UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

OCTUBRE 2018 – MARZO 2019

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERA EN SISTEMAS

TEMA:

Seguridad de la infraestructura de la red de datos del GAD Municipal del Cantón Vinces

EGRESADA:

Lissette Verónica Escobar Garzón

TUTORA:

Ing. Gladys Guevara Albán.Msc

AÑO: 2019

INTRODUCCIÓN

La seguridad de la información es fundamental para toda entidad pública, puesto que la documentación que se maneja es muy importante y en casos reservada, por los datos de los contribuyentes, debido a lo cual se tiene que tener todas las medidas de seguridad que exigen los estándares internacionales para evitar que los datos de los usuarios sean extraídos de manera fraudulenta.

El Gobierno Autónomo Descentralizado Municipal del cantón Vinces es una entidad de derecho público, que ejerce la representación del Estado en el territorio delimitado en el cantón Vinces, donde se cuenta con la información de todos los propietarios de los predios tanto urbanos como rurales, además de los usuarios de patentes u otros trámites que se realizan, por lo que para agilizar la información de los datos se los ha digitalizado y almacenado en programas informáticos, lo cual es a su vez se encuentran resguardados con protocolos de seguridad para evitar que sufran robo o secuestro por parte de delincuentes informáticos.

La investigación que se realiza es con el propósito de conocer los diferentes elementos que constituye la seguridad de la infraestructura de la red de datos del GAD Municipal del cantón Vinces, en donde se pretende conocer los niveles de seguridad que tiene dentro de la institución para evitar la pérdida de información valiosa de los contribuyentes y documentos internos de la entidad, así como la forma de distribución de

su red interna en todas las dependencias municipales, debido a que existen varios edificios municipales que se enlazan para tener el servicio de internet.

El presente trabajo se enmarca en la línea de investigación Desarrollo de sistemas de la información, comunicación y emprendimiento empresariales y tecnológicos, la sublínea Proceso de transmisión de datos y telecomunicaciones. Se utiliza el tipo de investigación será cualitativo que permitirá conocer aspectos de la calidad de la seguridad de la infraestructura de la red de datos del GAD Municipal del cantón Vinces, se usará la investigación descriptiva, se considera importante el uso del método inductivo – deductivo para la obtención de la información necesaria para comprender la problemática que se presenta en la institución, así mismo para conocer los diferentes elementos que permitirían una alternativa de solución de la misma, como técnicas se usará la entrevista y la observación.

En el presente estudio de caso se ha considerado que los datos informáticos del Gobierno Autónomo Descentralizado Municipal de Vinces deben contar con todas las medidas de seguridad, para lo cual la red de datos debe tener los protocolos que aseguren dicho propósito, lo que será analizado mediante el trabajo investigativo que se pretende realizar, para lo cual se procederá a utilizar diferentes herramientas de la investigación científica y las normas internacionales de Seguridad de datos, llegando a conclusiones que permitan elevar conclusiones sobre los diversos mecanismos que se usan en el GAD Municipal de Vinces para proteger los datos e información de la red.

El incremento del uso de la internet hace que esta red mundial sea fundamental para las operaciones de las empresas y entidades públicas, con lo que se reduce significativamente el uso del papel, además el tiempo que utilizan los trabajadores son menos y por lo tanto reduce los costos operativos de la entidad, también esto conlleva a la responsabilidad de garantizar la integridad, confidencialidad y disponibilidad de los datos.

La información de los usuarios y documentación que posee el Gobierno Autónomo Descentralizado Municipal del cantón Vinces se convierte en un elemento muy importante para la administración, sin embargo, existen personas que se dedican a la piratería informática, quienes hacen los ataques para tener acceso a la misma, por lo que las entidades deben procurar contar con todas las medidas de seguridad para prevenir dichos ataques e impedir que se extraiga la información de la entidad.

DESARROLLO

El Gobierno Autónomo Descentralizado Municipal del cantón Vinces es una entidad de derecho público que goza de autonomía administrativa y financiera, siendo el nivel de gobierno a nivel del territorio cantonal, tiene su sede administrativa en las calles Sucre y 9 de octubre, donde se encuentran las oficinas de los funcionarios: Alcalde, Concejales, Dirección Administrativa, Dirección de Desarrollo y Ordenamiento Territorial, Dirección de Planificación y Gestión Estratégica, Dirección de Gestión Ambiental y Seguridad Ciudadana, Dirección de Gestión Social y Desarrollo comunitario, Dirección de Obras

públicas municipales, Dirección de Servicios Comunitarios y espacios públicos, Dirección financiera, Coordinación general, Procuraduría síndica, y Secretaría general.

Al realizar una entrevista al Lcdo. Agustin Quintana Valenzuela encargado del Departamento de Sistemas informáticos, en cuanto a la infraestructura que posee el Gobierno Autónomo Descentralizado Municipal del cantón Vinces; manifestó que en la parte del cableado estructurado no cuenta con una buena distribución de ella, puesto que se los encuentra tirados en el piso, otros alzados de una forma no adecuada y además no cumplen con las normas establecidas por ISO 27001-2015.

En cuanto al plano de red o la distribución se observó que ha recibido la red ya establecida, y que en el tercer piso alto se encuentra distribuido las oficinas de Dirección financiera, el departamento de informática, salón de actos, y Auditoría externa. Dentro de la oficina de Dirección financiera se encuentra 4 servidores, el switch principal, el router de cnt, están las computadoras del Director, las computadoras del área de contabilidad, con el switch respectivo y una impresora, en la oficina donde yo estoy hay dos computadoras y una impresora, y en el área de auditoría externa se encuentra una computadora y una impresora, también existe un punto de red para dispositivos móviles.

En el segundo piso en el Departamento de Catastros hay un switch que da internet a todos los departamentos de este piso, hay 5 computadoras, en esa misma área funcionan las direcciones de Desarrollo y Ordenamiento territorial, hay 6 computadoras, en la oficina

de Gestión Ambiental hay 3 computadoras, 1 switch, en la oficina de Planificación hay 1 switch y 2 computadoras, en la oficina de Compras Públicas hay 2 computadoras y 1 switch; Secretaría General hay 3 computadoras, y 1 switch; Dirección administrativa 3 computadoras y 1 switch, Procuraduría sindica 4 computadoras y 1 switch, Dirección de Obras Públicas 6 computadoras y 1 switch, Relaciones Públicas y Comunicación 5 computadoras y 1 switch, finalmente Alcaldía 3 computadoras y 1 switch, también existe un punto de red para dispositivos móviles.

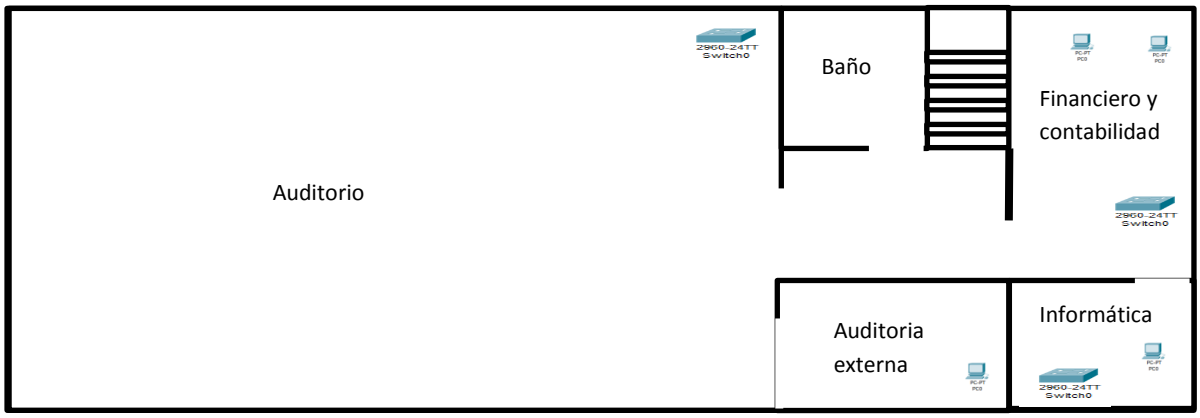
En la planta baja tenemos Vicealcaldía, donde hay un switch que da internet a todos los departamentos de este piso, hay 2 computadoras, en Recaudación hay 3 computadoras, en Tesorería hay 2 computadoras y 1 switch, Departamento de Coactiva Municipal hay 3 computadoras, 1 switch, y 1 punto de red para los dispositivos móviles, Rentas 3 computadoras y 1 switch, y por último Talento Humano tiene 4 computadoras y 1 switch, cada oficina tiene su punto de red para telefonía IP.

En otro de los problemas encontrados se observó que la estructura del edificio es antigua y es difícil hacer perforaciones en la pared para poner canaletas y otro factor es que no se pueden instalar por falta de presupuesto y además se comprobó que los equipos son antiguos, además en la parte de seguridad de la información no han sufrido ataques informáticos, no han analizado la red para comprobar si hay vulnerabilidad, también surgió la información que el GAD cuenta con 13 megabyte de banda de ancho en lo que están divididos en los distintos departamentos. Se tiene deficiencias en el cableado en cada oficina debido a la falta de prioridad en la inversión que se realiza dentro del área de

informática, lo cual origina problemas de diferentes aspectos que conllevan a brindar u servicio deficiente.

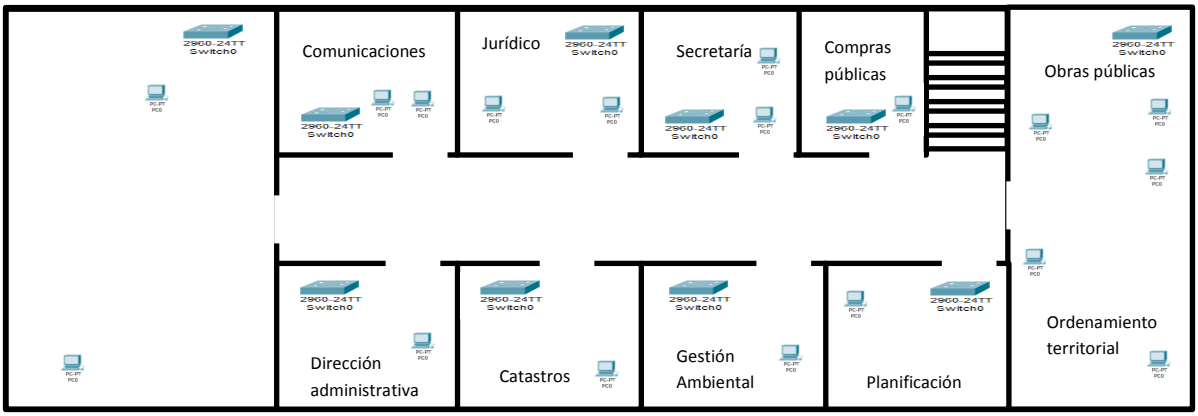
Gráfico Nº 1 Distribución de la Red en el edificio Municipal

Distribución de la red en el Tercer piso



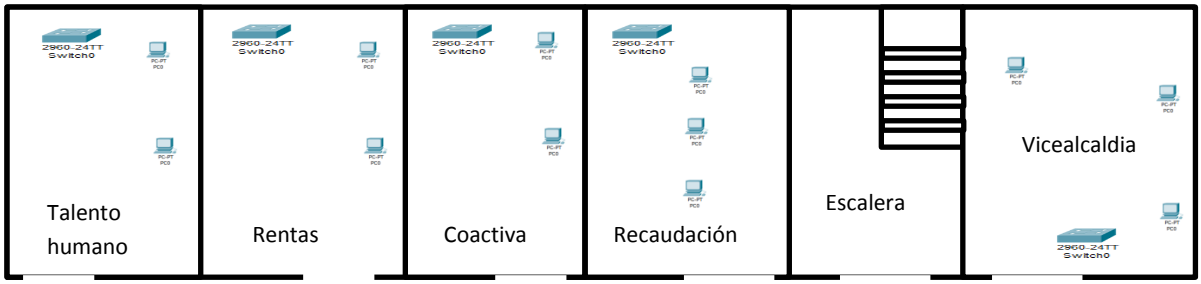
Fuente: Departamento de Informática
Elaborado por: Lissette Escobar G.

Gráfico Nº 2 Distribución de la red en el Segundo piso



Fuente: Departamento de Informática
Elaborado por: Lissette Escobar G.

Gráfico Nº 3 Distribución de la red en la Planta baja



Fuente: Departamento de Informática
Elaborado por: Lissette Escobar G.

Las redes de computadoras tienen una importancia fundamental en el trabajo de la transmisión y almacenamiento de información, para lo cual se consideran diferentes topologías que son el mapa físico o la estructura que se utiliza para interconectar a las computadoras de la red, siendo la más utilizada la topología de estrella. (Stalling, 2014)

La topología que se utiliza en el Gobierno Autónomo Descentralizado Municipal del cantón Vinces es de tipo de Estrella, puesto que se conecta desde el edificio matriz hacia los edificios La Cascada, Camal Municipal, Terminal Terrestre, y Departamento de Tránsito, y desde estos se recepta la señal por medio de enlaces y por switch se distribuye hacia los dispositivos o equipos que se conectan a la red. El cableado que se utiliza es UTP categoría 6, su tendido es horizontal en canaletas, distribuido para las 96 estaciones de trabajo, con el sistema operativo Windows 8.1, requiriendo hacer un mejoramiento del cableado y cambio de los equipos.

La central telefónica para la voz sobre IP se la ha configurado con el Contacvox Unified Communications System que se conecta a la red de datos, esta red se conecta a los

teléfonos IP Grand Stream GXP 285 que están en la mayoría de las oficinas, facilitando la comunicación interna. (Aguilera, 2016, pág. 48)

La seguridad de los datos informáticos en la actualidad es una constante preocupación entre los diferentes profesionales de las redes, considerando que una entidad pública maneja cierta información que es confidencial, datos de los usuarios que permiten tener un control de los ingresos de la administración municipal, así como la página web institucional, los sistemas informáticos que sirven para el uso de los trabajadores en las diferentes dependencias de la entidad. (Martínez, 2015)

En el Gobierno Autónomo Descentralizado Municipal del cantón Vinces se aplican medidas de seguridad como el uso de firewall, antivirus Eset Nod 32 con licencia que permiten la detección de programas malintencionados o dudosos que podrían afectar al equipo o a la red de datos, sin embargo, en los actuales momentos no son suficiente para que pongan freno a un ataque dirigido por profesionales con nuevos métodos y técnicas, también se tiene la vulnerabilidad de conectar dispositivos externos los cuales pueden ocasionar la introducción de todo tipo de virus.

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

con el fin de tener una idea clara de los procesos y procedimientos que se tienen para la seguridad de la información. (Estrada, 2017)

Con el paso del tiempo la internet se ha convertido en la herramienta principal de comunicación en todo el mundo, por lo que la información que se tiene en la base de datos de unas entidad debe resguardársela para lo cual se debe trabajar con los mecanismos y modelos de seguridad entre los que se pueden considerar: Modelo por oscuridad según (Eleclibre, 2014) señala que es uno de los primeros modelos aplicados en la informática, que tiene como base mantener en secreto la información que se posee; otro modelo es el perímetro de defensa que consiste en la separación de la red interna con una red externa, es decir el ataque se genera en el nivel externo lo cual permite proteger la red interna; también se considera el modelo Defensa en profundidad que consiste en tener un sistema de defensa de múltiples capas, al vulnerarse la primera seguridad proporciona tiempo para que los administradores puedan identificar a las personas que quieran vulnerar la red, además de permitir un espacio de tiempo para realizar la implementación de medidas para prevenir un nuevo ataque, para lo cual se debe tener un programa antivirus, firewall, software anti-spyware, contraseñas, detección de intrusos, verificación biométrica, capacitación permanente del personal.

La seguridad de la información tiene unos principios básicos que conllevan a garantizar la confidencialidad, integridad y disponibilidad, siendo estos el eje central para la protección de la información. (Díaz, 2015) La confidencialidad se refiere a que la información debe mantenerse con la absoluta reserva y manejada por las personas

autorizada. (López, 2016, pág. 15) La integralidad es mantener la información generada originalmente sin que pueda sufrir modificación alguna. (Guzmán, 2013) La disponibilidad es la accesibilidad para utilizarla en el momento que se la requiera. (Sánchez, 2016, pág. 103)

En la actualidad cada vez las entidades del sector público y empresas privadas son más dependientes de la internet y de diversos sistemas de información, teniendo en cuenta que los datos que se tienen pertenecen a sus contribuyentes o usuarios y clientes que es muy importante para el desarrollo de sus actividades, lo cual genera mayor cantidad de riesgo y amenazas de ataques por medio de los diferentes instrumentos como los códigos maliciosos, la piratería informática y otras herramientas. (Boquera, 2014, pág. 19)

En el Gobierno Autónomo Descentralizado Municipal de Vinces se utiliza el modelo TCP/IP que se encuentra compuesto 4 capas: acceso a red, internet, transporte y aplicación.

En la capa acceso a red se consideran los equipos de la red, el acceso al cuarto de telecomunicaciones, el cableado, dispositivos remotos, vulnerabilidades en el transporte del mensaje desde su origen hasta su destino. Las amenazas a las instalaciones se pueden dar por falta de un perímetro de seguridad, no implementación de barreras físicas, equipos sin protección, no autenticación de los usuarios, deficiente señalización del edificio,

información no clasificada, interrupción, interceptación, modificación o fabricación de los mensajes. (Benavides, 2014)

En la capa internet en ésta se puede vulnerar el sistema para lo cual se utilizan software espías, que recolectan y transmiten información sensible como el nombre del usuario y contraseña, falsificación de direcciones IP, lo cual hace que la información falsa llegue a la máquina o red víctima.

En la capa transporte se tiene como vulnerabilidad que se intercepta las conexiones TCP abierta, con lo que secuestran la TCP con fines que se desvíen a otra conexión ya establecida, se pueden dar ataques de denegación de servicio (DDoS), en la que se generan errores de conexión, también se tiene ataques por desbordamiento de búfer en donde se recibe un caudal mayor de datos al que tiene capacidad lo cual hace que el sistema no pueda comprobarlo de manera adecuada. (Rivera, 2014)

En la capa aplicación es donde se permite a los usuarios que accedan a los servicios de las demás capas, considerando protocolos estándares como: DNS, Telnet, HTTP y FTP. Una de las vulnerabilidades del servidor DNS es que puede ser modificada a voluntad de la persona que realiza el ataque, pudiendo entregar direcciones incorrectas o captar las peticiones de los usuarios considerando las cuentas. Telnet y FTP tienen la vulnerabilidad que podrían quedar expuestos a que se realice una captura de aplicación sensible de descarga de archivos de una zona restringida, HTTP por medio de este protocolo el

atacante puede ejecutar secuencias de comandos en el navegador web, logrando secuestrar la sesión de usuario, modifican sitios web, insertar contenidos de ataques. (Romero, 2014)

La ISO (International Organization for Standardization), es una entidad que tiene alcance a nivel mundial cuya finalidad es establecer estándares que normalicen diferentes procesos, estas normas se convierten en unas herramientas que regulen las actividades en diferentes áreas. Las Normas ISO permiten asegurar la calidad de los productos y servicios, mediante procesos estandarizados que conllevan a una mejora significativa en la producción y eficiencia. (Gallegos, 2014)

La norma ISO 27001 se encuentra vigente desde el 2013, tiene como enfoque principal el Sistema de Gestión de la Seguridad de la Información (SGSI); se consideran 130 requisitos para la evaluación, cuyos parámetros se encuentran en la Tabla 1. La Norma ISO 27001 como estructura tiene dos etapas según se lo muestra en la Figura 1, estas sirven de guía para elaborar e implementar las políticas de seguridad.

Gráfico Nº 4 Estructura de ISO 27001

Fuente: (Gallegos, 2014)

La norma ISO 27001 se basa en el cumplimiento del SGSI, el mismo que se desarrolla considerando los principios de la seguridad como: confidencialidad, integridad y disponibilidad de la información, procurando con ello tener mayor confianza entre la entidad y los usuarios, con el fin de que se garantice la seguridad de la información que posee la organización. (Boquera, 2014)

Tabla Nº 1 Norma ISO 27001

#	CLÁUSULAS	APARTADOS
0	Introducción	
1	Alcance	
2	Referencias normativas	
3	Términos y definiciones	
4	Contexto de la organización	4.1 Compresión de la organización y su contexto. 4.2 Comprensión de las necesidades y expectativas de las partes interesadas. 4.3 Determinación del alcance del sistema de gestión de continuidad de negocios. 4.4 Sistema de Gestión de Continuidad de Negocios
5	Liderazgo	5.1 Liderazgo y compromiso 5.2 Compromiso gerencial 5.3 Política 5.4 Roles, responsabilidades y autoridades de la organización.
6	Planificación	6.1 Acciones para atender los riesgos y las oportunidades. 6.2 Objetivos de continuidad de negocios y planes para lograrlos.
7	Soporte	7.1 Recursos 7.2 Competencia 7.3 Concientización 7.4 Comunicación 7.5 Información a documentar
8	Operación	8.1 Planificación y control operacional. 8.2 Análisis de impactos en los negocios y valuación de riesgos. 8.3 Estrategia de continuidad de negocios y planes para lograrlos. Establecimiento e implementación de los procedimientos de continuidad de negocios. 8.4 Establecimiento e implementación de los procedimientos de continuidad de negocios. 8.5 Ejercicios y pruebas.
9	Evaluación del desempeño	9.1 Monitoreo, medición, análisis y evaluación 9.2 Auditoría Interna. 9.3 Revisión gerencial.
10	Mejoramiento	10.1 No conformidades y acciones correctivas. 10.2 Mejoramiento continuo.

Fuente: (ISO, 2013)

Para la implementación de la norma ISO/IEC 27001 es importante cumplir las fases:

Fase 1.- Definición del alcance (scope) y los límites de SGSI. En la gestión de seguridad de la información se debe tener claro el ámbito de la aplicación para los diferentes campos y niveles. En el GAD Municipal de Vinces no se observa documentación o datos sobre la implementación de esta fase de la norma.

Fase 2.- Definición de la política de la seguridad. Se tiene que hacer la determinación en la organización de la política de seguridad que se debe adoptar para que la aplicación sea efectiva. No existe en el GAD Municipal de Vinces ninguna política de la seguridad que regule las acciones para hacer del proceso de la seguridad.

Fase 3.- Identificación de los activos de la empresa y sus riesgos asociados. Se deben considerar las siguientes preguntas ¿En qué parte se encuentran las debilidades? ¿Cuáles amenazas se deben priorizar? Dentro del GAD Municipal de Vinces no se evidencia que estén documentados los activos o los riesgos asociados, tampoco hay algún proceso de priorización de las amenazas.

Fase 4.- Control de riesgos. En esta fase se debe responder a las preguntas ¿Qué tipo de riesgos se tienen? ¿Se pueden asumir estos riesgos sin peligros? No se ha podido tener información que determine el control de riesgo que se haga dentro de la entidad lo cual hace que sea vulnerable a cualquier ataque.

Fase 5.- Fijación de controles y objetivos. Es fundamental que todo esté controlado, por lo que se debe contar con la seguridad plena que se cuenta con los objetivos claros y bien definidos para que todos los puedan aplicar. En el GAD Municipal de Vinces no existe documentación que contenga los objetivos y controles que se ejerzan para la seguridad.

Fase 6.- Definición de la Declaración de Aplicabilidad, la conocida SOA (Statement of Applicability), de la norma ISO/IEC 27001. Se considera fundamental que se realice un resumen de todas las decisiones que se tienen para el tratamiento del riesgo. (Stalling, 2014, pág. 11) No se tiene en el GAD Municipal de Vinces evidencia o documentación que permita conocer que exista la declaración de aplicabilidad de esta norma ISO/IEC 27001.

El departamento informático se encuentra encargado al funcionario responsable, se ha ejecutado el análisis de la red a través de la aplicación Sarg, la cual genera estadísticas en el formato html que utiliza como datos los logs de Squid, de todo el proceso de navegación que se ejecuta a través del proxy durante un tiempo determinado. No existe un plan de sistemas, se ha trabajado de manera empírica en la administración municipal, no existe un cuarto de equipos, ni políticas de seguridad de la información y de la red. (Tanenbaum, 2011, pág. 44)

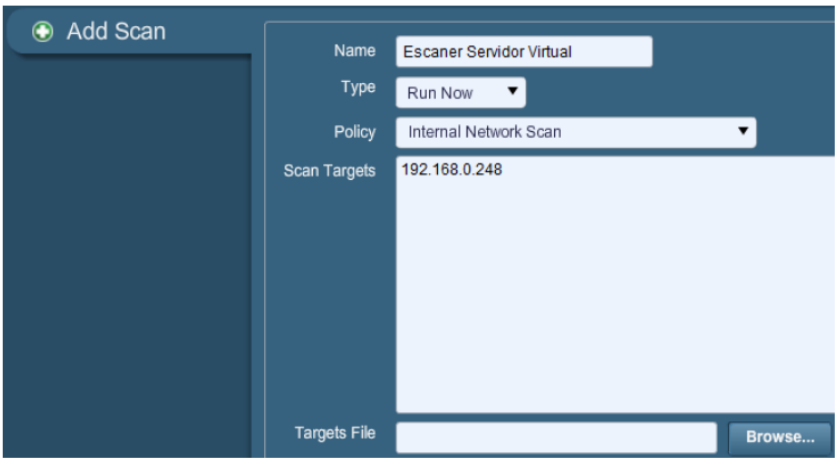
Se ejecutó un escaneo de vulnerabilidades con el programa Nessus a la red, a la página web institucional del Gobierno Autónomo descentralizado Municipal de Vinces www.vinces.gob.ec, este software permite el escaneo de forma más óptima y es de reconocimiento mundial, analiza las vulnerabilidades de los sitios web y realiza 4 análisis diferentes: escaneo interno de la red, escaneo externo de la red, escaneo de preparación para auditorías y escaneos de aplicaciones Web; con dichos datos se puede tomar decisiones que conlleven al mejoramiento y refuerzo de la seguridad.

Gráfico Nº 5 Pantalla principal de la herramienta Nessus

Fuente: (Stalling, 2014)

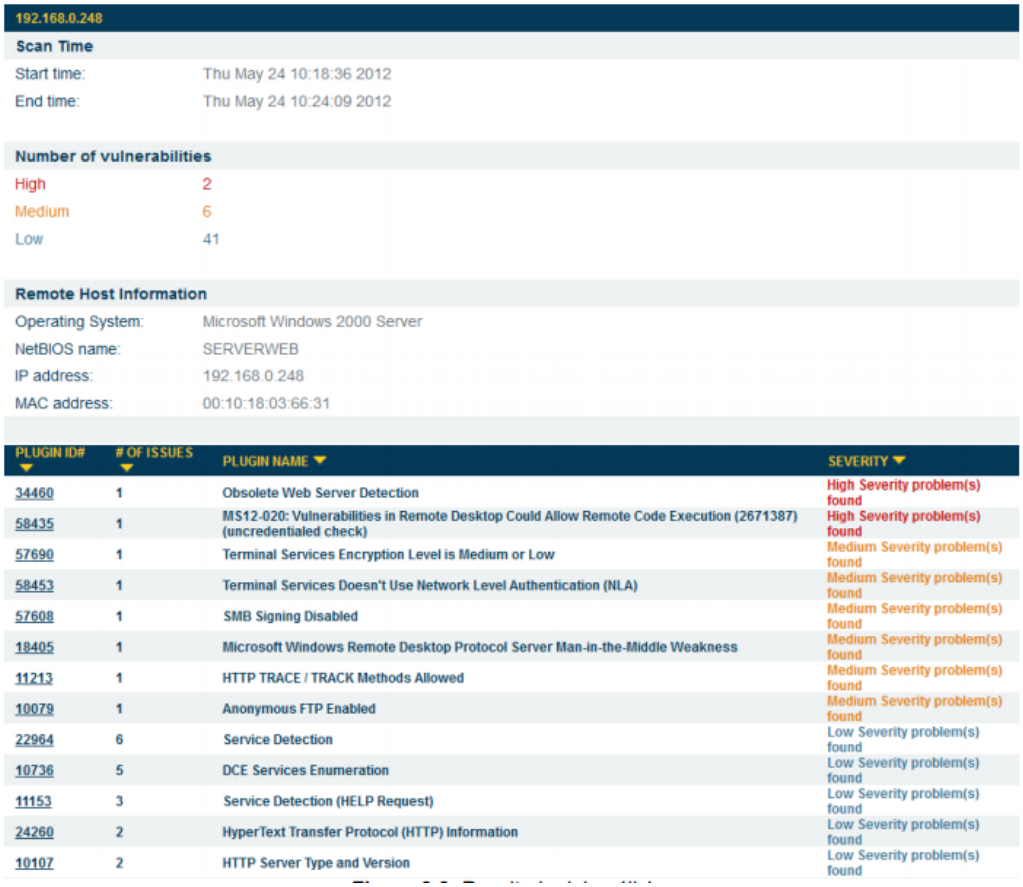
Al hacer clic en los tipos de análisis se despliega otra ventana, por ejemplo para realizar el escaneo interno de la red, se tendría la pantalla del gráfico 3, el mismo que analiza la red interna bajo la IP asignada en este caso será 192.168.0.248. Luego de esperar varios minutos se tiene un informe final sobre las vulnerabilidades que se encuentran en el servidor en la dirección IP que se encuentra en el objetivo, exponiendo los resultados según el gráfico 4.

Gráfico Nº 6 Pantalla del escáner Nessus



Fuente: (Stalling, 2014)

Gráfico Nº 7 Resultado del análisis - Nessus



192.168.0.248

Scan Time

Start time:	Thu May 24 10:18:36 2012
End time:	Thu May 24 10:24:09 2012

Number of vulnerabilities

High	2
Medium	6
Low	41

Remote Host Information

Operating System:	Microsoft Windows 2000 Server
NetBIOS name:	SERVERWEB
IP address:	192.168.0.248
MAC address:	00:10:18:03:66:31

PLUGIN ID#	# OF ISSUES	PLUGIN NAME	SEVERITY
34460	1	Obsolete Web Server Detection	High Severity problem(s) found
58435	1	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	High Severity problem(s) found
57690	1	Terminal Services Encryption Level is Medium or Low	Medium Severity problem(s) found
58453	1	Terminal Services Doesn't Use Network Level Authentication (NLA)	Medium Severity problem(s) found
57608	1	SMB Signing Disabled	Medium Severity problem(s) found
18405	1	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Medium Severity problem(s) found
11213	1	HTTP TRACE / TRACK Methods Allowed	Medium Severity problem(s) found
10079	1	Anonymous FTP Enabled	Medium Severity problem(s) found
22964	6	Service Detection	Low Severity problem(s) found
10736	5	DCE Services Enumeration	Low Severity problem(s) found
11153	3	Service Detection (HELP Request)	Low Severity problem(s) found
24260	2	HyperText Transfer Protocol (HTTP) Information	Low Severity problem(s) found
10107	2	HTTP Server Type and Version	Low Severity problem(s) found

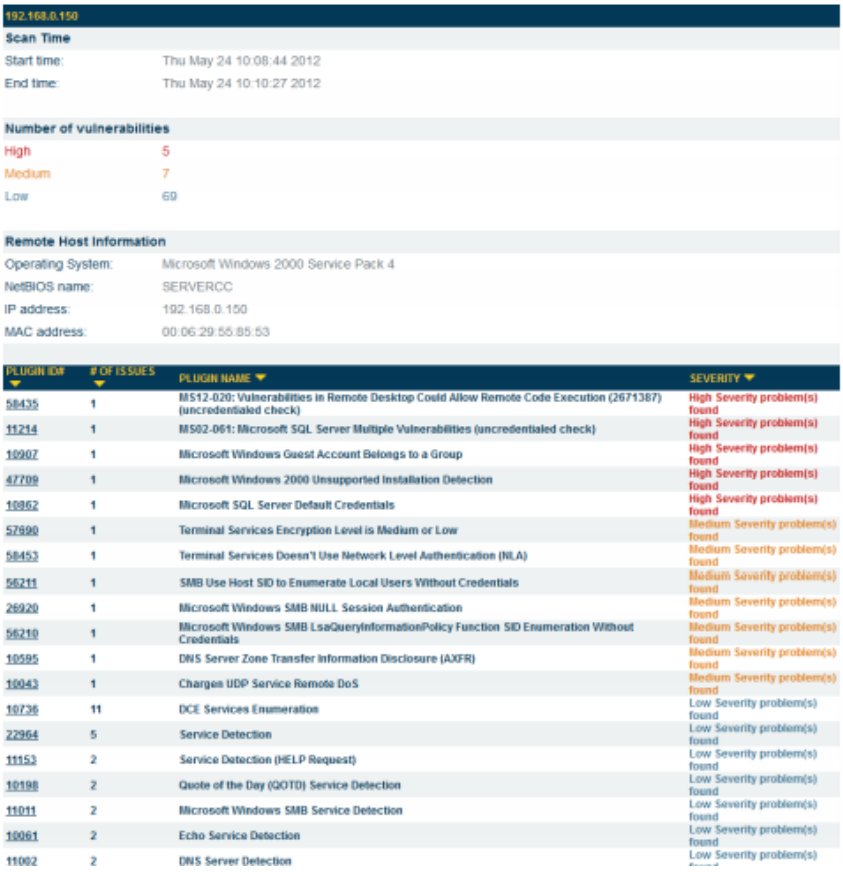
Fuente: (Stalling, 2014)

El resultado obtenido de acuerdo la aplicación Nessus contiene la fecha y hora en la que se hace referencia a la vulnerabilidad encontrada en el escaneo interno de red:

- 2 vulnerabilidades con severidad alta, que se encuentran de color rojo.
- 6 vulnerabilidades con severidad media, que se encuentran de color naranja.
- 41 vulnerabilidades con severidad baja, que se encuentran de color azul.

Se hizo el mismo procedimiento anterior para verificar la otra dirección IP generada 192.168.0.150 en el que se encontró el siguiente informe de vulnerabilidad.

Gráfico Nº 8 Resultado del análisis - Nessus



192.168.0.150

Scan Time

Start time:	Thu May 24 10:08:44 2012
End time:	Thu May 24 10:10:27 2012

Number of vulnerabilities

High	5
Medium	7
Low	69

Remote Host Information

Operating System:	Microsoft Windows 2000 Service Pack 4
NetBIOS name:	SERVERCC
IP address:	192.168.0.150
MAC address:	00:0C:29:55:85:53

PLUGIN ID#	# OF ISSUES	PLUGIN NAME	SEVERITY
58435	1	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check)	High Severity problem(s) found
11214	1	MS02-061: Microsoft SQL Server Multiple Vulnerabilities (uncredentialed check)	High Severity problem(s) found
10907	1	Microsoft Windows Guest Account Belongs to a Group	High Severity problem(s) found
47709	1	Microsoft Windows 2000 Unsupported Installation Detection	High Severity problem(s) found
10862	1	Microsoft SQL Server Default Credentials	High Severity problem(s) found
57690	1	Terminal Services Encryption Level is Medium or Low	Medium Severity problem(s) found
58453	1	Terminal Services Doesn't Use Network Level Authentication (NLA)	Medium Severity problem(s) found
56211	1	SMB Use Host SID to Enumerate Local Users Without Credentials	Medium Severity problem(s) found
26920	1	Microsoft Windows SMB NULL Session Authentication	Medium Severity problem(s) found
56210	1	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration Without Credentials	Medium Severity problem(s) found
10595	1	DNS Server Zone Transfer Information Disclosure (AXFR)	Medium Severity problem(s) found
10043	1	Chargen UDP Service Remote DoS	Medium Severity problem(s) found
10736	11	DCE Services Enumeration	Low Severity problem(s) found
22964	5	Service Detection	Low Severity problem(s) found
11153	2	Service Detection (HELP Request)	Low Severity problem(s) found
10198	2	Quote of the Day (QOTD) Service Detection	Low Severity problem(s) found
11011	2	Microsoft Windows SMB Service Detection	Low Severity problem(s) found
10061	2	Echo Service Detection	Low Severity problem(s) found
11002	2	DNS Server Detection	Low Severity problem(s) found

Fuente: (Stalling, 2014)

CONCLUSIONES

El estudio de caso que se ha realizado ha podido conocer que existen estándares internacionales de la seguridad de la infraestructura de redes de datos, lo cual ha llevado a analizar el departamento de sistemas e investigar los diferentes procesos y procedimientos que se siguen para garantizar la seguridad de la información puesto que no hay un esquema de seguridad que permita la disminución del riesgo de sufrir riesgos de ataques que logren vulnerar el sistema informático.

El Departamento de informática del GAD Municipal del cantón Vinces no tiene una oficina, y que los equipos de redes no poseen un cuarto aislado, sino que funcionan en el misma área que el departamento financiero, donde existe cierto peligro que pone el riesgo la seguridad de la red, además dificulta el trabajo que realiza el funcionario de sistemas, no se cuenta con un plan de seguridad de la información.

Una vez que se terminó el trabajo investigativo se pudo conocer que la seguridad es escaza, que existe mucha vulnerabilidad en un nivel muy alto por lo que se tiene que trabajar para lograr mejorar los niveles de seguridad que se utilizan en la actualidad para que en todas las dependencias de la municipalidad exista la seguridad y las garantías necesarias para el trabajo adecuado de los funcionarios municipales.

No se cumple con los estándares internacionales de seguridad de la información como la ISO/IEC 27001, el cableado es realizado de forma empírica con los equipos no

apropiados lo cual genera inconformidad en los trabajadores municipales, no se cuenta con una bitácora de los eventos que se puedan presentar de forma diaria.

No se cuenta con un plano del edificio de la entidad, ni tampoco un plano de red, lo que hace que la red de datos del Gobierno Autónomo Descentralizado Municipal del cantón Vinces sea diseñada de forma empírica, lo cual dificulta la seguridad en la transmisión de los datos, no pudiendo calcular los requerimientos dando la importancia que tiene esta área para que exista el cuarto de telecomunicaciones de acuerdo con la Norma ANSI/EIA/TIA 569-A, la puesta a tierra según la norma ANS/EIA/TIA-J-STD-607-A.

BIBLIOGRAFÍA

Aguilera. (2016). *Seguridad informática.* Lima: Editex.

Benavides, O. (2014). *Redes de computadoras.* Lima: Usershop .

Boquera, M. (2014). *Servicios avanzados de telecomunicaciones.* Madrid: Librotex.

Díaz, A. (2015). *Vulnerabilidades en redes TDP/IP.* México: Ediciones de la U.

Eleclibre, J. (2014). *La seguridad informática.* Quito: Ediciones Vida.

Estrada, M. (2017). *La red informática.* Quito: Ediciones Adba Yala.

Gallegos, J. (2014). *Fundamentos en seguridad de la información en redes.* México: Editora Editex.

Guzmán, P. (2013). *Auditoría de seguridad informática.* Lima: Ediciones Real.

López, A. (2016). *Seguridad informática.* México: Editex.

Martínez, A. (2015). *La red y su seguridad.* Bogotá: Ecoe Ediciones.

Rivera, L. (2014). *El modelo OSI.* Bogotá: Ecoe Ediciones.

Romero, J. (2014). *Comunicaciones y redes informáticas.* Barcelona: SIGOC.

Sánchez, J. (2016). *Ingeniería de Proyectos Informáticos de seguridad.* México: Unversitad Jaume.

Stalling, W. (2014). *Fundamentos de seguridad en redes aplicaciones y estándares.* Madrid : Editorial Pearson Educación.

Tanenbaum, A. (2011). *Redes de computadoras.* México: Editorial Pearson Educación.

ANEXOS

ANEXOS

Entrevista al Jefe de Informática del Gobierno Autónomo Descentralizado Municipal del cantón Vinces

¿Cuál es su título y cargo?
Soy Licenciado en Informática Educativa, tengo el cargo de Jefe de Informática del GADM del cantón Vinces.

¿Cuál es la topología de red que se utiliza en la Institución?
Se usa una topología de red de tipo estrella.

¿De qué forma se distribuye el cableado?
Se encuentra en forma de cascada.

¿Existe un plano de red en el GADM del cantón Vinces?
No existe un plano de red, ni en el departamento de obras públicas, las oficinas la utilizan de acuerdo a la necesidad.

¿Cómo se encuentra distribuida la red en el Gobierno Autónomo Descentralizado Municipal del cantón Vinces?
Hemos recibido la red ya establecida, en el tercer piso alto se encuentra distribuido de la siguiente forma:

Área	Oficina	Servidor	Computadoras	Switch	Router	Impresora	Telefonía IP
Tercer Piso	Dirección financiera	4	1	1	1	1	1
	Contabilidad		5	1		1	1
	Informática		2	1		0	1
	Auditoría externa		1	0		1	1
	Salón de actos						
Segundo Piso	Departamento de Castros		5	1		1	1
	Desarrollo y Ordenamiento Territorial		6	1			1
	Gestión ambiental		3	1		1	1
	Planificación		2	1		1	1
	Compras públicas		2	1			1
	Secretaria		3	1		1	1
	Dirección administrativa		3	1		1	1
	Procuraduría síndica		4	1		1	1
	Obras públicas		6	1		1	1
	Relaciones públicas y comunicación		5	1		1	1
	Alcaldía		3	1	1	1	1
Planta baja	Vicealcaldía		2	1		1	1
	Recaudación		3	1		3	1
	Tesorería		2	1		1	1
	Coactiva		3	1	1	1	1
	Rentas		3	1		1	1
	Talento humano		4	1		1	1

Otro edificio donde se tienen oficinas es el local del Centro comercial La Cascada, donde hay un enlace de datos de 2 megas.

Área	Oficina	Computadoras	Switch	Impresora	Telefonía IP
Segundo Piso	Oficina	3	1	1	
Primer Piso	Oficina de turismo	2	1	1	
	Comisaría Municipal	2	0	0	
	Oficina Servicios públicos	1	0	1	1

En el Camal Municipal hay un enlace de datos.

Área	Oficina	Computadoras	Switch	Impresora	Telefonía IP
Administración	Camal	2	1	0	1

La Unidad Municipal de Tránsito hay un Cisco de enlace de datos.

Área	Oficina	Computadoras	Switch	Router	Impresora	Telefonía IP
Planta baja	Unidad de Tránsito	7	1	1	1	1
Segundo piso	Gestión social	6			1	1
	Salud ocupacional	2	0	0	0	0

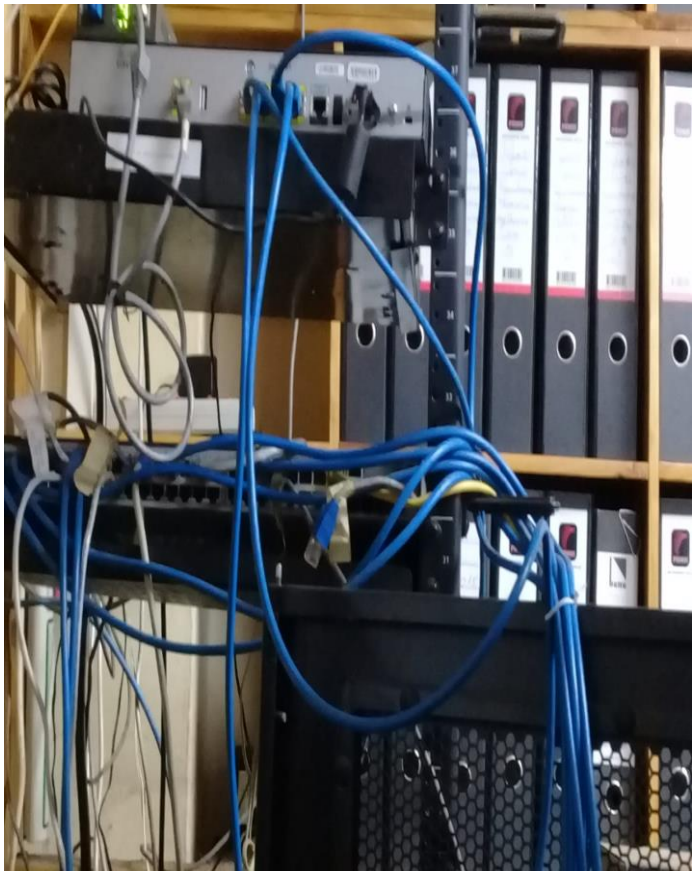
En el Camal Municipal hay un enlace de datos.

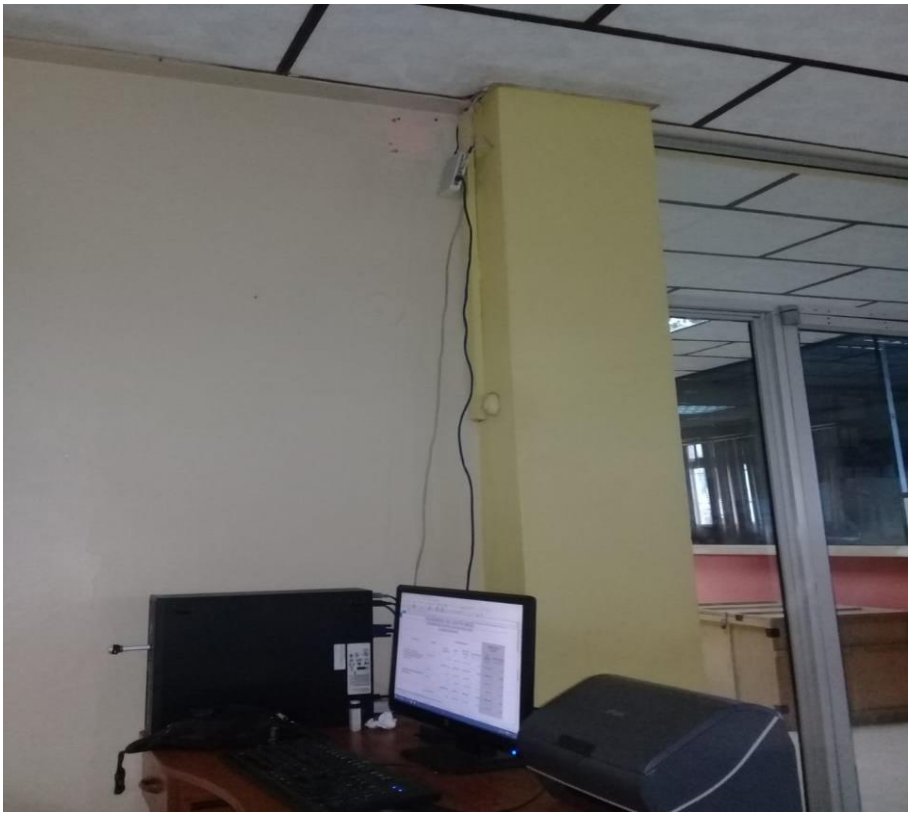
Área	Oficina	Computadoras	Switch	Router	Impresora	Telefonía IP
Administración	Camal	2	1	1	0	1

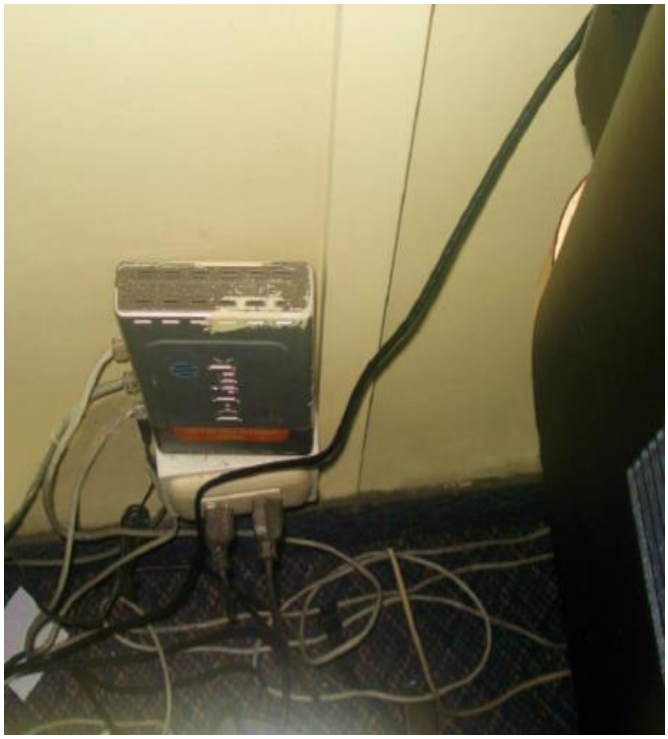
¿Se tiene previsto ampliar la red a otras oficinas o dependencias?
Sí, la Planta de tratamiento de agua pero todavía no se han hecho los estudios para dicho fin.

¿Se utiliza alguna norma para la seguridad de la red de datos?
Tengo poco tiempo en la oficina, no he podido observar que se apique o se haya aplicado alguna norma, aquí todo se ha hecho de manera empírica, el edificio es viejo, no existe el cableado estructurado, hemos mejorado la disposición de los cables dentro de canaletas, ya no hay cables fuera del edificio, hay mucho por hacer pero no se asignan los recursos necesarios por lo que no se puede avanzar en este objetivo.

Evidencias Fotográficas







ÍNDICE

ÍNDICE GRÁFICOS

ÍNDICE DE TABLAS