, lo que puede crear puntos de acceso desconocidos hasta para el mismo personal que labora en ésta dependencia gubernamental.

Este hecho y el no poseer una reglamentación establecida para la administración de la red, deja a ésta vulnerable a ataques tanto de personal endógeno como exógeno.

Dada la importancia de esta institución gubernamental, la mejor solución a este problema es implementar una serie de políticas que sirvan tanto para controlar el acceso de usuarios a la red como la administración de la misma.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Evaluar los controles a nivel informático, analizar la seguridad de los sistemas, realizar la evaluación de las políticas de seguridad informática propuestas para la Alcaldía de Santiago de Cali.

2.2 OBJETIVOS ESPECÍFICOS

- Revisar la documentación existente en la Alcaldía de Santiago de Cali sobre políticas de seguridad.
- Investigar en fuentes externas a la Alcaldía sobre normas, certificaciones y procedimientos para implementar unas adecuadas políticas de seguridad.
- Realizar una evaluación piso por piso, dependencia por dependencia de cómo se están aplicando políticas de seguridad informática, si es que se aplican.
- Realizar la valoración de la seguridad informática de la red en la Alcaldía de Santiago de Cali a nivel interno y externo.
- Realizar los cambios que sean necesarios para mejorar el documento de Políticas de Seguridad Informática.
- Realizar el proceso para la aprobación de las políticas por parte de la Alcaldía de Santiago de Cali.
- Desarrollar un plan para difundir las políticas que han sido aprobadas en la Alcaldía al personal que allí laboran.
- Realizar una auditoria informática de comunicaciones y redes.
- Realizar una auditoria de la seguridad informática.

3 JUSTIFICACIÓN

Es de vital importancia para la Alcaldía de Santiago de Cali realizar diferentes pruebas de revisión y evaluación de los controles, sistemas, procedimientos de informática; de los equipos de computo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que, por medio del señalamiento de cursos alternativos, se logre una utilización mas eficiente y segura de la información que servirá para una adecuada toma de decisiones.

La auditoria comprendió no solo la evaluación de los equipos de cómputo, de un sistema o procedimiento especifico, sino que a demás evaluó los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

Este proyecto es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y cuenten con un buen nivel de seguridad. Además, la evaluación debe ser integral (Informática, Organización, Hardware y Software).

4 MARCO TEÓRICO

Se realizó una evaluación en cada dependencia para saber si se están aplicando políticas de seguridad informática, a través de encuestas dirigidas a cada uno de los encargados de sistemas y usuarios de red. Luego, se procedió a valorar la seguridad informática de la red en la Alcaldía de Santiago de Cali a nivel interno, y finalmente se realizaron los cambios necesarios para mejorar el documento de Políticas de Seguridad Informática existente. De ésta manera, la Asesoría de informática y telemática quiere mantener un alto nivel de seguridad en la Red de telecomunicaciones de la Alcaldía.

Existen múltiples estándares para el análisis de diferentes componentes de seguridad. Como se indica en la tabla 1, en donde se aprecia que el estándar ISO/IEC 17799 se encuentra como herramienta de análisis en cada uno de los componentes, lo que nos inclinó a adoptarlo, debido a que recoge todas las áreas a evaluar en lo referente a seguridad informática.

Cabe anotar que la norma ISO 17799 se complementa con el estándar BS 7799 para formar las recomendaciones más acordes a los avances informáticos. De aquí nacen las descripciones mencionadas a continuación.

- ISO 17799 (parte 1): es un conjunto de controles basados en las mejores prácticas en seguridad de la información; ésta contiene consejos y recomendaciones que permiten asegurar la seguridad de la información de una empresa.

- BS 7799 (parte 2) / UNE 71502: es el estándar internacional que cubre todos los aspectos de la seguridad informática con respecto a equipos, políticas de gestión, recursos humanos, y aspectos jurídicos. Aquí se proponen recomendaciones con el fin de establecer un sistema de gestión de seguridad de la información (SGSI).

Las características más importantes de la norma BS 7799 son:

- Cobertura de la norma a diversos ambientes.
- Probada y aprobada en diversas entidades.
- Pública.
- Internacional.
- Imagen de marca asociada a "la calidad".
- Evolutiva y flexible (se adapta a los contextos).
- Disponibilidad de herramientas y soporte.

Tabla 1. Estándares Existentes en el análisis de seguridad informática

Sección 1.01 Componente	Estándar (*)
Análisis de riesgos	ISO/IEC 17799, NIST SP 800-30, NIST SP 800-6
Análisis de requerimientos y establecimiento de políticas de seguridad informática	ISO/IEC 17799, CSC-STD-001-83, ISO 15408, NIST SP 800-55, NIST SP 800-42, NIST SP 800-26, NIST SP 800-18, NIST SP 800-16
Aseguramiento de Componentes de Datos	ISO/IEC 17799, IEEE P1363, NIST SP 800-36, NIST SP 800-21, NIST SP 800-14, NIST SP 800-12
Aseguramiento de Componentes de Software	ISO/IEC 17799, NIST FIPS 73, NIST SP 800-44, NIST SP 800-41, NIST SP 800-36, NIST SP 800-14, NIST SP 800-5
Aseguramiento de Componentes de Hardware	ISO/IEC 17799, NSA/CSS Manual 130-2, NACSIM 5000, NIST SP 800-36, NIST SP 800-14
Aseguramiento de Componente Humano	ISO/IEC 17799, NSA Security Guidelines Handbook, NIST SP 800-50, NIST SP 800-36, NIST SP 800-16, NIST SP 800-14, NSTISSI 4011, NSTISSD 500, NSTISSI 4013, NSTISSI 4014, NSTISSI 4015, CSC-STD-002-85
Aseguramiento de Componentes de Ínter conectividad	ISO/IEC 17799, IEEE P1363, NIST SP 800-45, NIST SP 800-47, NIST SP 800-41, NIST SP 800-36, NIST SP 800-25, NIST SP 800-21, NIST SP 800-14, NIST SP 800-13
Aseguramiento de Infraestructura Física	ISO/IEC 17799, DoD 5220.22-M, NSA Security Guidelines Handbook, NSTISSI 7000, NIST SP 800-36, NIST SP 800-14, NIST SP 800-12
Administración de la seguridad informática	ISO/IEC 17799, ISO/IEC DTR 13335, ISO/IEC DIS 14980, NIST SP 800-64, NIST SP 800-61, NIST SP 800-50, NIST SP 800-55, NIST SP 800-42, NIST SP 800-40, NIST SP 800-36, NIST SP 800-35, NIST SP 800-34, NIST SP 800-18, NIST SP 800-16, NIST SP 800-6, NIST SP 800-5

Fuente: Agenda de conectividad. Republica de Colombia, 2005. p. 1.

4.1. ¿POR QUÉ UTILIZAR LA NORMA ISO 17799?

De acuerdo a lo indicado en la tabla 1, este parámetro reúne información acerca de los aspectos más importante a tener en cuenta para la evaluación de seguridad informática; lo que facilita el hecho de tomar toda la información necesaria de la misma fuente, ya que de esta forma se garantiza una mayor coherencia en la documentación. Los estándares BS 7799 / UNE 71502 / ISO 17799 pueden ser utilizados por cualquier organismo u empresa. Basta que la organización utilice sistemas informáticos, internos o externos, que posea datos confidenciales, que dependa de sistemas de información en el marco de sus actividades comerciales o que desee adoptar un nivel de seguridad elevada conformándose una norma.
Referente a la utilización de la norma ISO 177799 hay que tener en consideración lo siguiente:

- No existe por el momento certificación en el estándar ISO 17799 en el mundo.
- Una empresa puede acogerse a ISO 17799 y luego certificarse BS 7799-2: 2002 o UNE 71502:2004.
- Una gestión de auditoria puede ser apoyada por:
  - Verificación interna
  - Verificación externa (carta de opinión)
  - Oficina de registro del BSI (certificación oficial).

Este mecanismo permite obtener las siguientes ventajas:

- Acogerse a las normas en materia de gestión del riesgo.
- Una mejor protección de la información confidencial de la empresa.
- Una reducción de riesgos de ataques.

- Una recuperación más rápida y más fácil de las operaciones después de un ataque.

Existe una empresa llamada Callio Seguridad, la cual se encarga de implementar redes seguras a nivel físico y político. En la Web de esta empresa (www.callio.com) se ofrece un formato de encuestas utilizada por ellos para la evaluación del estado de las empresas, esta información fue filtrada y de allí se obtuvieron los siguientes dos tipos de encuestas:

- Encuesta para encargados de red.: Indicando como encargados de red o encargados de piso, a las personas que se ocupan del mantenimiento de equipos dentro de sus respectivas dependencias, además de constituir el primer escaño en la solución de problemas que se presente en los computadores u otros componentes de la red.
- Encuesta para usuarios: usuarios son todas aquellas personas que laboran en la entidad y tienen un computador a su cargo, o hacen uso de un computador.

5 MARCO CONTEXTUAL

Este proyecto se realizó en las instalaciones del Centro Administrativo Municipal (C.A.M.), teniendo como área de desarrollo todas las dependencias que funcionan en la torre de la Alcaldía excepto Contraloría, quienes por razones de seguridad y excesiva burocracia dificultaron la participación de ésta. La Alcaldía actualmente cuenta con una Oficina de Informática y Telemática ubicada en el piso 15 que funciona como oficina asesora del señor Alcalde, esta oficina en cabeza del ingeniero Gilbert Corrales, se debe adecuar para convertirla en una Dirección de Informática y Telemática. Para tal propósito se necesitan definir ciertos niveles de seguridad a nivel físico y a nivel informático. A pesar de que existe un documento preeliminar relacionado con las políticas de seguridad, éste debe estar sujeto a revisiones y actualizaciones; además era necesario realizar una evaluación a la Red de informática, en todo lo referente a vulnerabilidades, de manera que el documento de políticas esté adaptado a los nuevos riesgos y amenazas existentes en el manejo de información, y a los estándares más actuales.

Con la finalidad de lograr el nivel de Dirección de Informática y Telemática, la actual Oficina de Informática y telemática se apoya en los siguientes pilares:

PROPÓSITO GENERAL: Facilitar procesos a través de la Oficina de Informática y Telemática para permitir que la gestión pública en el Municipio de Santiago de Cali sea eficiente y eficaz.

MISIÓN: Apoyar y asesorar al señor Alcalde y a la Administración Central del Municipio de Santiago de Cali, mediante la definición de directrices tecnológicas y la administración del portal y la red municipal, para garantizar un eficiente, ágil y seguro sistema integrado de información.

VISIÓN: Ser reconocida como una Dirección Modelo dentro de la estructura del Municipio de Santiago de Cali, que se caracterice por la eficiencia y eficacia con que realiza sus funciones.

6 METODOLOGÍA

La metodología a seguir para el desarrollo de este proyecto se soportó inicialmente en la recopilación de toda la información encontrada en la Alcaldía de Santiago de Cali referente a Políticas de Seguridad Informática, equipos utilizados en la red y manejo de usuarios, después de analizar toda esta información se continuó con la investigación de los mismos temas en fuentes externas, al finalizar el proceso de documentación se realizó un paralelo entre la información encontrada en la Alcaldía y la encontrada en otras fuentes, con el cual se pudo realizar cambios y mejoras al documento de normas propuesto.

El paso siguiente en el desarrollo del proyecto, fue la visita a todos los pisos de la Alcaldía, recorriendo todas las dependencias de cada piso, evaluando si tienen una practica segura por parte de los usuarios a la hora de acceder a la red (Ej. manejo de cuentas, utilización de software, manejo de claves, correo electrónico), todo esto mediante un formato que fue creado para tal fin. Con los resultados que arrojó esta etapa se dio una valoración de cómo se está manejando el tema de seguridad por parte de los usuarios de la red en la Alcaldía.

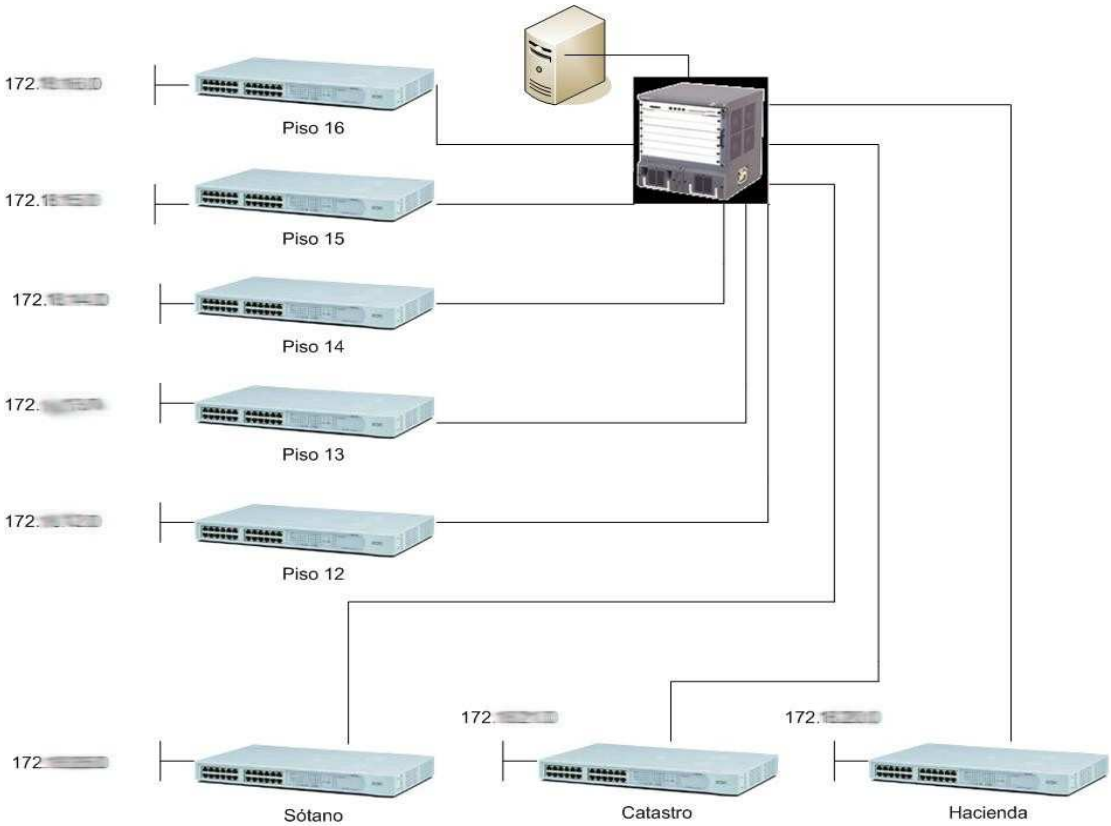
Después de la evaluación de las dependencias a nivel de políticas de seguridad informática, se procedió con la evaluación de la vulnerabilidad de la red. De esta manera se probaron los equipos (Routers, Servidores, Firewalls, Switches, Concentradores, Proxys y estaciones de trabajo) que hacen parte de la misma a diferentes tipos de ataques. Al final de esta evaluación se presentó un informe indicando que fallas posee la red y sugerencias, indicando que se debe corregir para mejorar su nivel de seguridad.

Luego de reunir toda la información y elaborar un documento acorde a los requerimientos de la entidad estatal, se procedió a realizar la gestión necesaria para su aprobación por parte de la Alcaldía de Santiago de Cali.

Al culminar favorablemente con la aprobación de las políticas desarrolladas en este proyecto se finalizó con la realización de sugerencias de actividades para difundir estas políticas entre el personal que labora en la Alcaldía.

A continuación se muestra un bosquejo de la red que se administran a través de la Oficina de Informática y Telemática de la Alcaldía.

Figura 1. Estructura de la Red Alcaldía de Cali



Fuente: Oficina de Informática y Telemática de la Alcaldía de Cali. SANTIAGO DE CALI, C.A.M 2006.

7. ANÁLISIS DE RESULTADOS

7.1 ENCUESTAS

7.1.1 Encuesta para el personal Encargado de Sistemas.

La encuesta se elaboró con las siguientes preguntas:

1. ¿Conoce usted los riesgos y amenazas existentes en el manejo de la información en la red?

Se pretende conocer la sensibilidad de las personas que se encuentran directamente relacionadas con la red, en cuanto al conocimiento de las múltiples posibilidades de perjuicio existentes en el manejo de la información en la red.

2. ¿Sabe usted si existen políticas de seguridad informática implementadas en la Alcaldía de Santiago de Cali?

A pesar de que en el área de la oficina Asesora de Informática y Telemática cuenta con un documento preliminar sobre políticas de seguridad informática, se desea saber si el personal encargado conoce dicho documento, o si es independiente a esto, o cada dependencia posee sus propias políticas de seguridad.

3. ¿Practica las políticas de seguridad?

Teniendo en cuenta la pregunta anterior, relacionada con el conocimiento de las políticas de seguridad en la Alcaldía, se pretende conocer que prácticas tienen los Encargados de Sistemas en lo que respecta al manejo de la información y los equipos.

4. ¿Existen sanciones disciplinarias por faltas a las políticas de seguridad?

Con este interrogante se quería conocer si existe alguna forma a nivel

disciplinario para controlar el uso indebido de la red, para mantener en condiciones óptimas la disponibilidad de la misma. El énfasis que se hizo en esta pregunta fue en cuanto al uso del Chat, portales para adultos entre otros sitios de riesgo.

5. ¿Realiza mantenimiento en los equipos? ¿Con que frecuencia?

Al igual que las sanciones disciplinarias, es muy importante conocer en que condiciones se encuentran los equipos para saber cuanto riesgo corre la red y como la falta de un mantenimiento periódico – preventivo puede afectar su rendimiento.

6. ¿Lleva algún tipo de inventario de los activos importantes para cada sistema de información?

Se desea conocer si se mantiene o no, un registro que indique con que equipos cuenta la red, que tipo de información se maneja y en que estado se encuentran los activos para tener una idea más clara a cerca de donde pueden presentarse las fallas más comunes.

7. ¿Existen planes de contingencia para casos excepcionales? Daños, recuperación de datos.

¿Qué tan pronto se resuelven las fallas, cuanto se afecta la Red y el desempeño de los empleados de la Alcaldía de Santiago de Cali?, estas son las incógnitas que se quieren resolver en este punto de la encuesta; puesto que para la Alcaldía es de vital importancia mantenerse en condiciones óptimas para la atención al cliente, y las comunicaciones entre dependencias (Continuidad de negocio).

8. ¿Realiza copias de seguridad de la información importante?

En este punto se desea conocer si los Encargados de Sistemas realizan una rutina de copias de respaldo de la información, elementos importantes para planes de contingencia.

9. ¿Tiene acceso a todo el nivel de seguridad en su piso y controla el uso a la información externa?

Se pretende conocer cuanta libertad de tráfico de información se tiene por parte de los Encargados de Sistemas. Saber si se manejan algún tipo de jerarquía y/o privilegios al acceder a la información que se encuentra en la Red.

10. ¿Existe un procedimiento para montar programas nuevos en los equipos?, ¿Existe un inventario de software? (licencias).

Esta pregunta da conocer bajo que términos se realiza la instalación de programas, si se realiza algún tipo de procedimiento por medio de un conducto definido y si se tiene en cuenta la modalidad de licenciamiento para evitar inconvenientes legales y técnicos.

11. ¿Designa a un propietario para cada equipo de la dependencia a su cargo?

Teniendo en cuenta que el Centro Administrativo Municipal - C.A.M es una dependencia pública, los equipos pueden estar en cierta forma un poco obsoletos; por lo que se quiso determinar la disponibilidad de recursos que tienen los Usurarios. También se quiere conocer si cada equipo en la Alcaldía tiene uno o más usuarios autorizados o si al equipo puede acceder cualquier persona.

12. ¿Ejerce algún control para garantizar el buen uso de los equipos?

El buen uso de los equipos implica tanto saber usar los equipos como protegerlos contra daños o eventualidades que reduzcan su rendimiento; por eso se consideró importante conocer como se maneja esta parte, y que tan capacitados están los Usuarios de red por parte de los encargados de cada piso.

13. ¿Cómo se mantiene la seguridad informática de la red en su piso?

Saber quien es el responsable de la seguridad de cada piso es muy importante para conocer a quien acuden los Encargados de Sistemas en caso de alguna eventualidad en la red, si la manejan ellos mismos o acuden a la oficina Asesora de Informática y Telemática.

14. ¿Está restringida y controlada la designación y utilización de privilegios? ¿Como? (Contraseñas, sesiones, etc.).

Es muy importante a nivel de seguridad informática, que los usuarios solo tengan

acceso a la información necesaria. Debido a que de esta forma se minimiza el riesgo de intromisiones indebidas en otras dependencias o en otras aplicaciones. Por esta razón se introdujo esta pregunta en el formulario de la encuesta.

15. ¿Conoce cuál es la topología de la red en este piso?

Es necesario que la persona que vaya a realizar "administración de red" conozca que clase de red va a administrar; por eso se consideró pertinente hacer esta pregunta, como un método evaluativo para los encargados.

16. ¿Informa usted a alguien sobre un fallo en los equipos si usted no puede solucionarlo? ¿A quien?

Se pretende conocer el nivel de independencia que tienen los Encargados de Sistemas con el área de Soporte Técnico de Informática y Telemática, a la hora de resolver problemas.

17. ¿Existe un cuarto de computo aislado para los equipos sensibles? (switches, servidores) y ¿como se controla el acceso?

Sabiendo la importancia de los equipos que enlazan la Red, es necesario que estos trabajen bajo ciertas condiciones (físicas y de seguridad), para reducir la posibilidad de "caídas" en la comunicación. Por eso nació la inquietud de saber cuales son las condiciones en las que funcionan los equipos activos de la Red.

18. ¿Existe un parámetro para el manejo de equipos portátiles y equipo móvil?

Se esperaba conocer cuál es el tratamiento que se les da a las personas que utilizan equipos que no son de ubicación fija con los cuales puedan extraer, dañar, o modificar información de la Alcaldía de Santiago de Cali.

19. ¿Cuando se hace el mantenimiento previo de los equipos y actualizaciones se realiza un documento donde se informe las acciones realizadas?

En este punto se quiere conocer si los operadores mantienen un registro de nombre de usuario, de los errores, de una acción correctiva realizada, y también si los registros del operador son comprobados regularmente contra los procedimientos de funcionamiento.

20. ¿Mantiene una base de datos sobre los fallos ocurridos en los activos informáticos en la alcaldía?

La intención es saber si los problemas están bien divulgados y manejados. Esto incluye la acción correctiva que es tomada, la revisión de los registros de problemas y comprobar las acciones realizadas. Con esta información se facilita la labor de mantenimiento, además, se realiza más rápidamente la acción restauradora si se repite una falla registrada.

21. ¿Han sido incorporados métodos de chequeo o validación en los sistemas para detectar la corrupción de datos? (encriptación, firma digital).

Con este interrogante se pretendía determinar si existe cualquier mecanismo de autenticación para las conexiones externas. Ejemplos: La criptografía, tokens de hardware, tokens de software, el protocolo de respuesta, etc.

Lo anterior para saber si las conexiones a los sistemas informáticos tanto locales como remotos son autenticadas para comprobar que son realmente ellos y que pertenecen a la Red.

22. ¿Esta permitido el acceso remoto de los usuarios a los equipos de computo y a la Intranet en general (acceso remoto asegurado, túneles, protocolos de seguridad?

Se esperaba conocer si las dependencias permiten el acceso remoto a la Red y saber si todos los accesos son autorizados.

23. ¿Cómo se controla el uso del correo electrónico y descarga de programas? (manejo de Internet).

En este punto se pretendía determinar si hay controles instalados tales como antivirus, control del Spam, control de descargas, todo esto para reducir los riesgos creados por el correo electrónico y descargas directas de zonas desconocidas o potencialmente riesgosas.

7.1.2 Encuesta para los Usuarios de Red

La encuesta dirigida fue elaborada con las siguientes preguntas:

1. ¿Conoce usted los riesgos y amenazas existentes en el manejo de la información en la red?

Al igual que en la pregunta a los Encargados de sistemas, se esperaba evaluar el conocimiento que poseen los Usuarios sobre las amenazas latentes en la Red.

2. ¿Sabe usted si existen políticas de seguridad informática implementadas en la Alcaldía de Santiago de Cali?

Con esta pregunta igualmente que en la encuesta de Encargados de Sistemas, se desea mostrar si los usuarios poseen algún conocimiento de políticas de seguridad informática implementadas en esta dependencia del Estado.

3. ¿Practica las políticas de seguridad?

Se esperaba saber si los Usuarios practican políticas de seguridad informática cuando manejan información en la Red.

4. ¿Informa usted a alguien sobre un fallo en los equipos si usted no puede solucionarlo? ¿A quien?

Al igual que en la encuesta a Encargados de Sistemas, se deseaba conocer el nivel de independencia que tienen los usuarios cuando sufren algún problema en su equipo o en la Red, y además conocer cual es su primera opción de consulta.

5. ¿Realiza mantenimiento de su equipo? ¿Con que frecuencia?

Los Usuarios finales deben realizar un manejo adecuado de los equipos a su cargo. Con esta pregunta se desea saber si en realidad los Usuarios dan

un buen manejo a su equipo, si este manejo es frecuente o esporádico, y además que nivel de acceso tienen al equipo.

6. ¿Permite que otras personas manipulen su equipo?

Esta pregunta sirve como medio de corroboración a la pregunta 11 de la encuesta de Encargados de Sistemas, porque nos muestra si en realidad los equipos son utilizados por las personas autorizadas o no.

7. ¿En su ambiente de trabajo conserva la mesa despejada y pantalla bloqueada para proteger la información de perdidas, daños o uso no autorizado?

Aquí se pretendía establecer el nivel de discreción que manejan los usuarios cuando se encuentran en su entorno de trabajo. Saber si permiten que otras personas tengan fácil acceso a la información que ellos manipulan.

8. ¿Sabe hacer copias de seguridad de la información importante? ¿Cómo?

A nivel de usuarios, esta pregunta muestra si existe capacitación para realizar copias de la información y el medio en el que las realizan. Evaluando de igual manera a los Encargados de Sistemas, si están dando capacitación a los Usuarios de su dependencia sobre estos temas.

9. ¿Tiene acceso a todo el nivel de seguridad los usuarios en su piso y controlan el uso a de la información a externos?

Esta pregunta sirve para evaluar el nivel de privilegios que manejan los usuarios cuando acceden a la información en la red, de esta pregunta se puede saber si los usuarios tienen acceso a información que no les compete.

10. ¿Existe un procedimiento para montar programas nuevos en los equipos? (licencias).

Otra pregunta de evaluación, diseñada para comprobar si los usuarios

conocen algún procedimiento para instalar nuevos programas.

11. ¿Tiene instalado en el computador programas que no competen a su labor en la Alcaldía?

Con esta pregunta se pretendía conocer si los usuarios manejan aplicaciones innecesarias en su labor, y comprobar si ellos pueden instalar algún programa sin permiso.

12. ¿Ejerce algún control para garantizar el buen uso de los equipos?

Al igual que en la encuesta de encargados, se deseaba conocer si los usuarios tiene el conocimiento suficiente para darle una buena manipulación a los equipos, y si además de cumplirlo, son también veedores de que sus compañeros lo cumplan.

13. ¿Cómo se mantiene la seguridad de su equipo?

Se quería establecer, a quien reconocen los usuarios como los encargados de la seguridad en su equipo y en la red.

14. ¿Sabe como crear y cambiar la contraseña de su equipo? ¿Con que frecuencia la cambia?

La intención de ésta pregunta es conocer, que tanto conocen de este tema los Usuarios, para realizar la sugerencia de capacitación dentro de las políticas de seguridad informática; en caso de ser necesario.

15. ¿Sabe que hacer al recibir un correo electrónico de origen desconocido?

Se pretende observar y evaluar el conocimiento de los Usuarios y si los Encargados realizan la labor de capacitación pertinente

.

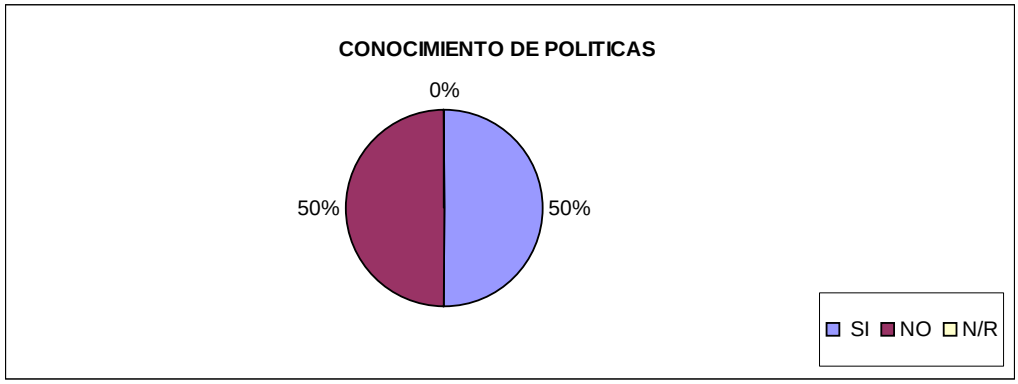
7.2 RESULTADOS DE LAS ENCUESTAS PARA ENCARGADOS DE SISTEMAS Y USUARIOS DE RED

7.2.1 Resultados en la Encuesta para Encargados de Red

Figura 2. Pregunta 1-Riesgos y amenazas

El 100% de los encuestados manifestó conocer los riesgos que se pueden presentar tanto a nivel de software como a nivel de hardware, y como prevenirlos.

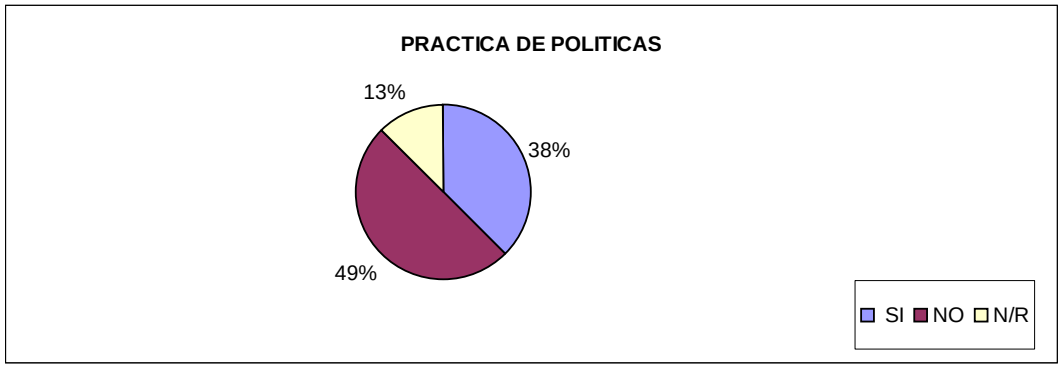
(a) Figura 3. Pregunta 2-Conocimiento de políticas



Ante esta pregunta el 50% de los encuestados manifestó conocer unas políticas de seguridad, mientras que el otro 50% reconoce que no sabe si existen; cabe

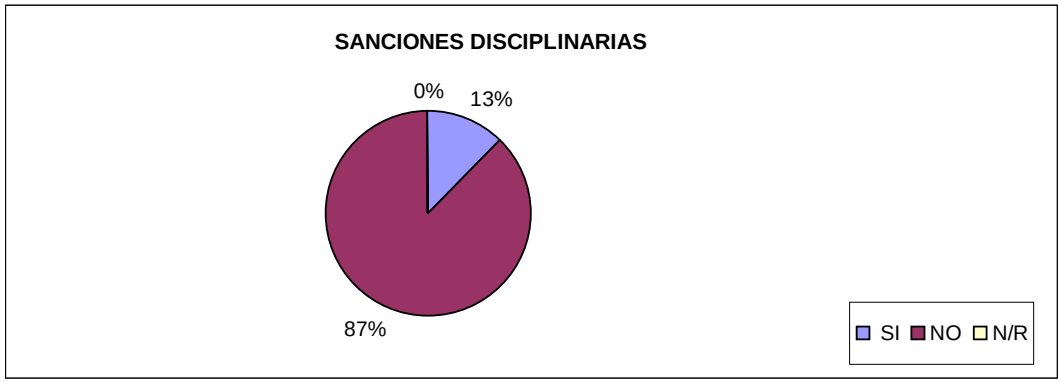
anotar que en algunos casos se relacionó políticas de seguridad informáticas con protección contra virus únicamente.

(b) Figura 4. Pregunta 3-Práctica de políticas



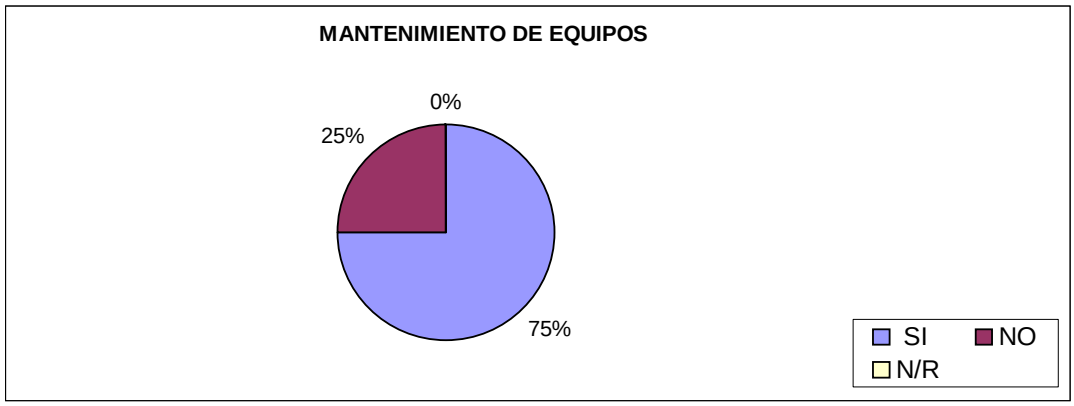
Los datos obtenidos fueron: El 37.5% dice practicar políticas de seguridad, el 50% definitivamente no tiene conocimiento de éstas políticas y el 12.5% no respondió si lo hace o no.

(c) Figura 5. Pregunta 4-Sanciones disciplinarias



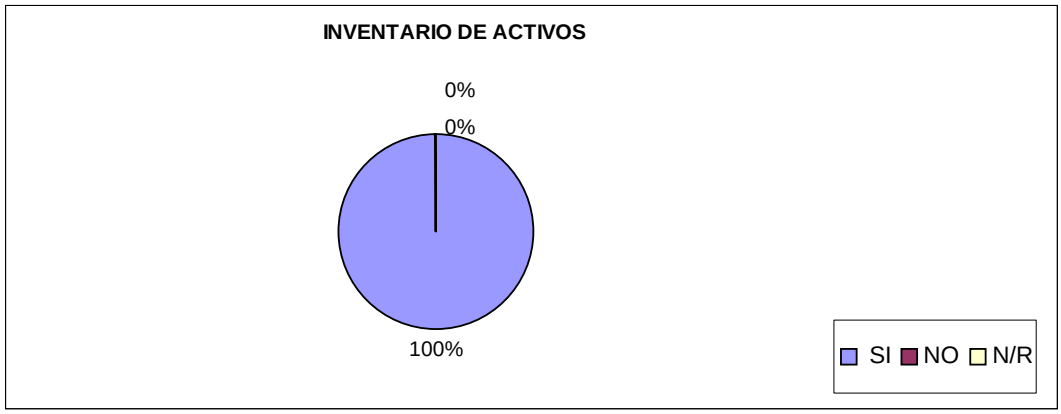
El 12.5% de los encargados, manifestaron que si hay algún tipo de sanción relacionada con estas faltas, mientras que el 87.5% reconoce que no hay ningún tipo de sanción.

(d) Figura 6. Pregunta 5-Mantenimiento de equipos



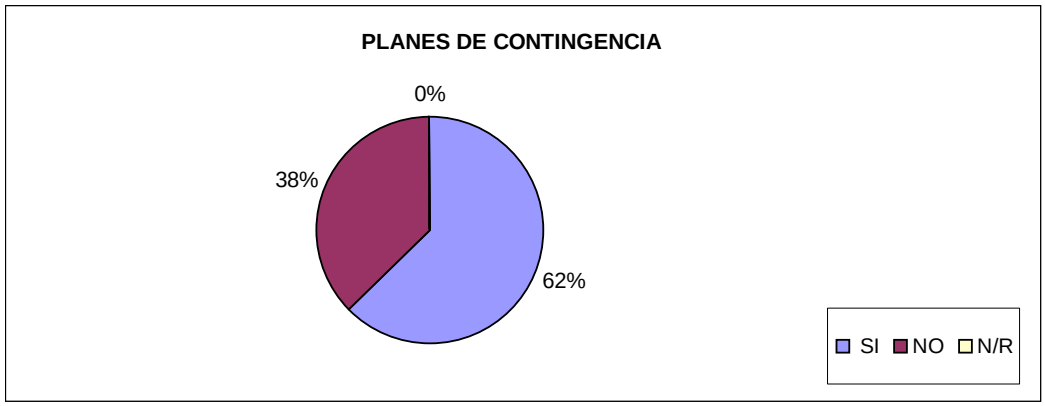
Con respecto a este interrogante, se encontró que el 75% de los encargados realiza mantenimiento en los equipos y el 25% no lo hace; aún cuando manifestaron conocer los riesgos a que puede estar expuesta la información en la red.

(e) Figura 7. Pregunta 6-Inventario de activos



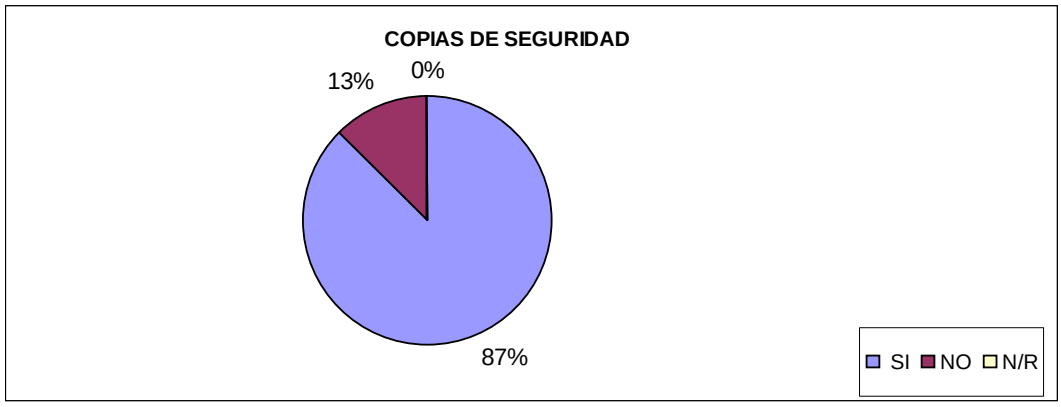
La respuesta que se obtuvo fue del 100%, indicando que sí se tiene registrada la información en cuanto al manejo de activos.

(f) Figura 8. Pregunta 7-Planes de contingencia



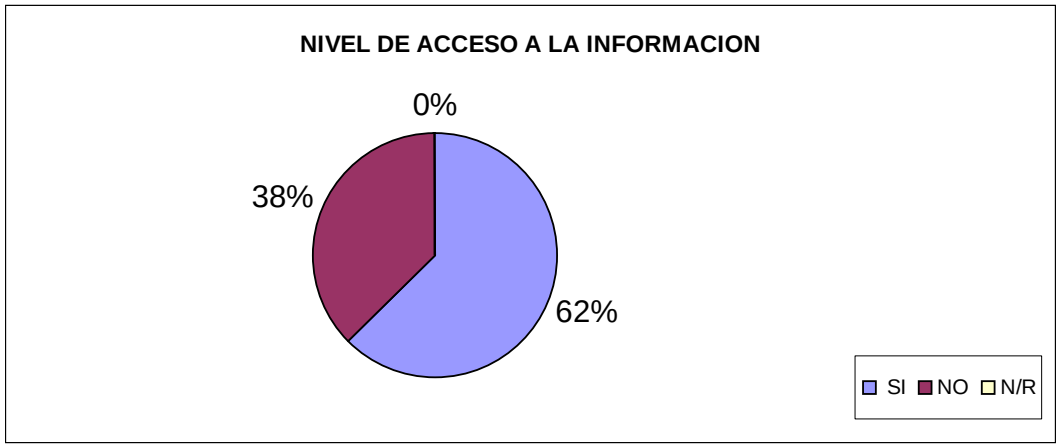
Al analizar esta respuesta se encontró que el 62.5% manifestó tener planes alternativos en caso de fallas; mientras el otro 37.5% no los tiene.

(g) Figura 9. Pregunta 8-Copias de seguridad



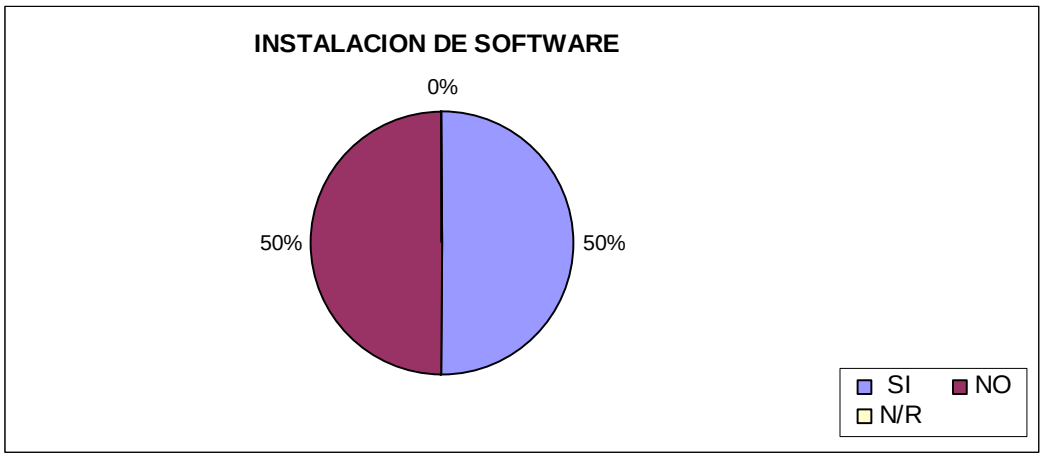
El 87.5% de los encuestados respondió que sí realiza las copias de seguridad, haciendo uso de diferentes medios, el 12.5% manifestó no realizar las copias.

(h) Figura 10. Pregunta 9-Nivel de acceso a la información



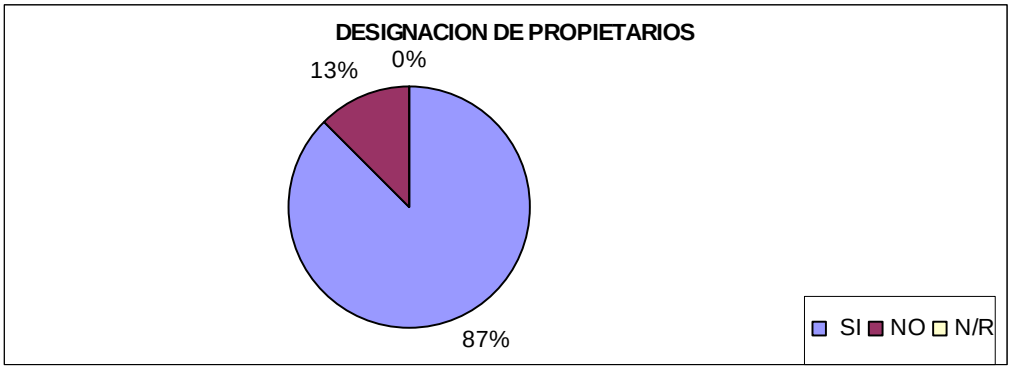
El 62.5% de los encargados de sistemas respondió que tiene total acceso a la red, el 37.5% dijo que tiene acceso restringido a la información y niveles de red.

(i) Figura 11. Pregunta 10-Instalación de software



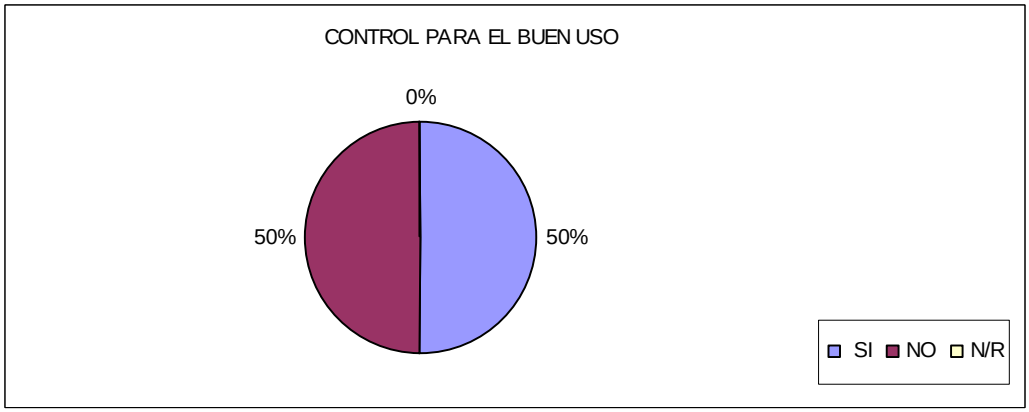
Como resultado se obtuvo que el 50% de los administradores de red manifestó tener inventario de software y procedimientos específicos para instalarlos, mientras el 50% dijo no tener inventario de software ni un procedimiento determinado para la instalación de los mismos.

(j) Figura 12. Pregunta 11-Designación de propietarios



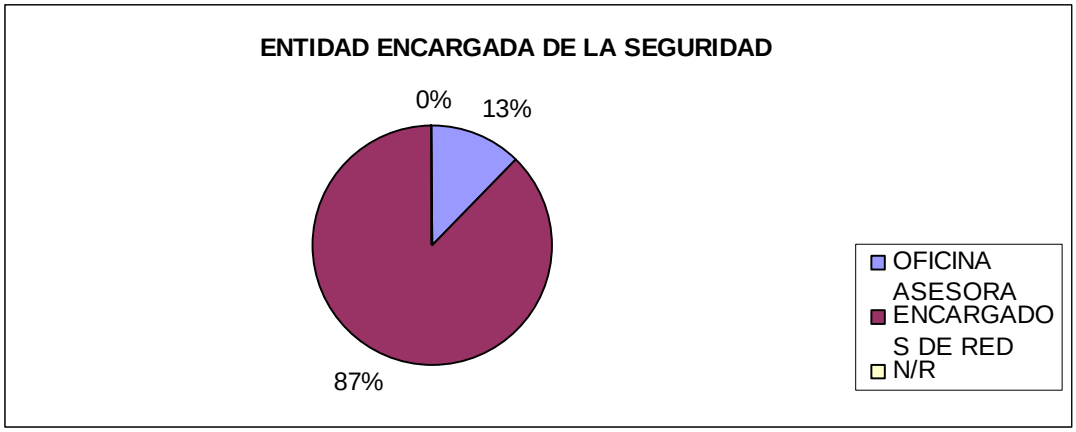
El 87.5% de los encargados autoriza el uso de un equipo a uno o varios usuarios, mientras que el 12.5% no posee implementada esta reglamentación.

(k) Figura 13. Pregunta 12-Control para el buen uso



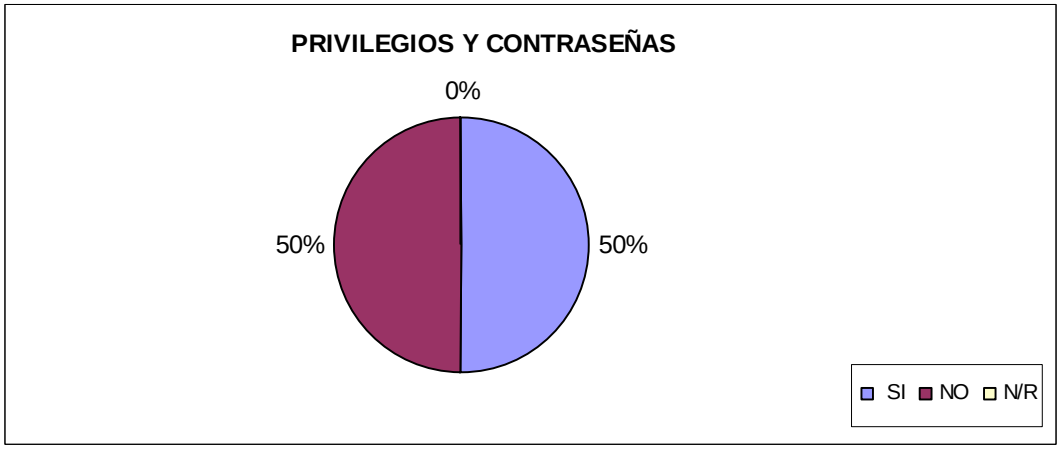
El resultado que arrojó esta pregunta fue que el 50% ha intentado ejercer algún tipo de control, por ejemplo en algunos pisos se realiza capacitación o se da a conocer ciertas pautas. El otro 50% no ejerce control debido a que no se han implementado las políticas de seguridad o por que están en proceso de implementar los controles que consideran necesarios.

(l) Figura 14. Pregunta 13-Entidad encargada de la seguridad



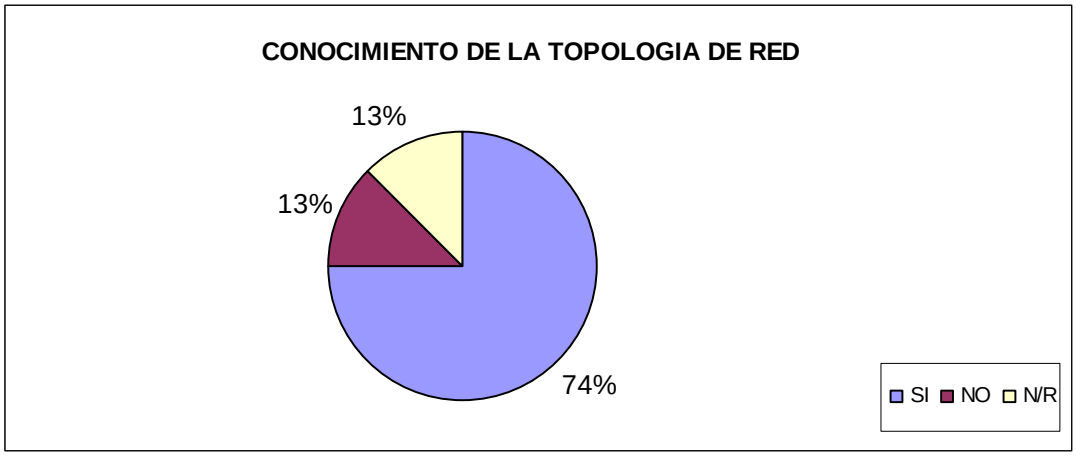
Con esta pregunta se conoció que el 12.5% de los pisos esta a cargo de Informática y Telemática; mientras que el 87.5% tiene su propio encargado de sistemas.

(m) Figura 15. Pregunta 14-Privilegios y Contraseñas



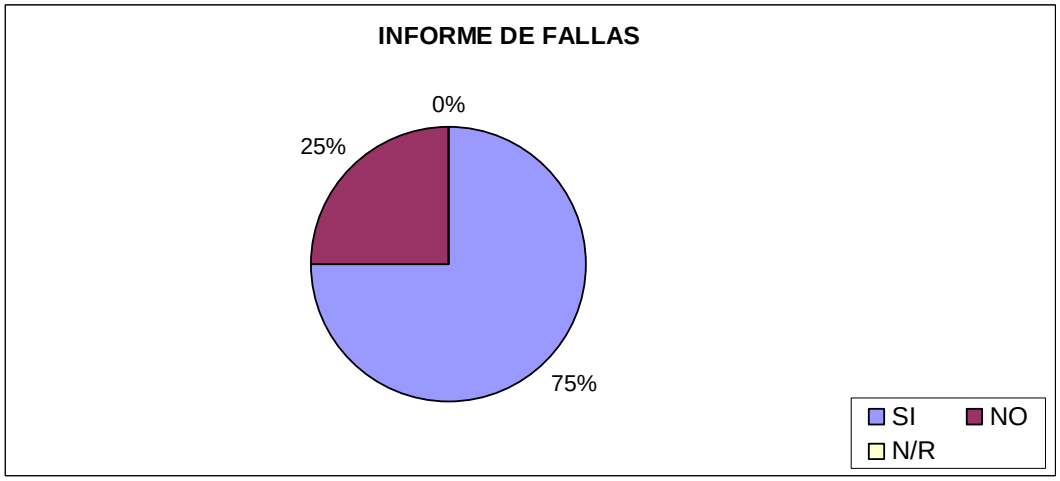
Con esta pregunta se encontró que el 50% restringe el acceso de los usuarios a lugares no autorizados, mientras que otro 50% no lo hace.

(n) Figura 16. Pregunta 15-Conocimiento de topología de red



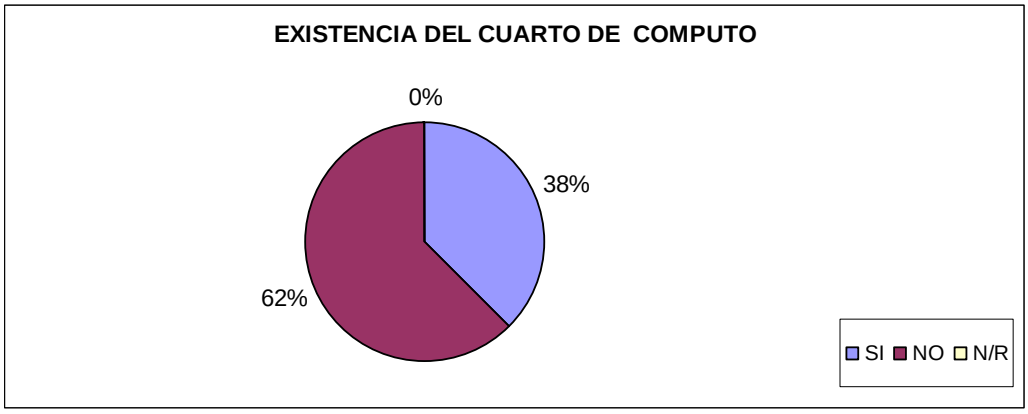
El 75% de los encargados de piso conocen la topología de red, el 12.5% no la conocen, y el 16.67% no respondió, por lo cual se asume que el 29.17% de los encargados de piso desconocen que es lo que tiene a su cargo.

(o) Figura 17. Pregunta 16-Informe de fallas



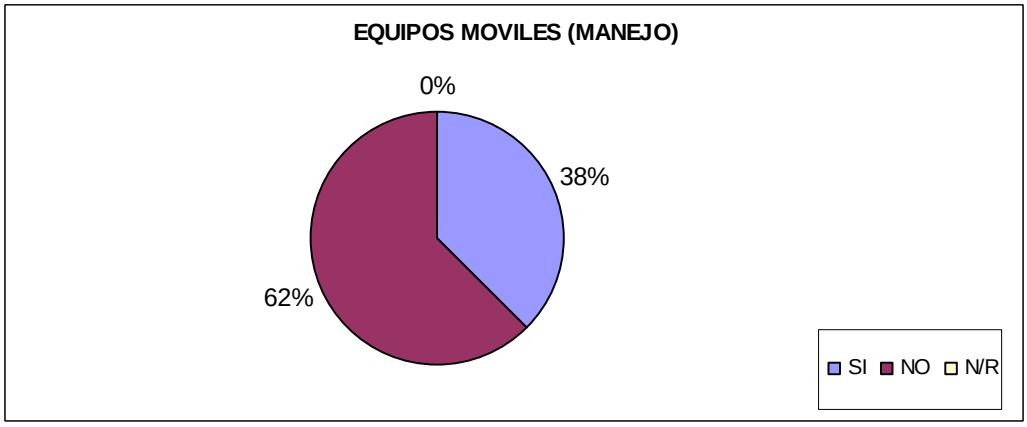
Se encontró con la respuesta que el 75% de los encargados de piso se apoya en Informática y Telemática, mientras que el 25% trata siempre de resolver ellos mismos los inconvenientes que se presentan.

(p) Figura 18. Pregunta 17-Existencia del cuarto de cómputo



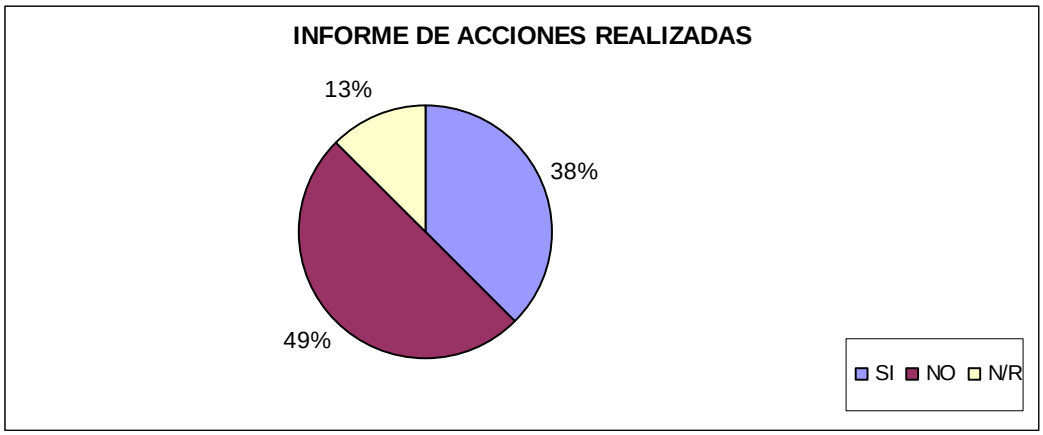
El resultado arrojo que en el 37.5% de los pisos se encuentra en un nivel optimo el área de funcionamiento de los equipos activos de la red, mientras que el 62.5% de los pisos adolece de las condiciones mínimas de funcionamiento.

(q) Figura 19. Pregunta 18-Manejo de equipos móviles



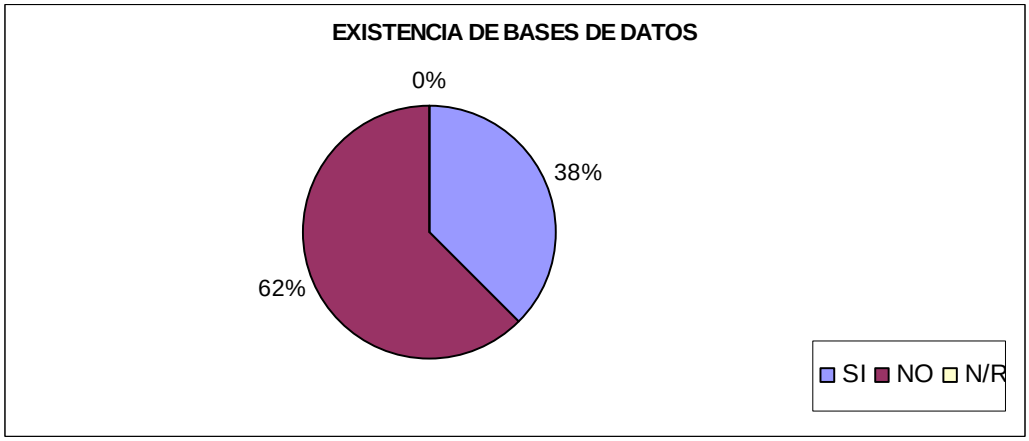
Con esta pregunta se obtuvo que el 37.5% de los encargados de piso ejercen algún control al respecto, y el 62.5% no lo hace.

(r) Figura 20. Pregunta 19-Informe de acciones realizadas



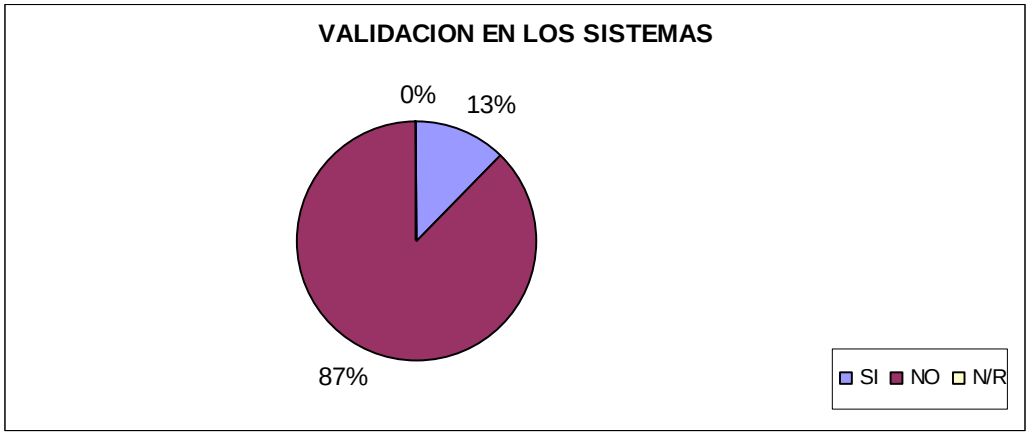
El 37.5% de los encargados de piso respondió que si genera este tipo de reporte, el 50% no lo hace y el 12.5% no respondió; por lo que se puede decir que el 37.5% de los encargados de piso genera el reporte y el otro 62.5% no lo hace.

(s) Figura 21. Pregunta 20-Existencia de bases de datos



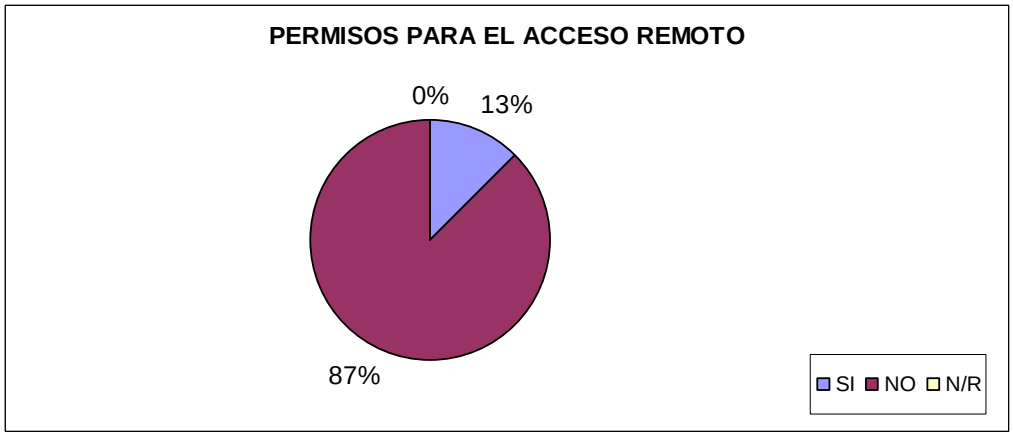
A esta pregunta el 37.5% de los encargados de piso manifestó tener esta base de datos, el 62.5% dijo que no la ha creado.

(t) Figura 22. Pregunta 21-Validación en los sistemas



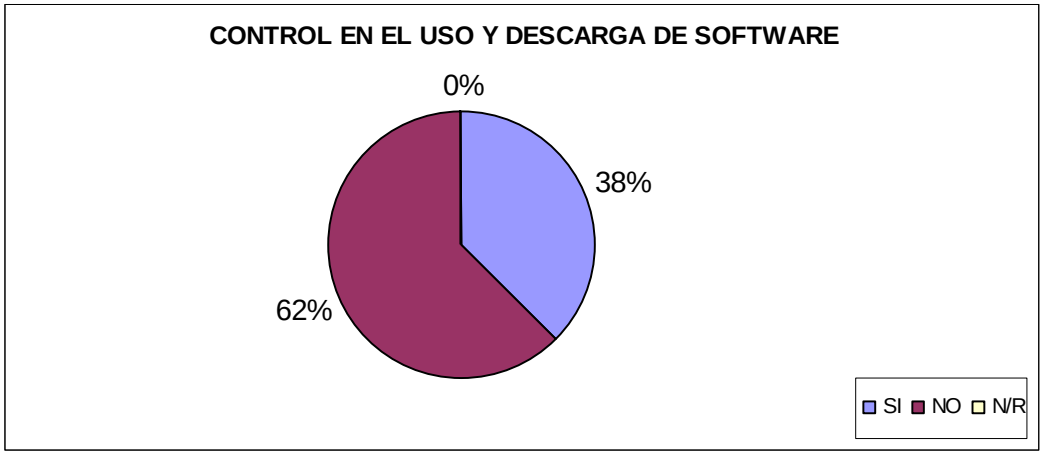
A esta pregunta el 87.5% de los encargados manifestó que no realiza chequeo de validación, mientras que el 12.5% respondió que si tiene algún tipo de validación; lo que implica que el nivel de seguridad es muy deficiente en cuanto a autenticación de datos.

(u) Figura 23. Pregunta 22-Permisos para el acceso remoto



El 12.5% dicen que el acceso remoto esta permitido y el 87.5% dicen que el acceso remoto no es permitido en su dependencia.

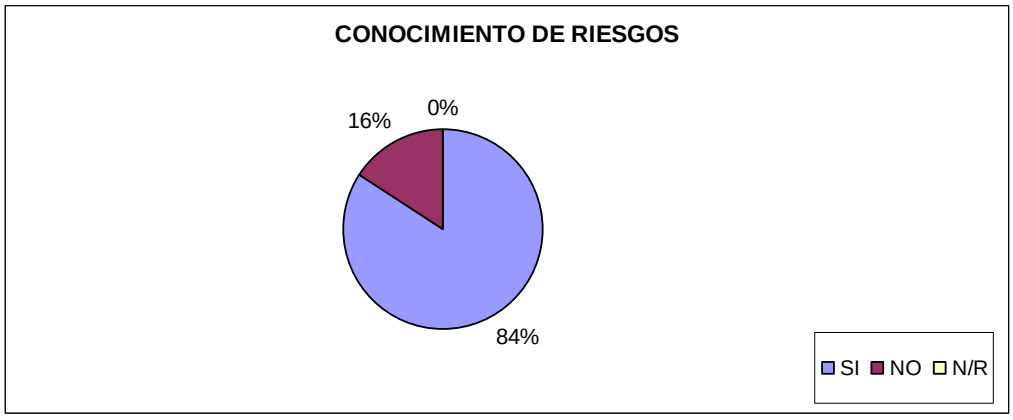
(v) Figura 24. Pregunta 23-Control en el uso y descarga de software



El 37.5% de los encargados de piso respondió que el acceso a Internet se controla normalmente por contraseñas. Mientras que el 62.5% respondió que no hace ningún control, cabe anotar que en algunos pisos se encuentran casos en los que no hay acceso a Internet en ciertos equipos.

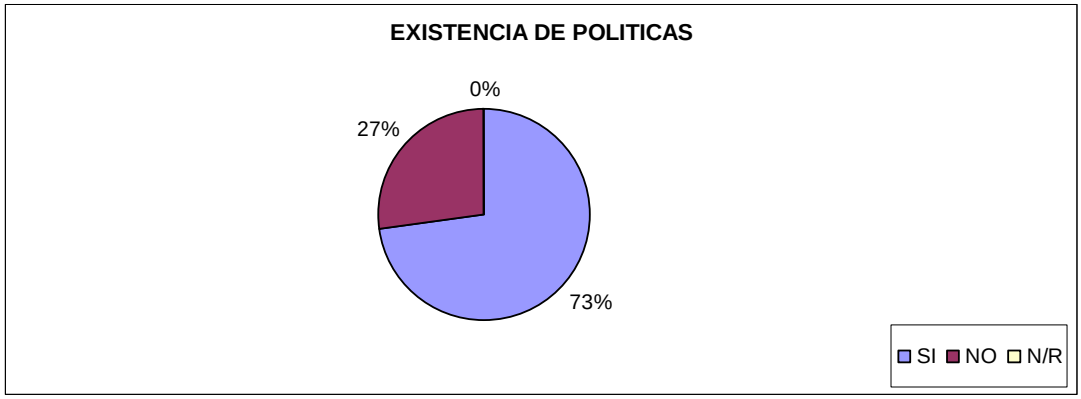
7.2.2 Resultados en la Encuesta para Usuarios de Red

(w) Figura 25. Pregunta 1-Conocimiento de riesgos



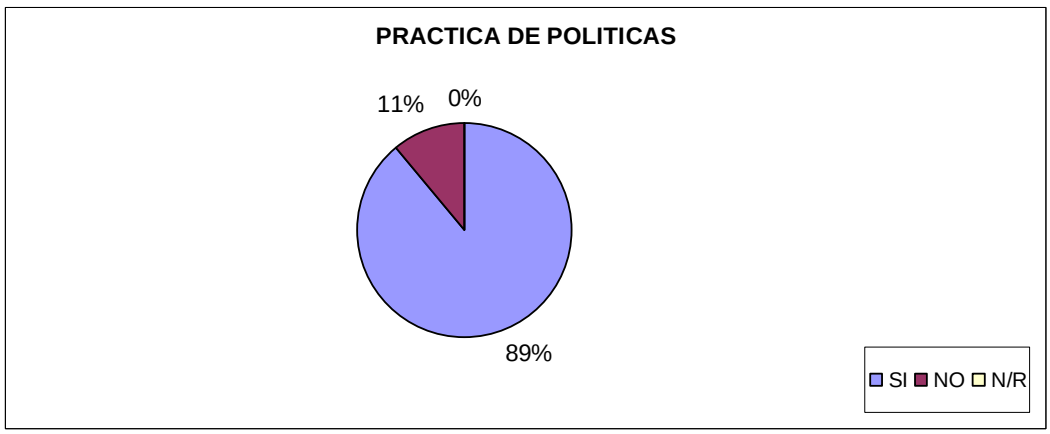
En la figura 24 se puede apreciar que, del total de encuestados el 84% contesto conocer los riesgos existen en la red a la hora de manipular información, aunque la mayoría solo reconozca los virus como riesgos, el 16% restante no conoce sobre riesgos y amenazas

(i) **Figura 26.** Pregunta 2-Existencia de políticas



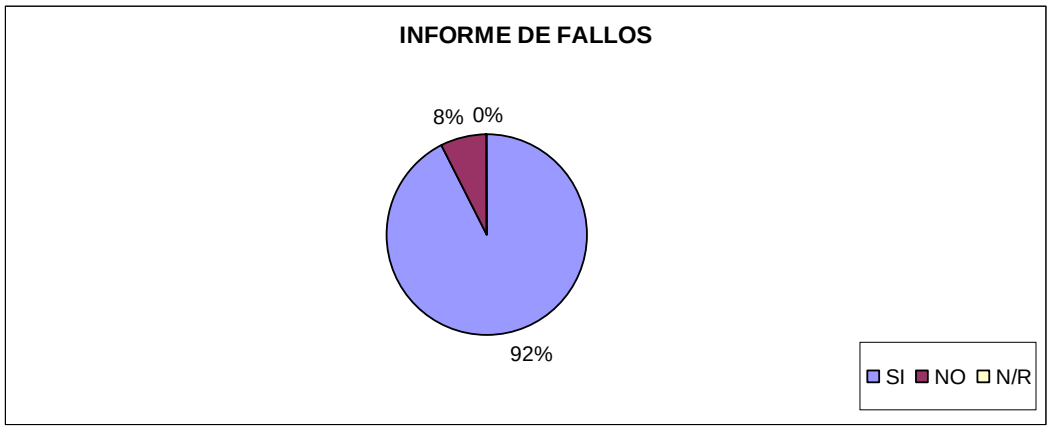
Ante esta pregunta el 73% de los encuestados manifestó conocer políticas de seguridad en la Alcaldía o ha escuchado al respecto, mientras que el otro 27% indica que no sabe si existen estas políticas; igualmente que la encuesta de encargados se relaciono políticas de seguridad con protección contra virus.

Figura 27. Pregunta 3-Práctica de políticas



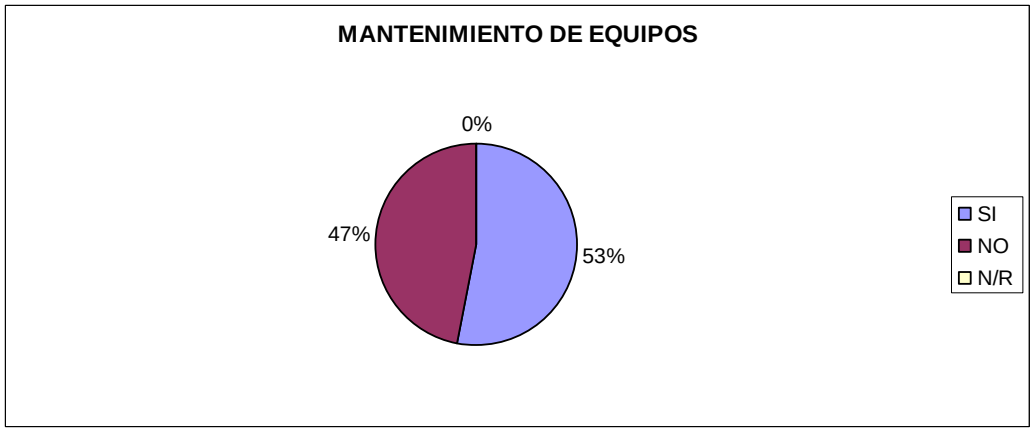
Para la figura 26, los datos obtenidos fueron: El 89% informan poner en práctica políticas de seguridad, en cambio el 11% definitivamente no tiene conocimiento de políticas de seguridad ni siquiera practican algún tipo.

Figura 28. Pregunta 4-Informe de fallos



A esta pregunta, el 92% respondió informar inmediatamente a algún encargado o a la oficina de Informática y Telemática sobre algún fallo, mientras que el 8% no lo hace, observando una falta de comunicación en estas personas.

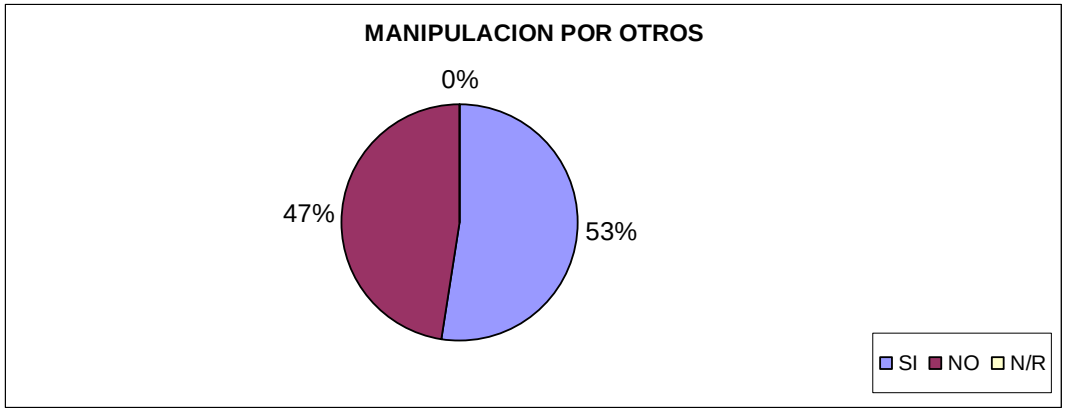
Figura 29. Pregunta 5-Mantenimiento de equipos



Al revisar la respuesta obtenida se encontró que el 53% de usuarios se realiza un mantenimiento (limpieza exterior, borrar información necesaria) en su equipo, por

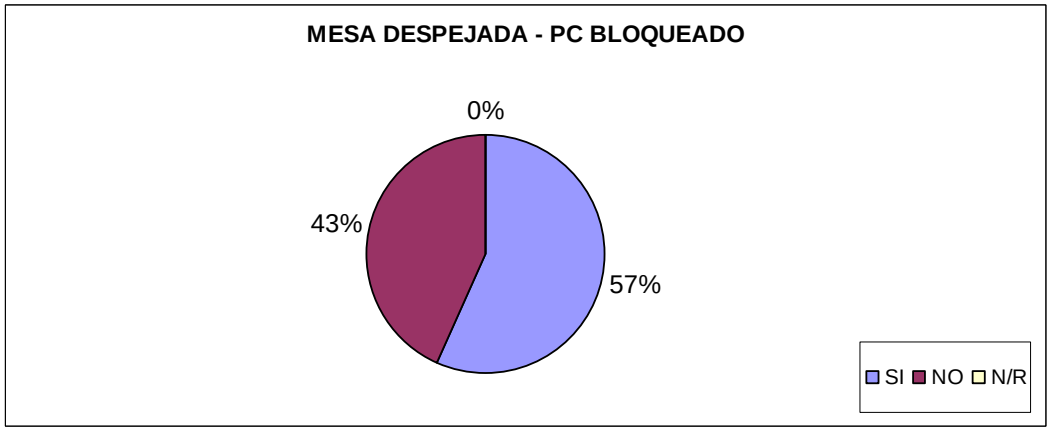
otro lado el 47% no lo hace; dando como razón que los equipos son alquilados por empresas externas.

Figura 30. Pregunta 6-Manipulación por otros usuarios



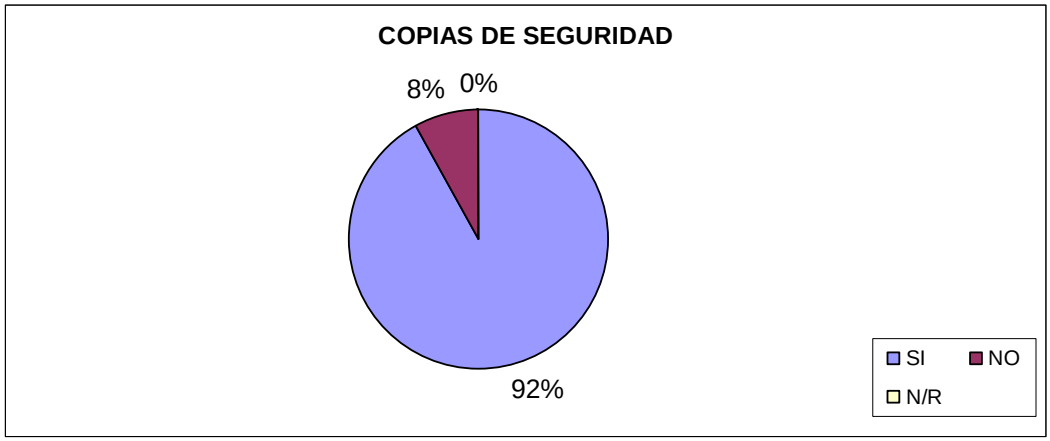
Al igual que en la pregunta anterior se observa que el 53% de los usuarios permiten que otras personas manipulen su equipo, argumentado que como hay poco equipo toca prestarlo, en cambio el 47% indican que no lo permiten.

Figura 31. Pregunta 7-Mesa despejada-PC bloqueado



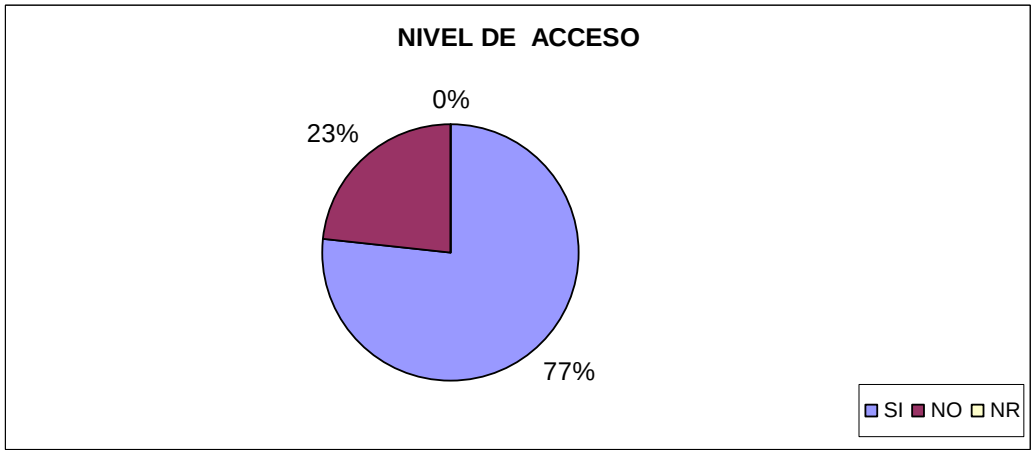
A esta pregunta el 57% informa que mantiene el escritorio despejado y el computador bloqueado con contraseña para evitar perdidas de información, en cambio el 47% no lo realiza.

Figura 32. Pregunta 8-Copias de seguridad



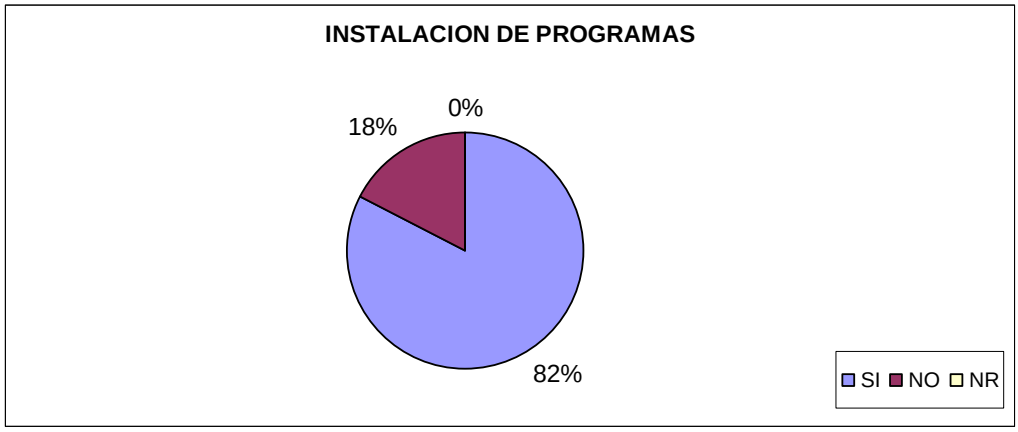
El 92% de los usuarios encuestados respondió que sí realiza las copias de seguridad en algún tipo de medio, comúnmente en CD, el 12.5% manifestó no realizar las copias y no sabe.

Figura 33. Pregunta 9-Nivel de acceso



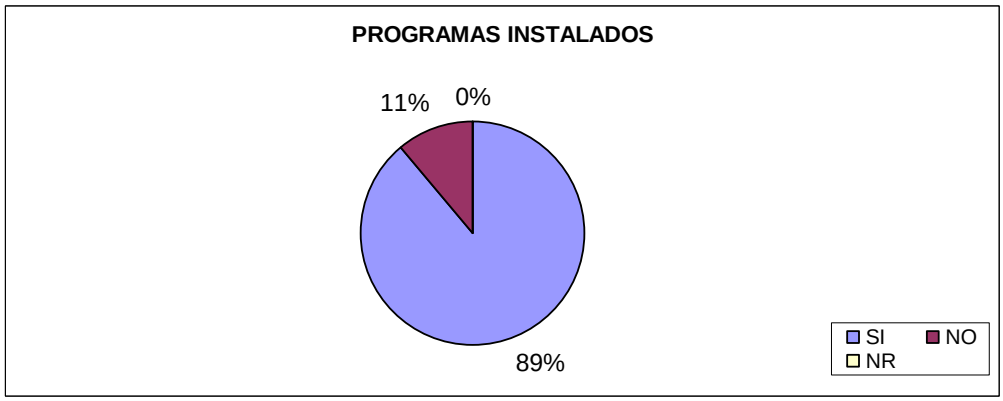
El 77% de los usuarios respondió que tiene total acceso a la red y a los equipos que la componen, por otro lado el 23% dijo que tiene acceso restringido a la información y niveles de red, todo manejado a través de contraseñas.

Figura 34. Pregunta 10-Instalación de programas



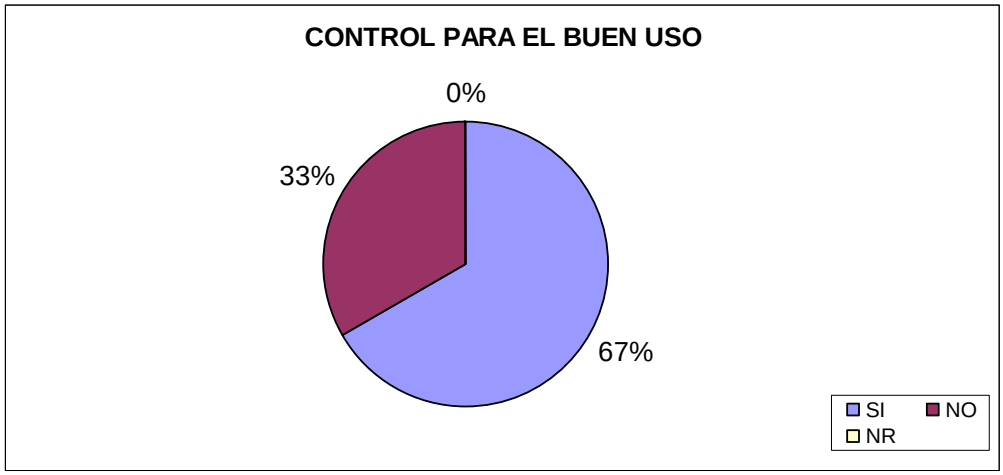
Como resultado se obtuvo que el 82% de los usuarios manifiesta que conocen o manejan algún tipo de procedimiento de instalación de programas y licenciamiento, mientras el 18% restante manifestó que no conoce procedimiento alguno.

Figura 35. Pregunta 11-Programas instalados



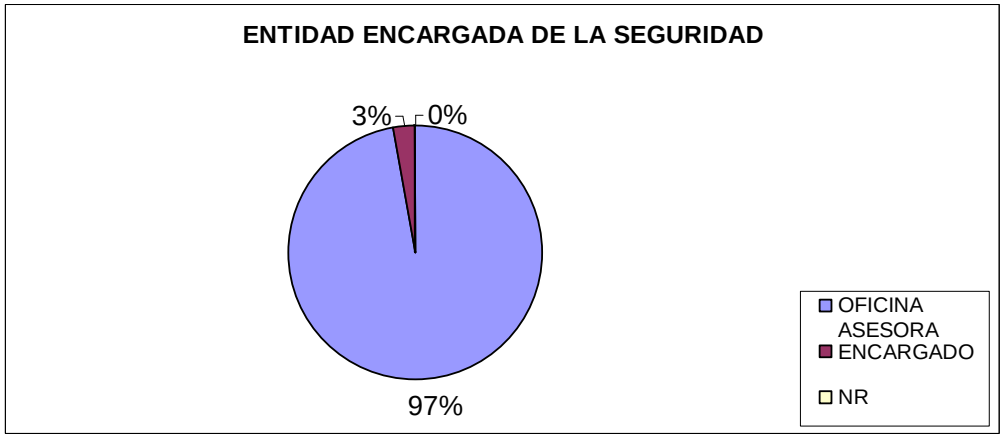
El 89% de los usuarios indicaron que no posee aplicaciones ajenas a su labor en la Alcaldía, indicando que si los encargados no lo autorizan, no se puede instalar nada, en cambio el 11% informan tener aplicaciones como reproductores de música, video, juegos, aplicaciones de mensajería instantánea.

Figura 36. Pregunta 12-Control para el buen uso



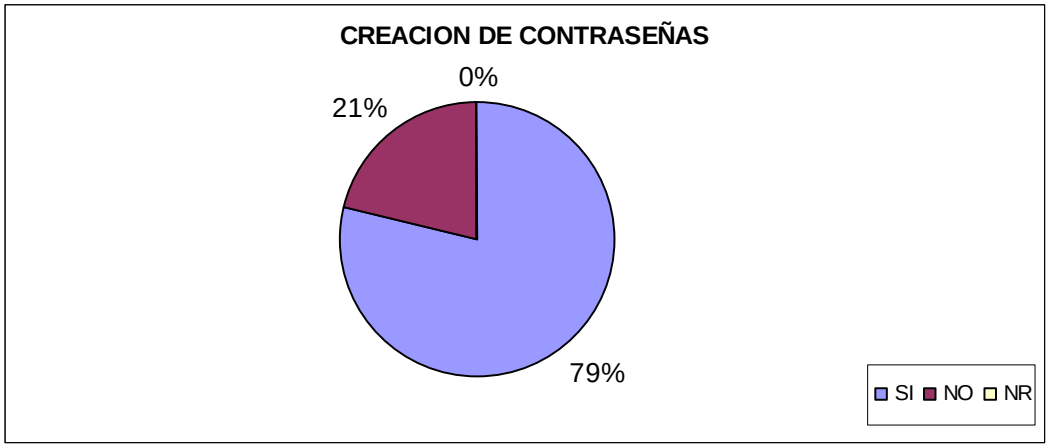
Esta pegunta arrojo como resultado que el 67% realiza algún tipo de control para mantener en buen estado el equipo que se encuentra bajo su responsabilidad, el 33% informa que no realiza ningún tipo de control.

Figura 37. Pregunta 13-Entidad encargada de la seguridad



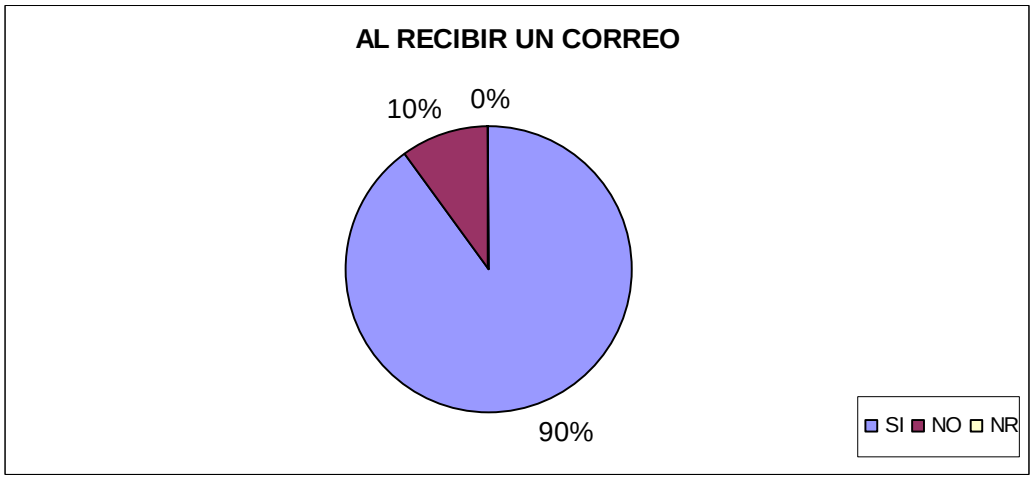
Con esta pregunta se identifico a la Oficina Asesora de Informática y Telemática como entidad encargada de la seguridad en la red con un 97% de reconocimiento por parte de los usuarios, y que el 3% de los usuarios reconocen a los encargados de cada piso como encargados de la seguridad en la red.

Figura 38. Pregunta 14-Creación de contraseñas



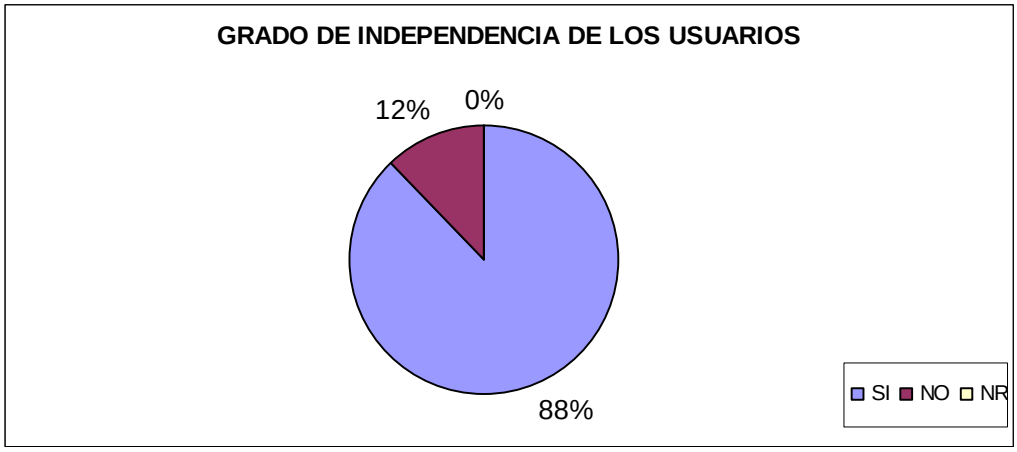
Con esta pregunta se observo que el 79% de los usuarios sabe cambiar y crear la contraseña de su equipo, cambiándola periódicamente, el 21% restante de usuarios no lo sabe hacer.

Figura 39. Pregunta 15 -Al recibir un correo



El 90% de los usuarios informo realizar dos procedimiento al recibir un correo de origen desconocido, primero no abrirlo y segundo eliminarlo inmediatamente, el 10% restante informo no conocer ningún procedimiento a realizar ante este evento.

Figura 40. Pregunta 16-Grado de dependencia de los usuarios



Con esta pregunta se observa que el 88% de los usuarios informa primero al encargado o a soporte técnico en la oficina Asesora de Informática y Telemática ante un problema en el equipo o en la red, por otro lado el 12% de usuarios indico que primero tratan de solucionarlo.

Ficha técnica:

La encuesta se realizó a 14 Encargados de Sistemas, debido a que no se pudo tener contacto con Liliam Barrera encargada de los pisos 10 y 11. Por parte de los Usuarios de Red se encuesto a 319 personas.

7.3 ANÁLISIS DE LA INFORMACIÓN RECOLECTADA

Con la información recopilada se evaluó que tan alejada de la norma ISO 17799, se encuentra actualmente la red de telecomunicaciones de la Alcaldía de Santiago de Cali; con lo cual se realizó el documento de políticas de seguridad informática, corrigiendo las fallas encontradas (dentro de lo posible) y, finalmente se realizó el proceso de difusión y aplicación este documento en la Institución.

Tabla 2. Problemas y Recomendaciones (Encargados de red)

PROBLEMAS ENCONTRADOS	RECOMENDACIONES
Encargados de Sistemas:	
Desconocimiento por parte de algunos encargados de la existencia de un documento de políticas	Se hace imprescindible la completa difusión del documento de políticas aprobado.
Falta de sanciones para el comportamiento inadecuado de los usuarios.	Reglamentar sanciones para el comportamiento inadecuado.
La continuidad de la organización corre un riesgo muy alto debido a que algunos encargados de piso no tienen planes de contingencia para garantizar la continuidad del negocio.	Es necesario determinar en las políticas de seguridad informática, cual es el procedimiento a seguir cuando se presentan inconvenientes de tipo físico y/o lógico.
La mayoría de los Encargados de Red poseen acceso a altos niveles de seguridad.	Es importante solo dar privilegios de cuentas de acuerdo a los servicios que se requieran y a la información que se necesite.
No existen procedimientos dedicados al manejo y montaje de software por que no hay administración de sesión por parte de los Encargados de Red.	– Se debe dar acceso a cuentas controladas a los Usuarios y que solo los encargados tengan los privilegios para instalar el software específico para cada Usuario. – Debe haber un procedimiento relacionado al manejo de software libre y licenciado que garantice unos niveles óptimos, respecto a los aspectos legales.
Los Encargados de Red permiten el libre acceso de varios Usuarios a un mismo equipo, dificultando un seguimiento a los que se encuentran trabajando y a los usuarios que están accediendo.	Se debe instalar un software para seguimiento de usuarios y administración de sesiones.
Desconocimiento del tipo de red a su cargo, por parte de algunos Encargados de Red.	Capacitación a los Encargados de Red sobre la conformación de las dependencias, distribución estructural y tipo de red.
Se ejerce poco control al uso de equipos móviles en cuanto al ingreso en la red.	Se debe informar a los Encargados de Red a cerca de la importancia de ejercer control sobre este tipo de equipos.
No se maneja en la mayoría de las dependencias de la Alcaldía una documentación detallada de los informes de fallas ni las operaciones de mantenimiento realizada a los equipos.	Unificar el comportamiento de las dependencias en cuanto al manejo de los informes de fallas, y la creación de bases de datos que contenga las acciones realizadas de acuerdo a los problemas encontrados.
La mayoría de los Encargados de Red no controla el acceso a Internet.	Indicar a los Encargados de Red, la importancia de que los Usuarios se conecten a Internet con ciertas restricciones y medidas de seguridad.

Tabla 3. Problemas y recomendaciones (Usuarios de red)

PROBLEMAS ENCONTRADOS	**RECOMENDACIONES**
Usuarios de Red:	
Desinformación en cuanto a riesgos, amenazas y políticas de seguridad informática. Lo que genera una falta de prácticas de las mismas.	Difusión de normas de seguridad informática por parte de la Asesoría de informática y telemática.
Falta de comunicación entre Usuarios y Encargados de Red, a la hora de informar fallas en los equipos.	Estimular la cultura para solicitar ayuda en caso de tener fallos en los equipos.
Los Usuarios no realizan el mantenimiento básico en los computadores por desconocimiento.	Capacitar en cuanto al uso y mantenimiento diario de los computadores.
Falta de equipos, varios Usuarios utilizan un mismo equipo. De esta manera no se puede garantizar un buen uso de los computadores, ni la confidencialidad de los datos.	Teniendo en cuenta insuficiencia presupuestal en la entidad. Se deben habilitar varias sesiones por equipo, de acuerdo a la cantidad de personas que lo utilizan.
Los Usuarios dejan sus sesiones abiertas cuando ellos no están. Cualquier infiltrado puede obtener información.	Se debe implementar una política de sesión que bloquee automáticamente los equipos cuando transcurra un tiempo sin ser usados.
Algunos Usuarios no realizan copias de seguridad de la información importante, por que no saben como hacerlo o no lo consideran necesario	Para garantizar la confidencialidad en la información y evitar daños en la misma, se debe capacitar a los Usuarios en este aspecto.
Un gran porcentaje de usuarios no garantizan el buen uso de los equipos.	Se debe crear la cultura necesaria para que los Usuarios conozcan el funcionamiento básico de los computadores y sus programas.
Los Usuarios no consideran necesario el uso de contraseñas, ya que según ellos toda la información que manejan es de dominio público “no hay nada que esconder”.	Crear conciencia en los usuarios a cerca de la importancia del manejo de sesiones y el uso de contraseñas. Capacitar a los Usuarios sobre como crear y cambiar la contraseña.

7.4 AUDITORIA INFORMÁTICA.

Esta etapa del trabajo consistió en la revisión de la vulnerabilidad de la red tanto externa como interna. Para realizar esta auditoria se redacto una guía en la que se describe el procedimiento de las pruebas que se realizaron a los servicios de correo, FTP, y Web, montados en la plataforma Linux/Unix.

7.4.1 ¿Qué son las vulnerabilidades?. Las vulnerabilidades de un sistema surgen a partir de errores individuales en un componente, sin embargo nuevas y complejas vulnerabilidades surgen de la interacción entre varios componentes como el kernel del sistema, sistemas de archivos, servidores de procesos, entre otros. Estas vulnerabilidades generan problemas de seguridad para la red en cuestión. Entre las vulnerabilidades más conocidas se encuentran el “finger username” y la notificación de mensajes de correo a través de “comsat”. Para el primero, la vulnerabilidad es originada en la interacción entre el servidor fingerprint y la forma en que el sistema de archivos representa los links para acceder al directorio raíz de username. En el segundo caso, el programa comsat supone que etc/utmp es correcto, el sistema de archivos configura este archivo para otorgar permisos y el programa de correo asume que todo esta correcto.

Por otra parte, existen diversas formas de realizar auditorias de seguridad apoyadas en las herramientas determinadas para tal fin. Estas herramientas que detectan fallas de seguridad pueden ser utilizadas de dos formas diferentes: interna o externamente a la máquina que se analiza. Cuando se aplican internamente, se realiza la auditoría desde el interior de la máquina a analizar (generalmente utilizando la cuenta de Administrador), lo que otorga numerosas ventajas para la detección de vulnerabilidades ya que se tiene acceso a los archivos críticos del sistema. En el caso de las auditorias externas, la detección de

vulnerabilidades se realiza desde una máquina diferente a la que está siendo analizada. En este tipo de auditorias, se realizan ataques para verificar la existencia de vulnerabilidades. De la variedad y cantidad de ataques que alguna de estas herramientas sea capaz de realizar, dependerá, en gran parte, el éxito en la detección de vulnerabilidades. Aunque este factor es, probablemente, el más importante, conviene considerar otros aspectos como por ejemplo la forma de realizar los ataques. Cabe anotar que las herramientas descritas en este documento realizan un análisis de debilidades externas del sistema; presentando, tal vez, el punto de vista más realista para analizar vulnerabilidades, ya que asumen el papel de Hacker externo que pretende comprometer una máquina a través de la red.

En la auditoria se utilizaron 3 analizadores de vulnerabilidades con distintas características y se detallarán sus características y su funcionamiento.

7.4.2 Herramientas De Análisis. Para realizar una valoración de equipos que administran la red y los servicios que brinda la Alcaldía de Santiago de Cali, fue necesario hacer pruebas y análisis de vulnerabilidades desde el interior y el exterior de la red, utilizando un equipo de computo portátil.

En la realización de la valoración se utilizaron algunas herramientas que se pueden descargar desde Internet, tanto en versiones gratuitas como de prueba. Herramientas tales como:

- Caín y Abel v2.67 (versión gratuita).
- Nessus 2.0.10 (Versión gratuita)
- S.A.T.A.N (Versión de prueba)

- Putty (versión libre)
- GFi Languard Security Network (versión de prueba).
- NStealth (versión de prueba).
- Shadow Secure Scanner (versión prueba).
- Atelier Web Commander Remote v5.35 (versión de prueba).
- John the Ripper (versión gratuita).
- Netcat (version gratuita)

Y del sistema operativo en uso, la utilización de comandos propios como ping, telnet, arp –a.

7.4.2.1 Evaluación Interna. Seguido del procedimiento de evaluación de políticas de seguridad realizada a nivel de usuarios de sistemas y encargados de red, se realizo la valoración de los equipos y servicios prestados por estos en la red. La Alcaldía cuenta con servidores de correo, Web, FTP, datos (contratación). Para evaluar estos equipos fue necesaria la utilización de algunas herramientas de escaneo, interceptación y control, las herramientas utilizadas fueron:

- Para escaneo: Caín y Abel, Shadow, Ip scanner, GFI, Nstealth.
- Para interceptación: Caín y Abel, Ethereal, Netcat.
- Para control: Netcat, Atelier Web commander
- Para descifrar password: Caín y Abel, John ripper.

Las herramientas mencionadas anteriormente fueron seleccionadas por su popularidad en la Internet, su fácil uso, distribución gratuita o versiones de prueba; entre estas herramientas se conoció la existencia de otras como Nessus, SATAN, y Putty, que aunque no se utilizaron en este proyecto, pueden ser muy útiles a la hora de realizar una auditoria informática.

Para la evaluación de equipos y servicios, primero se realizo una revisión por medio de escaneo de puertos para conocer cuales se encontraban a la escucha de peticiones (Abiertos), con los resultados obtenidos se pudo deducir cuales son los servicios que provee la Alcaldía y dónde están ubicados, a nivel de LAN, se utilizó el Caín y Abel, el cual nos arroja los equipos y los dominios de colisión existentes en la Alcaldía.

A nivel externo, herramientas como el Shadow, el GFi, Ip scanner, y el Netcat proporcionaron los puertos que se observan abiertos desde Internet y el rango de las direcciones que se manejan en la institución.

Luego del escaneo se utilizó un sniffer en la red para observar el tráfico interno y recopilar la información suficiente para conocer nombres de cuentas, passwords, en este punto el Caín y Abel fue de vital importancia porque gracias a que cuenta con la capacidad de capturar hashes, se pudo desencriptar las claves de algunos usuarios, como se pudo hacer en el caso del Administrador Web quien tiene por clave “caramba”. A nivel externo se utilizaron las herramientas Shadow, Nstealth, y GFI, que son herramientas para la realización de auditorias informáticas.

Estas herramientas arrojaron los resultados mostrados a continuación:

Telnet: Es un servicio del sistema operativo Unix/Linux. Se utilizó para escanear los puertos que estaban abiertos, aclarando que se puede realizar telnet a cualquier puerto, por ejemplo >telnet 192.168.11.3 80 éste sería un telnet al servidor Web. Por otro lado en la Alcaldía la conexión por telnet al puerto 23 está restringida ya que éste servicio permite el control remoto de equipos

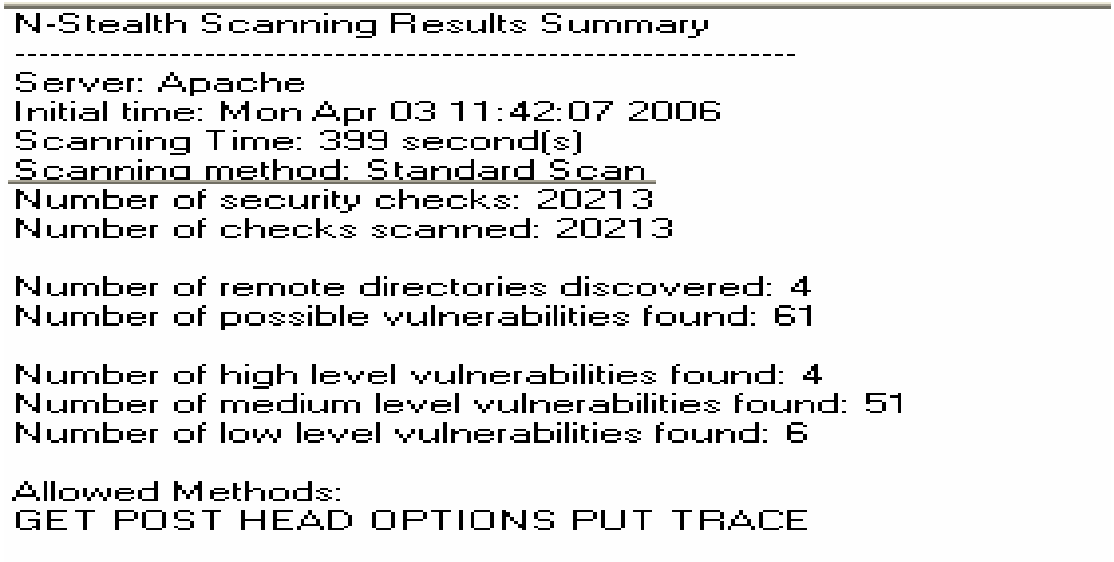
Caín y Abel versión 2.67: se realizo crackeo de contraseñas de Windows, ya que el programa cuenta con un sniffer con múltiples ataques, como es la fuerza bruta y el diccionario de password; de este programa se obtuvo un informe completo del tráfico en red en sus diferentes protocolos, siendo el más importante el protocolo SMB y el trafico de SNMP de mensajes porque con ellos se obtiene la identificación de la máquina para ser crackeada.

Análisis de prueba de fuerza bruta con Caín: A través de los programas Caín y Abel v2.67 y Atelier Web commander se pudo analizar que existen vulnerabilidades en la identificación de IP´s para realizar accesos remotos a cualquier equipo en la red de la Alcaldía dentro de la Intranet, como también revelación de contraseñas de usuario de Windows en este caso.

Caín y Abel versión 2.67 para denegación de servicio: El propósito de esta práctica fue comprobar los servicios de Internet y servicios de protocolos, en los cuales se realizo una denegación de servicio por envenenamiento de rutas a un usuario en particular y ver que fue posible negarle acceso o disponibilidad en Internet.

NStealth: Con el Nstealth se obtuvo un escaneo de puertos abiertos para encontrar posibles vulnerabilidades en el servidor www.cali.gov.co. Los reportes son poco detallados como se puede ver a continuación en la prueba realizada al Servidor Web de la Alcaldía Santiago de Cali:

Figura 41. Respuesta del Servidor Web (Cali.gov.co).



Fuente: programa N-Stealth Alcaldía de Cali, Santiago de Cali, 2006. P.1.

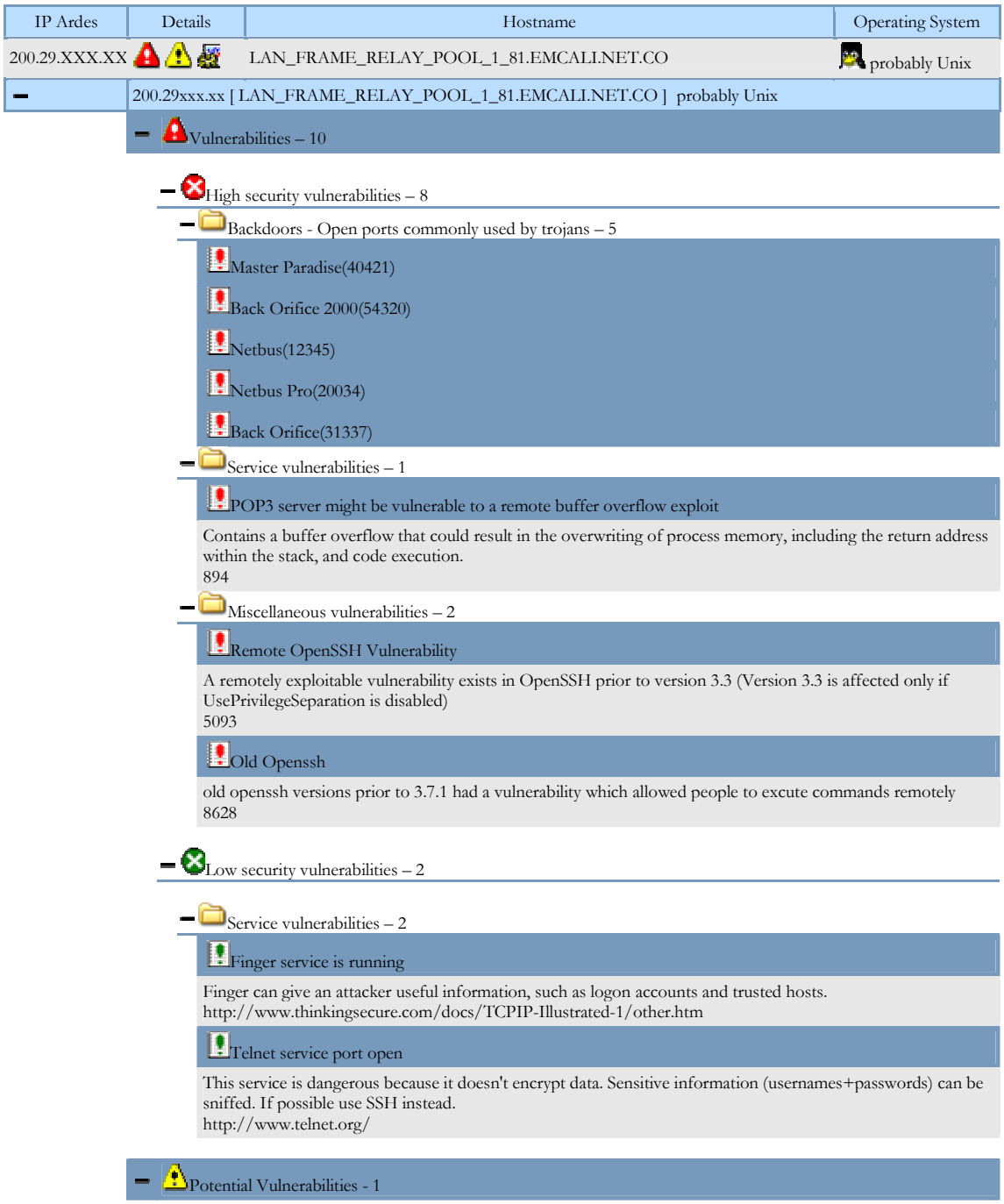
La respuesta arrojada solo indica que existen cuatro vulnerabilidades de nivel alto, cincuenta y una vulnerabilidades de nivel medio y seis vulnerabilidades de nivel bajo, teniendo en cuenta que estas son posibles vulnerabilidades.

7.4.2.2 Evaluación Externa

Lannetscan GFI secure: este programa se utilizo para realizar el escaneo de puertos, revisar vulnerabilidades en la red local. Además analiza los posibles scripts que afecten a la red. Una vez GFI LANguard N.S.S. completó el análisis de los servidores, organizó las debilidades de seguridad. Cuando se identificaron puertos clave abiertos (como WWW, FTP, Telnet, SMTP) mediante procesamiento de banner, el programa consultó también el servicio que está tras el puerto abierto detectado para asegurar que no se está secuestrando el puerto.

Especificaciones técnicas obtenidas al escanear las direcciones de interés con el programa GFI Lanscanner network.

Figura 42. Reporte GFI para el servidor Firewall Santiago.



IP Ardes	Details	Hostname	Operating System
200.29.XXX.XX		LAN_FRAME_RELAY_POOL_1_81.EMCALI.NET.CO	probably Unix

200.29xxx.xx [LAN_FRAME_RELAY_POOL_1_81.EMCALI.NET.CO] probably Unix

Vulnerabilities – 10

High security vulnerabilities – 8

Backdoors - Open ports commonly used by trojans – 5

- Master Paradise(40421)
- Back Orifice 2000(54320)
- Netbus(12345)
- Netbus Pro(20034)
- Back Orifice(31337)

Service vulnerabilities – 1

POP3 server might be vulnerable to a remote buffer overflow exploit

Contains a buffer overflow that could result in the overwriting of process memory, including the return address within the stack, and code execution.
894

Miscellaneous vulnerabilities – 2

Remote OpenSSH Vulnerability

A remotely exploitable vulnerability exists in OpenSSH prior to version 3.3 (Version 3.3 is affected only if UsePrivilegeSeparation is disabled)
5093

Old Openssh

old openssh versions prior to 3.7.1 had a vulnerability which allowed people to excute commands remotely
8628

Low security vulnerabilities – 2

Service vulnerabilities – 2

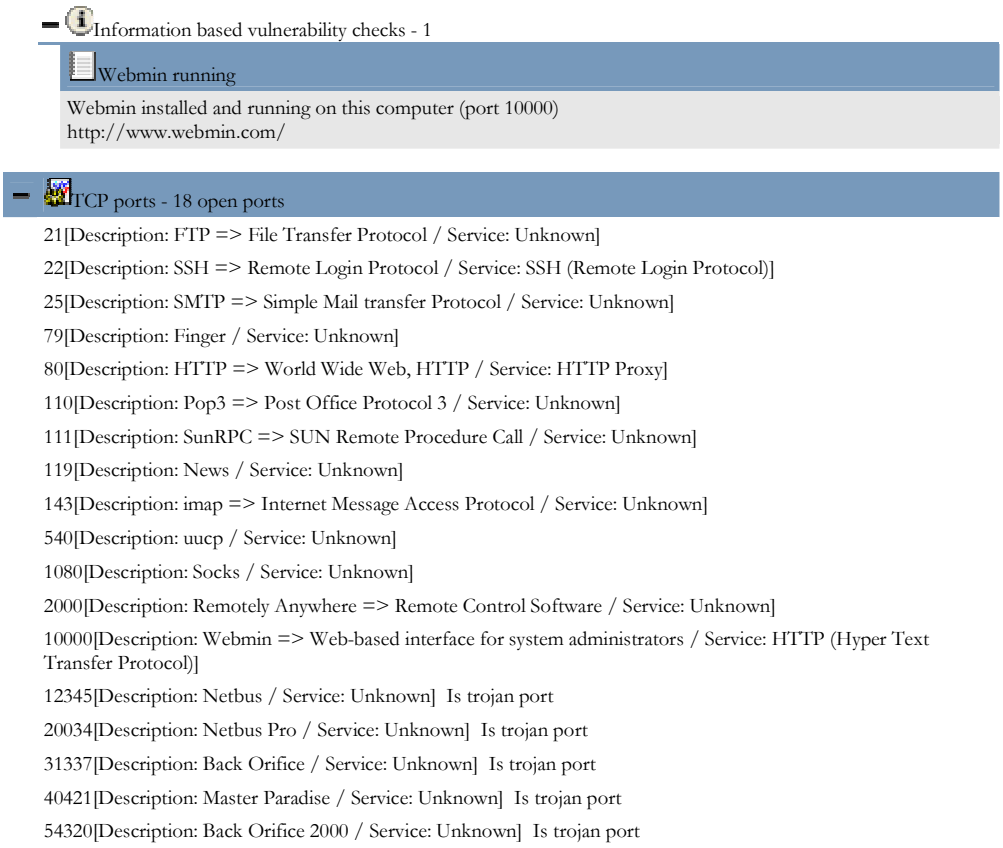
Finger service is running

Finger can give an attacker useful information, such as logon accounts and trusted hosts.
http://www.thinkingsecure.com/docs/TCPIP-Illustrated-1/other.htm

Telnet service port open

This service is dangerous because it doesn't encrypt data. Sensitive information (usernames+passwords) can be sniffed. If possible use SSH instead.
http://www.telnet.org/

Potential Vulnerabilities - 1



En este servidor se encontraron 18 puertos abiertos y 10 vulnerabilidades las cuales se describen a continuación:

Vulnerabilidades de alta seguridad: 8

- Backdoors: se refiere a cinco puertos abiertos que son usados comúnmente por troyanos (puertos: 40421, 54320, 12345, 20034,31337).
- Vulnerabilidades de servicios: se refiere a que un servidor POP3 puede ser atacado por un buffer remoto con exploits y causar desbordamientos, que reflejarían en sobre escritura de procesos en la memoria.
- Vulnerabilidades varias: en estas se encuentran, una vulnerabilidad relacionada con OpenSSH remoto, que consiste en una vulnerabilidad que

puede ser explotable en versiones anteriores a OpenSSH 3.3, esta versión es afectada solo si esta deshabilitado el UsePrivilegeSeparation (UPS). La otra vulnerabilidad está relacionada con una versión de OpenSSH anterior a la versión OpenSSH 3.7.1, que permite ejecutar órdenes de manera remota.

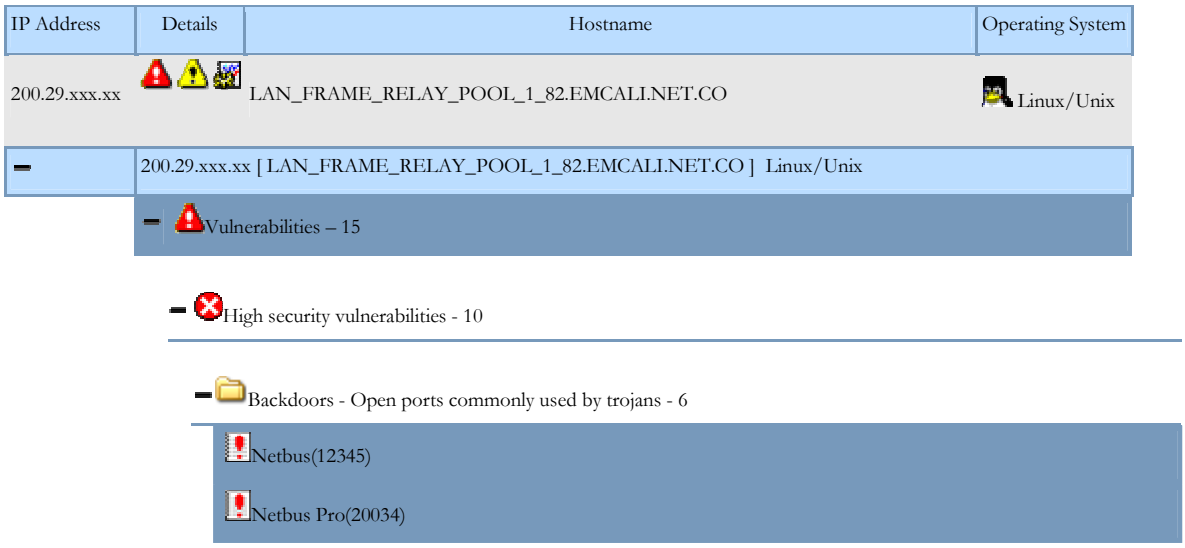
Vulnerabilidades de baja seguridad: 2

- Vulnerabilidades de servicios: la primera vulnerabilidad se refiere a que el servicio Finger se encuentra funcionando y puede dar información útil como cuentas logon y host verdaderos. La segunda vulnerabilidad se refiere a que el puerto de servicio Telnet se encuentra abierto, lo cual es peligroso porque este no encripta la información y posibilita la realización de sniffer a información sensible como nombres de usuarios y contraseñas.

Vulnerabilidades potenciales: 1

- Vulnerabilidad basada en la información: Se refiere a que el Webmin (que es una herramienta gráfica para la configuración de servicios de red, y es poco segura para utilizar en red) se encuentra en funcionamiento usando el puerto 10000.

Figura 43. Respuesta GFI para el servidor Web



Back Orifice(31337)

Master Paradise(40421)

Back Orifice 2000(54320)

Back Orifice 2000(54321)

Mail vulnerabilities - 2

Remote Buffer Overflow in Sendmail

Sendmail versions from 5.79 to 8.12.7 are vulnerable to this buffer overflow.
http://nvd.nist.gov/nvd.cfm?cvename=CVE-2002-1337

Sendmail is older than 8.12.9

Various buffer overflows can be found in old Sendmail version including some that allow remote users to gain root privilieges.
http://www.sendmail.org/patchps.html

Service vulnerabilities - 1

PHP older than 4.3.8

PHP older than 4.3.8 is vulnerable to a remote code execution vulnerability
http://www.securityfocus.com/bid/10724/

Miscellaneous vulnerabilities - 1

Old Openssh

old openssh versions prior to 3.7.1 had a vulnerability which allowed people to excute commands remotely
8628

Medium security vulnerabilities - 1

Miscellaneous vulnerabilities - 1

SSH server accepts Version 1.x connections

SSH protocol Version 1 has various vulnerabilties, this should be disabled and only version 2 clients should be allowed to connect
http://www.ssh.com/company/newsroom/article/210/

Low security vulnerabilities - 4

CGI abuses - 2

Apache: Apache manual

Apache online manual has not been removed

Vulnerable url : ///manual/

Bugtraq url :

Netscape: Netscape PageServices

List page directory

Vulnerable url : ///?PageServices

Bugtraq url :

Service vulnerabilities - 2

Finger service is running

Finger can give an attacker useful information, such as logon accounts and trusted hosts.

http://www.thinkingsecure.com/docs/TCPIP-Illustrated-1/other.htm

Telnet service port open

This service is dangerous because it doesn't encrypt data. Sensitive information (usernames+passwords) can be sniffed.

If possible use SSH instead.

http://www.telnet.org/

Potential Vulnerabilities - 2

Information based vulnerability checks - 2

Some POP3 server banners providing information to attacker

The script displays the information provided by the POP3 server. This information could help an attacker choose the best attack vector for the server.

IMAP4 server banner provides information to attacker

IMAP4 server banner provides information that might help an attacker

TCP ports - 23 open ports

21[Description: FTP => File Transfer Protocol / Service: FTP (File Transfer Protocol)]

22[Description: SSH => Remote Login Protocol / Service: SSH (Remote Login Protocol)]

25[Description: SMTP => Simple Mail transfer Protocol / Service: SMTP (Simple Mail Transfer Protocol)]

53[Description: Domain => Domain Name Server / Service: Unknown]

79[Description: Finger / Service: Unknown]

80[Description: HTTP => World Wide Web, HTTP / Service: HTTP Proxy]

110[Description: Pop3 => Post Office Protocol 3 / Service: POP3 (Port Office Protocol 3)]

111[Description: SunRPC => SUN Remote Procedure Call / Service: Unknown]

119[Description: News / Service: Unknown]

143[Description: imap => Internet Message Access Protocol / Service: IMAP (Internet Message Access Protocol)]

443[Description: HttpS => Secure HTTP / Service: HTTP (Hyper Text Transfer Protocol)]

540[Description: uucp / Service: Unknown]

993[Description: imaps => imap over TLS/SSL / Service: Unknown]

995[Description: pop3s => POP3 over TLS/SSL / Service: Unknown]

1080[Description: Socks / Service: Unknown]

2000[Description: Remotely Anywhere => Remote Control Software / Service: Unknown]

3306[Description: MySQL / Service: Unknown]

12345[Description: Netbus / Service: Unknown] Is trojan port

20034[Description: Netbus Pro / Service: Unknown] Is trojan port

31337[Description: Back Orifice / Service: Unknown] Is trojan port

40421[Description: Master Paradise / Service: Unknown] Is trojan port

54320[Description: Back Orifice 2000 / Service: Unknown] Is trojan port

54321[Description: Back Orifice 2000 / Service: HTTP (Hyper Text Transfer Protocol)] Is trojan port

En el servidor Web se encontraron 15 vulnerabilidades las cuales se describen a continuación:

Vulnerabilidades de alta seguridad: 10

- Backdoors: se refiere a seis puertos abiertos que son usados comúnmente por troyanos (puertos: 40421, 54320, 12345, 20034, 31337, 54321).
- Vulnerabilidades de correo: Existen dos vulnerabilidades de este tipo. La primera consiste en el desbordamiento del bufer remoto en Sendmail, debido a que la versión de Sendmail que tiene el servidor es vulnerable a este desbordamiento de bufer. La segunda consiste en que el servidor tiene una versión inferior a Sendmail 8.12.9, esto puede permitir a los usuarios obtener privilegios del root.
- Vulnerabilidades de servicios: se refiere a que el servidor tiene una versión de PHP (motor de SMPT que se distribuye bajo licencia GPL) más antigua que la versión 4.3.8, por lo que es vulnerable a un ataque por ejecución de código.

- Vulnerabilidades varias: se encuentra una vulnerabilidad que está relacionada con una versión de OpenSSH anterior a la versión OpenSSH 3.7.1, que permite ejecutar órdenes de manera remota.

Vulnerabilidades de media seguridad: 1

- Vulnerabilidades varias: el protocolo SSH versión 1 tiene varias vulnerabilidades, esta versión debe deshabilitarse y permitirse la conexión de dos clientes solamente.

Vulnerabilidades de baja seguridad: 4

- Abusos CGI: la primera vulnerabilidad se refiere a que el manual en línea de Apache no ha sido removido, lo que genera una vulnerabilidad por url. La segunda vulnerabilidad se refiere a los servicios de página de Netscape.
- Vulnerabilidades en los servicios: se dan dos vulnerabilidades. La primera vulnerabilidad se refiere a que el servicio Finger se encuentra funcionando y puede dar información útil como cuentas logon y host verdaderos. La segunda vulnerabilidad se refiere a que el puerto de servicio Telnet se encuentra abierto, lo cual es peligroso porque éste no encripta la información y posibilita la realización de sniffer a información sensible como nombres de usuarios y contraseñas.

Vulnerabilidades potenciales: 2

- Vulnerabilidad basada en la información: Se refiere a que Algunos banners del servidor POP3 proporciona información al posible atacante, este podría elegir cual es el mejor vector para atacar al servidor. La segunda posibilidad se presenta con el IMAP4, ya que el servidor de banner proporciona información que podría ayudar al atacante.

Adicional a esto se encontró que hay 23 puertos abiertos.

Figura 44. Respuesta GFI para el servidor Riverita

IP Address	Details	Hostname	Operating System
200.29.xxx.xx		LAN_FRAME_RELAY_POOL_1_84.EMCALI.NET.CO	probably Unix

200.29.xxx.xx [LAN_FRAME_RELAY_POOL_1_84.EMCALI.NET.CO] probably Unix

Vulnerabilities – 3

High security vulnerabilities – 2

Service vulnerabilities – 1

POP3 server might be vulnerable to a remote buffer overflow exploit

Contains a buffer overflow that could result in the overwriting of process memory, including the return address within the stack, and code execution.

894

Miscellaneous vulnerabilities - 1

Old Openssh

old openssh versions prior to 3.7.1 had a vulnerability which allowed people to excute commands remotely

8628

Medium security vulnerabilities - 1

Miscellaneous vulnerabilities - 1

SSH server accepts Version 1.x connections

SSH protocol Version 1 has various vulnerabilties, this should be disabled and only version 2 clients should be allowed to connect

http://www.ssh.com/company/newsroom/article/210/

TCP ports - 11 open ports

21[Description: FTP => File Transfer Protocol / Service: Unknown]

22[Description: SSH => Remote Login Protocol / Service: SSH (Remote Login Protocol)]

25[Description: SMTP => Simple Mail transfer Protocol / Service: Unknown]

53[Description: Domain => Domain Name Server / Service: Unknown]

80[Description: HTTP => World Wide Web, HTTP / Service: HTTP Proxy]

110[Description: Pop3 => Post Office Protocol 3 / Service: Unknown]

111[Description: SunRPC => SUN Remote Procedure Call / Service: Unknown]

119[Description: News / Service: Unknown]

143[Description: imap => Internet Message Access Protocol / Service: Unknown]

3128[Description: Proxy/Socks / Service: HTTP Proxy]

3306[Description: MySQL / Service: Unknown]

En el servidor Proxy se encontraron 3 vulnerabilidades las cuales se describen a continuación:

Vulnerabilidades de alta seguridad: 2

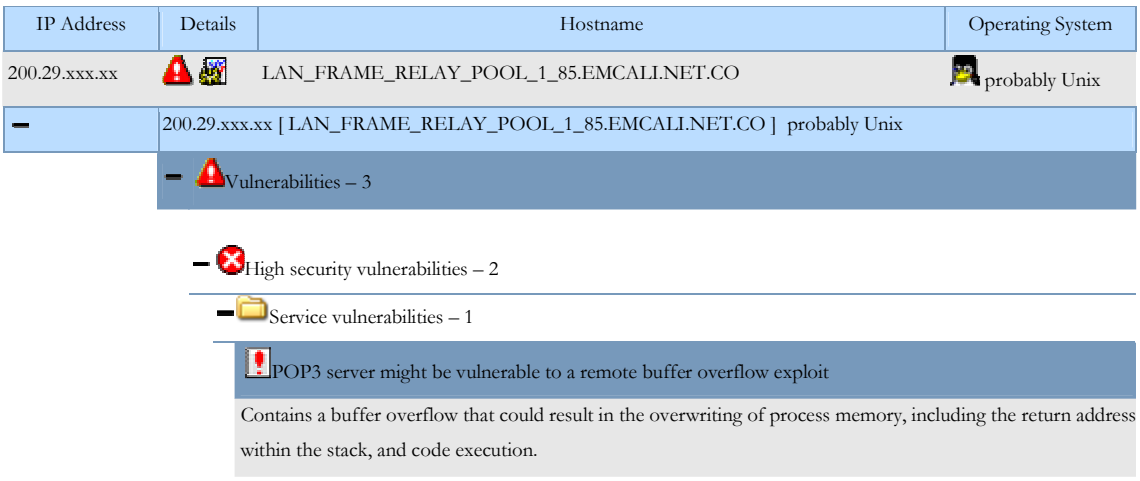
- Vulnerabilidades de servicios: se refiere a que un servidor POP3 puede ser atacado por un buffer remoto con exploits y causar desbordamientos, que se reflejarían en sobre escritura de procesos en la memoria.
- Vulnerabilidades varias: La otra vulnerabilidad está relacionada con una versión de OpenSSH anterior a la versión OpenSSH 3.7.1, que permite ejecutar órdenes de manera remota.

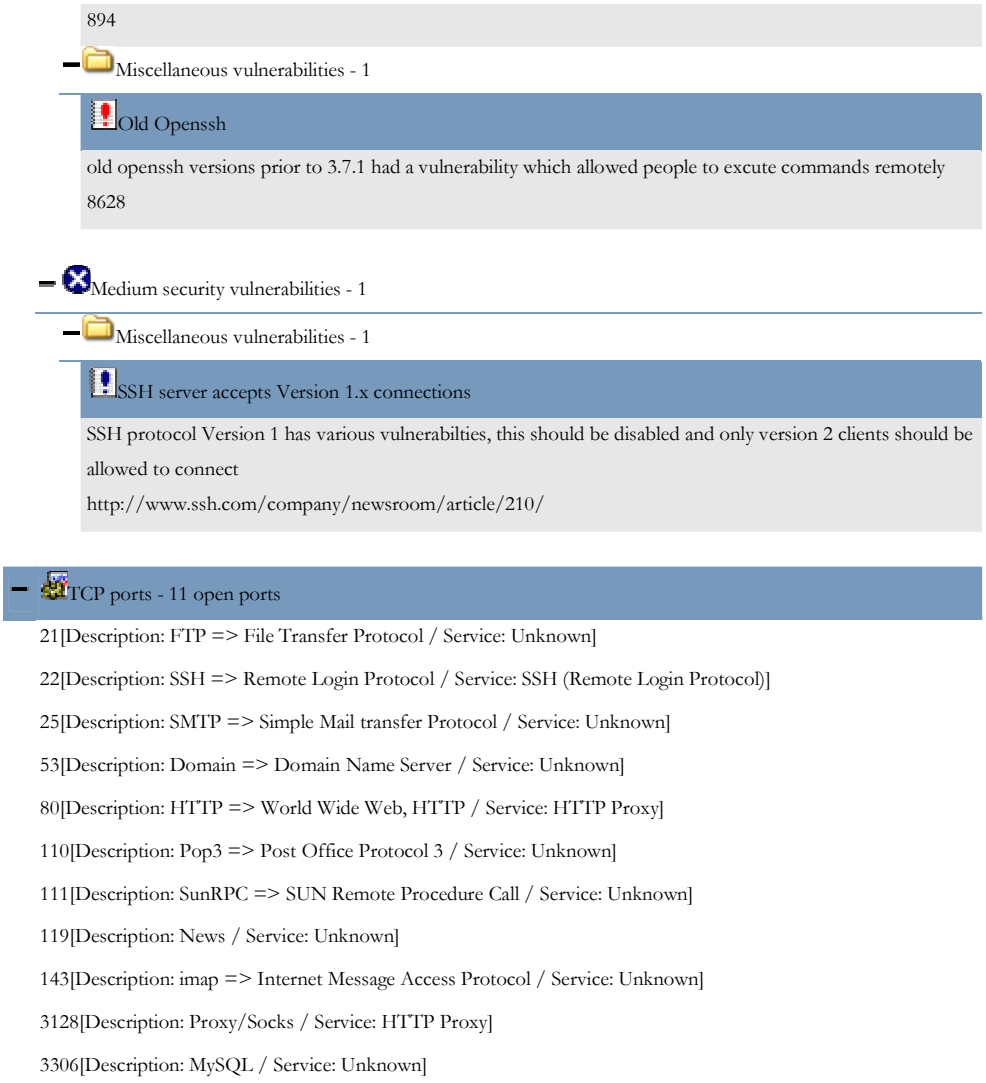
Vulnerabilidades de media seguridad: 1

- Vulnerabilidades varias: el protocolo SSH versión 1 tiene varias vulnerabilidades, esta versión debe deshabilitarse y permitirse la conexión de dos clientes solamente.

Adicional a esto se encontró que hay 11 puertos abiertos.

Figura 45. Respuesta GFI para el servidor Hacienda





En el servidor Hacienda se encontraron 3 vulnerabilidades las cuales se describen a continuación:

Vulnerabilidades de alta seguridad: 2

- Vulnerabilidades de servicios: se refiere a que un servidor POP3 puede ser atacado por un buffer remoto con exploits y causar desbordamientos, que se reflejarían en sobre escritura de procesos en la memoria.

- Vulnerabilidades varias: La otra vulnerabilidad está relacionada con una versión de OpenSSH anterior a la versión OpenSSH 3.7.1, que permite ejecutar órdenes de manera remota.

Vulnerabilidades de media seguridad: 1

- Vulnerabilidades variadas: el protocolo SSH versión 1 tiene varias vulnerabilidades, esta versión debe deshabilitarse y permitirse la conexión de dos clientes solamente.

Adicional a esto se encontró que hay 11 puertos abiertos.

Figura 46. Reporte servidor de Correo

IP Address	Details	Hostname	Operating System
200.29.xxx.xx		LAN_FRAME_RELAY_POOL_1_89.EMCALI.NET.CO	probably Unix
−	200.29.xxx.xx [LAN_FRAME_RELAY_POOL_1_89.EMCALI.NET.CO] probably Unix		

− Vulnerabilities – 3

− Medium security vulnerabilities – 2

− CGI abuses – 1

All Servers: dig Arbitrary File Inclusion

Possible to View arbitrary files (Web server level privileges)

Vulnerable url : /cgi-bin/htsearch

Bugtraq url : 1026

− Miscellaneous vulnerabilities – 1

SSH server accepts Version 1.x connections

SSH protocol Version 1 has various vulnerabilties, this should be disabled and only version 2 clients should be allowed to connect

http://www.ssh.com/company/newsroom/article/210/

− Low security vulnerabilities – 1

Mail vulnerabilities - 1

SMTP server allows relaying

Mail server allows remote users to send emails. This configuration is often abused by spammers and hackers to avoid email protection systems.
http://www.mind.net/home/articles/no_relay.shtml

Potential Vulnerabilities - 1

Information based vulnerability checks - 1

Webmin running

Webmin installed and running on this computer (port 10000)
http://www.webmin.com/

TCP ports - 10 open ports

21[Description: FTP => File Transfer Protocol / Service: Unknown]

22[Description: SSH => Remote Login Protocol / Service: SSH (Remote Login Protocol)]

25[Description: SMTP => Simple Mail transfer Protocol / Service: SMTP (Simple Mail Transfer Protocol)]

80[Description: HTTP => World Wide Web, HTTP / Service: HTTP Proxy]

110[Description: Pop3 => Post Office Protocol 3 / Service: POP3 (Port Office Protocol 3)]

119[Description: News / Service: Unknown]

143[Description: imap => Internet Message Access Protocol / Service: IMAP (Internet Message Access Protocol)]

993[Description: imaps => imap over TLS/SSL / Service: Unknown]

995[Description: pop3s => POP3 over TLS/SSL / Service: Unknown]

10000[Description: Webmin => Web-based interface for system administrators / Service: HTTP (Hyper Text Transfer Protocol)]

En el servidor de Correo se encontraron 3 vulnerabilidades las cuales se describen a continuación:

Vulnerabilidades de media seguridad: 2

- Abuso CGI: permite la penetración arbitraria de archivos
- Vulnerabilidades variadas: el protocolo SSH versión 1 tiene varias vulnerabilidades, esta versión debe deshabilitarse y permitirse la conexión de dos clientes solamente.

Vulnerabilidades de baja seguridad: 1

- Vulnerabilidades de correos: El servidor de SMTP permite relevar, el servidor del correo les permite a los usuarios remotos enviar emailes. Esta configuración se abusa a menudo por los spammers y hackers para evitar los sistemas de protecciones del email.

Vulnerabilidades potenciales: 1

- Vulnerabilidad basada en la información: Se refiere a que el Webmin se encuentra en funcionamiento usando el puerto 10000.

Adicional a esto se encontró que hay 10 puertos abiertos.

Tabla 4. Resumen de vulnerabilidades con GFI

	Servidores				
Vulnerabilidad	F.W (Sebastián)	Web (Santiago)	Proxy (Riverita)	Hacienda	Correo
Backdoors	Si	Si	No	No	No
De servicios	Si	Si	Si	Si	No
Basada en la Inf.	Si	Si	No	No	Si
De correo	No	Si	No	No	Si
Abusos CGI	No	Si	No	No	Si
Varias	Si	Si	Si	Si	Si
Puertos abiertos	Si	Si	Si	Si	Si

NOTA: El sistema operativo de los servidores relacionados en la tabla 4 es Linux.

Shadow Security Scanner (SSS): para esta practica se tomaron en cuenta los libros de hackxcrak de la Web de dragón www.drangonjar.us; con los cuales, mediante procedimientos descritos en dichas revistas para el manejo de este programa, se realizo un análisis de vulnerabilidades para los diferentes servidores en la alcaldía; generando un reporte por servidor en sus scripts, vulnerabilidades, fallas y puertos abiertos. El Análisis realizado en el shadow security network scanner para los servidores públicos en la red de la Alcaldía de Cali es el siguiente:

Especificaciones técnicas obtenidas al escanear las direcciones ubicadas en un intervalo de interés, con en programa Shadow Security Scanner.

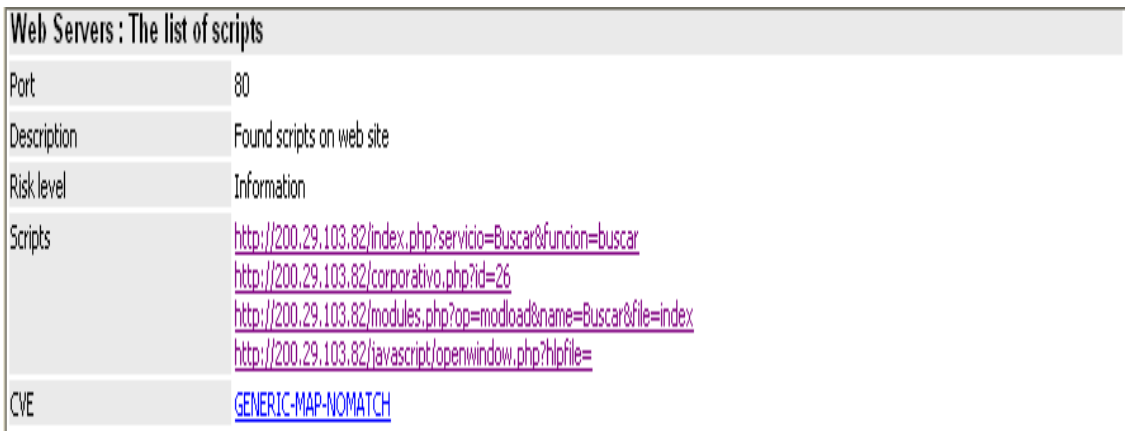
En el Firewall Sebastián existen vulnerabilidades en SSH por múltiple conexión para usuarios, como también en el comando OPENSSH por directrices de solicitud de servicio, vulnerabilidades de conexión y solicitud en el Proxy squid y de versión de squid 2.5.

En el servidor Web existen las siguientes vulnerabilidades:

- En acceso remoto por página Web a un servicio en URL por parte de ejecución de órdenes en algún sistema que tenga software de foro; el servidor finger tiene una insuficiencia por funcionalidad en sitio Web por acceso remoto a usuarios no autenticados.
- Se encuentra una debilidad en SSH por múltiple conexión de usuarios.
- Por OpenSSH existe negación remota por conexiones fuera del área de cobertura.
- Negación remota en conexión y solicitud en servidor Proxy squid.

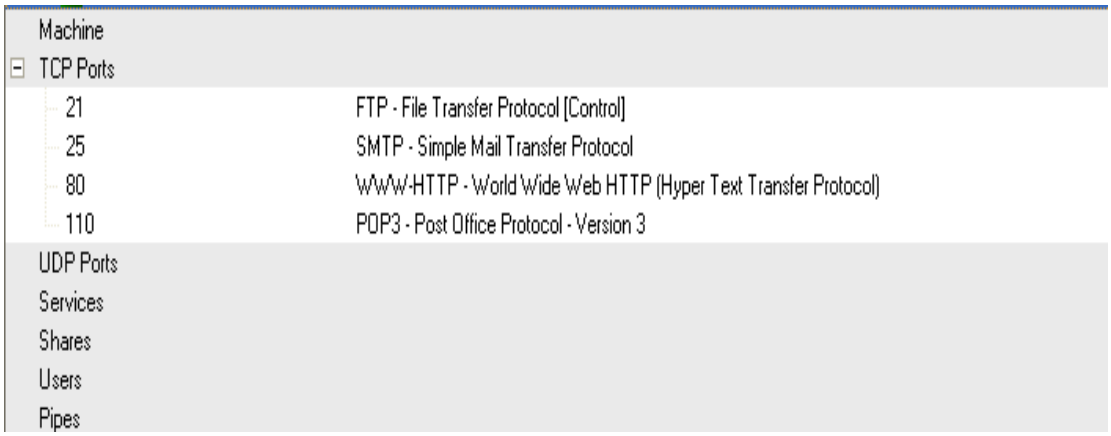
Además tiene scripts instalados, los cuales se listan en la figura 47.

Figura 47. Lista de scripts en el servidor WebShadow security scanner en el Servidor



Proxy encontró los puertos abiertos descritos en la figura 48.

Figura 48. Puertos abiertos en el Proxy



En el Servidor Hacienda se encontraron los puertos abiertos relacionados en la figura 49.

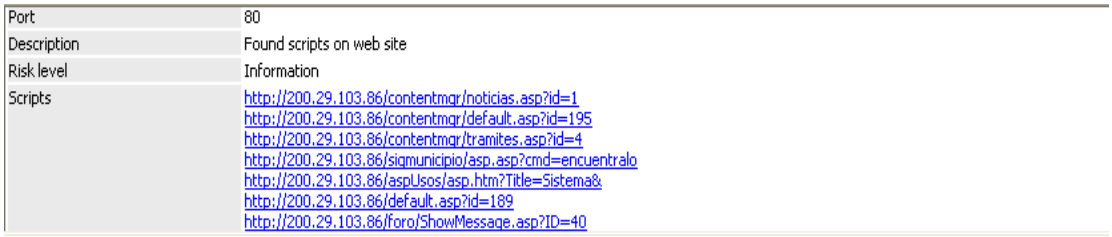
Figura 49. Puertos abiertos en el servidor Hacienda

En el Servidor Planeación se encontraron las vulnerabilidades referidas en la figura 50:

Figura 50. Vulnerabilidad en netbios del servidor Planeación

Además la figura 51muestra los scripts encontrados sobre el sitio Web.

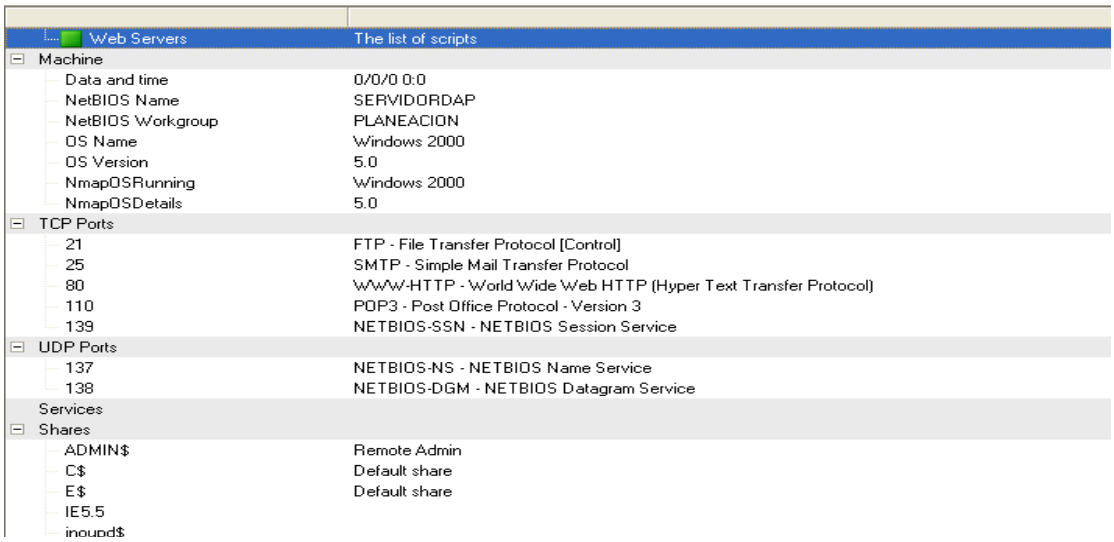
Figura 51. Lista de scripts Planeación



Port	80
Description	Found scripts on web site
Risk level	Information
Scripts	http://200.29.103.86/contentmgr/noticias.asp?id=1 http://200.29.103.86/contentmgr/default.asp?id=195 http://200.29.103.86/contentmgr/tramites.asp?id=4 http://200.29.103.86/sigmunicipio/asp.asp?cmd=encuentralo http://200.29.103.86/aspUsos/asp.htm?Title=Sistema& http://200.29.103.86/default.asp?id=189 http://200.29.103.86/foro/ShowMessage.asp?ID=40

- Shadow security scanner encontró los siguientes puertos abiertos y resultados de máquina en el servidor Planeación (Ver figura 52).

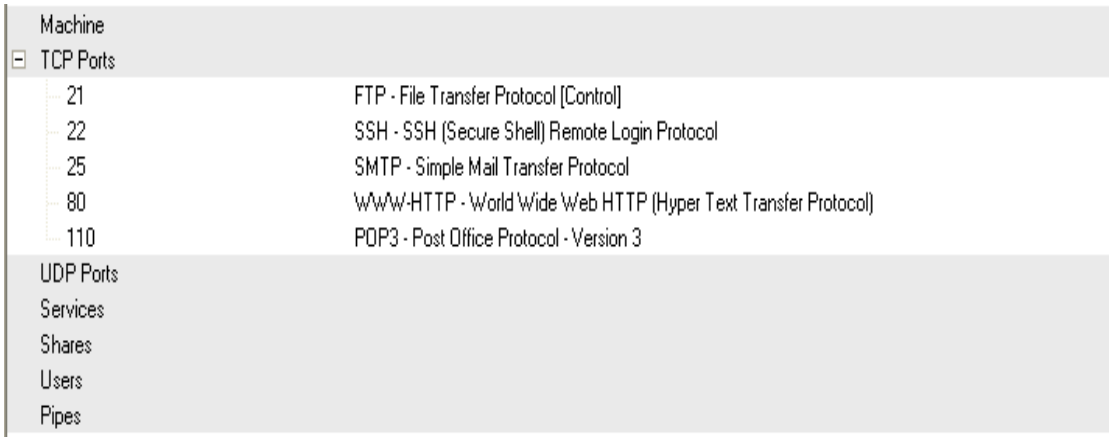
Figura 52. Puertos abiertos y resultados de servidor PlaneaciónEn el servidor de correo



Web Servers	The list of scripts
Machine	
Data and time	0/0/0 0:0
NetBIOS Name	SERVIDORDAP
NetBIOS Workgroup	PLANEACION
OS Name	Windows 2000
OS Version	5.0
NmapOSRunning	Windows 2000
NmapOSDetails	5.0
TCP Ports	
21	FTP - File Transfer Protocol [Control]
25	SMTP - Simple Mail Transfer Protocol
80	WWW-HTTP - World Wide Web HTTP (Hyper Text Transfer Protocol)
110	POP3 - Post Office Protocol - Version 3
139	NETBIOS-SSN - NETBIOS Session Service
UDP Ports	
137	NETBIOS-NS - NETBIOS Name Service
138	NETBIOS-DGM - NETBIOS Datagram Service
Services	
Shares	
ADMIN$	Remote Admin
C$	Default share
E$	Default share
IE5.5	
inoupd$	

Shadow security scanner encontró los siguientes puertos abiertos (Ver figura 53).

Figura 53. Puertos abiertos servidor de Correo



En la tabla 5 se muestra un resumen de vulnerabilidades obtenidas con la herramienta Shadow Security Scanner.

Tabla 5. Resumen de vulnerabilidades con SSS.

Servidor	Vulnerabilidades
FireWall Sebastián	− En SSH por múltiples conexión para usuarios. − En el comando OpenSSH por directrices de solicitud de servicio. − De conexión y solicitud en el proxy squid.
Web Santiago	− En acceso remoto por página Web a un servicio en URL por ejecución de órdenes en algún sistema que tenga software de foro. − El servidor finger tiene una insuficiencia por funcionalidad en sitio Web por acceso remoto a usuarios no autenticados. − Se encuentra una debilidad en SSH por Múltiple conexión a usuarios.
Proxy Riverita	− En negación remota por conexión y solicitud en PUT o POST para el proxy squid. − OpennSSh es susceptible a una negación remota de vulnerabilidad de servicio. − PHP es susceptible a una vulnerabilidad de desbordamiento para el búfer de manejo de imágenes JPEG.
Hacienda	− Se encontró que el cURL permite a usuarios malévolos evitar restricciones 'open_basedir' en escrituras PHP. − En OpenSSH, negación remota por conexiones fuera del área de cobertura. − Vulnerabilidad por ataque masivo en el sistema proFTPD por búsqueda de usernames por diccionario y realizar acceso remoto.
Planeación	− Por establecimiento de una sesión nula en NETBIOS con un anfitrión de NT. − En el NETBIOS, ya que puede ser logueado internamente y revela el nombre del Host.
Correo	− El servidor Web de Apache es afectado por una variable de ambiente de archivo de configuración.

NOTA: El SSS reportó puertos abiertos en todos los casos.

7.4.2.3 Resumen de la auditoria. Finalmente, de los resultados obtenidos en la etapa de auditoria informática se concluye lo siguiente:

- El servicio de correo se encuentra abierto, sin ningún tipo de autorización permitiendo el acceso a cualquier persona, y esta persona puede enviar correos al destino que desee.
- El ataque en forma externa está restringido porque la configuración del firewall no permite que equipos externos hagan solicitudes de conexión a equipos internos, solo a través de: www.cali.gov.co.
- El servicio de FTP está restringido para la mayoría de los servidores, puesto que este no es un puerto tan seguro ya que se utiliza SSH (puerto22) con un loggin y contraseña válidos.
- Teniendo en cuenta que la red de la Alcaldía es un sistema de información y de tráfico de datos se conocieron los diferentes ataques, métodos y vulnerabilidades en la red a través de ciertos programas especializados en seguridad informática, cabe aclarar que existen infinidad de programas dedicados a estas funciones.
- Se realizo la valoración de la seguridad informática de la red en la Alcaldía de Santiago de Cali a nivel interno y externo encontrando varios sistemas poco seguros pero listos para mejorar
- Existen ciertos servidores que aun presentan vulnerabilidades considerables según los análisis de vulnerabilidades hechos en shadow security y gfi languard scanner.
- También se generaron informes hechos en los programas ya mencionados que ayudan para una gestión informática en los servidores y equipos con vulnerabilidades y así tener un mejor control de estos ataques a la red de la Alcaldía de Cali.

7.4.3 Recomendaciones en la red. Para solucionar las debilidades encontradas en los servidores analizados en el apartado anterior, se recomienda:

- Revisar periódicamente que puertos están siendo utilizados, y cerrar los que no estén en uso.
- Actualizar las versiones de los programas que se utilizan en los servidores para evitar vulnerabilidad por versiones antiguas.
- Utilizar paquetes aplicativos licenciados (puede ser cualquiera de los usados en este proyecto), que permitan realizar análisis periódicos y más exhaustivos a la red.
- Dentro de lo posible contar con una empresa externa especializada en auditoria informática.

De esta forma, la Red de Telecomunicaciones de la Alcaldía de Cali disminuye los riesgos que se puedan presentar en cuanto al manejo de la información.

7.4.4 Implementación. Además del proceso de diagnostico llevado a cabo en el desarrollo del proyecto de políticas de seguridad informática, Se implemento también un proceso piloto para proponer soluciones a ciertas vulnerabilidades, estas fueron:

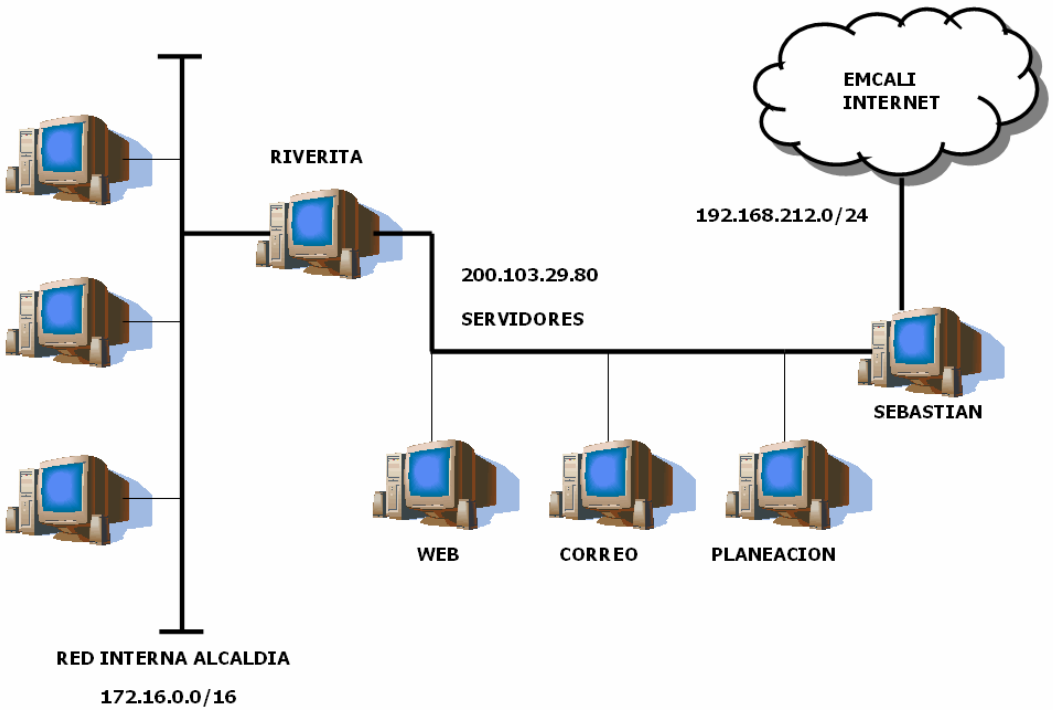
A. Paso de las listas de control de acceso del firewall SEBASTIAN al firewall PIX 515E.
B. Falta de conocimiento seguridad de la información por parte de los usuarios.
C. Bases de datos sobre incidentes, soporte técnico, copias de seguridad realizadas e inventario.
D. Vulnerabilidad de correo abierto.

A continuación se detalla cada uno de los ítems mencionados anteriormente.

A. Listas de control de acceso.

Actualmente la alcaldía en su estructura de red de información cuenta con un segmento en el cual se encuentran los servidores con direcciones públicas, encasillado en sus extremos por un Proxy y firewall, ver figura siguiente.

Figura 54. Red interna Alcaldía



De acuerdo a investigaciones en fuentes externas se encontró que esta estructura no era la más adecuada, dado que la Intranet de la Alcaldía solo es separada de los servidores los cuales eran accedidos más repetidamente desde el exterior por un Proxy.

Con la consecución del firewall Pix515E, en el proceso de reestructuración de la Alcaldía, se vio la necesidad de trasladar las políticas existentes en el firewall Sebastián. Para realizar este procedimiento se inicio con una búsqueda de información referente a la configuración del PIX y como se encontraban constituidas la listas de acceso en un firewall de tipo software (iptables e ipchains). Después, se plasmaron en un archivo de configuración específico para el PIX, todas las políticas del firewal Sebastián, teniendo en cuenta que se debía realizar

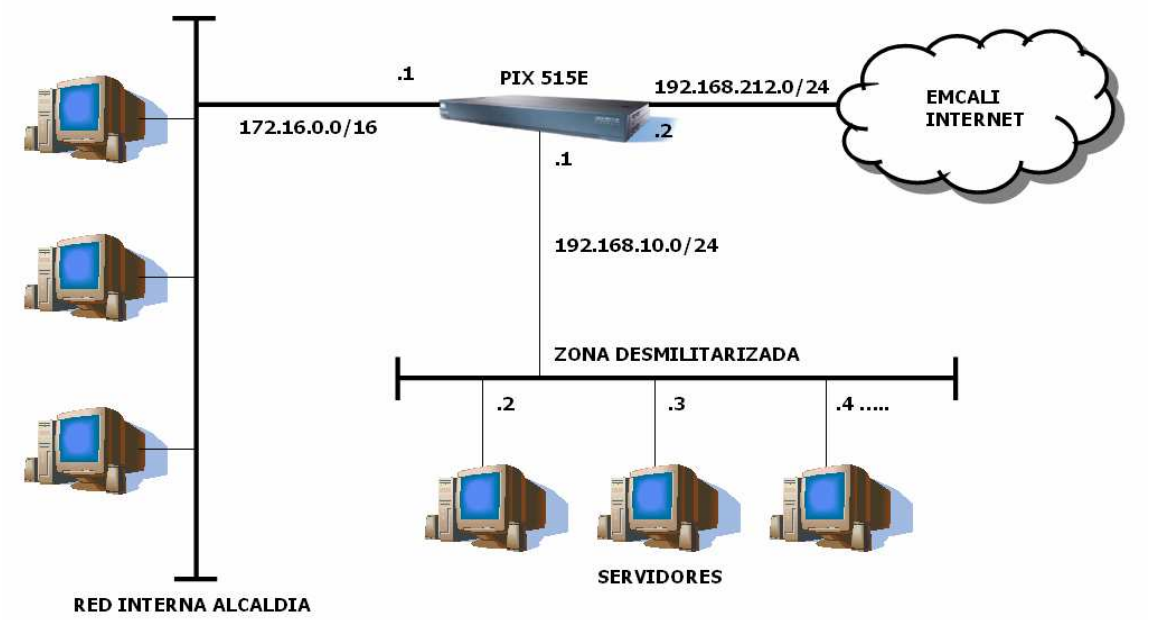
un análisis de las conexiones que se encontraban caducas o puertos solicitados por dependencias para aplicaciones especificas.

En este punto de la implementación del PIX, se recomendó una nueva configuración, donde la funcionalidad del PIX sea utilizada correctamente, refiriéndonos más concretamente a la característica de realizar NAT y soportar VPN.

En esta recomendación, se propone crear una zona desmilitarizada para los servidores, con un nivel de seguridad menor al de la Intranet de la Alcaldía, y mayor al de Internet, logrando evitar de esta manera que un intruso que haya ingresado a los servidores, pueda ingresar a la Red interna.

Esta configuración se muestra en la figura siguiente.

Figura 55. Propuesta nueva red Alcaldía



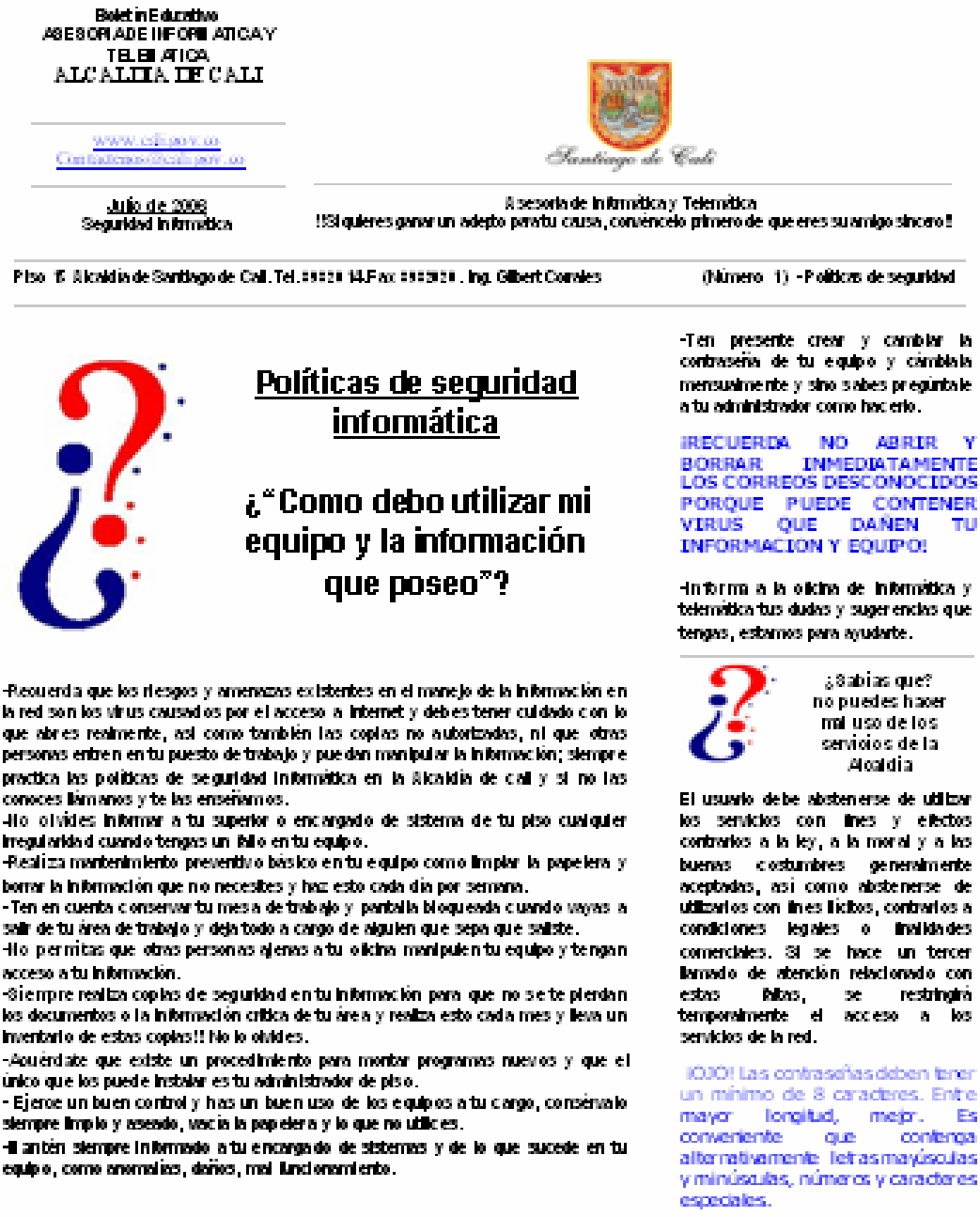
Para esta topología también se creó un archivo de configuración, que junto con el archivo de configuración actual le fueron entregados al administrador de red y de seguridad de la Alcaldía.

B. divulgación políticas de seguridad

Para la divulgación de las políticas de seguridad se utilizaron diferentes recursos con el propósito de promoverlas; entre los cuales está el correo masivo, boletines informáticos, carteleras, noticias en Internet y en la revista mensual de la alcaldía.

A continuación se presenta una muestra del boletín en el cual se informara sobre políticas de seguridad, de incidentes ocurridos, aviso de capacitaciones a realizar y otros temas.

Figura 56. Boletín informativo políticas de seguridad



Boletin Educativo
ASESORIA DE INFORMATICA Y
TELEMATICA
ALCALDIA DE CALI

www.cali.gov.co
Contactenos@cali.gov.co

Julio de 2008
Seguridad Informática

Asesoría de Informática y Telemática
!!Si quieres ganar un adepto para tu causa, convéncelo primero de que eres su amigo sincero!

Piso 6 Alcaldía de Santiago de Cali. Tel. [illegible] Fax [illegible]. Ing. Gilbert Corrales (Número 1) - Políticas de seguridad

Políticas de seguridad informática

¿"Como debo utilizar mi equipo y la información que poseo"?

-Recuerda que los riesgos y amenazas existentes en el manejo de la información en la red son los virus causados por el acceso a Internet y debes tener cuidado con lo que abres realmente, así como también las copias no autorizadas, ni que otras personas entren en tu puesto de trabajo y puedan manipular la información; siempre practica las políticas de seguridad informática en la Alcaldía de cali y si no las conoces llámanos y te las enseñamos.
-No olvides informar a tu superior o encargado de sistema de tu piso cualquier irregularidad cuando tengas un fallo en tu equipo.
-Realiza mantenimiento preventivo básico en tu equipo como limpiar la papelera y borrar la información que no necesites y haz esto cada día por semana.
-Ten en cuenta conservar tu mesa de trabajo y pantalla bloqueada cuando vayas a salir de tu área de trabajo y deja todo a cargo de alguien que sepa que saliste.
-No permitas que otras personas ajenas a tu oficina manipulen tu equipo y tengan acceso a tu información.
-Siempre realiza copias de seguridad en tu información para que no se te pierdan los documentos o la información crítica de tu área y realiza esto cada mes y lleva un inventario de estas copias!! No lo olvides.
-Acuérdate que existe un procedimiento para montar programas nuevos y que el único que los puede instalar es tu administrador de piso.
- Ejerce un buen control y has un buen uso de los equipos a tu cargo, consérvalo siempre limpio y aseado, vacía la papelera y lo que no utilices.
-Mantén siempre informado a tu encargado de sistemas y de lo que sucede en tu equipo, como anomalías, daños, mal funcionamiento.

-Ten presente crear y cambiar la contraseña de tu equipo y cámbiala mensualmente y sino sabes pregúntale a tu administrador como hacerlo.

¡RECUERDA NO ABRIR Y BORRAR INMEDIATAMENTE LOS CORREOS DESCONOCIDOS PORQUE PUEDE CONTENER VIRUS QUE DAÑEN TU INFORMACION Y EQUIPO!

-Informa a la oficina de Informática y telemática tus dudas y sugerencias que tengas, estamos para ayudarte.

¿Sabías que? no puedes hacer mal uso de los servicios de la Alcaldía

El usuario debe abstenerse de utilizar los servicios con fines y efectos contrarios a la ley, a la moral y a las buenas costumbres generalmente aceptadas, así como abstenerse de utilizarlos con fines ilícitos, contrarios a condiciones legales o lesividades comerciales. Si se hace un tercer llamado de atención relacionado con estos fallos, se restringirá temporalmente el acceso a los servicios de la red.

¡OJO! Las contraseñas deben tener un mínimo de 8 caracteres. Entre mayor longitud, mejor. Es conveniente que contenga alternativamente letras mayúsculas y minúsculas, números y caracteres especiales.

C. Bitácoras.

Esta implementación se realizó con el propósito de agilizar el proceso de manejo de inventarios, copias de seguridad, seguimiento a incidentes en la red y soporte técnico. Esto le va a permitir a la entidad implementar planes de contingencia adecuados y ayudará a reducir los tiempos de respuesta a los incidentes que se presenten.

Los formatos están diseñados de acuerdo a las especificaciones indicadas en el documento de políticas de seguridad y se detallan en los anexos1, 2 3, y 4 en las páginas 109-112.

La sugerencia para el manejo de los consecutivos para archivar, consiste en indicar en los dos primeros caracteres (XX) las iniciales de la entidad a la cual corresponde manejar el registro, seguido por la fecha tal como se ha indicado en los formatos (ddmmaa); y finalmente el número del registro (x). Así se controlará la localización de esta información, que a su vez puede consignarse en una base de datos en el servidor dedicado a la oficina de Informática y Telemática.

D. Vulnerabilidad de correo abierto.

En cuanto a esta vulnerabilidad se presentaba el problema de acceso libre al servicio de correo sin tener login ni contraseña, permitiendo hacer uso indiscriminado del mismo. Para eliminar este riesgo se le recomendó al ingeniero encargado de la seguridad en la red, implementar en el servidor de correo la autenticación de usuarios para evitar que se pueda acceder a el fácilmente.

8 ADICIONES Y MODIFICACIONES REALIZADAS AL DOCUMENTO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

Como propósito general se pretendía elaborar un documento oficial de políticas de seguridad informática; este propósito se logró a partir de un documento preliminar llamado “Políticas de Seguridad Informática para la Alcaldía de Santiago de Cali”, éste contiene una estructura acorde a las investigaciones hechas por los realizadores del documento previo. Respetando esta estructura se hicieron cambios al documento tanto de adiciones como modificaciones. A continuación se muestra un listado de dichos cambios.

ADICIONES

En esta parte se mencionan los puntos que han sido añadidos al documento, destacando el subtitulo y el numeral en que se hizo la adición.

¿Qué es la seguridad de la información?

La información constituye un activo que, como todos los demás activos comerciales importantes, es valioso para toda organización; por eso es necesario protegerlo de una manera apropiada. La seguridad de la información protege la información contra amenazas muy diversas, para asegurar la continuidad de las actividades de la empresa, minimizar el perjuicio que puede ser causado y maximizar el rendimiento del capital invertido y las posibilidades de negocios.

La información se presenta de diversas formas. Puede ser impresa o escrita sobre papel, almacenada en soportes electrónicos, transmitida por correo o utilizando medios electrónicos, expuesta sobre películas o hablada en conversaciones. Cualquiera sea la forma que tenga la información o los medios por los cuales es transmitida o almacenada, ella debe ser siempre protegida de manera apropiada.

La seguridad de la información se caracteriza por como se preserva:

Confidencialidad: procurar que la información sea accesible sólo a las personas autorizadas a acceder a su utilización.

Integridad: asegurar la exactitud y la completitud de la información y los métodos de su procesamiento.

Disponibilidad: asegurar que los usuarios autorizados puedan acceder a la información y a los activos asociados cuando la requieran.

La seguridad de la información se obtiene aplicando un conjunto de medidas de control, que pueden tomar la forma de políticas, de prácticas, de procedimientos, de estructuras organizacionales y de funciones de software. Estas medidas de control deben ser establecidas con el fin de que se cumplan los objetivos de seguridad específicos de la organización.

ELEMENTOS DE LA SEGURIDAD

El objetivo final en la red informática de la Alcaldía es conseguir la certificación de la ISO *17799* por lo cual es importante conocer de qué se trata.

ISO 17799: tiene por objetivo "proporcionar una base común para la elaboración de las normas de seguridad de las organizaciones, un método de gestión eficaz de la seguridad y establecer informes de confianza en las transacciones y las relaciones entre empresas".

ISO *17799* se presenta bajo la forma de notas de orientación y recomendaciones. Contiene diez dominios específicos compuestos de 36 objetivos y de 127 medidas de seguridad. He aquí una breve reseña de cada uno de los dominios:

Política de seguridad: proporcionar directivas y consejos de gestión para mejorar la seguridad de los datos.

Seguridad de la organización: facilitar la gestión de la seguridad de la información en el seno de la organización.

ISO/CEI 17799 (1ª parte)

Clasificación y control de los activos: catalogar los activos y protegerlos eficazmente.

Seguridad del personal: reducir los riesgos de error humano, robo, fraude y utilización abusiva de los equipamientos.

Seguridad física y medioambiental: impedir la violación, el deterioro y la perturbación de las instalaciones y datos industriales.

Gestión de las telecomunicaciones y operaciones: garantizar un funcionamiento seguro y adecuado de los dispositivos de tratamiento de la información.

Control de accesos: controlar el acceso a los datos.

Desarrollo y mantenimiento de los sistemas: garantizar que la seguridad esté incorporada a los sistemas de información.

Gestión de la continuidad de las operaciones de la empresa: reducir los efectos de las interrupciones de actividad y proteger los procesos esenciales de la empresa contra las averías y los siniestros mayores.

Conformidad: prevenir los incumplimientos de las leyes penales o civiles, de las obligaciones reglamentarias o contractuales y las exigencias de seguridad.

POLÍTICAS Y NORMAS DE SEGURIDAD

La Oficina de Informática y telemática debe garantizar que se lleven a cabo correctamente todos los procedimientos de seguridad en el área de telecomunicaciones. Así mismo, debe considerar la implementación de una revisión periódica de todas las dependencias para garantizar el cumplimiento de las políticas y estándares de seguridad.

8.1.1.1.2 El ingreso a través de la puerta principal hacia la oficina de asesoría informática y telemática, cuarto de gabinetes, y cuarto eléctrico, debe ser restringido mediante mecanismos electrónicos que permitan y registren el ingreso de personal autorizado.

8.1.1.1.3 Se debe revisar y actualizar periódicamente (cada seis meses) los derechos de acceso a las áreas protegidas.
8.1.1.1.8 A menos que se autorice expresamente, no debe permitirse el ingreso de equipos fotográficos, de video, audio u otro tipo de equipamiento que registre información.

8.1.1.2 Centro de cómputo

8.1.1.2.1 Los relojes de los equipos de cómputo deben estar sincronizados, para garantizar que los registros realizados para cualquier eventualidad tengan ese nivel de coincidencia, al momento de realizar una auditoria.

8.1.2.1 Inventario de equipos

8.1.2.1.5 Llevar a cabo un registro de los equipos de suministro eléctrico y aire acondicionado. Este registro debe contener la siguiente información:

- Código del equipo
- Descripción detallada de la configuración del equipo
- Responsable del equipo
- Ubicación del equipo
- Fecha de adquisición
- Proveedor
- Tiempo de garantía
- Referencia de fabrica del equipo
- Mantenimientos realizados

8.1.2.3 Manejo de recursos de información

8.1.2.3.1 llevar un inventario detallado y actualizado que incluya discriminadamente: bases de datos y archivos, documentación de sistemas,

manuales de usuario, material de capacitación, información archivada. Indicando en cada caso, fecha de adquisición y fecha en que fue archivada (según el caso).

8.1.2.3.2 La información detallada anteriormente debe ser recopilada y almacenada por el encargado de cada dependencia, quien a su vez debe remitir una copia de dicha información a la oficina de asesoría informática y telemática, en donde se acopiará la información al respecto, de todas las dependencias.

8.2.4 Administración de medios de almacenamiento removibles

8.2.4.6 La eliminación de cualquier activo de información sensible debe ser registrada, con el fin de mantener una pista de auditoria.

8.4.1 Administración

8.4.1.1 Se debe capacitar al personal que no tenga conocimientos en cuanto al manejo del correo electrónico.

8.5.1 Seguridad del personal

8.5.1.1 Al momento de realizar una contratación se debe verificar la información presentada por el aspirante al puesto, incluyendo las aptitudes académicas y profesionales alegadas.

8.5.1.2 Si el aspirante aplica para un cargo de gran responsabilidad (manejo de información financiera o altamente confidencial), se debe llevar a cabo una verificación de crédito.

8.5.1.3 Para casos de contratación a supernumerarios y personal temporal a través de una agencia, el contrato celebrado debe especificar claramente las responsabilidades de la agencia por la selección y los procedimientos de notificación que ésta debe seguir.

8.5.2 **Capacitación de usuarios**

8.5.2.9 Capacitar a los usuarios a cerca de cómo garantizar el buen uso de los equipos, y ejercer los controles necesarios.

8.5.2.10Capacitar a los empleados cada seis meses, en cuanto a las funciones que debe realizar de acuerdo al cargo que realiza. Esto para prevenir que existan personas nuevas o antiguas, que desconozcan parcialmente las tareas que se deben realizar.

8.7.2 Respuesta a incidentes y mal funcionamiento

8.7.2.1 Deben advertirse y registrarse los síntomas de los problemas del software, y los mensajes que aparecen en pantalla.

8.7.2.2 Al presentarse un fallo, la computadora debe ser aislada, si es posible, y debe detenerse el uso de la misma. Se debe alertar de inmediato al encargado de sistemas de la dependencia.

8.7.2.3 Si se ha de revisar un equipo, este debe ser desconectado de la red antes de ser activado nuevamente. Los disquetes no deben trasferirse a otras computadoras.

8.7.3 Segregaciones de funciones

8.7.3.4 El empleo de un contratista externo para la administración de las instalaciones de procesamiento de información puede generar un gran riesgo. Por lo tanto, es necesario que los encargados de estas funciones sea personal de planta (ver 7.1).

8.2 Responsabilidades con respecto al equipo

8.2.5 Las computadoras personales, terminales e impresoras no deben dejarse conectadas cuando están desatendidas y éstas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso.

8.2.6 La información sensible o confidencial, una vez impresa, debe ser retirada de la impresora inmediatamente.

8.8 NORMAS DE SEGURIDAD

8.8.1 Seguridad frente al acceso por parte de terceros. El acceso a las instalaciones de procesamiento de información por parte de terceros debe ser controlado. Cuando se permita dicho acceso, debe realizarse una evaluación de riesgos para determinar las incidencias en la seguridad y los requerimientos de control.

- Tipos de acceso: la evaluación de riesgos debe diferenciar acceso físico (oficinas, sala de computo, armarios), y acceso lógico (bases de datos, sistemas de información); puesto que los riesgos existentes en el acceso a través de una conexión de red, son diferentes de los riegos existentes relativos al acceso físico.
- Justificaciones para el acceso: dentro de la evaluación de riesgos se debe analizar el motivo que va a generar dicho acceso. Ya que el acceso puede realizarse por distintas razones, por ejemplo, socios con riesgos compartidos (join ventures) quienes pueden intercambiar información, acceder a sistemas de información o compartir bases de datos. Otro ejemplo es el personal de mantenimiento, quienes necesitan eventualmente ingresar a la sala de cómputo.
- Contratistas in situ: las personas que sean ubicadas in situ por un periodo de tiempo determinado según contrato (pasantes académicos, personal de limpieza), deben firmar un documento de confidencialidad o de no divulgación por un tiempo definido.
- Personal vital para el funcionamiento: el personal encargado de realizar funciones de gran importancia para el buen funcionamiento del sistema de información (administradores de red, administradores de seguridad

informática), debe ser contratado como personal de planta, puesto que estas personas tienen acceso a la red de manera irrestricta, y lo ideal es que se cuente con este personal de manera permanente para evitar inestabilidad en la seguridad.

8.8.3 RECURSOS

8.8.3.1 La oficina de informática y telemática por medio de los encargados de sistemas, debe ejercer un seguimiento (por software) de las actividades realizadas por los usuarios; con el fin de que los recursos de la red se utilicen de manera adecuada.

8.8.6 DERECHOS Y RESPONSABILIDADES DE LOS USUARIOS DE LA RED

Tanto los encargados de sistemas como los usuarios de red tienen el derecho, y, la responsabilidad de conocer las políticas de seguridad informáticas referidas en este documento.

8.8.6.6 **Derechos**

- Los cambios efectuados a nivel operativo, de responsabilidades, ó, en las políticas de seguridad deben ser notificadas al personal.
- Los cambios mencionados anteriormente se deben hacer teniendo en cuenta: evaluación del posible impacto de dichos cambios, el procedimiento de aprobación formal de los cambios propuestos, los procedimientos que identifican las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto a los mismos.
- Debe entregarse a los usuarios un detalle escrito de sus derechos de acceso a red.

8.9.3.2 ESTRATEGIAS DE CONTINUIDAD

Otro factor importante dentro de la continuidad de negocio, es la capacidad de procesamiento de información en los equipos. Debido a los nuevos requerimientos de sistemas y tendencias que surgen. Los criterios de aprobación para nuevos sistemas de información deben incluir una prueba previa, ésto teniendo en cuenta:

- desempeño y requerimientos de capacidad de las computadoras;
- recuperación ante errores y procedimientos de reinicio, y planes de contingencia;
- preparación y prueba de procedimientos operativos de rutina según estándares definidos
- conjunto acordado de controles de seguridad implementados
- procedimientos manuales eficaces
- evidencia que la instalación del nuevo sistema no afectará negativamente los sistemas existentes, especialmente en los períodos pico de procesamiento, como durante los últimos días del mes
- evidencia de que se ha tomado en cuenta el efecto que tiene el nuevo sistema en la seguridad global de la organización
- entrenamiento en la operación o uso de nuevos sistemas.

MODIFICACIONES

En esta parte se mencionan los puntos que han sido modificados en el documento de políticas de seguridad informática, destacando el numeral en que se hizo la adición y como se encontraba anteriormente.

POLÍTICAS GENERALES DE SEGURIDAD

El desconocimiento del mismo debe de exonerar a la persona de las responsabilidades asignadas.

Se cambió por

El desconocimiento del mismo no debe exonerar a la persona de las responsabilidades asignadas.

8.1.2.4 Manejo de software

8.1.2.3.3 Cada que se realice una compra, instalación o desinstalación de software, se debe reflejar en el inventario.

Se cambió por

8.1.2.3.3 Cada que se realice una compra, instalación o desinstalación de software, se debe reflejar en el inventario. A demás debe existir un procedimiento que indique como hacerlo.

8.1.2.4.3 Cada que se realice una compra, instalación o desinstalación de software, se debe reflejar en el inventario.

Se cambió por

8.1.2.4.3 Cada que se realice una compra, instalación o desinstalación de software, se debe reflejar en el inventario. A demás debe existir un procedimiento de autorización en donde se considere lo siguiente:

- Las nuevas instalaciones deben ser adecuadamente aprobadas por los encargados de sistemas, autorizando su propósito y uso. La aprobación también debe obtenerse del director de la oficina de informática y telemática, a fin de garantizar que se cumplen todas las políticas y requerimientos de seguridad pertinentes.
- Cuando corresponda, debe verificarse el hardware y software para garantizar que son compatibles con los componentes de otros sistemas.

Nota: Puede ser necesaria la comprobación de categorías para ciertas conexiones.

- Deben ser autorizados el uso de las instalaciones personales de procesamiento de información, para el procesamiento de información de la empresa, y los controles necesarios.
- El uso de instalaciones personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades y en consecuencia debe ser evaluado y autorizado.

8.2 Plan de respaldo

8.2.2 Se constituirá un Comité de Seguridad a nivel institucional, que velará por el cumplimiento de las normas y las políticas de seguridad de los equipos y medios de procesamiento de la información, el cual se recomienda que esté presidido por el Jefe del área u otro funcionario de nivel equivalente.

Se cambió por

8.2.2 Se constituirá un Comité de Seguridad a nivel institucional, que velará por el cumplimiento de las normas y las políticas de seguridad de los equipos y medios de procesamiento de la información, el cual se recomienda que esté presidido por el Jefe del área u otro funcionario de nivel equivalente.

Dicho comité debe contar con los encargados de sistemas de cada dependencia; este comité debe promover la seguridad dentro del C.A.M mediante un adecuado

compromiso y una apropiada reasignación de recursos. El comité de seguridad debe cumplir con las siguientes acciones:

- revisar y aprobar la política y las responsabilidades generales en materia de seguridad de la información;
- monitorear cambios significativos en la exposición de los recursos de información frente a las amenazas más importantes;
- revisar y monitorear los incidentes relativos a la seguridad;
- aprobar las principales iniciativas para incrementar la seguridad de la información.

8.2.3.7 Debe existir un responsable de la supervisión del proceso de copias de seguridad, su almacenamiento, e incluso de verificar que las copias se hayan realizado correctamente y funcionen.

Se cambió por

8.2.3.7Debe existir un responsable de la supervisión del proceso de copias de seguridad, su almacenamiento, e incluso de verificar que las copias se hayan realizado correctamente y funcionen. Adicional a esto debe haber una verificación periódica a cerca del conocimiento de los usuarios de red, en cuanto a la realización de copias de seguridad.

8.2.6 Planes de respuesta a emergencias y recuperación ante desastres

8.2.6.2 Seleccionar organizaciones afines a la Institución y establecer con una o más de ellas convenios de mutuo apoyo, para los casos de desastres que inhabiliten el procesamiento de información. El principal criterio será la confiabilidad, también habrá que analizar la capacidad del centro de cómputo para efectuar el servicio recíproco.

Se cambió por

8.2.6.2 Seleccionar organizaciones afines a la Institución y establecer con una o más de ellas convenios de mutuo apoyo, para los casos de desastres que inhabiliten el procesamiento de información. El principal criterio será la confiabilidad sin dejar de lado los límites que deben existir en el intercambio de información de seguridad, para garantizar que no se divulgue información confidencial, perteneciente a la Alcaldía, o entre personas no autorizadas, también habrá que analizar la capacidad del centro de cómputo para efectuar el servicio recíproco.

8.3 Autenticación y seguridad en la red

8.3.9 El monitoreo y registro de eventos es necesario para respaldar futuros controles de acceso.

Se cambió por

8.3.9 Se debe monitorear y registrar los eventos presentados; es necesario para respaldar futuros controles de acceso.

8.3.8 Se recomienda para las aplicaciones de alto riesgo, manejar límites en el tiempo de conexión.

Se cambió por

8.3.8 Para las aplicaciones de alto riesgo, se debe manejar límites en el tiempo de conexión.

8.3.10 Para el establecimiento de las contraseñas se deben seguir los siguientes lineamientos:

- Establecer un tiempo para la caducidad de las contraseñas de entre 30 y 60 días.

- Las contraseñas deben tener un mínimo de 8 caracteres. Entre mayor longitud, mejor. Es conveniente que contenga alternativamente letras mayúsculas y minúsculas, números y caracteres especiales.
- Cambiar de Clave de Acceso por lo menos cada 3 meses. Aunque lo ideal es hacerlo mensualmente.
- Tener contraseñas diferentes en máquinas diferentes. Es posible usar una contraseña base y ciertas variaciones lógicas de la misma para distintas máquinas.
- Deben ser fáciles de recordar para no verse obligado a escribirlas.

Se cambió por

8.3.10 Para el establecimiento de las contraseñas se deben seguir los siguientes lineamientos:

- Capacitar al personal de la Alcaldía, sobre como crear y cambiar las contraseñas.
- Establecer un tiempo para la caducidad de las contraseñas de entre 30 y 60 días.
- Las contraseñas deben tener un mínimo de 8 caracteres. Entre mayor longitud, mejor. Es conveniente que contenga alternativamente letras mayúsculas y minúsculas, números y caracteres especiales.
- Tener contraseñas diferentes en máquinas diferentes. Es posible usar una contraseña base y ciertas variaciones lógicas de la misma para distintas máquinas.
- Deben ser fáciles de recordar para no verse obligado a escribirlas.

8.4 SERGURIDAD EN EL MAIL

8.4.1Administración

8.5.6 Educar a los usuarios acerca de las distintas amenazas de las pueden ser víctimas (virus, malware, etc.), y como defenderse de éstas.

Se cambió por

8.5.6 Educar a los usuarios acerca de las distintas amenazas de las pueden ser víctimas (virus, malware, etc.), y como defenderse de éstas. A demás de los riesgos de perdida de información existentes en el manejo de la información.

8.7 GERENCIA DE LA CONTINUIDAD DEL NEGOCIO

8.7.1 Manejo de bitácoras

8.7.1.4 Las plantillas para el manejo de las bitácoras deben contener como mínimo los siguientes aspectos:

- Registro diario de actividades realizadas
- Problemas presentados
- Persona que realizó la actividad (Fecha y hora)
- Documentar solución en caso de fallos

Se cambió por

8.7.1.4 Las plantillas para el manejo de las bitácoras deben contener como mínimo los siguientes aspectos:

- Tiempos de inicio y cierre del sistema
- Registro diario de actividades realizadas
- Problemas presentados
- Persona que realizó la actividad (Fecha y hora)
- Documentar solución en caso de fallos

8.8 POLÍTICAS DE USUARIO

Como se nombró anteriormente, todas las personas hagan uso de los servicios que ofrece la Red de la Alcaldía deberán conocer y aceptar el reglamento vigente sobre su uso. El desconocimiento del mismo debe de exonerar a la persona de las responsabilidades asignadas.

Se cambió por

Como se nombró anteriormente, todas las personas que hagan uso de los servicios que ofrece la Red de la Alcaldía deberán conocer y aceptar el reglamento vigente sobre su uso. El desconocimiento del mismo no debe de exonerar a la persona de las responsabilidades asignadas.

8.8.1.13 Los únicos autorizados parar realizar instalación y desinstalación de programas, así como cambios de configuración en el sistema operativo, son los encargados de sistemas de cada dependencia. Esto con el fin de evitar malas configuraciones y deficiencias en el sistema operativo.

Se cambió por

8.8.1.13 Los únicos autorizados parar realizar instalación y desinstalación de programas, así como cambios de configuración en el sistema operativo, son los encargados de sistemas de cada dependencia; estas acciones deben estar regidas por un procedimiento para hacerlo. Esto con el fin de evitar malas configuraciones y deficiencias en el sistema operativo.

8.8.1.15 El usuario debe abstenerse de utilizar los servicios con fines y efectos contrarios a la ley, a la moral y a las buenas costumbres generalmente aceptadas, así como abstenerse de utilizarlos con fines ilícitos, contrarios a condiciones legales o finalidades comerciales.

Se cambió por

8.8.1.15El usuario debe abstenerse de utilizar los servicios con fines y efectos contrarios a la ley, a la moral y a las buenas costumbres generalmente aceptadas, así como abstenerse de utilizarlos con fines ilícitos, contrarios a condiciones legales o finalidades comerciales. Si se hace un tercer llamado de atención relacionado con estas faltas, se restringirá temporalmente el acceso a los servicios de la red.

9 CONCLUSIONES

- Se reviso y analizo la información existente en la Alcaldía de Cali en cuanto a políticas de seguridad informática.
- Investigando en fuentes externas, se pudo encontrar información a cerca de las normas, certificaciones, y procedimientos necesarios para implementar las más adecuadas políticas de seguridad.
- Al realizar la evaluación por dependencias del comportamiento general en cuanto al manejo de la red, se pudieron apreciar que tan profundas son las fallas que se presentan en la entidad gubernamental.
- Se realizo la valoración de la seguridad informática de la red de la Alcaldía de Cali a nivel interno y externo para conocer el nivel de vulnerabilidad que se presenta en ella.
- Con la revisión del documento de políticas de seguridad informática más los documentos encontrados en las fuentes externas, se pudieron realizar los cambios pertinentes que conllevaron a la realización del documento formal de políticas de seguridad informática para la Alcaldía.
- Se realizo vía portal www.cali.gov.co, la difusión de las políticas aprobadas por parte de la Alcaldía.

10 RECOMENDACIONES

Para que las políticas de seguridad informática aprobadas en la Alcaldía de Cali sean puestas en práctica, es necesario que el personal que labora en esta entidad las conozca. Para tal fin la Oficina de informática y telemática en conjunto con los encargados de red de cada dependencia, deben ponerse en la tarea de desarrollar actividades para la difusión y control de dichas políticas.

Como ejemplo de estas actividades se pueden tener en cuenta las siguientes:

- Diseñar y repartir una cartilla con la información más relevante sobre el documento aprobado de políticas de seguridad, para garantizar el buen uso de los recursos existentes en la Red. Haciendo de esta manera que los usuarios se familiaricen con las mismas.
- La utilización del correo interno y el portal Web de la entidad para enviar información pertinente a todos los usuarios, acerca de las novedades que se vayan a implementar en cuanto a seguridad informática.
- Actualización del **Active Desktop** (interfaz que permite colocar en el escritorio contenido activo de páginas Web, que se actualizará continuamente a través de Internet) para informar periódicamente a los usuarios de eventos, capacitaciones o de las misma políticas.
- Generar en todas las personas que laboren en la Alcaldía la cultura de remitirse inicialmente al documento de políticas, cuando se requiera realizar cambios lógicos como físicos a la institución.

BIBLIOGRAFÍA

CAJIAO, Hernando; COLLAZOS, Diego. Pasantía. Mapeo de la red de datos instalada de 1 al 8 piso en el centro administrativo “CAM” del municipio Santiago de Cali, Universidad Autónoma de Occidente, Facultad de Ingeniería. Cali, 2005. 156 p.

Caín y Abel [en línea]. Madrid, 1998. [consultado 5 de diciembre, 2005]. Disponible en Internet: http://jungla.dit.upm.es/~albertoh/faq203.html

Callio Secura Technologies [en línea]. Québec, Canadá: Callio Technologies BS7799 ISO 17799, 2006. [consultado 14 de diciembre, 2005]. Disponible en Internet: http://www.callio.com

Estándares de la ISO/IEC [en línea]. [consultado 14 de diciembre, 2005]. Disponibles en Internet: http://www.iso.org

GFI LanGuard Scanner [en línea]. Madrid: el hacker, 2001. [consultado 14 de diciembre, 2005]. Disponible en Internet: http://www.elhacker.net

Shadow Security Scanner [en línea]. Barcelona: hacking y herramientas, 2000. [consultado 17 de diciembre, 2005]. Disponible en Internet: http://www.levantalatapa.com/utilidadeshackingyherramientashack.htm

VILLALÓN HUERTA, Antonio. Códigos de buenas prácticas de seguridad UNE-ISO/IEC 17799. Sistema de gestión de seguridad de la información “La nueva norma UNE 71502” .Valencia, grupo S2, 2004. 34 p.

ANEXOS

Anexo 1. Formato de registro de equipos activos.

FORMATO DE REGISTRO DE EQUIPOS ACTIVOS
Oficina de Informática y Telemática

Consecutivo: XX ddmmaax

Tipo de equipo: _____

Código del equipo: _____

Configuración del equipo:
_____

_____

Responsable del equipo: _____

Ubicación del equipo: _____

Fecha de adquisición: _____

Proveedor: _____

Duración de la garantía: _____

Software instalado:
_____

_____

Mantenimientos realizados: _____

Anexo 2. Formato de registro para manejo de bitácoras mantenimiento.

FORMATO DE REGISTRO PARA EL MANEJO DE BITACORAS DE MANTENIMIENTO (RED)

Oficina de Informática y Telemática

Consecutivo: XX ddmmaax

Dependencia: _____

Encargado: _____

Incidente reportado por: _____

Actividades realizadas comprobación: _____

_____

_____

Tipo de mantenimiento: Correctivo_____ Preventivo_____

Descripción: _____

_____

Mantenimiento realizado por: _____

Inicio:

Día: _____ Mes: _____ Año: _____ Hora: _____

Finalización:

Día: _____ Mes: _____ Año: _____ Hora: _____

Acciones realizadas: _____

_____

Anexo 3. Formato de registro de almacenamiento de copias seguridad.

FORMATO DE REGISTRO DE ALMACENAMIENTO DE COPIAS DE SEGURIDAD

Oficina de Informática y Telemática

Consecutivo: XX ddmmaax

Tipo de medio (*): _____

Código del medio (**): _____

Contenido: _____

Fecha de adquisición: Día: _____ Mes: _____ Año: _____

Última utilización. Día: _____ Mes: _____ Año: _____

Tiempo de vida útil: _____

(*)Medio magnético, Memoria Flash, Servidor.

(**) Si el medio no pertenece a la entidad, escribir el nombre del propietario.

Anexo 4. Formato de registro manejo de bitácoras de mantenimiento.

FORMATO DE REGISTRO PARA EL MANEJO DE BITACORAS DE MANTENIMIENTO (EQUIPOS)

Oficina de Informática y Telemática

Consecutivo: XX ddmmaax

Serial equipo: _____

Responsable: _____

Hora de inicio del sistema: _____

Hora de cierre del sistema: _____

Actividades realizadas diariamente: _____

_____

Tipo de mantenimiento: Correctivo_____ Preventivo_____

Descripción: _____

_____

Mantenimiento realizado por: _____

Inicio:

Día: _____ Mes: _____ Año: _____ Hora: _____

Finalización:

Día: _____ Mes: _____ Año: _____ Hora: _____

Acciones realizadas: _____

_____

_____ _____

Responsable Técnico

APÉNDICE

(*) Los estándares mencionados se especifican brevemente a continuación:

CSC-STD-001-83	DOD Trusted Computer System Evaluation Criteria, 1983
CSC-STD-002-85	DOD Password Management Guidelines, 1985
DOD 5220.22-M	National Industrial Security Program Operating Manual, 1995
ISO/IEC 17799	Information Technology, Code of Practice for Information Security Management, February 2001
ISO/IEC DTR 13335-1	Information technology -- Guidelines for the management of IT security
ISO/IEC 15408	Common Criteria for Information Technology Security Evaluation, August 1999
ISO/IEC DIS 14980	Information technology -- Code of practice for information security management
NSA Security Guidelines Handbook	
NSA/CSS Manual 130-2	Media Declassification and Destruction Manual
NACSIM 5000	TEMPEST Fundamentals
NSTISSI 7000	Tempest Countermeasures for Facilities, September 1993.
NSTISSI 4011	National Training Standard for Information Systems Professionals, June 1994.
NSTISSD 500	Information Systems Security Education, Training and Awareness, February 1993
NSTISSI 4013	National Training Standard for System Administration in Information Systems Security, August 1997

NSTISSI 4014	National Training Standard for Information Systems Security Officers (ISSO), August 1997
NSTISSI 4015	National Training Standard for Systems Certifiers, December 2000
IEEE P1363	Standard Specifications For Public-Key Cryptography, 2003
NIST FIPS 73	Guidelines for Security of Computer Applications, 1980
NIST SP 800-64	Security Considerations in the Information System Development Life Cycle, October 2003
NIST SP 800-61	Computer Security Incident Handling Guide
NIST SP 800-50	Building an Information Technology Security Awareness and Training Program, October 2003
NIST SP 800-55	Security Metrics Guide for Information Technology Systems, July 2003
NIST SP 800-47	Security Guide for Interconnecting Information Technology Systems, September 2002
NIST SP 800-45	Guidelines on Electronic Mail Security, September 2002
NIST SP 800-44	Guidelines on Securing Public Web Servers, September 2002
NIST SP 800-42	Guideline on Network Security Testing, October 2003
NIST SP 800-41	Guidelines on Firewalls and Firewall Policy, January 2002
NIST SP 800-40	Procedures for Handling Security Patches, September 2002
NIST SP 800-36	Guide to Selecting Information Security Products, October 2003
NIST SP 800-35	Guide to Information Technology Security Services, October 2003

NIST SP 800-34	Contingency Planning Guide for Information Technology Systems, June 2002
NIST SP 800-30	Risk Management Guide for Information Technology Systems, January 2002
NIST SP 800-26	Security Self-Assessment Guide for Information Technology Systems, November 2001
NIST SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication, October 2000
NIST SP 800-21	Guideline for Implementing Cryptography in the Federal Government, November 1999
NIST SP 800-18	Guide for Developing Security Plans for Information Technology Systems, December 1998
NIST SP 800-16	Information Technology Security Training Requirements: A Role- and Performance-Based Model, April 1998
NIST SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996
NIST SP 800-13	Telecommunications Security Guidelines for Telecommunications Management Network, October 1995
NIST SP 800-12	an Introduction to Computer Security: The NIST Handbook, October 1995
NIST SP 800-6	Automated Tools for Testing Computer System Vulnerability, December 1992
NIST SP 800-5	A Guide to the Selection of Anti-Virus Tools and Techniques, December 1992

Dónde obtener los estándares

Todos los estándares se pueden obtener de manera gratuita de sitios Web en la Internet, excepto los estándares de la ISO/IEC que sólo pueden ser bajados al comprarlos en el sitio Web de la ISO. Si alguna de las direcciones no lo lleva al estándar buscado, realice una búsqueda en algún motor de búsqueda como Google (www.google.com) con la referencia del estándar.

Estándares del DoD/CSC: http://www.radium.ncsc.mil/tpep/library/rainbow/
http://www.dss.mil/isec/nispom_0195.htm

Estándares de la ISO/IEC: http://www.iso.org

Estándares de la NSTISSC: http://www.nstissc.gov/html/library.html

Estándares de la NSA: http://www.politrix.org/foia/nsa/

Estándares del NIST: http://csrc.nist.gov/publications/

Estándares de la IEEE: http://grouper.ieee.org/groups/1363/

Otros enlaces:
http://www.securityportal.com

Fluid signal Group S.A
http://www.fluidsignal.com