UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

MAYO - OCTUBRE 2018

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERO EN SISTEMAS

TEMA:

ESTUDIO PARA MEJORAR LA SEGURIDAD DE LA RED DE LA EMPRESA PARIS.NET DEL CANTÓN VINCES

EGRESADO:

BENITES HIDALGO JORGE LUIS

TUTOR:

LSI. FREDY M. JORDAN C. MSC

AÑO 2018

INTRODUCCIÓN

En la actualidad en varias empresas es necesario incorporar e implementar tecnologías informáticas, con la finalidad de mejorar la organización, la automatización, la información generada y optimizar los recursos sin embargo esta realidad no será factible, sin tener una buena política de seguridad. París.Net es una empresa ISP (Proveedor de Servicios de Internet), se encuentra ubicada en las calles Quito y Machinaza del cantón Vinces, Provincia de Los Ríos, su actividad comercial es de proveer servicios de internet a la comunidad.

Proteger un sistema requiere muchas veces desactivar servicios, bloquear y limitar características de software que pueden ser fácilmente la puerta de ingreso a un sistema, de ésta manera se está comprimiendo en gran medida un número de debilidades. Se busca identificar las diferentes vulnerabilidades que dejaron los ex responsables encargados de configurar y administrar las redes, debilitar los posibles ataques que realizan los virus y hackers, así como corregir los errores en las comunicaciones".

El desarrollo de este estudio de caso, describe a la sub-línea de investigación de la carrera que son los procesos de transmisión de datos y telecomunicaciones, la metodología utilizada es el método cuantitativo, debido a que este método es el más empleado para esta investigación la cual permite realizar preguntas abiertas, cerradas y de opciones múltiples usando las variables de información y datos. Es decir, que trata de analizar y delimitar la asociación, la generalización y el objeto de los resultados que se obtiene al estudiar una población. La técnica que se utilizo es la encuesta.

DESARROLLO

París.Net dio sus inicios en el año 2018 como un ISP (Proveedor de Servicios de Internet), es una empresa dedicada a prestar servicios de internet a la ciudadanía de Vinces, Santa Matha y Palenque, la cual se encuentra ubicada en las calles Quito y Machinaza del cantón Vinces, Provincia de Los Ríos. En la actualidad la empresa cuenta con siete empleados distribuidos en cuatro áreas departamentales que son: Gerencia, Financiera-Contable, Ventas-Cobranzas y Departamento Técnico. La actividad principal de esta organización es proveer el servicio de internet y televisión por fibra óptica con tecnología GPON a sus clientes.

Por esta razón se realiza el presente informe que muestra el estudio de caso **"**Estudio para mejorar la seguridad de la red de la empresa Paris.Net del Cantón Vinces" con la finalidad de corregir la seguridad de la red interna de dicha organización porque nos permitirá identificar de mejor manera los accesos no permitidos, puertos o servicios innecesariamente activos, equipos sin contraseñas, accesos remotos no autorizados.

La inseguridad viene de varias formas, en las redes es igual. Un gran conglomerado de organizaciones e instituciones educativas como por ejemplo universidades. Desean obtener una dominante seguridad, para no tener pérdidas económicas, de privacidad y de confidencialidad. Para poder estar tranquilos, sin preocupaciones simplemente se debe tener una buena planeación, y organización para poder proteger una infraestructura lógica y física de una red.

Según (Areitio, 2014) indica que “La seguridad en la red es el nombre genérico para el conjunto de herramientas diseñadas para proteger los datos durante su transmisión a través de una red de telecomunicación. Las conquistas de las compañías dependen en su gran totalidad de la tecnología que se use, por esta razón es de gran importancia la seguridad en la red ya que se centraliza en la defensa de los datos durante su transferencia.

La información es una primacía para usuarios perversos que ejecutan eventos fraudulentos, de las cuales utilizan cuantiosas formas para adquirir información. La seguridad es el aspecto fundamental para obtener un óptimo funcionamiento en las redes, ya que por medio de esta se respalda la integridad y confidencialidad de los datos e información. Una ilegalidad en la seguridad genera serios daños en la estabilidad de la red. La evasión de las políticas de seguridad va a generar la perdida de datos importantes dentro de una organización. Se plantea en este estudio de caso la necesidad de identificar las vulnerabilidades en la red y que tipos de amenazas se encuentra expuestas.

Definir una política de seguridad de la red significa desarrollar procedimientos y planes que resguarden los recursos de la red en contra de la perdida y daño de la misma. Según (DIAZ ORUETA , ALZÓRRIZ ARMENDÁRIZ, SANCRISTÓBAL RUIZ , & CASTROL GIL, 2014) que “Son unas series de normas que deben cumplir todas las personas que tengan acceso a cualquier información y/o tecnología de una organización”. Para crear estas políticas se debe tener en cuenta que recursos se van a proteger, de quienes se debe proteger, las probables amenazas y qué medidas se pueden ejecutar para resguardar los recursos. Consecutivamente inspeccionar periódicamente la red y así poder ver si es factible realizar cambios en la política de seguridad.

En la empresa Paris.Net no existe un control de acceso, ya que los empleados no asignados a las áreas administrativas y familiares de los mismos toman uso de los equipos informáticos existentes, habiendo una gran vulnerabilidad en la red. Como menciona (Alonso, 2013) que "Los métodos para controlar el acceso al medio son necesarios para garantizar que solo un usuario de la red pueda transmitir en cada momento evitando conflictos y errores. El control de acceso al medio condiciona las características más importantes de la red como la disponibilidad, la fiabilidad, el rendimiento y la gestión de la propia red".

La poca seguridad que existe se debe a que el propietario no está de acuerdo en tener una seguridad para cada computadora, ahí surge la problemática cuando acuden otras personas que no trabajan en el sitio y utilizan cualquier computadora desocupada sin pensar en los problemas que le causarían al trabajador. Según (Blanco Antón & Calvo Vérgez, 2013) que "En los lugares en los que se encuentren ubicados o instalados los equipos físicos que den servicios a los sistemas de información con datos de carácter personal deberán tener restringido su acceso. Estos lugares se consideran como espacios con acceso restringido y únicamente el personal autorizado en el documento de seguridad puede acceder a ellos"

Los equipos informáticos no cuentan con ningún tipo de seguridad de autenticación y esto conlleva a que todos los colaboradores puedan acceder a la importante información que existe en los ordenadores la cual ocasiona que se pierdan archivos por el mal uso de los equipos, encontrándose que algunas de las personas que laboran en el misma suelen entretenerse en otras actividades tales como las redes sociales, descarga de programas y música.

Como menciona (Teheràn Sierra, 2014) “Es de gran importancia conocer sobre la inseguridad y los riesgos que puedan afectar a una red de datos dentro de una institución por lo tanto sin la búsqueda de vulnerabilidades en una las organizaciones crean una idea equivocada de su seguridad, cave recalcar que algunas de las debilidades que se generan frecuentemente son el hecho de usar contraseñas predeterminadas o débiles en seguridad”.

Los colaboradores no tienen ningún medio seguro para la transferencia de información ya que lo hacen por medio de USB muchas veces infectados y correo electrónico, evidenciándose que esta forma tampoco es segura al momento del intercambio de información porque los empleados abren cualquier mail que reciben sin darse cuenta lo peligroso que puede ser, los sistemas están propensos a ser invadidos de virus informáticos, los cuales son programas generalmente destructivos y pueden provocar perdida de la información almacenada en los discos duros. El personal desconoce casi todos los riesgos que hay sobre la inseguridad.

Según (Ortiz Orellana & Villegas Lara, 2014) expresa que “En la seguridad de la información es importante señalar que su manejo está basado en la tecnología y debemos saber que puede ser confidenciales: la información está centralizada y puede tener un alto valor. Puede ser divulgada, mal utilizada, ser robada, borrada o saboteada. Esto afecta su disponibilidad y la pone en riesgo. La información es poder, y según las posibilidades estratégicas que ofrece tener acceso a cierta información”, esta se clasifica como:

- **Critica**: es indispensable para la operación de la empresa
- **Valiosa:** es un activo de la empresa y muy valioso.

- **Sensible:** debe de ser conocida por las personas autorizadas

En la empresa París.Net se puede evidenciar donde hay varios puertos abiertos que de tal manera que estos son una vulnerabilidad a la seguridad como ya mencione antes, cualquier familiar de los colaboradores o incluso del mismo dueño tienen acceso a los equipos informáticos existiendo una gran amenaza, como determina (Santo Orcero, 2018) que "Kali Linux trae preinstalados una gran cantidad de programas relacionados con el tema de la seguridad informática (más de 600 programas), siendo algunas de las más conocidas Nmap (un escáner de puertos), Wireshark (un sniffer), John the Ripper (Un crackeador de passwords) y la suite Aircrack-ng (Software para pruebas de seguridad en redes inalámbricas), además del inigualable Metasploit, la gran suite de explotación de vulnerabilidades".

Se encuentra que hay 3 equipos informáticos con sus actualizaciones de seguridad desactivadas lo cual esto implica un grave riesgo para la seguridad de cada computadora y a la red. Como menciona (Pardo Muñoz, 2014) "lo único que no podemos descuidar son las actualizaciones de seguridad (para evitar vulnerabilidades del sistema por donde puedan colarse virus). Las actualizaciones podemos conseguirla por diversos medios, algunas como los Updates (actualizaciones) de Windows podemos conseguirlas de forma automatizadas, pero las actualizaciones de drivers en la página de los fabricantes suelen ser mensuales".

Los antivirus que están instalados son de prueba, limitando la protección a 30 días, cuando este tiempo se cancela se puede aprovechar las vulnerabilidades de los sistemas operativos donde fácilmente se pueden alojar virus comprometiendo los recursos de los equipos de la red y de los

programas instalados. Esto genera perdida de la productividad al no poder utilizar los equipos informáticos no contando con el tiempo de reinstalación del S.O. en consecuencia la perdida de datos y el periodo de tiempo para poder recuperar la información. Los colaboradores al utilizar una USB no se toman ni el tiempo de analizar esta herramienta informática aunque esto no sería de gran ayuda porque los antivirus que utilizan no cuentan con una licencia valida.

Como menciona (Cerra, 2010) “Las amenazas de seguridad que se presenta de manera más frecuente en una PC son los famosos virus informáticos y el malware. Esta última pertenece a una nueva generación de amenazas informáticas que incluyen los adware y spyware; las maquinas infectadas por ellos suelen funcionar con lentitud. Además, la privacidad del usuario no está asegurada en los equipos infectados”.

Se ejecutó un ataque de inundación de direcciones MAC, donde se realizó un mapeo de la red con Nmap que es una aplicación de software libre que sirve para administrar y explorar la seguridad de las redes de ordenadores. Detectan los puertos abiertos**,** vulnerabilidades de los hosts de la red, sus sistemas operativos, la versión, las aplicaciones que están activas. Nmap envía diferentes tipos de paquetes a cada uno de los puertos que responderán con señales que permiten escanear y poder encontrar versiones y servicios.

Utilizamos metasploit que es un instrumento de código abierto creado para ejecutar exploits, viene incluida en las herramientas de explotación de vulnerabilidades de seguridad de Kali Linux. Vamos a intentar ingresar a los 4 ordenadores de la empresa Paris.Net del cantón Vinces que a simple vista se puede observar las vulnerabilidades que poseen. Como menciona

(Astudillo Basilio, 2013) “Los niveles de riesgos se clasifican en bajo, medio y alto, conforme a la siguiente escala:

Riesgo Alto: se considera alto cuando el equipo escaneado tiene una o más vulnerabilidades críticas que podrían ser explotadas fácilmente por un atacante y que podría conllevar total control del sistema o comprometer la seguridad de la información contenida. Los equipos que tengan este nivel de riegos requieren acciones correctivas inmediatas.

Riesgo Medio: cuando el equipo tiene una o más vulnerabilidades severas que requieren una mayor complejidad y tiempo para poder ser explotadas y que podrían no brindar el mismo nivel de acceso. Los equipos con riegos severos requieren atención a corto plazo.

Riesgo Bajo: cuando un equipo tiene unas más vulnerabilidades que podrían brindar información al momento de atacar, la cual podría usarse para realizar ataques posteriores. Estos riesgos deben ser mitigados adecuadamente, pero no tienen un nivel de urgencia alto”.

Ejecutaremos un ataque con MAC Flooding Attack (Ataque de Inundación de Direcciones MAC) Es una forma de atacar a la tabla CAM (Memoria de Contenido Direccionable) que traen los switch internamente a esto se asignan direcciones MAC individuales a los puertos físicos del switch. Esto permite que se dirijan los datos fuera de los puertos físicos donde se encuentra el destinatario. Según (Caballero Gonzàlez & Matamala Peinado, 2017) expresa que “el filtrado de una dirección MAC es una estrategia de seguridad para impedir o permitir que un determinado host pueda acceder a la red, se puede aplicar a distintos dispositivos a nivel de enlace, como un

switch o un punto de acceso. El filtrado MAC se puede hacer por listas blancas, que especifican los host que pueden acceder a la red, y por listas negras, que indican las direcciones físicas de los host bloqueados.

Los tres modos de violación de seguridad son:

- Shutdown: La interfaz se desactiva (err-disable) cuando hay violación de seguridad y se notifica (Default).
- Restrict: Las direcciones MAC de origen que no cumplan la política son detenidos y se notifica.
- Protect: Las direcciones MAC de origen que no cumplan la política son detenidos y no se notifica.

VULNERABILIDADES Y RIESGOS ENCONTRADOS EN PARIS.NET DEL CANTON VINCES					
DEPARTAMENTO	**EQUIPOS**	**SISTEMAS OPERATIVOS**	**VULNERABILIDADES**	**NIVEL DE RIESGO**	**NIVEL DE SEGURIDAD**
GERENCIA	ORDENADOR 1	WINDOWS 10 HOME DE 64 BITS	• Actualizaciones del sistema deshabilitadas. • Antivirus sin licencia • Puertos vulnerables • Equipos sin contraseñas • Acceso sin restricción • Transferencia de información en flash memory	ALTO	BAJO
FINANCIERA/CONTABLE				ALTO	BAJO

	ORDENADOR 2	WINDOWS 10 HOME DE 64 BITS	• Actualizaciones del sistema deshabilitadas. • Antivirus sin licencia • Puertos vulnerables • Equipos sin contraseñas • Acceso sin restricción • Transferencia de información en flash memory		
VENTAS Y COBRANZAS	ORDENADOR 3	WINDOWS 10 HOME DE 64 BITS	• Actualizaciones del sistema deshabilitadas. • Antivirus sin licencia • Puertos vulnerables	ALTO	BAJO

			• Equipos sin contraseñas • Acceso sin restricción • Transferencia de información en flash memory		

Tabla N°1

Elaborado por: Jorge Benites

CONCLUSIONES

Se ejecutó un escaneo completo a la red con Nmap, encontrándose varios puertos abiertos que a mi criterio personal son los más importantes el 4444, 80 por los cuales pueden tener acceso no autorizado a los ordenadores de la empresa Paris.Net.

Dados a los niveles bajos de seguridad se concluye que en la empresa Paris.Net del cantón Vinces los colaboradores pueden provocar una crisis general en cualquier momento, en una organización donde intervienen factores como la gran cantidad de información delicada que existe, pese a esto tienen la confianza que mejore estos aspectos relacionados a la seguridad.

De acuerdo a la inseguridad que existe en los procesos administrativos por parte de los empleados en especial las personas que no trabajan en la empresa y como se ha analizado en este estudio, esto se debe a la falta de conocimiento sobre los equipos que utilizan ya que no han recibido ninguna capacitación los empleados de Paris.Net.

Concluyendo las decisiones tardías que tome el gerente propietario pueden llegar a ser perjudiciales para los colaboradores que conforman los diferentes departamentos, porque la inseguridad es latente y persistente. Se debe tomar acciones inmediatas respecto a la seguridad para evitar ataques dentro y fuera de la red.

BIBLIOGRAFÌA

1. Alonso, O. N. (2013). *Redes de Comunicación.* Madrid: Universidad Nacional de Educación a Distancia.
2. Astudillo Basilio, K. (2013). *Hacking Ètico.* Guayaquil: Createspace Independent.
3. Blanco Antón, J., & Calvo Vérgez, L. (2013). *Protección de Datos Comtarios al Reglamento.* Lex Nova.
4. Caballero Gonzàlez, L., & Matamala Peinado, M. (2017). *Verificacion e incidencia en una red de àrea local.* Madrid: Paraninfo.
5. Cerra, M. (2010). *200 Respuestas: Seguridad.* Buenos Aires: Fox Andina.
6. DIAZ ORUETA , G., ALZÓRRIZ ARMENDÁRIZ, I., SANCRISTÓBAL RUIZ , E., & CASTROL GIL, M. (2014). *Procesos y herramientas para la seguridad en redes.* Madrid: UNED.
7. Ortiz Orellana, A., & Villegas Lara, R. (2014). *Seguridad de la Información.* Guatemala: Universidad de San Carlos de Guatemala.
8. Pardo Muñoz, F. (2014). *Instalaciòn y actualizaciòn de sistemas operativos.* España: Editorial Elearning S.L.
9. Santo Orcero, D. (2018). *Kali Linux.* Madrid: Ra-Ma.
10. Teheràn Sierra, L. (2014). *Mecanismos de autenticaciòn y Control de acceso.* Madrid: Uniandes.

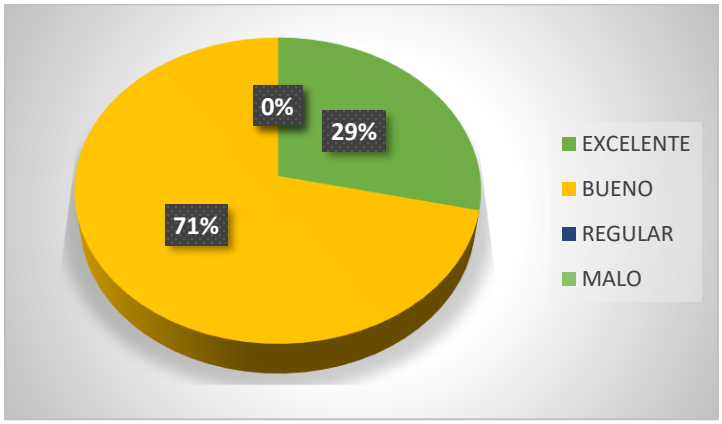
ANEXO 1

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

ENCUESTA.
DIRIGIDA: A los colaboradores que trabajan en la empresa Paris.Net
OBJETIVO: Conseguir información para poder analizarla.
Grave con una X la respuesta que usted considere.

1.- ¿Qué considera usted sobre la seguridad de las Tecnologías de información y comunicación de la empresa Paris.Net del cantón Vinces?

DESCRIPCIÒN	RESULTADOS	
	#	%
EXCELENTE	0	0%
BUENO	0	0%
REGULAR	4	57%
MALO	3	43%
TOTAL	7	100%

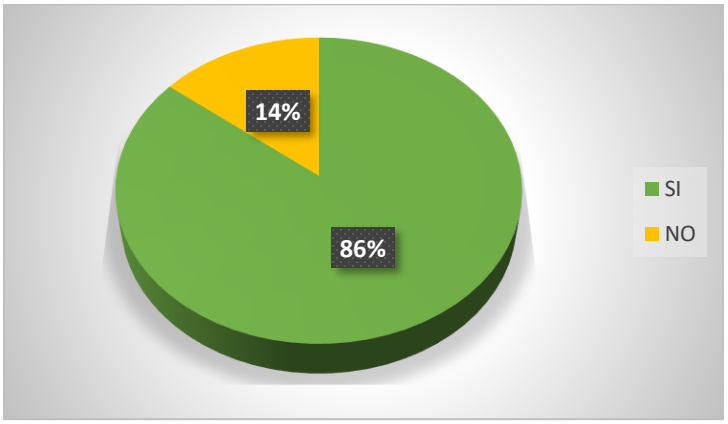


Elaborado por: Jorge Benites

Análisis.- De acuerdo a los resultados obtenidos de la encuesta aplicada el 43% de los colaboradores respondió que la seguridad de las TIC es regular, el 57% contesto que es malo.

2.- ¿Piensa que es necesario ejecutar una auditoria informática para calcular los niveles de seguridad de las Tecnologías de información y comunicación en la empresa Paris.Net del cantón Vinces?

DESCRIPCIÒN	RESULTADOS	
	#	%
SI	6	86%
NO	1	14%
TOTAL	7	100%

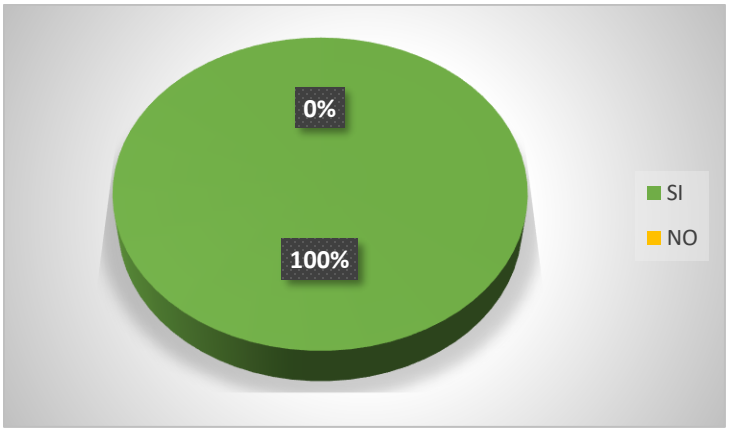


Elaborado por: Jorge Benites

Análisis.- De acuerdo a los resultados obtenidos de la encuesta aplicada el 86% de los colaboradores respondió que si es necesario realizar una auditoria informática, el 14% contesto que no es necesario porque retardaría el trabajo de los compañeros.

3.- ¿Al formalizar la auditoria informática se hallará problemas en la seguridad de las Tecnologías de información y comunicación en la empresa Paris.Net del cantón Vinces?

DESCRIPCIÒN	RESULTADOS	
	#	%
SI	7	100%
NO	0	0%
TOTAL	7	100%

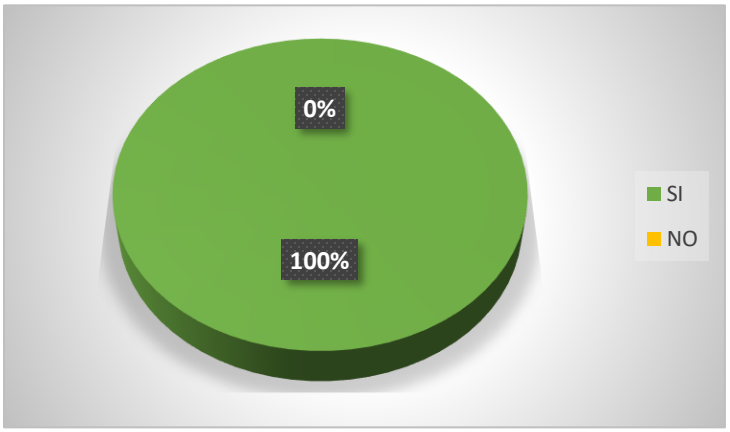


Elaborado por: Jorge Benites

Análisis.- De acuerdo a los resultados obtenidos de la encuesta aplicada el 100% de los colaboradores respondió que si se encontraran problemas en las seguridades de las TIC.

4.- ¿Será necesario violar la seguridad de la red y los equipos de cómputo para encontrar soluciones en la empresa Paris.Net del cantón Vinces?

DESCRIPCIÒN	RESULTADOS	
	#	%
SI	7	100%
NO	0	0%
TOTAL	7	100%

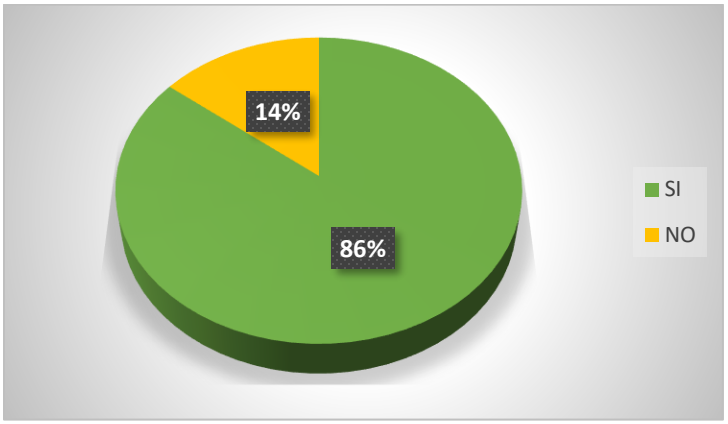


Elaborado por: Jorge Benites

Análisis.- De acuerdo a los resultados obtenidos de la encuesta aplicada el 100% de los colaboradores respondió que si se necesita vulnerar la seguridad de la red para encontrar problemas y soluciones.

5.- ¿Si se encuentra vulnerabilidades el gerente debe tomar medidas urgentes para proteger la integridad de la empresa Paris.Net del cantón Vinces?

DESCRIPCIÒN	RESULTADOS	
	#	%
SI	6	86%
NO	1	14%
TOTAL	7	100%

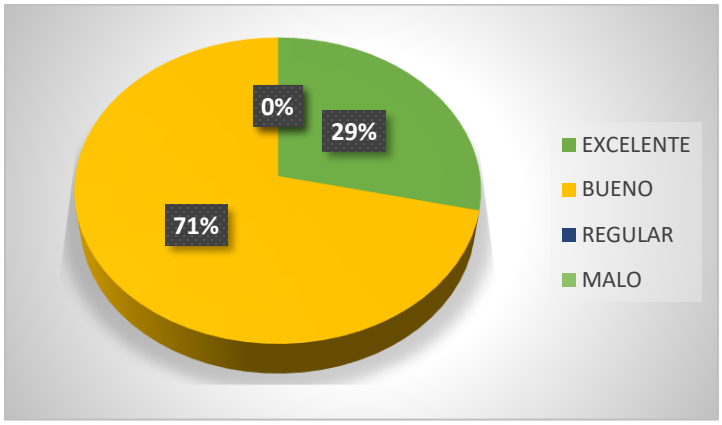


Elaborado por: Jorge Benites

Análisis.- De acuerdo a los resultados obtenidos de la encuesta aplicada el 86% de los colaboradores respondió que el gerente debería tomar acciones inmediatamente, el 14% contesto que no es necesario porque retardaría el trabajo de los compañeros.

6.- ¿Qué piensa usted sobre la auditoria informática que se va a realizar en la empresa Paris.Net del cantón Vinces?

DESCRIPCIÒN	RESULTADOS	
	#	%
EXCELENTE	2	29%
BUENO	5	71%
REGULAR	0	0%
MALO	0	0%
TOTAL	7	0%



Elaborado por: Jorge Benites

Análisis.- De acuerdo a los resultados obtenidos de la encuesta aplicada el 71% de los colaboradores respondió que es excelente realizar una auditoria informática, el 14% contesto que es bueno la auditoria.

ANEXO 2

Mapeo del segmento completo de la red LAN

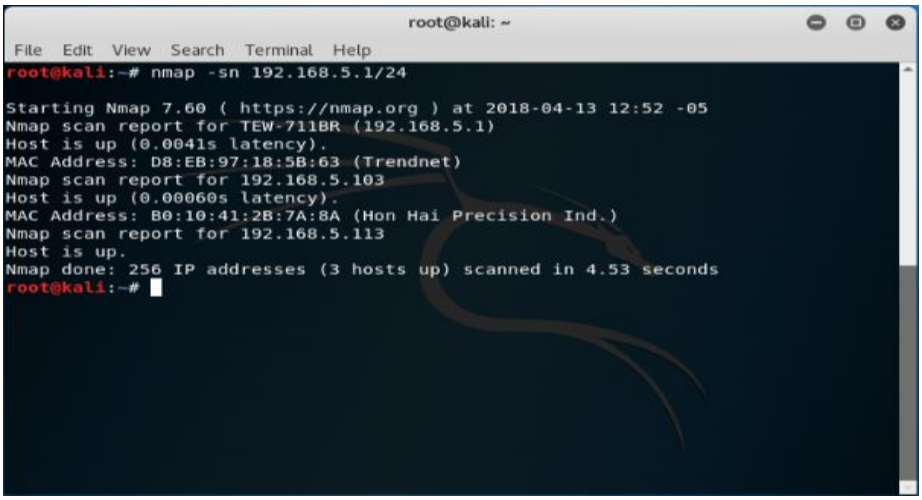


Gráfico N° 1

Elaborado por: Jorge Benites

Escaneo de cada host con Nmap

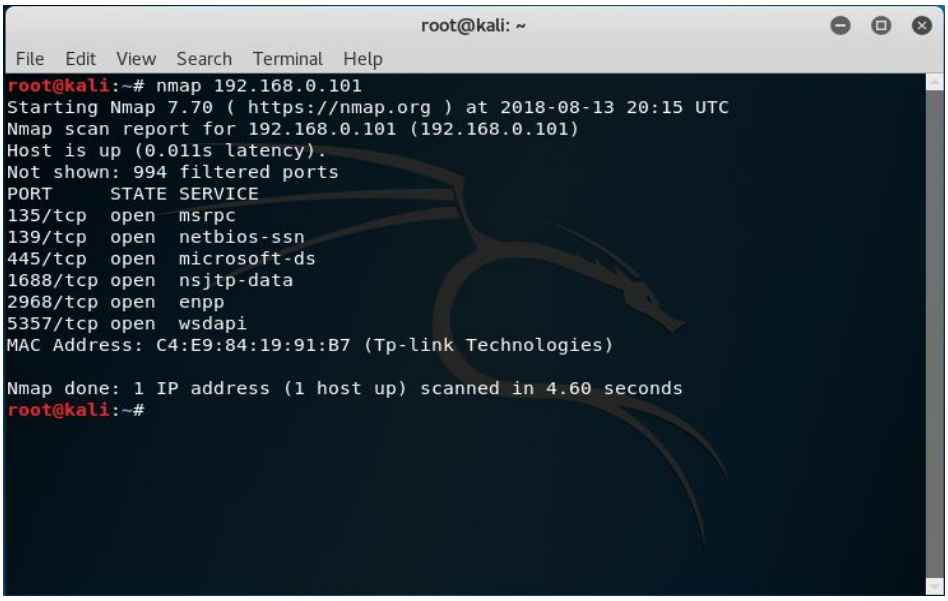


Gráfico N° 2

Elaborado por: Jorge Benites

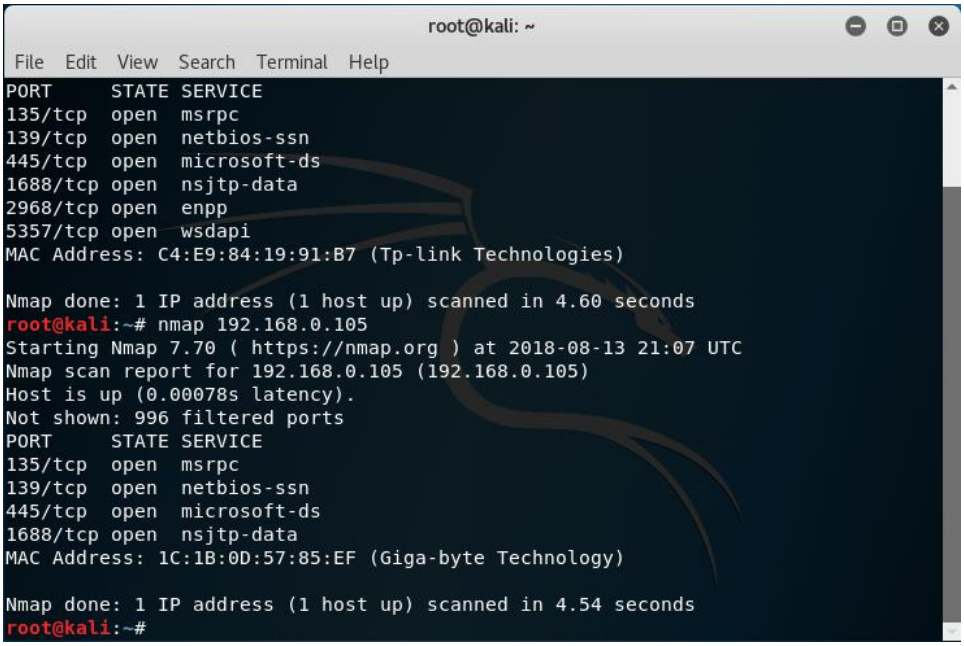


Gráfico N° 3

Elaborado por: Jorge Benites

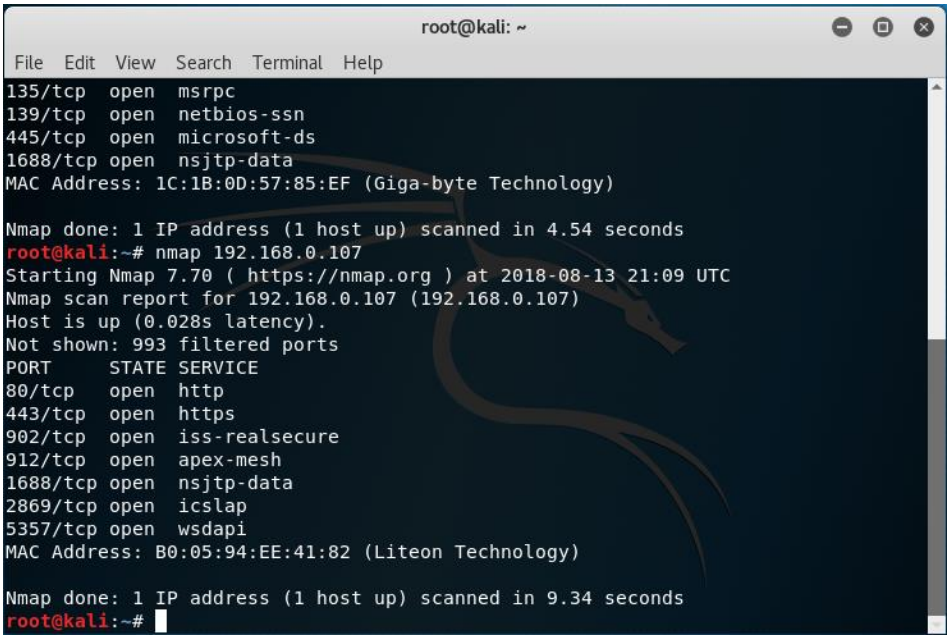


Gráfico N° 4

Elaborado por: Jorge Benites

Consola de Metasploit

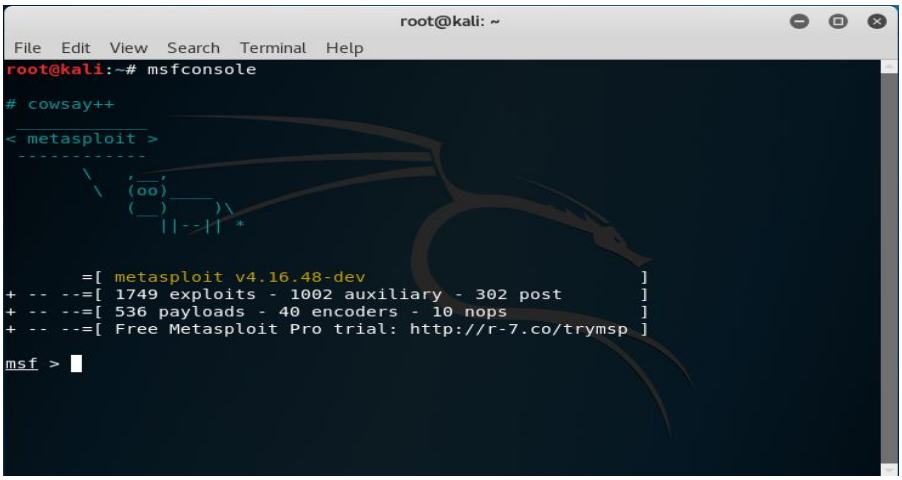


Gráfico N° 5

Elaborado por: Jorge Benites

ANEXO 3

Ataque con MAC Flooding Attack (Ataque de Inundación de Direcciones MAC)

Topología de la red que vamos a utilizar

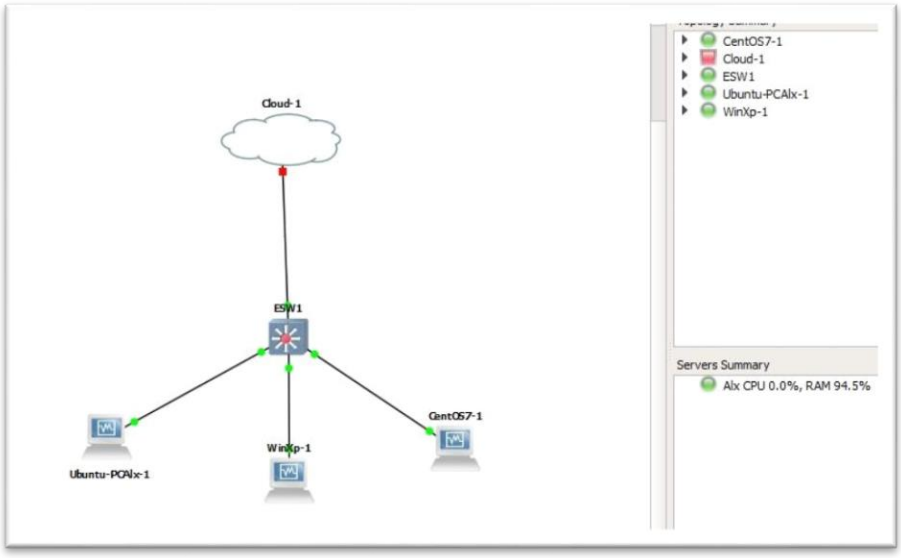


Gráfico N° 6

Elaborado por: Jorge Benites

Vista de la tabla CAM dentro del switch

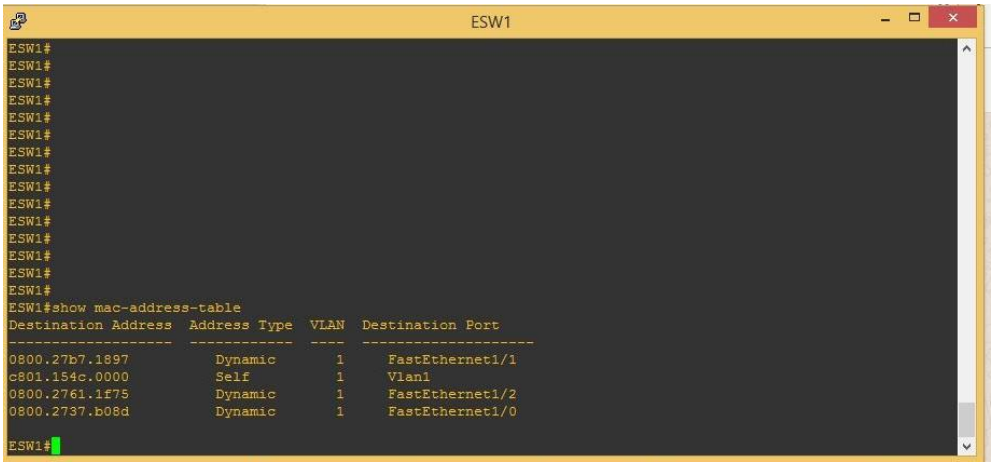


Gráfico N° 7
Elaborado por: Jorge Benites

Ataque con el comando macof.

Gráfico N° 8
Elaborado por: Jorge Benites

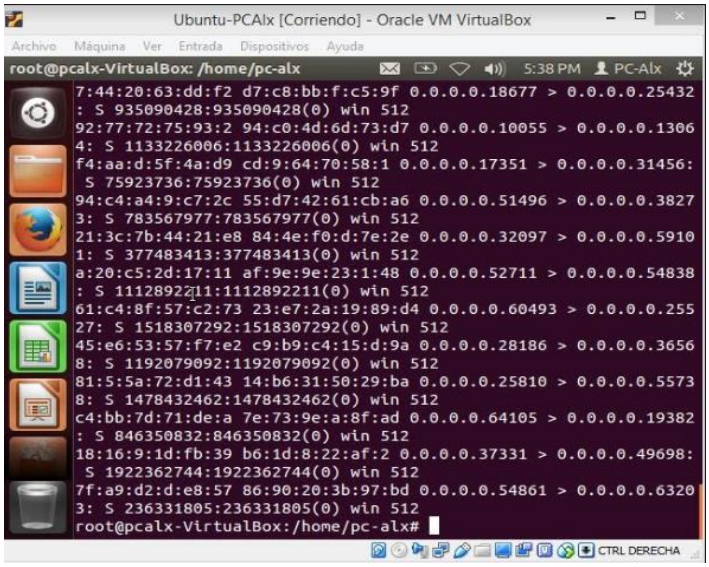


Gráfico N° 9
Elaborado por: Jorge Benites

Ataque completado con el comando macof

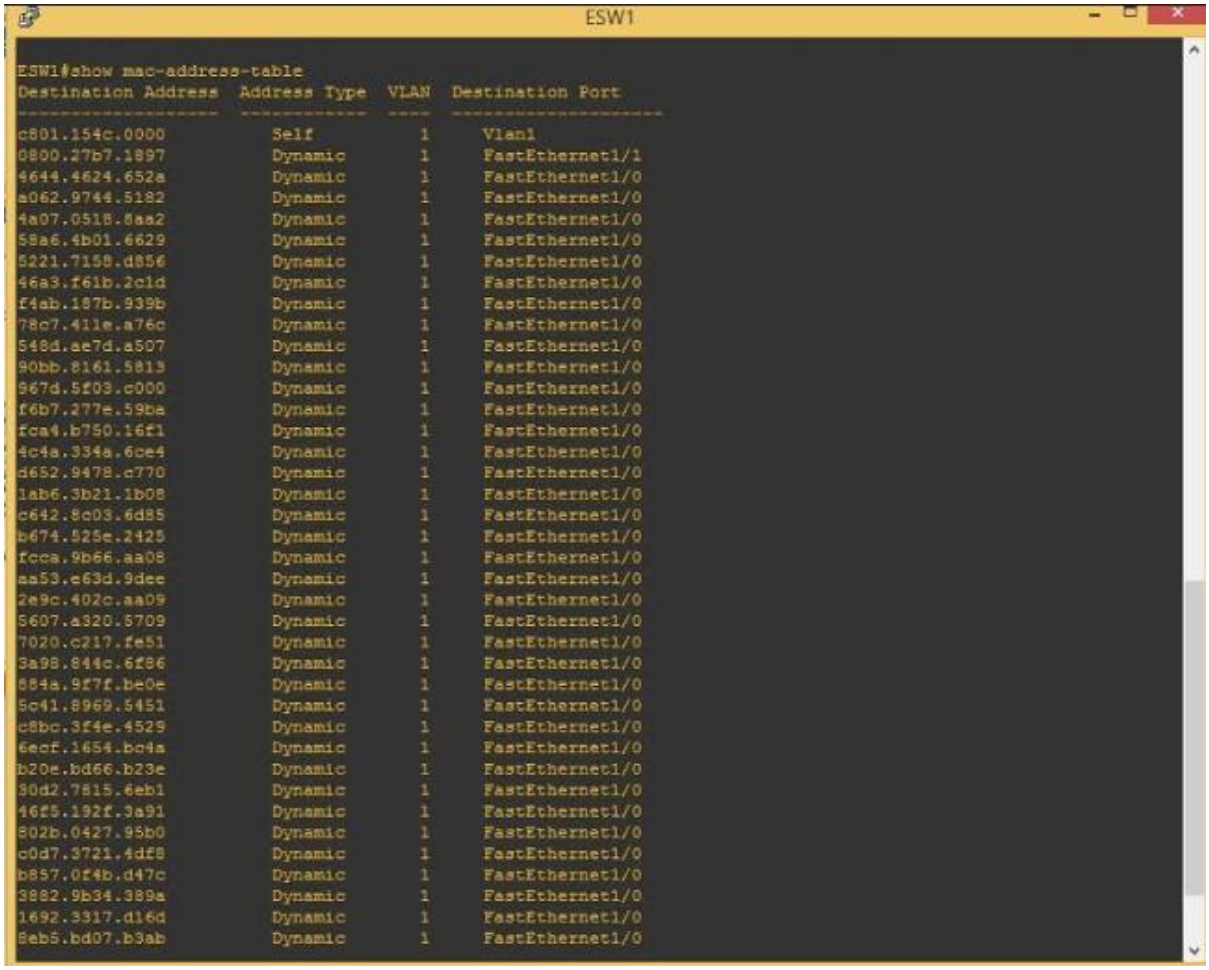


Gráfico N° 10

Elaborado por: Jorge Benites

ANEXO 4

Diseño de la red de la empresa Paris.Net

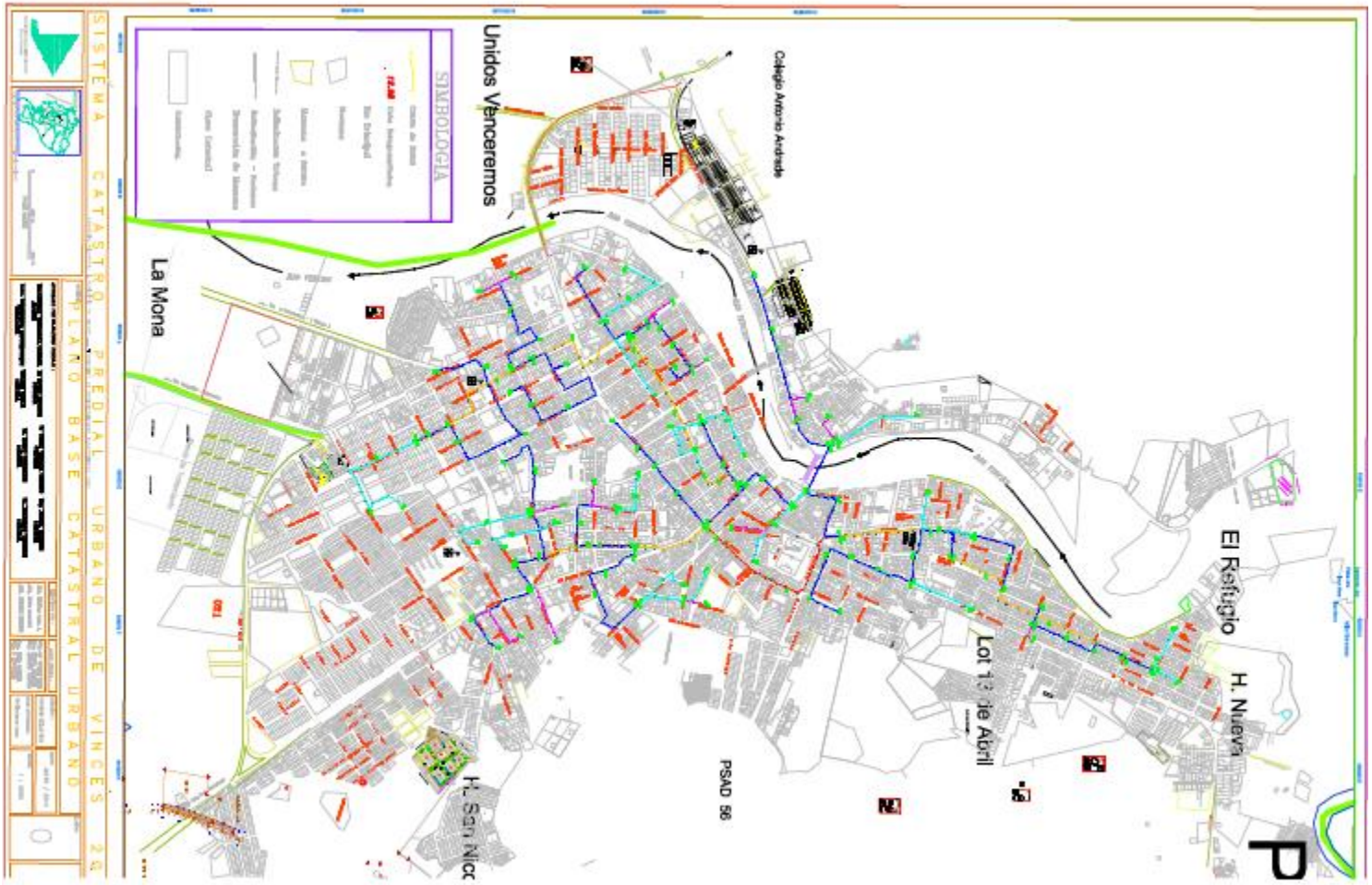


Gráfico N° 11

Elaborado por: TelecomAustro