ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"DISMINUIR LA FUGA DE INFORMACIÓN EN EL DEPARTAMENTO DE INVESTIGACIÓN Y DESARROLLO DE PINTURAS UNIDAS S.A."

INFORME DE PROYECTO INTEGRADOR

Previo a la obtención del Título de:

LICENCIADO/A EN REDES Y SISTEMAS OPERATIVOS

AHMED JAYR PEREZ MORALES

STEPHANIE DEL ROSARIO VILLACÍS ALVIA

GUAYAQUIL – ECUADOR

AÑO: 2018

AGRADECIMIENTOS

Mi más sincero agradecimiento en primer lugar a Dios por darme sabiduría y fuerza para seguir adelante, venciendo cada obstáculo presentado en el camino; en segundo lugar, a mis padres, quienes han sido mi guía y pilar fundamental a lo largo de mi vida universitaria; ofreciéndome su apoyo y consejo siempre. Gracias a ello he podido llegar a lograr este objetivo. A mis docentes y compañeros de la carrera, que en su momento me compartieron sus conocimientos y a mi director de tesis quién me motivó en todo momento para hacer posible este logro, Ing. Robert Andrade Troya.

Stephanie del Rosario Villacís Alvia.

Mis agradecimientos a cada uno de los profesores que aportaron en mi formación profesional, a mi familia por su soporte y comprensión durante todos estos años, a mi esposa por ser el pilar fundamental de mi paciencia y ayudarme a recuperar el enfoque cuando suelo perder la concentración, a mis compañeros de la carrera y amigos que desde el inicio de la carrera supieron contribuir de forma oportuna a cada uno de los retos que se nos presentaba.

Ahmed Jayr Pérez Morales.

DEDICATORIA

El presente proyecto lo dedico en primer lugar a Dios, en segundo lugar, a mis padres, quienes han sido mis pilares fundamentales a lo largo de mi vida universitaria. Ellos fueron motivo por el cual he trabajado con ahínco para lograr esta meta. Su ejemplo de lucha y paciencia ante cualquier obstáculo me hicieron aprender y saber tomar decisiones correctas, que al final me ayudaron a cumplir mis objetivos. También dedico este proyecto a mi novio, quien ha sido mi fiel compañero y consejero en todo momento durante la realización de este proceso, dándome fuerzas para no desistir en cumplir esta meta; a mi gatito Isaías por haber sido mi fiel mascota a lo largo de mi período académico. Sin ellos, no hubiese podido tener motivos para lograrlo.

Stephanie del Rosario Villacís Alvia.

Este proyecto se lo dedico a mi hijo Liam quien ha sido la razón de mi esfuerzo y el motivo por el cuál he puesto lo mejor de mí para poder realizar este proyecto de mejor manera, espero que, en un futuro, si es que así el destino lo permite, este documento pueda servirte como una ayuda o guía en tu vida estudiantil y profesional.

Ahmed Jayr Pérez Morales.

DECLARACIÓN EXPRESA

"La responsabilidad y la autoría del contenido de este Trabajo de Titulación, nos corresponde exclusivamente; y damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

Ahmed Jayr Pérez Morales

Stephanie del Rosario Villacís Alvia

EVALUADORES

Ing. Andrade Troya, Robert Stalin

PROFESOR DE LA MATERIA

Ing. Criollo Bonilla, Ronald Raúl

PROFESOR TUTOR

RESUMEN

En este proyecto se busca mejorar la seguridad de red gracias al uso de herramientas que puedan mitigar el robo de información o ataques informáticos dentro de la red empresarial de “Pinturas Unidas”. Se demostrará la manera en que actualmente, trabajadores de esta empresa manipulan y registran la información sobre fórmulas de productos de pinturas.

En la actualidad la industria de pinturas ha ido creciendo en el mercado nacional hasta el punto de buscar un posicionamiento competitivo muy alto que pudiera demostrar la calidad y unicidad de sus productos. Esto lleva a que compañías similares en la fabricación de pinturas busquen mejorar su posición en el mercado, llevando a la mala acción de acceder a redes privadas de la empresa “Pinturas Unidas” para el plagio de información sobre la formulación de productos y con esto beneficiarse para ser pioneros en el mercado.

Como aporte de nuestro proyecto se propone un aseguramiento de toda la infraestructura de red de la empresa, capaz de restringir el acceso a puertos y servicios específicos, aplicando políticas de seguridad dentro de cada departamento. Se sugiere tener una mejor organización directiva en la que el Gerente de Sistemas tenga la capacidad para detectar cualquier acto malicioso dentro de toda la red de la empresa mediante el uso de Kali Linux para el escaneo de puertos.

Este aplicativo se diseña tomando como base la minicomputadora Raspberry Pi 3 B+ con una distribución GNU/Linux. Por medio de un pentesting, se realiza todo el escaneo de puertos de una red, así como también se visualiza y reportan todas las intrusiones que se están presentando en el acto, a fin de evitar la fuga de información sobre la formulación de productos. Entre los beneficios que se pretende lograr con el proyecto son: empleo de nuevas tecnologías, reducción de costos en la mejora de la infraestructura de red y ahorrar de tiempo al momento de detectar cualquier ataque informático futuro a la empresa.

Palabras Clave: Linux, Raspberry Pi, infraestructura, ataque informático, pentesting.

ABSTRACT

This project seeks to improve network security thanks to the use of tools that can mitigate the theft of information or computer attacks within the business network of "Pinturas Unidas". It will demonstrate the way in which currently, workers of this company manipulate and record the information on formulas of paint products.

Currently the paint industry has been growing in the national market to the point of seeking a highly competitive position that could demonstrate the quality and uniqueness of its products. This leads to similar companies in the manufacture of paints seeking to improve their position in the market, leading to the bad action of accessing private networks of the company "Pinturas Unidas" for the plagiarism of information on the formulation of products and thus benefit to be pioneers in the market.

As a contribution of our project we propose an assurance of the entire network infrastructure of the company, capable of restricting access to ports and specific services, applying security policies within each department. It is suggested to have a better management organization in which the Systems Manager has the ability to detect any malicious act within the entire company network through the use of Kali Linux for port scanning.

This application is designed based on the Raspberry Pi 3 B + minicomputer with a GNU / Linux distribution. By means of a pentesting, all the scanning of ports of a network is carried out, as well as all the intrusions that are being presented in the act are visualized and reported, in order to avoid leakage of information on the formulation of products. Among the benefits to be achieved with the project are: use of new technologies, reduction of costs in the improvement of the network infrastructure and save time when detecting any future computer attack on the company.

Keywords: Linux, Raspberry Pi, infrastructure, attack computer, pentesting.

ÍNDICE GENERAL

ABREVIATURAS

ACL	Access List
AD	Active Directory
DC	Domain Controller
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
DT	Design Thinking
ESPOL	Escuela Superior Politécnica del Litoral
FODA	Fortalezas, Oportunidades, Debilidades, Amenazas
GPO	Group Policy Object
HDMI	High Definition Multimedia Interface
ID	Investigación y Desarrollo
IIS	Internet Information Services
IP	Internet Protocol
ISP	Internet Service Provide
IVA	Impuesto al valor agregado
LAN	Local Area Network
OU	Organizational Unit
PC	Personal Computer
SO	Sistema Operativo
TCP	Transmission Control Protocol
TCP	Transmission Control Protocol
TFT	Thin Film Transistor
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VLSM	Variable Length Subnet Mask
VTP	VLAN Trunk Protocol
WAN	World Area Network

SIMBOLOGÍA

%	porcentaje
″	pulgadas
$	dólar estadounidense
A	amperios
GB	gigabyte
ms	milisegundos
s	segundos
V	voltios

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1

1. INTRODUCCIÓN

Pinturas Unidas S.A. es una empresa ecuatoriana con más de 50 años en la industria ecuatoriana, líder en diseño, producción y comercialización de recubrimientos y pinturas de alta calidad. Ubicados en el Km. 16.5 Vía a Daule, en la ciudad de Guayaquil, provincia del Guayas, Ecuador. Tienen como misión fabricar pinturas en las líneas Arquitectónica, Automotriz, Madera, Industrial & Marina. Desarrollar procesos para prevenir el impacto ambiental a través del esfuerzo diario de quienes conforman la empresa, manteniendo una innovación constante dirigida a los clientes, quienes representan su razón de existencia en el mercado, reciban lo mejor.

Esta compañía tiene sus fortalezas frente al mercado, así como también sus amenazas cuando se trata de mantener su equipo de trabajo íntegro y reacio frente a malas intenciones de la competencia. No siempre una organización trabaja sin problemas, este es el caso de Pinturas Unidas, así como son pioneros en presentar nuevos productos al mercado, existe la posibilidad que otras empresas similares a esta, se vean en la necesidad de quitar aquellos privilegios de autenticidad e innovación para ganar mayor posición y demanda en el país.

En nuestro proyecto se implementó la metodología de Design Thinking (DT) [1] la cual nos ayudará a encontrar y estudiar la situación actual de la compañía, la visión y objetividad que nuestro cliente requiera cumplir para mantenerse siempre único y pionero frente al mercado ecuatoriano.

1.1 Descripción del problema

Pinturas Unidas S.A. como muchas de las empresas en el Ecuador, tiene como política mantener la originalidad de los productos que ofrece a sus clientes. Durante sus años en el mercado ecuatoriano, ha presentado notables pérdidas de clientes en sectores comerciales donde predominaban sin presencia de la competencia. Esto último se ha dado, no sólo por el crecimiento de numerosas industrias de pintura sino por lanzamientos de

productos de igual característica por parte de la competencia, cuya composición química es muy similar a los productos que Pinturas Unidas aún tiene en fase de desarrollo e investigación. Esto ha llevado a los directivos a realizar auditorías de manera general en todas las áreas y subáreas de la empresa, mediante las cuales se logró encontrar algunas vulnerabilidades en el departamento de Investigación y Desarrollo (ID), tales como:

- Copias no controladas de archivos en todos los terminales de la empresa.
- Fácil acceso a las fórmulas de fabricación.
- Falta de control a las bases de datos.
- Alteración de información sobre procesos de producción y cronogramas de mantenimiento.
- Carencia de protocolos de seguridad en las redes de datos.
- Fuga de información clasificada.
- Puertos abiertos de ciertos ordenadores, que están propensos a sufrir hackeo informático.

1.2 Justificación del problema

En la actualidad, se ve un gran nivel de competitividad en las empresas que están en la búsqueda de nuevas oportunidades de mercado teniendo como base la innovación, así como también en la búsqueda de necesidades no satisfechas que ayuden a alcanzar un éxito organizacional. La visión de nuestro proyecto es una oportunidad para demostrar que por medio de la innovación en el ámbito comercial y utilizando como soporte la tecnología, se puede cumplir con muchos objetivos establecidos. Como se ha mencionado, el caso de estudio de la empresa Pinturas Unidas S.A se centra en la búsqueda de vulnerabilidades y la reducción de información plagiada sobre el proceso de formulación de cada pintura, debido que no cuentan con una seguridad en la red corporativa que sea capaz de controlar el acceso no autorizado de usuarios ajenos a la empresa.

Además, existe poca cultura informática por parte de los empleados, debido a que no se garantiza que sean minuciosos en el registro de la información o no estén capacitados para mitigar ataques informáticos que se presenten sin previo aviso. Uno de los ataques más comunes que se han visto en la actualidad es la ingeniería social donde ciertos atacantes buscan la forma de engañar a los usuarios para conseguir información sobre fórmulas o procesos. Por tanto, se pretende mejorar desde la integridad laboral hasta la seguridad de la red de datos para el departamento de Investigación y Desarrollo de Pinturas Unidas S.A.

1.3 Objetivos

1.3.1 Objetivo General

Reducir las vulnerabilidades en la red de datos, para mitigar el acceso no autorizado mediante la gestión de políticas de seguridad a los grupos de trabajo dentro de la empresa.

1.3.2 Objetivos Específicos

- Crear itinerarios de evaluaciones internas en búsqueda de vulnerabilidades.
- Emplear el uso de un software que cifre los datos más confidenciales del departamento.
- Segmentar VLAN [2] para servicios, designadas a un departamento de acuerdo a las necesidades que presenten.
- Implementar una red de área local y virtual que garantice un nivel de seguridad adecuada para el cifrado de datos.
- Generar políticas de seguridad y reglas de firewall [3] para la prevención de ataques en la red.

CAPÍTULO 2

2. METODOLOGÍA

Para conocer realmente las necesidades de nuestro cliente hemos decidido establecer por medio de la metodología del DT, una serie de fases que nos ayudaron a analizar mejor el problema central que tiene por mejorar el departamento de investigación y desarrollo de Pinturas Unidas S.A. Para ello hicimos el levantamiento de información correspondiente a cada fase, el cual, nos ayudó a definir una solución óptima frente a la problemática encontrada.

2.1 Primera fase

Antes de empezar a definir el problema central de la empresa, se realizó una cita con los directivos de la misma compañía, donde hubo ciertas observaciones acerca de las necesidades más prioritarias para ellos, entre ellas, el uso inadecuado de las computadoras, la mala gestión de la red y el bajo control sobre la actividad de los usuarios. Con toda esta información empezamos a hacer uso de las herramientas de la metodología para encontrar soluciones rápidas y viables que cubran todas aquellas necesidades que estaba presentando la empresa.

Para comprender la situación actual de la empresa, elaboramos un mapa de stakeholders [4] (Figura. 2.1) donde se visualizan los integrantes relacionados de manera directa con la compañía. Así pudimos tener una visión panorámica de quién o quiénes son los posibles grupos de interesados en la adquisición de nuestra idea innovadora de proyecto. Al elaborar este esquema pudimos crear estrategias e ideas que satisfaga en gran demanda al grupo de clientes que se destacaron.

Figura. 2. 1 Mapa de Stakeholders.

Una vez que se determinó el grupo de interesados más influyentes dentro de la empresa, se estableció una reunión previa con cada uno de ellos, donde se dio a conocer la idea relacionada del proyecto y el alcance que se tendría al implementarse. Nuestros interesados más relevantes en la compañía fueron los siguientes:

- Gerente general del departamento de Investigación y Desarrollo.
- Gerente General de la empresa.
- Gerente de Sistemas.
- Jefe de soporte técnico de los usuarios de ID.

Por medio de una técnica de preguntas, establecimos una lluvia de ideas que nos sirvió para analizar los temas más destacados a realizarse durante la entrevista. Organizando las ideas, se pudo formular una por cada representante, dependiendo del cargo que desempeñaban. Al final se obtuvo información importante para iniciar nuestro estudio.

Gracias al uso de esta técnica tuvimos una relación más directa con el cliente, lo cual nos ayudó a entender mejor sus necesidades.

Cada entrevistado nos fue de gran ayuda para poder recopilar toda la información posible que requeríamos antes de comenzar a definir el problema. Para nuestro caso de estudio los autores más relevantes, fueron

el Gerente de sistemas y el jefe del departamento de investigación y desarrollo. Para visualizar todas las entrevistas realizadas, dirigirse al Anexo A.

Realizando la entrevista a cada uno, gracias a la información obtenida se elaboraron diferentes mapas de empatía que resumen todas las observaciones encontradas [5]. Nuestro cliente directo y a conocer fue el jefe del departamento de ID. (Figura 2.2)

Figura. 2. 2 Mapa de empatía Jefe de Departamento ID.

De acuerdo a la entrevista realizada al Gerente de la compañía, pudimos destacar ciertas similitudes en sus actitudes y pensamientos respecto al jefe del departamento de ID, siendo más comunes las siguientes:

- Ambos notaron que podrían existir vulnerabilidades dentro de su área.
- Piensan que conocer sobre el uso de nuevas tecnologías, le ayudaría a la empresa a mejorar su seguridad y rendimiento.
- Las políticas que han establecido en su departamento no son suficientes para prevenir ataques informáticos a futuro.

- Se muestran preocupados al saber que los usuarios dentro de su área no están muy capacitados para saber actuar frente al robo de información.
- Cada directivo conoce bien la función de su cargo y confían en su equipo de trabajo, pero piensan que no todos podrían ser muy discretos al momento de procesar información
- Se notó un poco de conformismo por parte de ellos con respecto al estado actual de red de datos, pero a la vez notamos un interés en querer revisar todos los servicios que disponen y aquellos que falten por agregar para así tener un mejor control en cada área de trabajo.

Con toda la información recopilada se pudo tener más clara la visión y el objetivo de nuestro cliente. Para nuestro caso investigativo el jefe de ID es a quien destacamos. Todas sus opiniones, sus relaciones laborales, sus inquietudes, propuestas y aspiraciones se analizaron minuciosamente con el fin de llegar a entenderlo. Por medio de los esquemas de los demás directivos se vieron ciertas similitudes en las preocupaciones y aspiraciones; es decir, pudimos llegar a la conclusión que todos buscaban mejorar ciertas normativas en sus departamentos, usar innovaciones tecnológicas con el propósito de ofrecer calidad y rendimiento óptimo en los procesos de sus productos. Para visualizar los otros mapas de empatías elaborados, dirigirse al Anexo B.

Mediante un análisis de las aseveraciones más relevantes y comunes entre los entrevistados, se destacaron todas aquellas que requirieron más atención a la hora de enfrentar el o los problemas a resolver.

Clasificamos todos los puntos de vista más destacados de la entrevista y se los calificó de manera cualitativa: bueno, regular y malo. Cabe destacar que para el entendimiento de cada observación nos basamos en dar un significado a cada calificación:

- Bueno: Cuando la persona conoce y entiende del tema.

- Regular: Cuando la persona conoce del tema, pero no lo suficiente para hacer frente a él.
- Malo: Cuando la persona no conoce nada del tema y sabe como enfrentarlo.

Pudimos observar situaciones específicas a mejorar (Tabla 2.1), dependiendo del conocimiento de cada entrevistado, se mostraron los resultados de los clientes que dominan bien el tema de seguridad en la red de datos y aquellos que no lo hacen del todo.

Análisis	Bueno	Regular	Malo	*Total*
1: Conocen medidas de seguridad en la red	1	3	0	4
2: Aplican el uso de políticas	3	1	0	4
3: Saben reaccionar frente a ataques informáticos	0	1	3	4
4: Uso de herramientas para proteger información	0	4	0	4
5: Uso de contraseñas seguras dentro de sus pc.	0	4	0	4
6: Buen respaldo de información.	1	3	0	4
7: Mantienen actualizadas sus licencias de software	3	1	0	4
Total	8	17	3	28

Tabla 2.1 Análisis de resultados de las entrevistas.

Teniendo los resultados, por medio de un diagrama estadístico (Figura 2.3) se pudo detectar mejor que área necesitaba ser evaluada y estudiada para disminuir su mala gestión dentro de la empresa.

Figura. 2. 3 Análisis de resultados de las entrevistas.

Pudimos determinar que la mayoría de los directivos dentro de la compañía no dominan ciertos temas que deberían tomar en consideración para el aseguramiento de su información, a fin de evitar el robo de datos y a su

vez, pérdidas para su organización. Es notable que existen diferencias grandes en cuanto a la calificación que se dio para cada situación que fue analizada, donde se visualizó que la opción “regular” tuvo más impacto sobre las observaciones.

Esto nos dio un entendimiento sobre lo que sucede dentro de la empresa, pudiendo concluir que gran parte de los directivos necesitan conocer mejor sobre la seguridad de la red, el uso de herramientas para asegurar la información e incluso poder mitigar ataques informáticos que podrían presentarse por las vulnerabilidades encontradas en su entorno.

Después se realizó el análisis FODA [6] de la empresa (Figura 2.4), el cual nos ayudó a conocer a fondo la situación actual, su visión y el compromiso con los clientes más frecuentes.

Figura. 2. 4 Análisis FODA de Pinturas Unidas.

Se destacaron fortalezas como: tener un producto único, un equipo de trabajo eficiente, Contribuir de forma positivo en el medio ambiente; por el contrario, se presentaron ciertas debilidades, tales como: la falta de conocimiento sobre seguridad informática por parte de sus empleados, el poco uso de nuevas tecnologías y falta de expansión en el mercado internacional.

Amenazas externas por las cuales puede verse afectada la compañía, tales como: el crecimiento de la competencia, la fuga de información sobre la formulación de productos, falta de activos necesarios para la compra de más materia prima, entre otros a destacar.

La empresa también cuenta con buenas oportunidades a nivel exterior, entre las más relevantes se destacan: la ampliación de su mercado en otros países, la gran demanda de clientes en aceptar sus productos y la innovación diaria para mostrar mercancía única.

Gracias a este análisis pudimos tomar en cuenta todos los puntos más relevantes con nuestro tema, para así empezar a contestar ciertas interrogantes o necesidades de cada uno de los directivos que conforman la empresa.

2.2 Segunda Fase

En esta fase buscamos definir el problema, para ello empleamos ciertas técnicas de estudio que nos ayudaron a descubrir las mayores causas y efectos que la empresa estaba presentando.

Debido a las entrevistas realizadas y el análisis FODA, pudimos detectar cuáles fueron todos los aspectos más relevantes que estaban afectando al entorno laboral, así como el impacto que estaban generando hacia nuestro cliente.

Es por esto que elaboramos el árbol de problemas (Figura 2.5) para su entendimiento. Con toda la información analizada y ya deducida, se realizaron diferentes discusiones sobre el asunto. Se tomaron en cuenta las causas más propensas a mejorarse y con ello obtuvimos una clara definición del problema.

A medida que observábamos la acción que se generaba dentro de la empresa al realizar ciertas actividades, pudimos llegar a la conclusión de un efecto central que englobaba todo el sentido de la problemática que tratábamos de definir para empezar la búsqueda de una solución.

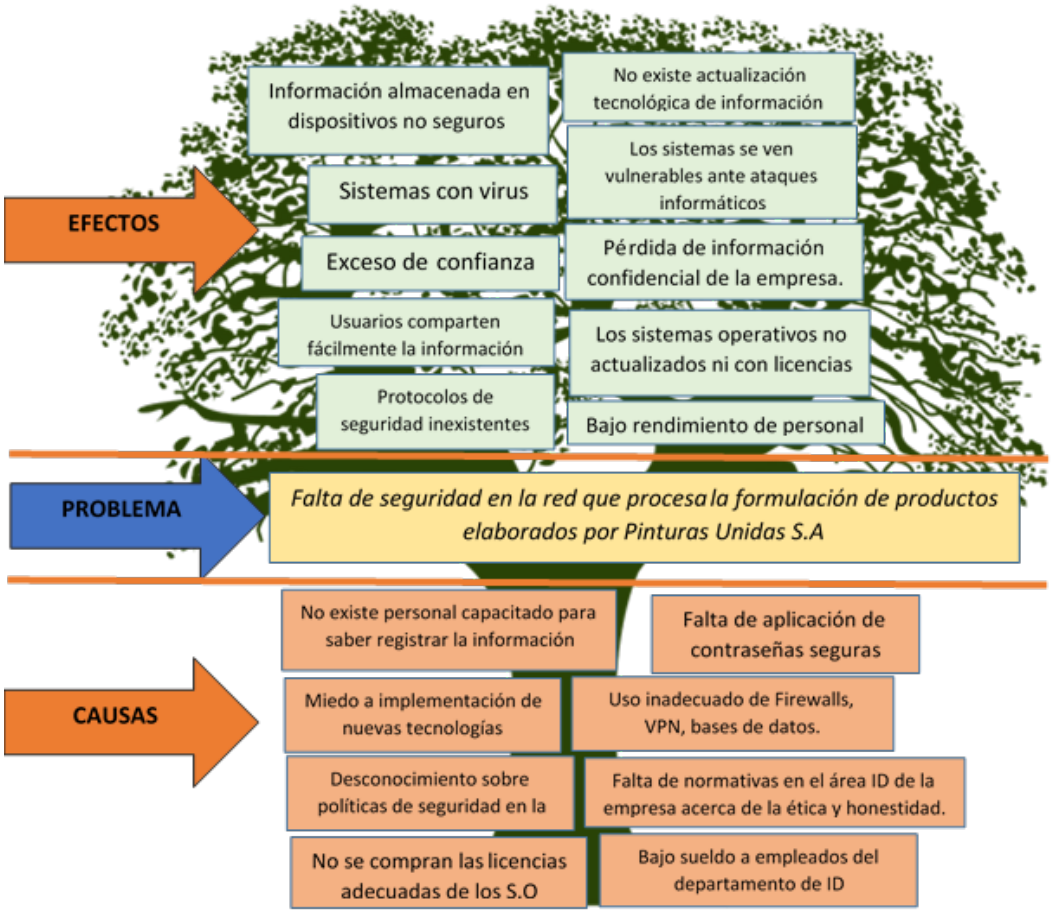


Figura. 2. 5 Árbol de problemas.

Como siguiente paso para tener otro punto de vista más claro sobre la necesidad prioritaria de nuestro cliente, se procedió a destacar los insights [7] de cada entrevistado. Esto resultó importante al momento de conocer con más profundidad, aspectos y actitudes que tenían con respecto a su área de trabajo correspondiente.

Para continuar con nuestro análisis, destacamos al jefe del departamento de ID (Figura 2.6) mediante la elaboración de una matriz de insight para su entendimiento.

Cliente / Cargo	Necesidad	Insights
Ing. Luis Santos - Jefe de Departamento ID	Cerciorarse que cada empleado sea integro	porque a veces hay usuarios que abusan de la confianza dada en la empresa
	Controlar mejor la asignación de contraseñas	porque se podría evitar que cualquier usuario manipule la información
	Autorizar a su grupo de trabajo a llevar mejor control de información	porque se mantiene actualizada la base de datos sobre el producto en proceso
	Restringir el uso de las redes sociales	porque incentiva a los empleados a dedicarse a su trabajo y no distraerse.
	Ofrecer cursos cortos sobre medidas de seguridad	porque los usuarios deben detectar cualquier intento de intrusión
	Supervisar las otras áreas de la empresa	porque se debe verificar que la información sobre la formula no sea compartida

Figura. 2. 6 Insights de Jefe de Departamento ID.

Por medio de todo el análisis realizado a los insights más destacados, se crearon frases para justificar sus necesidades. El planteamiento de todas las ideas nos dio un esquema sobre las posibles soluciones que pudieran satisfacer a nuestro cliente.

Partiendo de cada frase, procedimos a establecer preguntas a nuestro entrevistado, para establecer posibles soluciones que ayuden a confrontar el problema más relevante de la empresa. Las interrogantes establecidas fueron las siguientes:

- ¿Cómo lograríamos que los usuarios del área ID mantengan una confidencialidad de los productos elaborados por Pinturas Unidas?
- ¿Si en vez de dejar que los usuarios personalicen sus contraseñas, se establezca un patrón seguro para todos al momento de crearlas?
- ¿Cómo podríamos lograr que los dirigidos del área de ID presenten reportes sobre la información que almacenan en el sistema?
- ¿Cómo podríamos convencer al jefe de restringir el uso de las redes sociales entre los usuarios?
- ¿Cómo podríamos convencer a los empleados que se capaciten p sobre medidas de seguridad?
- ¿Cómo podríamos lograr que el jefe de área controle la salida y entrada de archivos desde el departamento?

2.3 Tercera Fase

Luego de haber conocido muy bien los intereses de nuestro cliente, el entorno de la empresa, así como las carencias y necesidades de ésta, pudimos hacer frente al problema principal del departamento ID de la compañía, el cual mencionamos a continuación: “Falta de seguridad en la red que procesa la formulación de productos elaborados por el departamento ID de Pinturas Unidas”. Por medio de la siguiente fase de desarrollo de la metodología, establecimos una lluvia de ideas partiendo desde los puntos de vista del cliente, sus necesidades y falencias en el área, para así presentar varias alternativas que pudieran solventar todas esas necesidades.

Una vez expuestas todas las ideas bien definidas, se elaboró una matriz de decisión *(*Tabla. 2.2) donde se anotó cada posible solución en base a los requerimientos de nuestro cliente, se evaluaron todas las variables relacionadas con el objetivo de nuestro proyecto.

Necesidad / Solución	Ampliar su conocimiento sobre medidas de seguridad informática	Controlar más la actividad de cada usuario	Mejorar la administración de la red	Cifrar la información confidencial de los productos innovados	Reducir el tiempo en caso de perder información	Compartir la información solo entre personas involucradas en el departamento	Buscar las vulnerabilidades más dañinas en los sistemas para mejorarlos.	TOTAL
Crear políticas de seguridad con Active Directory.	2	4	2	3	3	3	1	18
Implementación de BitLocker para cifrado de discos	2	1	0	4	3	2	1	13
Crear contraseñas seguras en el inicio de sesión	2	1	0	3	1	1	3	10
Software para el escaneo de los puertos de la red.	3	1	4	2	5	2	6	23
Usar certificados digitales	3	2	1	0	1	2	2	11
Segmentar servicios de voz y datos por medio de VLAN	2	4	8	1	3	3	3	24
Uso de solución antivirus y antispyware para los puntos terminales.	2	1	1	0	1	2	2	9
Creación de ambientes virtuales	2	0	1	0	1	1	2	7
Emplear uso de una VLAN administrable para departamentos	3	4	5	2	3	4	1	22
Actualización de Windows Server 2012 y Windows 10	0	2	5	3	1	6	3	19

Tabla 2.2 Matriz de decisión

Según la calificación obtenida de cada opción numerada en nuestra matriz de decisión pudimos observar el rango de aceptabilidad que tendría cada una de las opciones de acuerdo con el requerimiento que cada jefe buscaba cumplir en su departamento.

Debido a este análisis estuvimos en la capacidad de llegar a una solución óptima y decidir si hemos de ofrecer un producto o servicio que ayudara a reducir el impacto que estaba generando la problemática dentro de la empresa.

Con los resultados obtenidos fuimos capaces de tomar decisiones puntuales frente al problema central de todo el departamento, garantizándole a nuestro interesado la optimización de recursos, dinero y tiempo en la implementación de una innovación tecnológica.

Para tener la aprobación del jefe del departamento de ID y que cubra esa necesidad; se elaboró un prototipo que se basó en la implementación de un software que ayudó en la detección de vulnerabilidades en la red de datos, al igual que en detectar las intrusiones no autorizadas a la red de la empresa. Nuestro prototipo también permitió recibir amenazas presentes en la web e incluso, detectar el desfalco de la información más confidencial que estuviera procesando la compañía, lo cual estaba generando pérdidas comerciales y económicas; un alce de la competencia, despidos de empleados, falta de calidad en los productos y muchos otros factores que el gerente estimó prevenir en un futuro por el bien común de Pinturas Unidas.

Posibles soluciones para la empresa:

- Creación de políticas de seguridad más robustas para cada grupo de trabajo.
- Implementación de BitLocker [8] por medio de Windows Server para el cifrado de discos.

- Software para el escaneo de puertos más usados dentro de la red de cada departamento.
- Segmentación de servicios de datos y voz por medio del uso de VLAN.
- Aplicación de VLAN administrativas para los departamentos.
- Actualización de sistemas operativos a Windows 10 y servidor a Windows 2012 R2.

2.4 Cuarta Fase

Mediante la elaboración de un mapa de afinidades (Figura 2.7*)*, se realizó una evaluación de todas las variables relacionadas con el aseguramiento de la información empresarial, determinando el impacto, la viabilidad y la factibilidad del uso de tecnología; que, relacionadas entre sí, nos ayudó a definir una solución, a reducir tiempo y costo al momento de ser implementada.

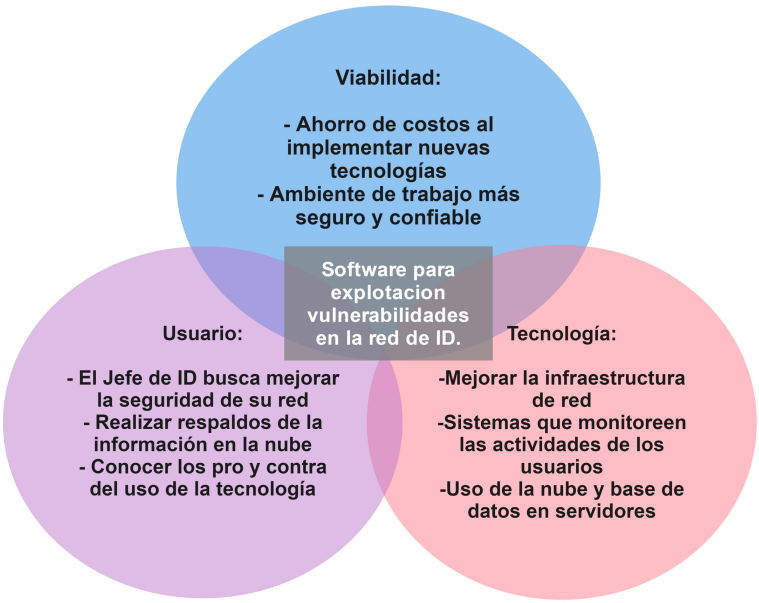


Figura. 2. 7 Mapa de afinidades.

- En el diseño de nuestro prototipo se usó una minicomputadora, Raspberry pi 3 +B, memoria 16 GB con SO “Kali Linux” [9]
- Pantalla táctil TFT de 7” con conexión HDMI y alimentación por USB.
- Fuente de energía de 5 V 2.5 A.
- Mouse y teclado con conexión USB inalámbrico. (Figura 2.8)

Figura. 2. 8 Prototipo para la búsqueda de vulnerabilidades de puertos.

El cliente ejecuta mediante el terminal de Kali Linux el comando “nmap” [10] donde pudo observar todos los equipos activos de su red y sacar información variada, en especial los puertos que estuvieran abiertos por cada dirección IPv4 reconocida y las direcciones IP sin uso dentro de la red, lo cual fue de mucho interés para realizar pruebas de explotación de vulnerabilidades por cada puerto escaneado y saber que aplicaciones se estaban ejecutando en el momento.

Con este prototipo, el jefe pudo tener una idea de las posibles vulnerabilidades *(*Figura 2.9 y Figura 2.10*)* en su red informática a la vez de visualizar un reporte que le ayude a tomar decisiones de mejoras en la seguridad informática de su departamento. Para realizar el escaneo de los puertos se utilizó la siguiente línea de comando:

@root# nmap –v –O –Sn 172.16.0.0/24

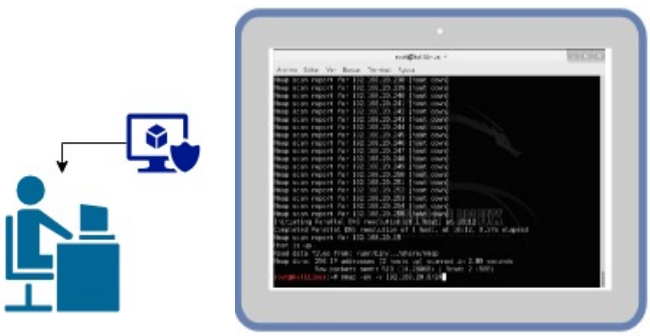


Figura. 2. 9 Escaneo de puertos por medio del comando “nmap”.

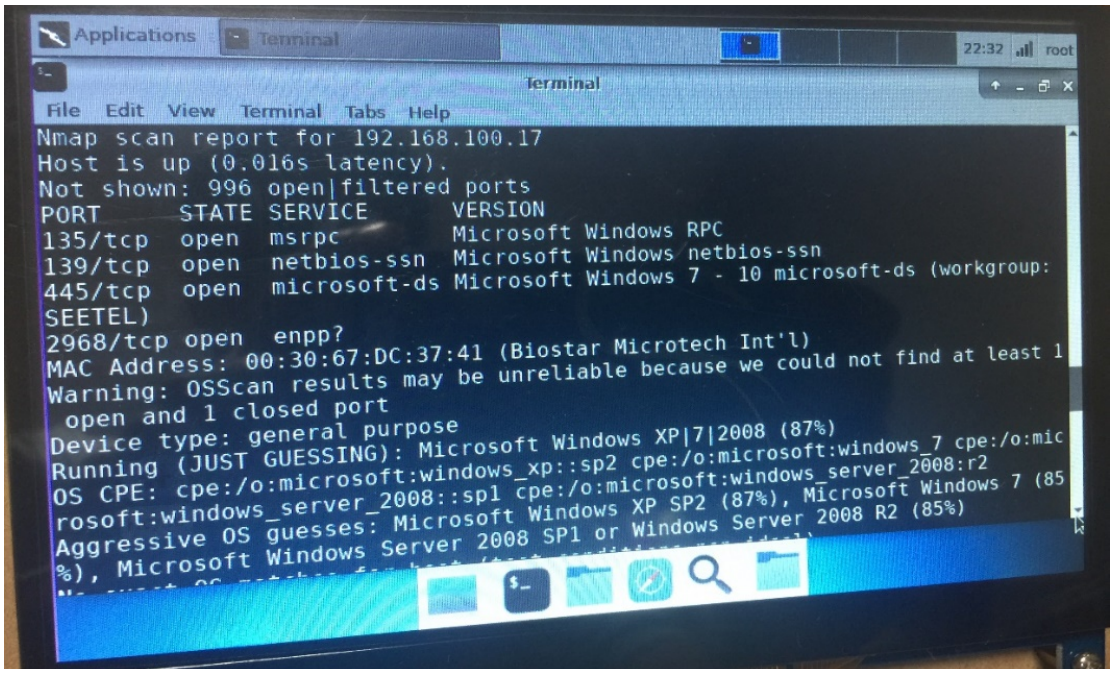


Figura. 2. 10 Reporte de escaneo de puertos en Kali Linux.

Para visualizar el funcionamiento del prototipo de manera real, dirigirse a Anexo C. Otras opciones que se pudieron visualizar por medio del comando dentro del sistema operativo fueron:

- Número de direcciones IP permitidas.
- Tipo de dispositivo conectado.
- Puertos abiertos de un equipo concreto.
- Visualización de la IP del servidor.
- Sistema operativo de la víctima.
- Protección de un host mediante [11] firewall.
- Gestión de horarios de servicios de actualización.

Con este análisis demostramos a nuestro cliente que la idea de nuestro proyecto va más allá de centrarse en buscar las fallas en la red empresarial, también está el poder mitigarlas. Mediante el uso del S.O Kali Linux, se podrá explotar a tiempo todas las posibles vulnerabilidades presentes en la red del departamento.

Con la aprobación del jefe, se realizó el testeo del prototipo. Con los resultados se empezó a hacer válida la propuesta, que sería capaz de reducir el robo de información y procesos de la compañía.

El personal de la organización no debe dejar pasar por alto todos aquellos tipos de ataques que podrían presentarse a futuro, tales como: ataques DoS [12], fragmentación de paquetes, virus maliciosos, explotación de los servicios TCP/IP [13], inundación de ancho de banda, ataques de ingeniería social, wardialing, entre otros. Para ello fue necesario tomar en cuenta que el gerente de Sistemas tuviera que capacitar a su personal de área para llegar a tener todos los conocimientos básicos sobre los tipos de ataques más comunes en una red, a fin de tener un ambiente de trabajo más colaborativo y seguro.

CAPÍTULO 3

3. DISEÑO DE LA SOLUCIÓN

Para mejorar la seguridad de la red se estudió el diseño actual de la estructura organizacional de la empresa junto con el departamento de ID (Figura.3.1) con la finalidad de tener un panorama de como implementar nuestra solución. En la siguiente ilustración se puede observar el diseño actual de la red de la empresa, destacando como posibles vulnerabilidades las siguientes:

- Puertos abiertos en la red lo que permitía que cualquier usuario tenga acceso a la data de los departamentos.
- La cantidad masiva de dispositivos conectados a la red.
- Direcciones IP no establecidas dentro de un rango definido.
- Sistemas configurados de manera inadecuada.
- Amenazas internas en la red.

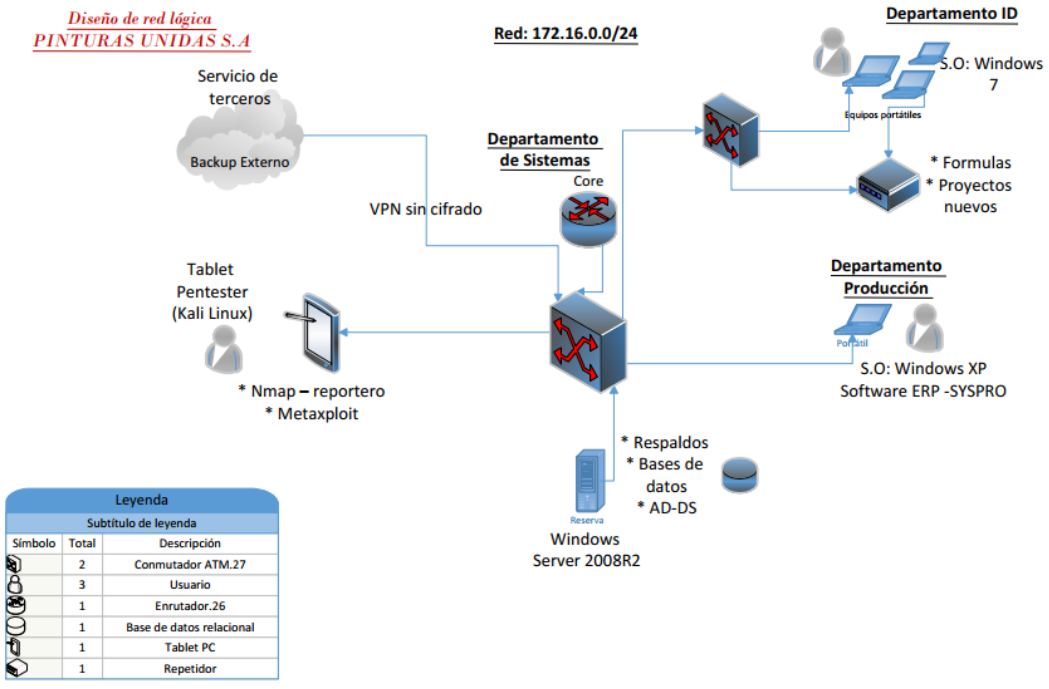


Figura. 3. 1 Red lógica actual de Pinturas Unidas.

En base a los problemas de direccionamiento de red, puertos no utilizados y abiertos sin función asignada, políticas de red insuficientes y poco efectivas, recursos compartidos en red de departamentos con información sensible, entre

otros, procedimos a rediseñar de una manera más organizada, los departamentos que conforman la empresa (Figura 3.2). Para visualizar mejor la forma de comunicación que van a tener los usuarios de cada área, se dividirá cada departamento por segmentos, de manera que cada uno de ellos tendrán su propia red a fin de la compartición de archivos no autorizados entre un computador de un departamento hacia otro. De esta manera los archivos compartidos y el acceso a los recursos de red serán controlados. También se evitará la pérdida o robo de información.

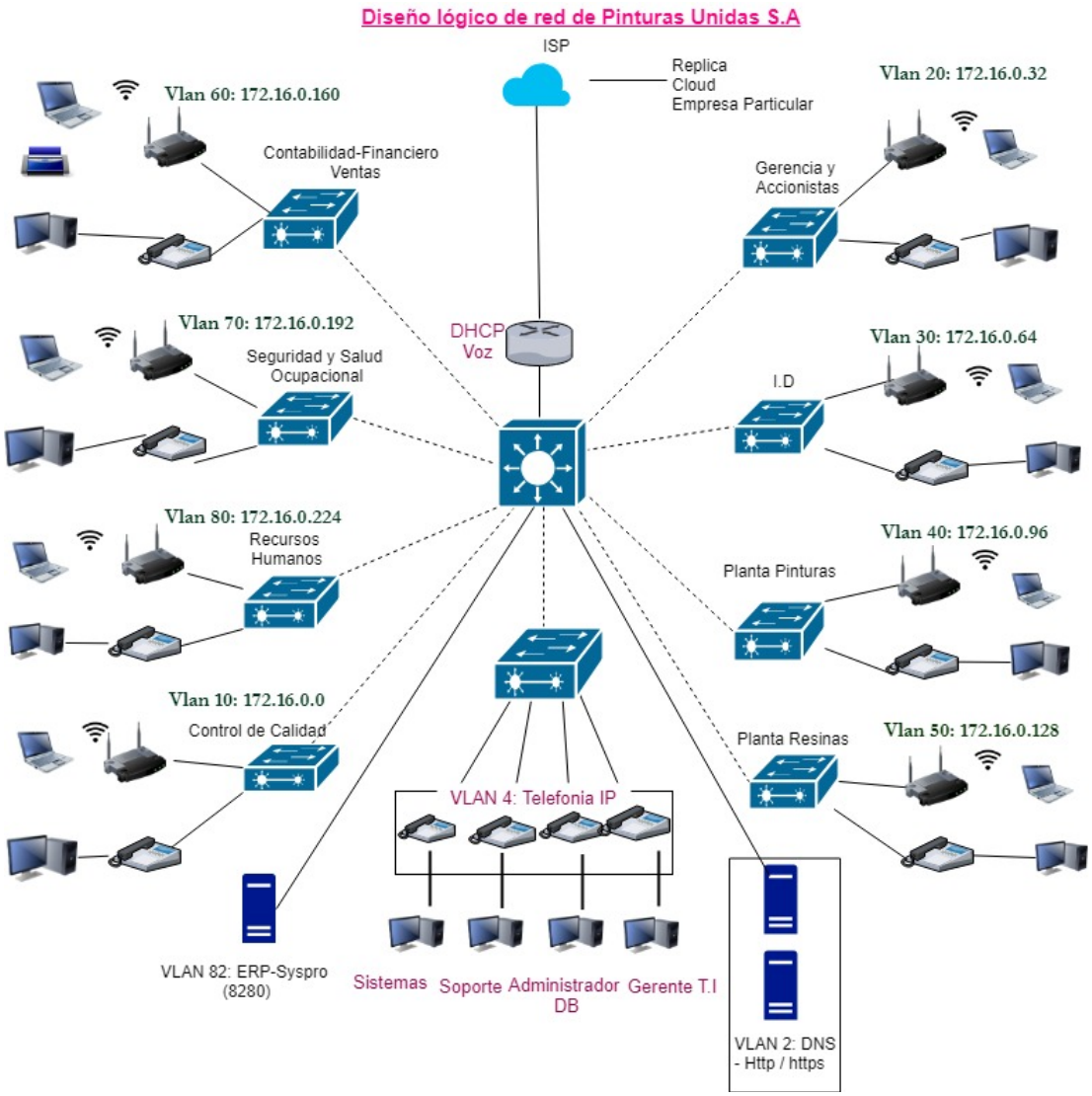


Figura. 3. 2 Diseño de red lógica para la distribución de departamentos.

Luego de haber rediseñado la ubicación de los equipos por cada departamento, realizaremos el subnetting de IP [14] que permitirá tener un direccionamiento

adecuado y organizado dentro de la red. Con el uso de direcciones de red fijas para cada dispositivo se podrá tener más control sobre cada uno de los computadores al momento de establecerse las conexiones.

Emplearemos el uso de VLSM [15] que garantiza tener más subredes dentro de un rango de red principal y así no desperdiciar direcciones de IP.

3.1 Cantidad de Hosts por servicios

Datos:

Departamentos	Cantidad de dispositivos locales	Cantidad de dispositivos inalámbricos
Gerencia – Accionistas	9 computadoras	1 router Wi-Fi
Planta Pinturas	8 computadoras	1 router Wi-Fi
Planta Resinas	8 computadoras	1 router Wi-Fi
ID	11 computadoras	1 router Wi-Fi
Financiero –Contabilidad – Ventas	6 computadoras	1 router Wi-Fi
Seguridad y Salud Ocupacional	5 computadoras	1 router Wi-Fi
Control de calidad	10 computadoras	1 router Wi-Fi
Recursos humanos	5 computadoras	1 router Wi-Fi
Sistemas (Seguridad –Soporte-Administrador BD –Gerente TI)	4 computadoras	1 router Wi-Fi

Tabla 3.1 Cantidad de equipos usados por departamentos

Voz:

Para el servicio de voz se configurará 50 líneas telefónicas que estarán listas para su conexión en caso de ser requeridas por el Gerente de la compañía.

Número total de Pc: 66
Número total de Router Wifi: 8
Número total de dispositivos: 74

Aplicaremos VLSM tomando en cuenta la dirección IP a asignar. Para este caso se aplicará una red de clase B debido a que son utilizadas en empresas grandes. La red por definir será la 172.16.0.0, la cual permite que la red de la empresa sea más privada.

El cubrimiento de nuestra red se hará bajo la estimación de un crecimiento del 100%. Pinturas Unidas, a lo largo de sus años, ha sabido manejar bien la parte laboral, por lo tanto, no se han presentado muchos cambios en cuanto al número de empleados que conforman cada área, pero no dejan pasar la oportunidad del crecimiento de su personal de trabajo.

Por tal motivo se estimaría que para nuestro direccionamiento se realice tomando en cuenta un 40% más de crecimiento en la red actual por cada departamento, dejando como requerimiento a los directivos, tener espacios disponibles cuando requieran contratar nuevos servicios o nuevo personal.

3.2 Direccionamiento IP

40% crecimiento de la red, cálculo de host se hace por cada departamento.
Cantidad de subredes: 32
Máscara de red: /27
Cantidad de hosts por red: 30

Como siguiente paso, se organizarán las direcciones IP tomando en cuenta como primer rango el departamento con mayor cantidad de usuarios. Desde la segunda hasta la penúltima dirección IP de cada segmento de red, quedará disponible para los equipos terminales, de esta manera seremos eficiente con las direcciones IP y optimizaremos los recursos de red. (Tabla 3.2).

Departamento & Servicios	Rango de IPs utilizables	Broadcast	Máscara	
Control de calidad	172.16.0.0-172.16.0.30	172.16.0.31	255.255.255.224	/27
Gerencia	172.16.0.32-172.16.0.62	172.16.0.63	255.255.255.224	/27
ID	172.16.0.64-172.16.0.94	172.16.0.95	255.255.255.224	/27
Planta Pinturas	172.16.0.96-172.16.0.126	172.16.0.127	255.255.255.224	/27
Planta Resinas	172.16.0.128-172.16.0.158	172.16.0.159	255.255.255.224	/27
Contabilidad – Financiero y Ventas	172.16.0.160-172.16.0.190	172.16.0.191	255.255.255.224	/27
Seguridad y Salud	172.16.0.192-172.16.0.222	172.16.0.223	255.255.255.224	/27
Recursos Humanos	172.16.0.224-172.16.0.254	172.16.0.255	255.255.255.224	/27
Sistemas	172.16.1.0-172.16.1.14	172.16.1.15	255.255.255.240	/28
Remote Desktop Server – DNS (Servers) – Http/https	172.16.1.16-172.16.1.22	172.16.1.23	255.255.255.248	/29
Datos ERP-Syspro	172.16.1.24-172.16.1.30	172.16.1.31	255.255.255.240	/28
Voz	172.16.2.0-172.16.2.254	172.16.2.255	255.255.255.0	/24

Tabla 3.2 Direcciones IP por cada departamento de Pinturas Unidas

Una vez finalizado el direccionamiento IP para cada departamento, se aplicará el uso de VLAN para crear una división lógica de redes de trabajo locales, esto es debido a que, por ejemplo, las necesidades de los distintos departamentos pueden ser diferente. Esto nos permitirá asignarle permisos necesarios a cada departamento de acuerdo con sus funciones y requerimientos dentro de la empresa, así como también asignar una directiva de seguridad apropiada para cada VLAN.

3.3 Asignación de VLAN por departamento

De acuerdo con el método aplicado y el rango de direcciones IP para cada departamento, quedará establecido un número de VLAN para cada uno de ellos (Tabla 3.3).

Departamentos	Número de VLAN
Control de calidad	10
Gerencia - Accionistas	20
Investigación y Desarrollo	30
Planta Pinturas	40
Planta Resinas	50
Contabilidad – Financiero - Ventas	60
Seguridad y Salud Ocupacional	70
Recursos Humanos	80
Sistemas	90

Tabla 3.3 VLAN asignada a cada departamento

Para el uso de recursos y archivos compartidos también se establecerá la implementación de VLAN por servicio (Tabla 3.4), debido a que no todos los departamentos cumplen con las mismas funciones. En ciertas áreas se trabaja de forma que los archivos manipulados se registran en papel y no por medio de un software. Por ello se prevé dejar como requerimiento al Gerente, delegar permisos específicos a sus usuarios para hacer uso de estos servicios en caso de ser necesario.

Número de VLAN	Servicios Asignados
4	Voz
82	ERP-Syspro
2	DNS, HTTP/HTTPS

Tabla 3.4 Asignación de VLAN por servicio

3.4 Especificaciones para el desarrollo de nuestra solución

Dentro del esquema de red, se debe tomar en cuenta otros parámetros a establecer como son:

- Actualización de Sistema Operativo Windows 2007 a Windows 10.
- Actualización de Windows Server 2008R2 a Windows Server 2012 R2.
- Replicación del servidor hacia la nube, para ello también cumplirá con funciones como: Active Directory Domain Controller AD-DC [16], establecer políticas de Firewall, reglas inbound y outbound para puertos específicos, configuración DNS [17] en el servidor, aplicación de políticas de seguridad a usuarios y computadoras.
- Aplicación de SQL-Server [18] para el análisis de bases de datos o consultas, integrado con el correo electrónico y la Internet. Añadir el IIS [19] para alojamiento de aplicaciones WEB.
- Configuración de una VLAN para servicios de voz, la cual será VLAN 4.
- Configuración de una VLAN 82 para el procesamiento de datos que maneja el ERP-Syspro con salida al puerto 8280.
- Configuración de una VLAN 2 para permitir servicios DNS, HTTP/HTTPS.
- Conexión de router a internet (ISP).
- Sólo los departamentos de Contabilidad, Gerencia, Recursos Humanos y Sistemas tendrán acceso a Internet.
- Los departamentos de Salud, ID, Planta Pintura, Planta Resina y Control de calidad solo podrán intercambiar información por medio del uso de correo electrónico, protocolo FTP [20] y la VLAN correspondiente al servicio OwnCloud. Adicional a esto, se plantea restringir el uso de Internet.
- Departamento de Sistemas se encargará de que sus usuarios realicen conexiones remotas para realizar un monitoreo a las diferentes computadoras de cada departamento.

Es necesario tomar en cuenta ciertos requerimientos al momento de hacer que la red sea administrable para la empresa, una vez que detectamos todas aquellas vulnerabilidades en cada departamento.

Se estableció un acuerdo con los directivos para definir el alcance del proyecto al momento de mejorar la administración y la seguridad de red empresarial.

Para ello se debe cumplir con ciertas solicitudes en caso de mejorar la distribución de la red:

- Datasheet de los equipos, la cantidad, ubicación y sus características.
- Determinar la viabilidad al implementar mejoras.
- Número total de equipos y su localización (equipos configurados y por instalar).
- Contratos de seguros.
- Políticas de uso para los equipos.
- Contratos de compra y servicio para mantenimiento.
- Configuraciones de los dispositivos.
- Manual de procedimientos de configuración de equipos.
- Planeación de fechas para la instalación de nuevos sistemas operativos o servidores.

3.5 Equipos requeridos para la topología de red del proyecto

Para mejorar la infraestructura de red de la empresa, el Gerente debe contar con los equipos y modelos necesarios para hacer válida la implementación de nuestros servicios. Entre ellos se debe contar con:

- Switch Cisco 3560, multilayer para distribución y Core.
- Switch Cisco 2960 para acceso.
- Router Cisco 2811 integrado con servicio de voz y datos.
- Servidores compatibles con el sistema operativo Windows Server 2012 R2 y soporte aplicaciones como: WEB, DNS, requerimientos o consultas SQL, generación de políticas de seguridad y reglas de Firewall.
- Router Wireless T300N para establecer comunicaciones inalámbricas de equipos hacia la red de cada departamento.

- Actualización del sistema operativo original Windows 7 a Windows 10.
- Raspberry Pi 3 +B para la configuración del sistema operativo Kali Linux que realizará la búsqueda de vulnerabilidades de puertos conectados y habilitados en la red.

3.6 Configuración de equipos

Una vez establecido el VLSM para el direccionamiento IP para cada computador, se procederá a realizar las configuraciones de cada dispositivo acorde a la función que cumplirán en cada departamento.

3.6.1 Configuración del switch distribución o principal

Para visualizar los comandos utilizados en la configuración del switch dirigirse al Anexo D.1. Adicional a esto, se tomará en cuenta ciertos pasos para la configuración del equipo.

- Tener un switch con capacidad de crear y administrar VLAN teniendo como soporte el protocolo 802.11Q [21].
- Todas las interfaces FastEthernet serán configuradas de manera troncal, con una VLAN nativa:90.
- Se conectará cada interfaz de red hacia los switches de los departamentos.
- Se asignará nombres a las VLAN por servicios (datos, voz, servidores).
- Se configurará VTP [22] para la administración de las VLAN de modo servidor, con un domain: Unidas y una contraseña: “unidas”.
- Se le asignará la primera IP utilizable de cada VLAN.
- Las interfaces serán configuradas con seguridad en los puertos de red (comando switchport).

3.6.2 Configuración del Router Unidas

Para visualizar los comandos utilizados en la configuración del router, dirigirse al Anexo D.2.

Los parámetros que se deben tomar en cuenta para configurar el router son los siguientes:

- Router que soporte servicio de voz.
- Se asignará un nombre que identifique al router, para este caso se llamará “Unidas”.
- Se establecerá una contraseña cifrada de longitud mínima para que solamente el administrador tenga acceso al sistema.
- Para establecer una conexión con el switch, se configurará por medio de la interfaz FastEthernet0/0 en modo de “no shutdown” levantando dicha interfaz.
- Se procederá con la configuración de ACL [23] para permitir o denegar tráfico de red, en nuestro diagrama de red: Access List para permitir salida a Internet hacia departamentos ya especificados y Access List para permitir envío de información por medio de correo electrónico entre las demás áreas.
- Se configurará una contraseña en la línea VTY para evitar que usuarios ajenos a la red empresarial ingresen y cambien la configuración del equipo.
- Se configurará el servicio de telefonía, añadiendo una VLAN para voz, distribuyéndose por toda la red entre los departamentos.
- Se configurará el pool de direcciones DHCP [24] para los teléfonos conectados. En nuestro diseño se asignará la red: 172.16.2.0 con máscara 255.255.255.0

3.6.3 Configuración de switch para departamento de sistemas

Para visualizar la configuración realizada en el equipo, dirigirse al Anexo D.3.

Las funciones que el switch va a cumplir dentro del departamento y sus configuraciones se detallan a continuación:

- Se configurará una contraseña de acceso.
- El rango de interfaces de las FastEthernet 0/1-3 en modo troncal.
- De las interfaces FastEthernet 0/4-15 pertenecerán a la VLAN de sistemas, del rango 0/16-21 serán para la VLAN de servidores y el restante para la VLAN de servicio ERP-SYSPRO [25].
- Las interfaces serán configuradas con seguridad en los puertos de red (switchport).
- Las interfaces que no están usándose quedarán en modo “shutdown”.

3.6.4 Configuración de switch por cada departamento.

La configuración de cada switch estará dada de acuerdo con las funciones y permisos correspondientes a cada departamento asignado, para visualizar los comandos utilizados en la configuración del switch, dirigirse al Anexo D.4. Las configuraciones por realizar son:

- Se establecerá contraseña de acceso al equipo.
- El rango de interfaces desde la FastEthernet 0/1-5 se configurará de modo troncal.
- Se configurará el VTP de modo “client” con el mismo domain y contraseña del switch de distribución para la sincronización de las VLAN creadas en el mismo.
- A las interfaces de red restantes se deberá añadir las VLAN respectivas de acceso.
- Las interfaces serán configuradas con seguridad a los puertos de red (switchport).
- Los puertos no utilizados quedarán en modo “shutdown”.

3.6.5 Configuración de Router Wireless

Para visualizar la configuración realizada en el equipo router, dirigirse al Anexo D.Las configuraciones por realizar son:

- Nombrar a cada router dependiendo de su ubicación dentro de cada departamento.
- Se asignarán direcciones IP que estén dentro del rango establecido en cada VLAN por departamento.
- Se establecerá una contraseña por cada equipo para controlar el acceso hacia el dispositivo.
- Se limitará el acceso de usuarios máximo a conectarse de manera inalámbrica.

3.6.6 Configuración del Server

Para visualizar la instalación del Windows Server 2012 y las características que aseguran la red, dirigirse al Anexo E.

- Se establecerá un nuevo dominio para toda la red de la empresa, en nuestro proyecto hemos designado como nombre de dominio: “pinturasunidas.local”, como se puede ver en la (Figura 3.3.1).
- Se configurará una contraseña para el acceso al servidor, la contraseña deber ser robusta y con caracteres especiales.

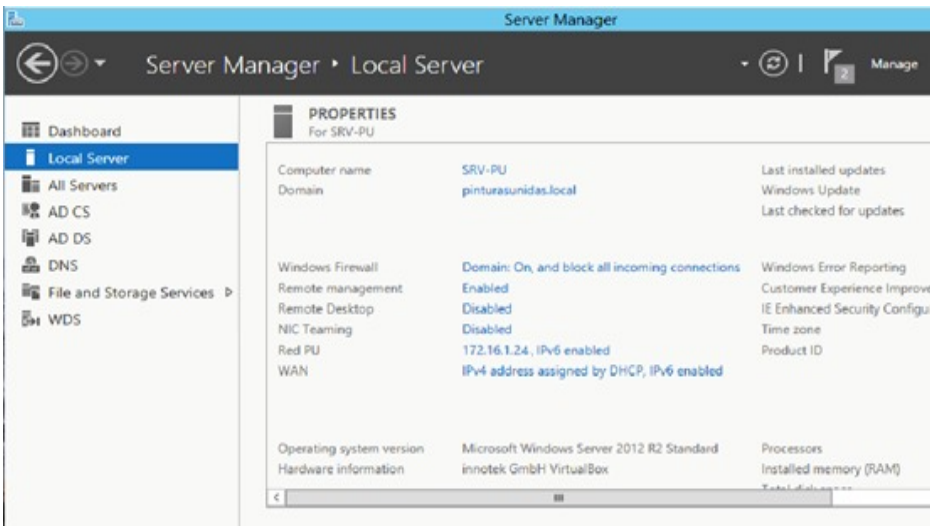


Figura. 3.3. 1 Plataforma de Windows Server 2012.

- Se establecerá una dirección IP para el servidor y se usarán las características de éste. Se asignará la IP: 172.16.1.24/28 (Figura 3.3.2).
- Se agregarán características para la gestión del grupo de políticas GPO [27].

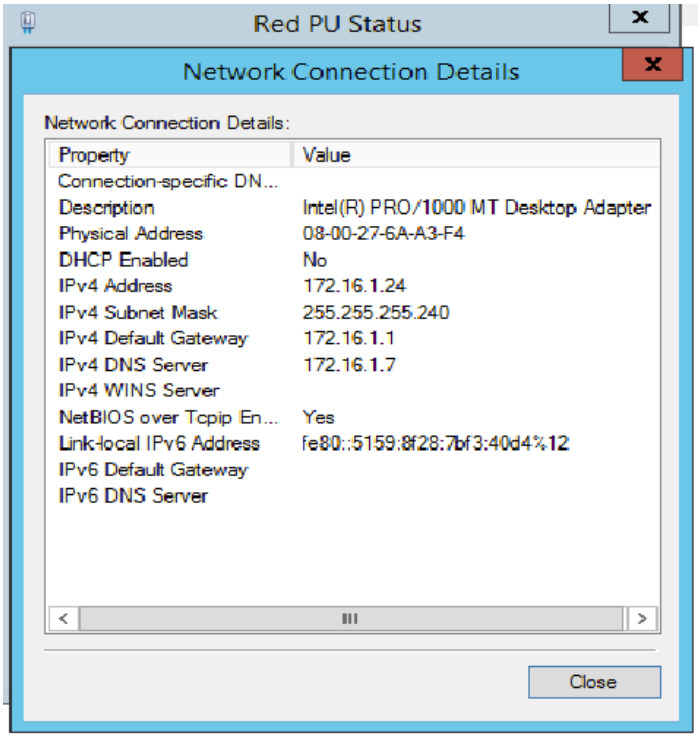


Figura. 3.3. 2 Detalles de configuración de dirección IP.

Se reinicia el servidor y al momento de volver a iniciar sesión, por medio de la opción “administrador de servidores | Herramientas”, se puede visualizar las características instaladas:

- El directorio como centro administrativo.
- Directorio dominios y confianzas.
- Módulo de directorio para Windows PowerShell [28].
- Directorio de sitios y servicios.
- Directorio para usuarios y equipos.
- DNS.
- Gestión de políticas.

Después de la instalación y configuración correcta del role Active Directory Domain Services aparecerán características que nos permitirán, entre otras cosas (Figura 3.3.3) instalar, configurar y administrar las diferentes herramientas que nos ofrece el sistema operativo en base a los roles que se hayan instalado.

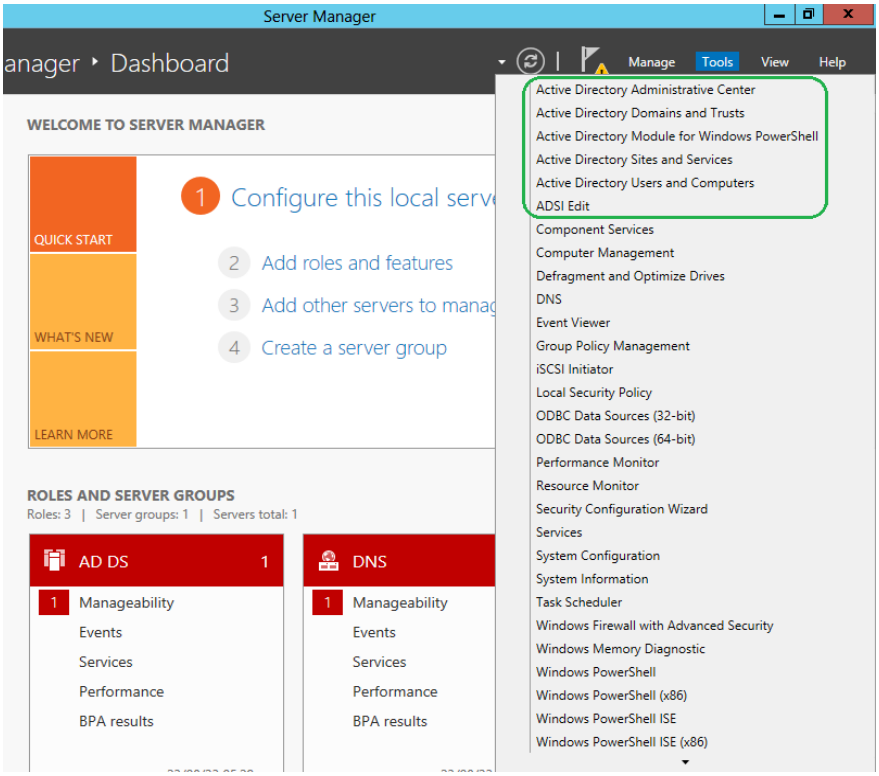


Figura. 3.3. 3 Herramientas más usadas en Windows Server 2012.

3.6.7 Configuración de Usuarios y Grupos en Active Directory

Para visualizar la configuración de usuarios y computadoras dentro de Windows Server 2012, dirigirse al Anexo F. Las configuraciones por realizar son las siguientes:

- Se realizará un registro de todos los empleados que conforman la empresa y se añadirán de acuerdo con el departamento que pertenezcan.
- Se les asignará contraseñas seguras para inicio de sesión a cada usuario.

- Se agregarán los usuarios a un grupo global de seguridad para aplicar políticas dentro de todo el dominio (forest).
- Las configuraciones de todos los departamentos quedarán bajo un árbol de dominio: “pinturasunidas.local”.
- Se asignará un mejor control sobre cada grupo y sus respectivos usuarios, gracias a la implementación de las unidades organizativas, OU [29]. (Figura. 3.3.4).

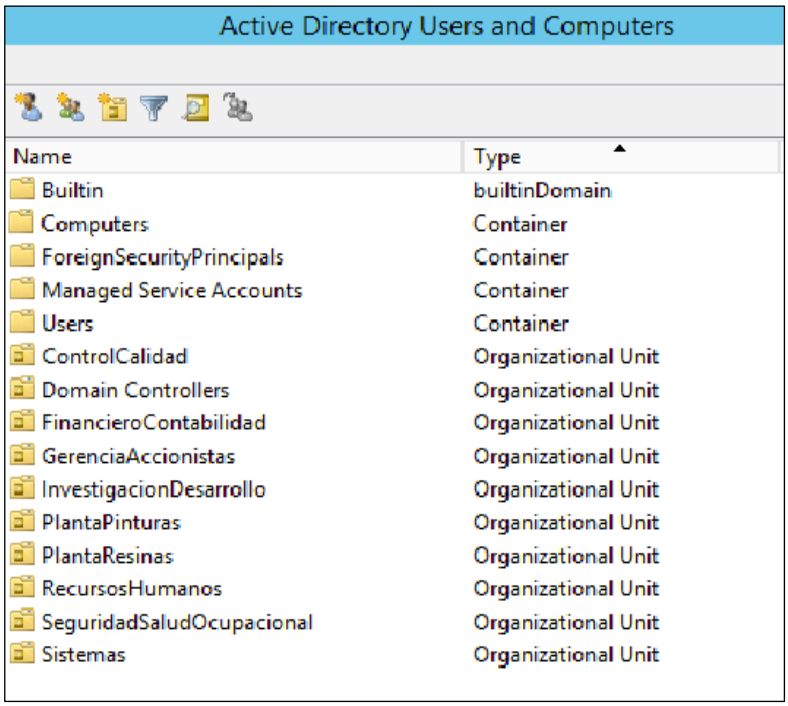


Figura. 3.3. 4 Unidades organizativas creadas para la empresa.

3.6.8 Creación de Grupo de Políticas en Windows Server

Para visualizar la configuración realizada sobre las políticas asignadas a cada departamento, dirigirse al Anexo G.

Para crear y asignar políticas a nuestro grupo de usuarios debemos tomar en cuenta la función que cada uno desempeña, no se trata sólo de generalizar sino de ver la necesidad por cada departamento y buscar la mejor manera posible de tener un control más organizado dentro de la empresa. Las configuraciones por realizar son las siguientes:

- Las políticas serán aplicadas en los equipos y usuarios dentro del dominio.
- Se asignarán nombres a cada GPO.
- Dentro de cada GPO creada se editarán las características que van a ser configuradas para cada política. Para nuestro proyecto hemos tomado en cuenta controlar las actividades en la Pc: no cambiar contraseñas, restringir cambios en la configuración de red, cambios en fondos de escritorio, prohibir instalaciones de programas no autorizados, prohibir al usuario que remueva un programa, no permitir cambiar políticas de firewall, entre otras. (Figura 3.3.5).

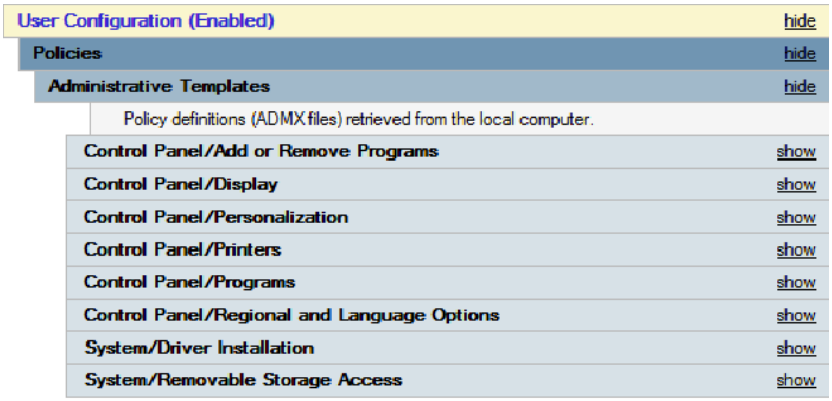


Figura. 3.3. 5 Grupo de políticas configuradas para los usuarios.

Otro grupo de políticas para el dominio de la empresa será la implementación de BitLocker para el cifrado de discos y unidades de almacenamiento, adicional al aseguramiento, hemos de utilizar un método de encriptación con AES 256-bit with Diffuser (Figura 3.3.6).

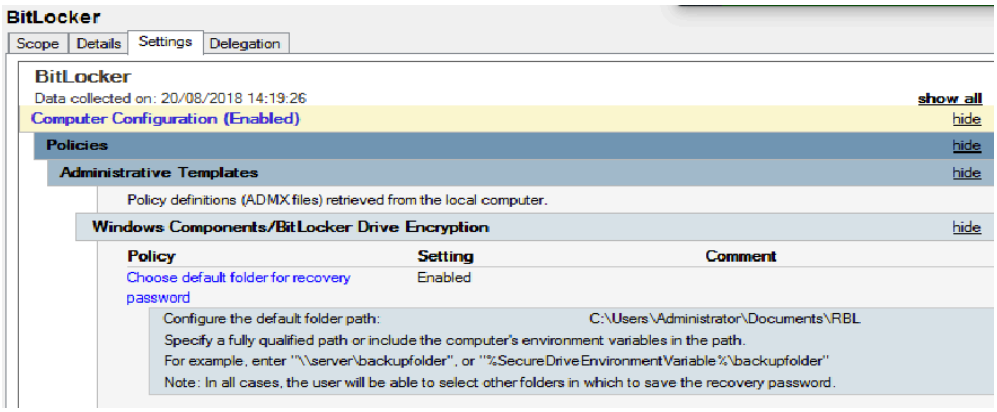


Figura. 3.3. 6 Política configurada para cifrado de unidades.

Entre otro grupo de políticas establecidas para nuestras unidades organizativas se aplicarán reglas de Firewall, que dependiendo del servicio que se necesite en cada departamento se aplicarán reglas de entrada y salida específicas (Figura.3.3.7) y (Figura.3.3.8), para ello se habilitó un Firewall que permitirá o denegará el acceso a ciertos servicios y puertos en base a lo que se requiera por cada área.

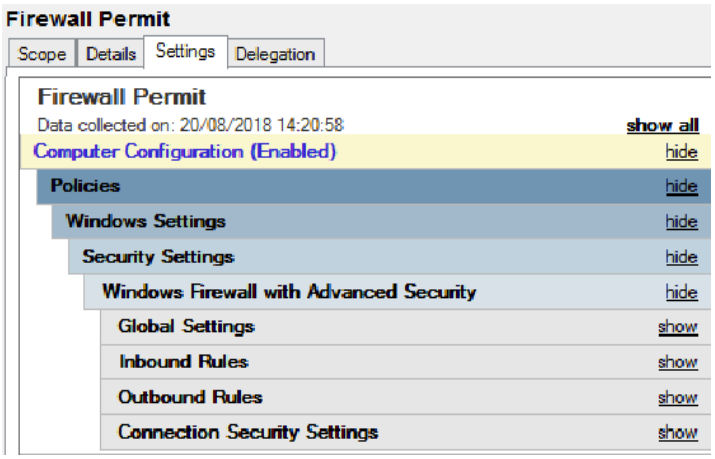


Figura. 3.3. 7 Reglas para permitir acceso a servicios en la red.

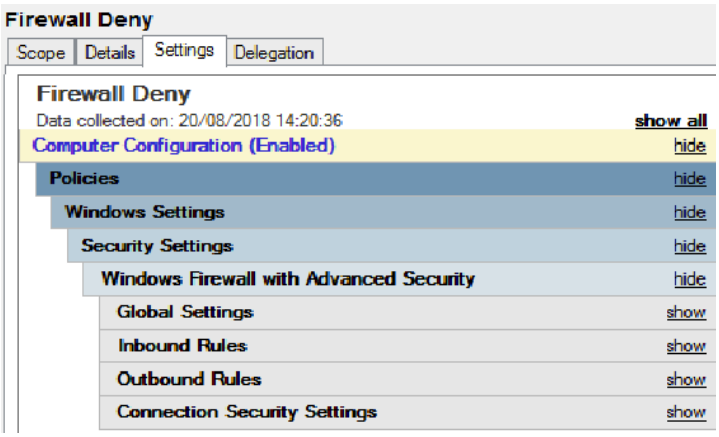


Figura. 3.3. 8 Reglas para denegar el acceso a servicios en la red.

De igual manera se aplicarán políticas de seguridad necesarias para asegurar la integridad de la información del pc en cada Unidad Organizativa de la empresa.

Con el fin de evitar que usuarios no autenticados o ajenos al domino puedan tener acceso a la información de los terminales de la empresa. (Figura.3.3.9).

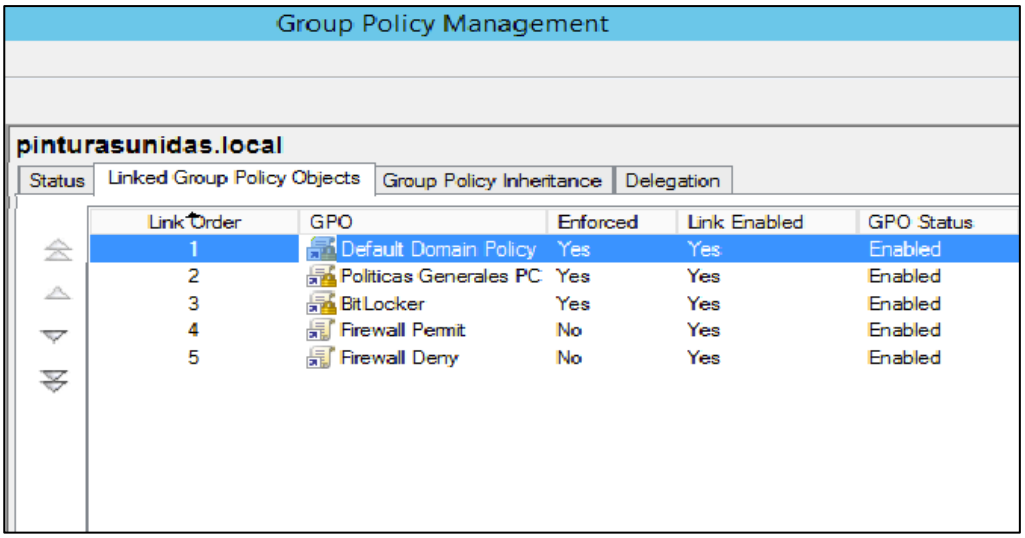


Figura. 3.3. 9 Grupo de políticas asignadas para la red de Pinturas Unidas.

Adicionalmente, debemos aclarar que las reglas establecidas en el Firewall (Tabla 3.5) se realizarán de acuerdo con el tipo de servicios que va a requerir cada departamento de la empresa, como se mencionan a continuación:

Departamento	Tipo de servicios
Gerencia – Accionistas	Owncloud, Mail Server, ERP-Syspro, Internet.
Planta Pinturas	Owncloud, ERP-Syspro, SQL Server, Mail Server (FTP)
Control de Calidad	Owncloud, Mail Server
I.D	Owncloud, ERP-Syspro, SQL Server, Mail Server
Planta Resinas	Owncloud, ERP-Syspro, SQL Server, Mail Server
Recursos Humanos	Owncloud, Mail Server, Internet.
Seguridad y salud ocupacional	Owncloud, Mail Server
Contabilidad- Financiero – Ventas	Owncloud, ERP-Syspro, SQL Server, Mail Server, Internet.
Sistemas	Owncloud, ERP-Syspro, Mail Server, Internet, SQL Server, Remote desktop.

Tabla 3.5 Tipos de servicios asignados por departamento

A continuación, podremos visualizar las políticas aplicadas a cada OU. (Figura. 3.3.10), es necesario indicar que no todos los departamentos van a contar con la misma aplicación de las políticas dentro de todo el dominio. La restricción de puertos nos permitirá tener un mejor control sobre los usuarios y pc de nuestra red.

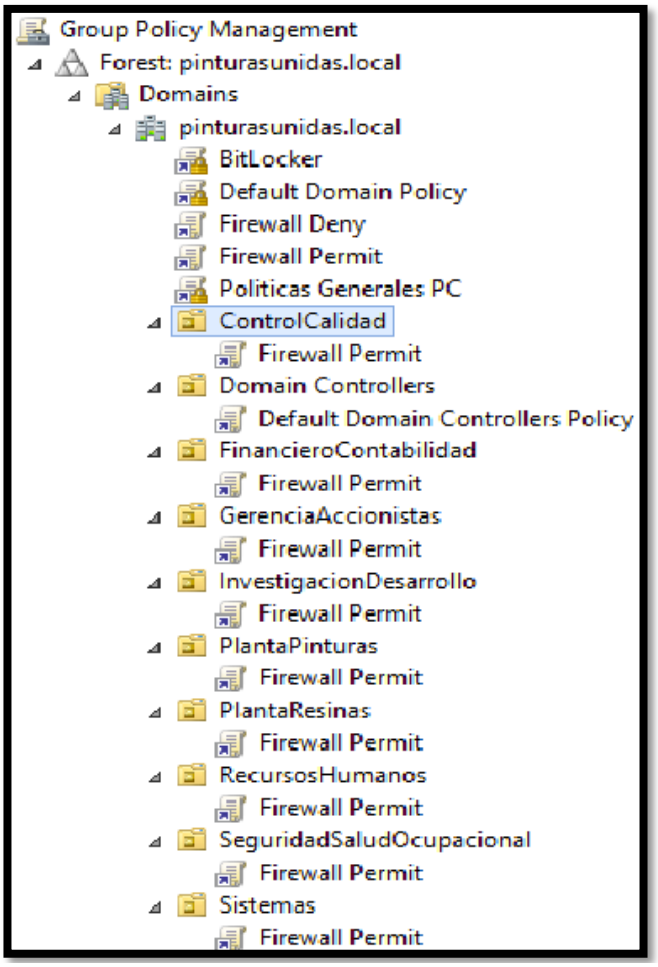


Figura. 3.3. 10 Gestión de políticas creadas para el dominio de Pinturas Unidas.

CAPÍTULO 4

4. PLAN DE IMPLEMENTACIÓN Y COSTOS

Para hacer válida y alcanzable nuestra propuesta de proyecto, se establecieron los precios de acuerdo a los requerimientos que el Gerente debe tomar en cuenta al momento de realizar mejoras dentro de su organización (Tabla 3.6). El propósito de nuestra solución es llegar a ofrecer servicios óptimos y viables para nuestro cliente. De tal manera que cuando se hagan cambios, no se deje pasar por alto el uso de las tecnologías y licenciamientos de software que se vayan a implementar.

Cantidad	Requerimiento	Precio Unitario	Valor Total
1	Licencia de Microsoft Windows Server 2012 R2 (64 bits).	$ 450	$ 450
66	Licencia de Microsoft Windows 10 Enterprise Edition.	$ 350	$ 23,100
12	Rediseño y configuración de red empresarial. (servicio y departamento).	$ 170	$ 2,040
1	Instalación y configuración de infraestructura Active Directory.	$ 380	$ 380
66	Aseguramiento de las unidades de almacenamiento (por disco duro).	$ 95	$ 6,720
32	Implementación de políticas de seguridad por pc y usuarios (por políticas).	$ 45	$ 1,440
12	Implementación de políticas de firewall (por cada política aplicada).	$ 55	$ 660
72	Servicio de ethical hacking (valor por hora de la fase de reconocimiento y escaneo).	$ 60	$ 4,320
Subtotal			$ 38,660
I.V.A			$ 4,639.20
TOTAL			$43,299.20

Tabla 3.6 Costos estimados para la implementación de la red

Es importante para nuestro cliente dejarle claro que tendrán garantía de un año en hacer uso del servicio, en caso de existir fallos en la implementación de los sistemas o políticas. Para cumplir con las fases de reconocimiento y escaneo (ethical hacking) tendrá una duración de 3 días, a un costo total de $4,320. Mientras que, para las configuraciones de GPO, implementación de Firewall, seguridades de puertos y protocolos, aseguramiento de unidades de discos y configuración de la red empresarial; se va a necesitar de un tiempo máximo de 7 días para su implementación, a un valor de $38,979.20.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

De acuerdo con lo visto en el desarrollo del documento, existe una necesidad apremiante al momento de tener una transmisión de datos segura, esto se debe a que cada día las empresas o instituciones están dependiendo más de los sistemas de redes de datos para el intercambio de información.

Conociendo la problemática central de la empresa, se contribuyó en ayudar a los directivos a mantener un estado de alerta y actualización permanente en los sistemas operativos, garantizando tener confidencialidad en la información que se comparte.

Se establecieron ciertos parámetros para mejorar la seguridad en la red como: el uso de políticas de seguridad, políticas de usuarios y generación de contraseñas seguras para cada uno de ellos. Para lograr que la gestión de la red sea bien administrada, se utilizó la implementación y configuración de VLAN.
Gracias a los servicios para voz y datos configurados, se dejó como requerimiento a nuestro cliente la libertad para implementar nuevos equipos o usuarios a la red.

Existen diferentes soluciones de software libre que ayudan en la búsqueda de vulnerabilidades en una red de manera más sencilla, por ello no debemos limitarnos con los sistemas conocidos.

Hacer una buena gestión de políticas de grupo aplicadas a los usuarios nos ayudará a tener un mejor control en los sistemas empresariales.

El alcance del análisis de las vulnerabilidades no solo se limitó en el departamento ID, sino que se extendió hacia el resto de la empresa.

Recomendaciones

Como recomendación es necesario que el Gerente de sistemas y encargados, estén en la capacidad de realizar auditorías a la red. El uso de los equipos para la aplicación de ciertos privilegios permitidos en un diagrama de red, los mismos deben ser robustos y con capacidades para soportar todo tipo de configuración.

El gerente o cualquier otro directivo no debe basarse en mejorar la infraestructura de sus sistemas operativos Windows, en caso de existir otros sistemas distintos a Microsoft o Linux, se pueda contratar a un personal capacitado para tratar con diferentes softwares y así realizar las configuraciones o cambios necesarios de los equipos.

Los usuarios deberían tomar en cuenta realizar sus respaldos hacia un servidor en la nube, los datos sobre la formulación de productos no deben ser visible para todos los empleados de la compañía.

Para tener un mejor entendimiento sobre la organización de la empresa se podría crear un dominio para agrupar a los usuarios dentro de OU y llevar un mejor control sobre ellos. Se debe recordar que la seguridad es un proceso constante que se debe monitorear, mediante continuas revisiones de las políticas de seguridad, con el fin de que día a día puedan responder de manera favorable ante nuevos retos.

Se debe tener un registro organizado en la base de datos de todos los usuarios y personal que conforman la empresa, así como se podría incentivarlos a capacitarse sobre la seguridad informática.

Es fundamental y necesario aclararle a nuestro cliente que una red no estará totalmente segura durante mucho tiempo y que los atacantes estarán a la espera de robar información. Por ello muchas de las empresas que manejan el uso de la Internet deberían conocer el medio donde se encuentran, las intenciones de sus usuarios, los sistemas operativos que manipulan, el tipo de información que

ingresa y sale de la empresa, para finalmente mitigar y reducir toda amenaza hacia la red.

Es necesario llegar a un acuerdo con los directivos de la empresa para aprobar nuestro proyecto, los directivos prefieren mejorar el entorno de seguridad a tiempo para evitar pérdidas masivas de información. Se debe contar con una persona o grupo de personas bien capacitadas para realizar las auditorías correspondientes, motivar al personal de trabajo para conocer más sobre la seguridad informática mediante cursos de aprendizaje. En una empresa y mucho más cuando se trabaja con el uso del Internet, siempre es bueno saber hacia qué mundo virtual se expone, tratar en lo posible, conocer las vulnerabilidades más frecuentes y los posibles ataques, a fin de lograr un aseguramiento de la información.

BIBLIOGRAFÍA

[1] F.Gonzalez, «dschool-Old Standford,» [En línea]. Available: https://dschool-old.stanford.edu/sandbox/groups/designresources/wiki. [Último acceso: 11 Mayo 2018].

[2] R.Reales, «WordPress,» 20 Abril 2015. [En línea]. Available: https://ronaldreales.wordpress.com/tag/vlan-administracion/. [Último acceso: 21 Junio 2018].

[3] «Tecnologia & Informatica,» [En línea]. Available: https://tecnologia-informatica.com/que-es-firewall-como-funciona-tipos-firewall/. [Último acceso: 21 Junio 2018].

[4] «Design Thinking services,» Disqus, 2017. [En línea]. Available: https://www.designthinking.services/herramientas-design-thinking/mapa-de-actores-stakeholders/. [Último acceso: 12 Mayo 2018].

[5] A.Prim, «Innokabi,» [En línea]. Available: https://innokabi.com/mapa-de-empatia-zoom-en-tu-segmento-de-cliente/. [Último acceso: 12 Mayo 2018].

[6] R.Espinosa, «Roberto Espinosa. Welcome to the new Market,» 29 Julio 2013. [En línea]. Available: https://robertoespinosa.es/2013/07/29/la-matriz-de-analisis-dafo-foda/. [Último acceso: 29 Mayo 2018].

[7] M.S.Seoane, «Innovacion Design Thinking,» 2017. [En línea]. Available: https://designthinking.gal/que-son-los-insights/. [Último acceso: 9 Junio 2018].

[8] Microsoft, «MSDN Library,» [En línea]. Available: https://msdn.microsoft.com/es-es/library/hh831713(v=ws.11).aspx. [Último acceso: 7 Julio 2018].

[9] R.Andres, «Computer Hoy,» 03 Abril 2016. [En línea]. Available: https://computerhoy.com/paso-a-paso/software/que-es-kali-linux-que-puedes-hacer-41671. [Último acceso: 17 Julio 2018].

[10] «Kali Linux en Español,» [En línea]. Available: https://kali-linux.net/article/nmap/. [Último acceso: 17 Julio 2018].

[11] «Concepto de definicion,» 2017. [En línea]. Available: http://conceptodefinicion.de/host/. [Último acceso: 18 Julio 2018].

[12] M.P.Esteso, «Geeky Theory,» 2017. [En línea]. Available: https://geekytheory.com/que-es-un-ataque-de-denegacion-de-servicio-dos. [Último acceso: 16 Junio 2018].

[13] C.Vialfa, «CCM,» Utbrain, 20 Febrero 2018. [En línea]. Available: https://es.ccm.net/contents/282-tcp-ip. [Último acceso: 16 Junio 2018].

[14] «Digital Guide,» 2017. [En línea]. Available: https://www.1and1.es/digitalguide/servidores/know-how/subnetting-como-funcionan-las-subredes/. [Último acceso: 6 Julio 2018].

[15] «El taller del bit,» 30 Julio 2012. [En línea]. Available: http://eltallerdelbit.com/subnetting-vlsm. [Último acceso: 22 Julio 2018].

[16] «Oracle Corporation,» [En línea]. Available: https://docs.oracle.com/cd/E19681-01/820-3746/gisdn/index.html. [Último acceso: 21 Julio 2018].

[17] B.Nelson, «tom's IT PRO,» Septiembre 2014. [En línea]. Available: http://www.tomsitpro.com/articles/configure-dns-windows-server-2012,2-793.html. [Último acceso: 21 Julio 2018].

[18] M.Rouse, «Search Data Center,» 2005. [En línea]. Available: https://searchdatacenter.techtarget.com/es/definicion/SQL-Server. [Último acceso: 21 Julio 2018].

[19] Microsoft, «MSDN Library,» 2010. [En línea]. Available: https://msdn.microsoft.com/es-es/library/hh831725(v=ws.11).aspx. [Último acceso: 22 Julio 2018].

[20] «Internet YA,» 10 Octubre 2016. [En línea]. Available: https://www.internetya.co/que-es-el-servicio-ftp-file-transfer-protocol/. [Último acceso: 22 Julio 2018].

[21] G. Valvo, «NetGear Community,» Mayo 2016. [En línea]. Available: https://community.netgear.com/t5/Managed-Switches/802-11q-VLAN/td-p/1085148. [Último acceso: 26 Julio 2018].

[22] «Cisco,» [En línea]. Available: https://www.cisco.com/c/es_mx/support/docs/lan-switching/vtp/10558-21.pdf. [Último acceso: 27 Julio 2018].

[23] «Cisco,» [En línea]. Available: https://www.cisco.com/c/es_mx/support/docs/security/ios-firewall/23602-confaccesslists.pdf. [Último acceso: 27 Julio 2018].

[24] C. Vialfa, «CCM,» 2017. [En línea]. Available: https://es.ccm.net/contents/261-el-protocolo-dhcp. [Último acceso: 26 Mayo 2018].

[25] Syspro, «Syspro Corporate,» Julio 2018. [En línea]. Available: https://www.syspro.com/. [Último acceso: 24 Julio 2018].

[26] «Todo Redes,» [En línea]. Available: https://todo-redes.com/equipos-de-redes/gateway-puerta-de-enlace. [Último acceso: 16 Junio 2018].

[27] F.Sierra, «CETATECH,» Diciembre 2014. [En línea]. Available: https://cetatech.ceta-ciemat.es/2014/12/directivas-de-grupo-gpo-en-windows-server-2012/. [Último acceso: 28 Julio 2018].

[28] Microsoft, «Docs.Microsoft,» [En línea]. Available: https://docs.microsoft.com/en-us/powershell/. [Último acceso: 28 Julio 2018].

[29] «Indiana University,» 2017. [En línea]. Available: https://kb.iu.edu/d/atvu. [Último acceso: 27 Julio 2018].

[30] A.Diaz, «Data Business Intelligence,» Enero 2017. [En línea]. Available: http://dbi.io/es/blog/que-son-los-logs/. [Último acceso: 16 Julio 2018].

[31] «GMS Seguridad de la informacion,» ARCOTEL, [En línea]. Available: https://gmsseguridad.com/ing-social-info.html. [Último acceso: 27 Julio 2018].

[32] MagPi, «Retro Computing,» *Raspberry Pi Magazine,* vol. I, nº 67, pp. 52-64, 2018.

[33] R.Hertzog, Kali Linux Revealed, California: Offsec Press, 2017.

[34] S.Blank, «Why the lean startup changes everything,» *Harvard Business Review,* p. 3, 2013.

[35] K.Astudillo, Linux Distros para pentesting, Amazon Books, 2013.

[36] K.Astudillo, Wireless Hacking, Amazon Books, 2017.

[37] I. H. Mancheno, «Tesis:Vulnerabilidades y seguridad en redes TCP/IP,» Guayaquil, 2013.

[38] F.Catoira, «We Live Security - Penetration Test,» Julio 2012. [En línea]. Available: https://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/. [Último acceso: 27 Julio 2018].

[39] D.Brand, «Nominalia - Seguridad del servidor Linux,» 2015. [En línea]. Available: https://www.nominalia.com/asistencia/seguridad-servidor-linux/. [Último acceso: 21 Julio 2018].

[40] Cisco, «Configuration Examples and TechNotes,» Abril 2016. [En línea]. Available: https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/. [Último acceso: 22 Julio 2018].

[41] L.D.Alvarez, «Tesis: Seguridad en Informática (Auditoría de Sistemas),» Mexico, 2005.

[42] A. Silgado, «MailRelay,» [En línea]. Available: https://blog.mailrelay.com/es/2017/04/25/que-es-el-smtp. [Último acceso: 22 Julio 2018].

ANEXOS

Anexo A

Entrevistas realizadas a nuestro grupo de interesados.

A.1. Gerente General de la empresa

Datos de la entrevista

Entrevistador: Ahmed Pérez
Fecha/día/hora: 09/07/2018
Nombre de la empresa: Pinturas Unidas S.A
Nombre del encuestado: Ec. Luis Domínguez
Edad:
Dirección: Km. 16.5 vía a Daule
Número telefónico:
Ocupación: Gerente General Pinturas Unidas S.A.
Tiempo laborando en la empresa: 20 años

Preguntas:

1. **¿Quién o quienes regulan la actividad del área de ID en su empresa?**
   El gerente técnico Ing. Luis santos

2. **¿Quién o quienes regulan la actividad del área de INFORMATICA en su empresa?**
   El departamento de sistemas

3. **¿Cuántos años lleva ejerciendo su cargo como gerente general de pinturas unidas s.a.?**
   20 años

4. **¿Qué tiempo lleva usando sistemas informáticos en la empresa?**
   Desde el año 2001
5. **¿Alguna vez se han sometido a alguna demanda o ustedes han demandado a algún empleado por robo de información o plagio de fórmulas y productos?**
   No nos hemos sometido a ninguna demanda ni hemos demandado a nadie tampoco

6. **¿Cada cuánto tiempo actualizan la información sobre sus productos en su base de datos?**
   Cada 3 meses

7. **¿Cada producto comercializado por ustedes, es único y pionero al salir en el mercado o ya hay otros productos similares en venta?**
   Nuestros productos son pioneros en el mercado nacional, hay productos similares, pero de calidad inferior.

8. **¿Conoce la función a cumplir de cada uno de sus usuarios dentro de su empresa?**
   Claro que sí, cada departamento tiene a su gerente y jefe de los cuales tienen a su cargo de 3 a 5 personas y sabemos muy bien que función cumple cada uno.

9. **¿Sus usuarios de su empresa son discretos al momento de mantener confidencial la información en el sistema?**

Tienen que cumplir un código de ética, confidencialidad y de integridad más pruebas de confianza que se les hace periódicamente.

10. **¿Está su personal del área de sistemas capacitado para actuar frente a ataques informáticos?**
    Tengo entendido que tienen respaldo que pueden volver a utilizar en caso de que falle alguna maquina o los servidores

11. **¿Su equipo de trabajo conoce sobre medidas de seguridad de información?**
    Cada equipo conoce las medidas se seguridad informática de acuerdo a su área.

12. **¿Cuántas políticas de seguridad informática manejan aproximadamente en su empresa?**
    Aproximadamente 10 políticas de seguridad.

13. **¿Qué políticas de seguridad informática aplican en su área? Explique a la brevedad.**
    Cambio de clave, respaldos periódicos, actualizaciones del Windows 7, poner en reposo cuando ha transcurrido 30 segundos.

14. **¿Están constantemente renovando sus políticas? ¿En base a qué la van mejorando o cambiando?**
    Se las renueva cada año y es en base a lo que se ha tenido que corregir o de los que se aprendió durando el año

15. **¿Realizan un registro de su información en la nube o en sus equipos informáticos? (base de datos, archivos, carpetas, servidores).**
    Tengo entendido que se hacen un servidor de archivos

16. **¿Qué matriz de riesgo tiene para sus equipos?**
    De eso se encarga el departamento de sistemas

17. **¿Sus claves de acceso a los equipos de cómputo constan de una clave segura, como caracteres especiales entre mayúsculas, minúsculas y alfanuméricas?**
    Solo mayúsculas y minúsculas

18. **¿Cada cuánto tiempo cambian sus contraseñas de seguridad? ¿Lo hacen de forma obligada por tiempo de expiración o por voluntad propia?**
    Lo hacemos por tiempo de expiración y es cada 3 meses
19. **¿Cuentan con algún software que bloquee el robo de información por medios de almacenamiento?**
    Por el momento no

20. **¿Cuántas veces han sido víctimas de la fuga de su información hacia usuarios ajenos a su empresa?**
    No hemos sido víctimas de algún robo de información directo, pero si tenemos nuestras sospechas

21. **¿Han recibido quejas por parte de sus usuarios por el robo de información? ¿sobre qué eran estas quejas?**
    Una vez recibimos una queja de un usuario de nosotros que había visto que se comercializaba un producto bastante similar al que estábamos desarrollando, pero de calidad inferior.

22. **¿Se ha despedido a empleados que en su momento plagiaron información? ¿Cuáles fueron los motivos más relevantes?**
    Se ha cesado de funciones a empleados sí, pero no por plagio de fórmulas, las razones han sido por mal desempeño laboral o conducta inadecuada dentro de la planta.

A.2. Usuario final

Datos de la entrevista

Entrevistador: Ahmed Pérez, Stephanie Villacis
Fecha/día/hora: 9/07/2018
Nombre de la empresa: Pinturas Unidas S.A
Nombre del encuestado:
Edad: _____
Dirección: Av. Rosavin solar 3 y Cobre Mz. H-8 Km. 16½ de la vía a Daule
Número telefónico: **Ocupación**: Jefe de soporte técnico
Tiempo laborando en la empresa: 10 años

Preguntas:

1. **¿Conoce la función que debe cumplir su departamento**? Las funciones del departamento es el desarrollo de nuevos productos, así como la modificación de la formulación e instructivos de fabricación según la variación de las características deseadas como la variación de materias primas.

2. **¿Cuál es su cargo y funciones que debe cumplir?** Jefe de supervisión y soporte técnico a los miembros del departamento en el desarrollo de nuevos productos y modificación de productos existente.

3. **¿Cuántos años lleva ejerciendo su cargo en el departamento de ID de Pinturas Unidas?** 10 años.

4. **¿Durante sus años de trabajo, ha notado anomalías en el departamento?** Si

5. **¿Conoce sobre medidas de seguridad de la red?** En forma muy escueta

6. **¿Qué tipo de información manejan en el departamento?** La Formula e instructivo de fabricación de los productos

7. **¿Qué sistema operativo usan en su departamento?** Windows 7

8. **¿Cada cuánto tiempo actualiza esta información?** Cuando sea necesario, no hay un tiempo determinado.

9. **¿Conoce usted sobre lo que es tener una contraseña segura al momento de iniciar sesión en su equipo de cómputo?** Por supuesto, es importante que ninguna persona ingrese y pueda observar o manipular la información.
10. **¿Conoce usted el concepto de un ataque informático?** Tengo entendido que una actividad informática no autorizada para dañar, borrar o copiar información sensible.

11. **En caso de presentarse algún ataque informático, ¿sabría cómo mitigarlo?** No tengo el conocimiento para evitarlo o mitigarlo.

12. **¿Su equipo de cómputo cuenta con antivirus o algún otro software de protección contra malwares o virus?** Si, Norton Antivirus.

13. **La información que maneja en su área, ¿con quién la comparte? (usuarios externos).** Solo con usuarios internos del mismo departamento, el departamento de producción.

14. **¿Maneja la información de forma remota?** No.

15. ¿**Cuenta con algún software que bloquee el robo de información por medios de almacenamiento?** Si el Norton antivirus

16. **¿Ha sufrido algún ataque informático?** No que yo sepa

17. **¿Cree usted que deba mejorar algo en su departamento en cuanto al procesamiento de datos?** No lo podría decir.

A.3. Gerente Técnico de ID

Datos de la entrevista

Entrevistador: Stephanie Villacís – Ahmed Pérez
Fecha/día/hora: martes 26 de junio, 15:30
Nombre de la empresa: Pinturas Unidas S.A
Nombre del encuestado: Msc. Ing. Luis Santos
Edad: 45 años
Dirección: Km. 16.5 vía a Daule
Número telefónico: 0987231795
Ocupación: Gerente Técnico en Investigación y Desarrollo de Pinturas Unidas S.A.
Tiempo laborando en la empresa: 40 años

Preguntas:

1. **¿Quién o quienes regulan la actividad del área de ID en su empresa?**

   El auditor interno y las auditorías externas realizadas por entidades que se encargan de verificar que se cumplan las normal ISO9000

2. **¿Cuántos años lleva ejerciendo su cargo en el departamento de ID?**

   10 años

3. **¿Qué tiempo llevan ofreciendo sus productos al mercado?**

   más de 40 años.

4. **¿Cada cuánto tiempo actualizan la información sobre sus productos en su base de datos?**

   La base de datos de productos la actualizamos cada 3 meses, ya sea por cambio de algún ingrediente de la formula o lanzamiento de nuevos productos.

5. **¿Cada producto comercializado por ustedes, es único y pionero al salir en el mercado o ya hay otros productos similares en venta?**

   Existen productos de similar composición y colores muy cercano, pero cuando se trata de lanzamientos nuevos si somos los pioneros.

6. **¿Conoce la función a cumplir de cada uno de sus usuarios dentro del área de ID?**

   Claro que si, tenemos a formulación, calidad, laboratorio de durabilidad, impacto ambiental y colorimetría.

7. **¿Sus usuarios son discretos al momento de mantener confidencial la información en el sistema?**

Confiamos mucho en el personal que trabaja en esta área, adicional al proceso de selección cada 6 meses se les hace una prueba de integridad.

8. **¿Está su personal capacitado para actuar frente a ataques informáticos?**

   Solo en uso correcto de los terminales dentro del área

9. **¿Su equipo de trabajo conoce sobre medidas de seguridad de información?**

   La única medida que conocen es sobre la no divulgación de fórmulas y procesos

10. **¿Cuántas políticas de seguridad manejan aproximadamente en su departamento ID?**

    Solo el usuario y la contraseña por maquina

11. **¿Qué políticas de seguridad aplica en su área? Explique a la brevedad.**

    Horarios de inicio de sesión que corresponden a la hora de entrada y salida del personal, restricción de copias por medios extraíbles USB.

12. **¿Están constantemente renovando sus políticas? ¿En base a qué la van mejorando o cambiando?**

    Solo cuando se añaden nuevos terminales en el área y es cada 2 años se amplía el alcance de las políticas.

13. **¿Realizan un registro de su información en la nube o en sus equipos informáticos? (base de datos, archivos, folders).**

    Realizamos un almacenamiento en un servidor de archivos.

14. **¿Tiene una matriz de riesgo para sus equipos?**

    Desconozco, quizás el departamento de sistemas la tenga

15. **¿Con que frecuencia actualizan sus servidores?**

    Cada mes

16. **¿Sus claves de acceso a los equipos de cómputo constan de una clave segura, como caracteres especiales entre mayúsculas, minúsculas y alfanuméricas?**

    Son claves personalizada por usuario, pero no se les exige robustez

17. **¿Cada cuánto tiempo cambian sus contraseñas de seguridad?**

    Con poca frecuencia, podría decirse que no la cambiamos

18. **¿Cuentan con algún software que bloquee el robo de información por medios de almacenamiento?**

    Solo contamos con control en los terminales en sitio, pero no en sus unidades de almacenamiento.

19. **¿Cuántas veces han sido víctimas de la fuga de su información hacia usuarios ajenos a su empresa?**

    Por usuarios ajenos a la empresa no hemos tenido conocimiento, pero tuvimos un incidente con un exempleado que sospechosamente puso su microempresa de pinturas y vendía productos muy similares a los nuestros

20. **¿Han recibido quejas por parte de sus usuarios por el robo de información? ¿sobre qué eran estas quejas?**

    Quejas no, pero si observaciones sobre productos muy similares, con respecto a la textura y la formulación de estas

21. **¿Ha habido despidos a empleados que en su momento plagiaron información? ¿Cuáles fueron los motivos más relevantes?**

    Despidos por plagio no, pero si despidos por culminación de contrato y es muy probable que tengan resentimientos.

A.4. Gerente de Sistemas

Datos de la entrevista

Entrevistador: Ahmed Pérez
Fecha/día/hora:
Nombre de la empresa: Pinturas Unidas S.A
Nombre del encuestado: Javier Valencia
Edad:
Dirección: Km. 16.5 vía a Daule
Número telefónico:
Ocupación: Gerente de Sistemas Pinturas Unidas S.A.
Tiempo laborando en la empresa: 4 años

Preguntas:

1. **¿Con que frecuencia actualizan sus servidores?**
   Cada 6 meses
2. **¿Cada cuánto tiempo cambian sus contraseñas de seguridad?**
   Cada mes
   ¿Lo hacen de forma obligada por tiempo de expiración o por voluntad propia?
   Por tiempo de expiración
3. **¿Cuántas veces han sido víctimas de la fuga de su información hacia usuarios ajenos a su empresa?**
   Puntualmente por fuga no hemos sido víctimas, pero si tenemos sospechas de que alguien sacó información incompleta de formulas
4. **¿Sus claves de acceso a los equipos de cómputo constan de una clave segura, como caracteres especiales entre mayúsculas, minúsculas y alfanuméricas?**
   Solo mayúsculas y minúsculas
5. **¿Realizan un registro de su información en la nube o en sus equipos informáticos? (base de datos, archivos, carpetas, servidores).**
   Servidor de archivos con Windows Server 2008
6. **¿Están constantemente renovando sus políticas? ¿En base a qué la van mejorando o cambiando?**
   Las políticas de seguridad informática se renuevan cada año, lo hacemos en base a las experiencias adquirida o algún incidente que se presente duran los 12 meses.
7. **¿Qué políticas de seguridad informática aplican en su área? Explique a la brevedad.**
   Suspender el S.O. después de 30 segundos de inactividad, registrar logs cuando se copia algo hacia alguna unidad de almacenamiento extraíble, copias de seguridad automáticas cada 2 semanas
8. **¿Cuántas políticas de seguridad informática manejan aproximadamente en su empresa?**
   Aproximadamente 10 políticas

9. **¿Está su personal del área de sistemas capacitado para actuar frente a ataques informáticos?**
   Contamos con respaldos del servidor y las copias de seguridad de las estaciones de trabajo para poder restaurar los equipos de ser necesario.
10. **¿Cuántos años lleva ejerciendo su cargo como gerente de sistemas de Pinturas Unidas S.A.?**
    4 años
11. **¿Qué tiempo lleva usando sistemas informáticos en la empresa?**
    Desde el año 2001

ANEXO B

Mapas de Empatía de los entrevistados

Figura. B. 1 Mapa de Empatía Gerente General.

Figura. B. 2 Mapa de Empatía Gerente de Sistemas.

Figura. B. 3 Mapa de empatía Jefe de Soporte Técnico.

ANEXO C

Funcionamiento del prototipo con la Raspberry Pi y software Kali Linux

Para realizar la muestra de que existen vulnerabilidades en la red de un departamento, por medio del uso de la Raspberry Pi y junto a demás dispositivos (Figura C.1) conectados hacia ella, pudimos hacer posible las pruebas de pentesting.

Figura. C. 1 Equipos usados para funcionamiento de prototipo.

Una vez que se haya encendido el dispositivo, se visualizan los paquetes cargados para el uso del software Kali Linux (Figura. C.2), se verá un reporte de todos los servicios habilitados en el sistema operativo.

Figura. C. 2 Descarga de paquetes para instalación de Kali Linux.

Cuando se hayan cargado y habilitado todos los servicios del software se inicia sesión en el sistema (Figura. C.3) para hacer uso de las propiedades para el testeo necesario en las redes y puertos del departamento ID.

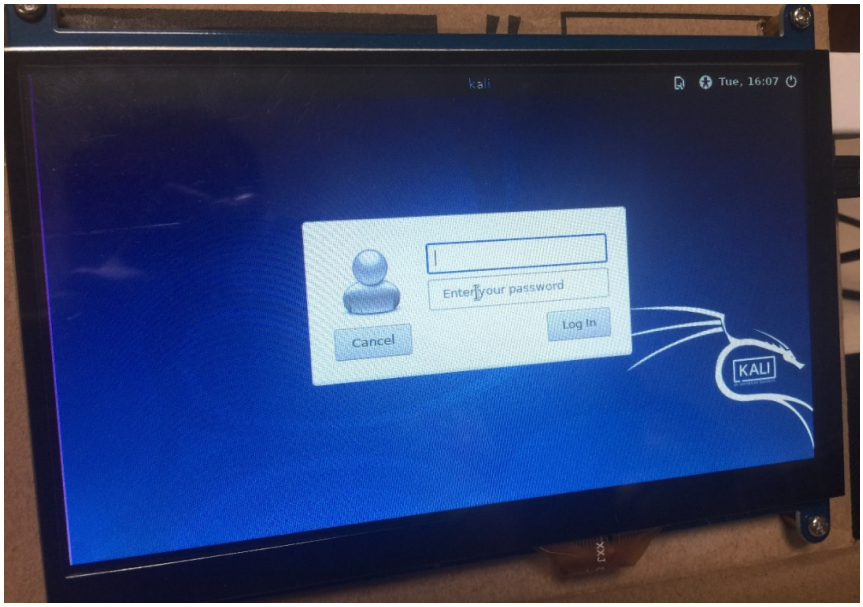


Figura. C. 3 Inicio de sesión de usuario al sistema.

Podremos visualizar el entorno de trabajo de Kali Linux asociado (Figura. C.4), como se aprecia, es una herramienta muy amigable y de fácil entendimiento.

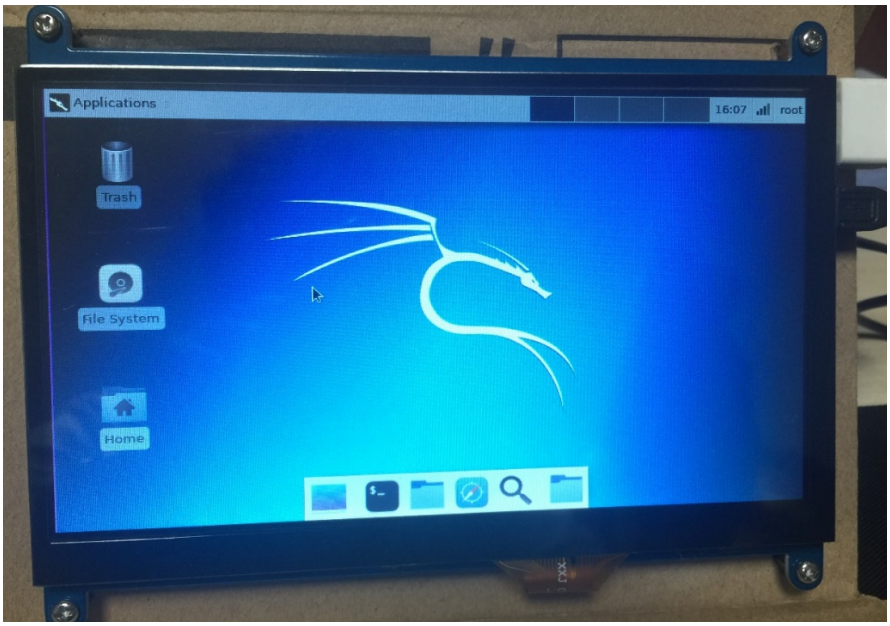


Figura. C. 4 Ambiente de trabajo de Kali Linux.

Seleccionamos la parte de applications (Figura. C.5), se desplegará una barra de opciones, donde nos dirigimos a abrir el terminal para hacer uso del comando “nmap”.

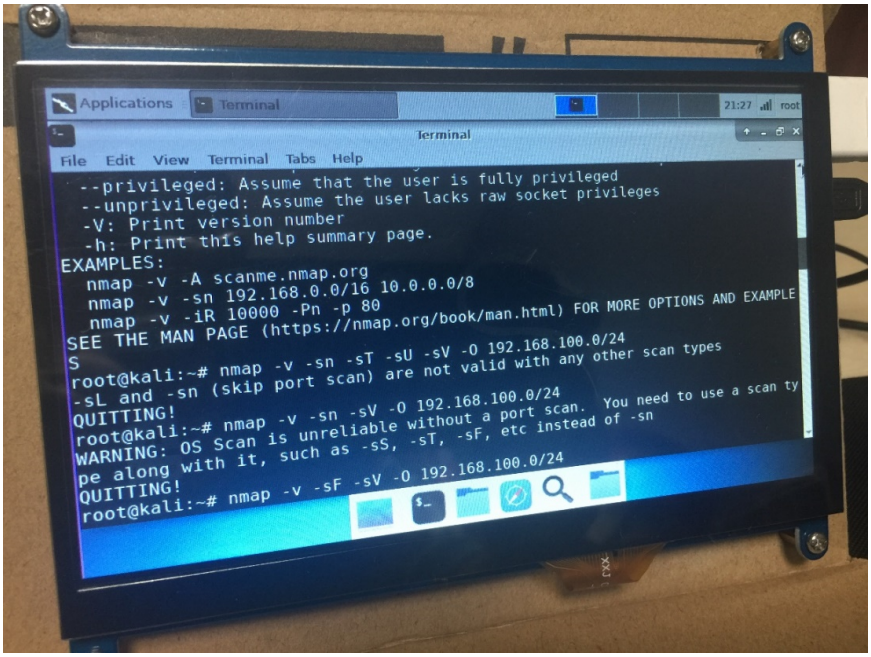


Figura. C. 5 Terminal para ejecución de comando en Kali Linux.

Hacemos uso del comando nmap dependiendo de los parámetros que buscamos durante el escaneo (Figura. C.6) y éste se encargará de generar todos los reportes en cuestión de segundos sobre las posibles vulnerabilidades en los puertos de la red.

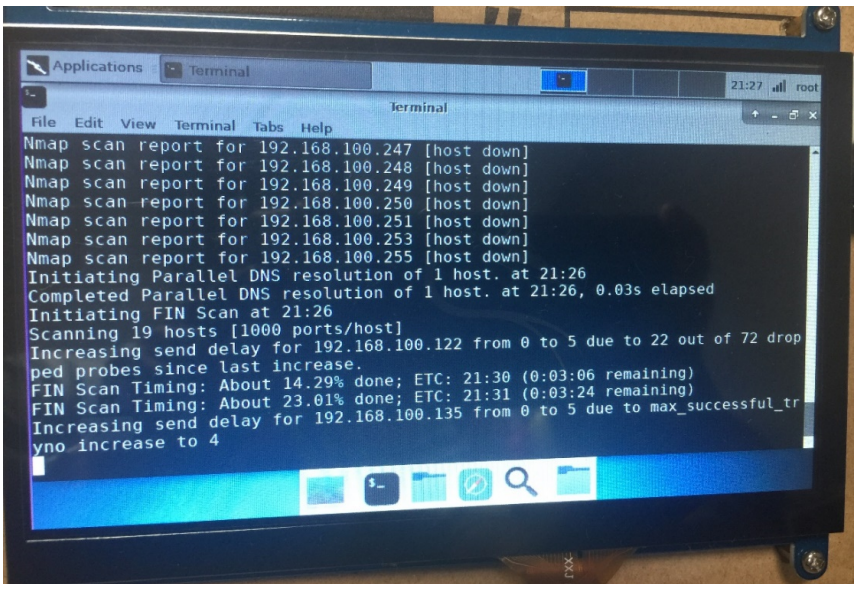


Figura. C. 6 Reporte generado del comando nmap.

Esperamos mientras se leen todos los puertos y protocolos de la red que queremos explotar (Figura. C.7) y durante el transcurso se fueron observando los servicios que estaban trabajando para la red que estábamos explorando.

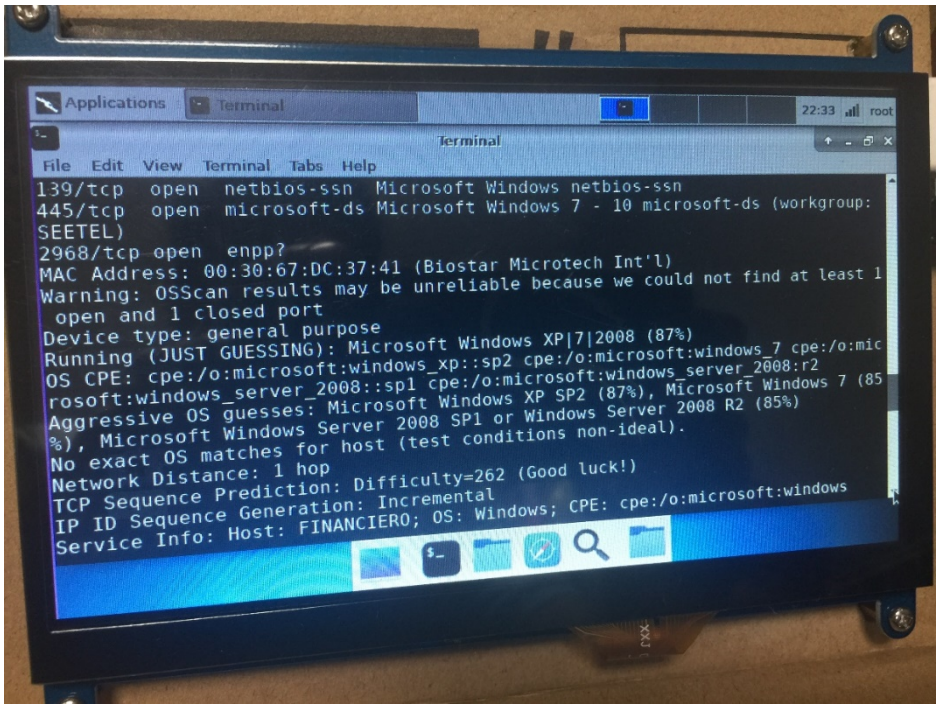


Figura. C. 7 Análisis de puertos por medio del comando nmap.

ANEXO D

Comandos de configuración de los equipos de red.

D.1 Switch Distribución:

Con el comando show running-config se muestra el contenido del archivo de configuración activo del equipo. El Switch denominado: Distribución, tiene lo siguiente configurado:

- Usuario y contraseña para consola y vty 0 4.
- VTP modo server con domain “Unidas” y password “unidas”.
- Interfaces configuradas en modo de troncal para la comunicación con los Switch de cada departamento y con el Router.
- VLANs con sus respectivos nombres.
- Asignación de la primer IP disponible de cada segmento de red por VLAN.
- Seguridad a los puertos que estén siendo usados con “switchport port-security”.
- Los puertos que no están siendo utilizados están deshabilitados.

```
Building configuration...
Current configuration: 7714 bytes
!
version 12.2(37)SE1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SC
!
!
!
!
!
!
ip routing
!
!
!
!
username admin secret 5
$1$mERr$vTbHul1N28cEp8lkLqr0f/
username monitoreo secret 5
$1$mERr$YWBjyix9xTRBr/9YX/qL80
!
!
!
!
!
!
!
!
!
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
!
!
!
!
!
```

-Se configurará la fastEthernet0/1 en modo trunk y se habilita la VLAN de voz. Como se muestra a continuación:

```
interface FastEthernet0/1
 switchport trunk native vlan 90
```

```
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport voice vlan 4
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!
```

-Las mismas propiedades en modo trunk desde la interfaz 0/2-0/19, como se muestra a continuación:

```
interface FastEthernet0/2
 switchport trunk native vlan 90
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!
interface FastEthernet0/3
 switchport trunk native vlan 90
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!
```

-A partir de la interfaz 0/20 -0/24 se habilita el servicio para voz, como se muestra a continuación:

```
interface FastEthernet0/20
 switchport trunk native vlan 90
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport voice vlan 4
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 shutdown
!
interface FastEthernet0/21
 switchport trunk native vlan 90
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport voice vlan 4
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 shutdown
!
interface GigabitEthernet0/1
 switchport trunk native vlan 90
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan2
 mac-address 0040.0b9e.080a
 ip address 172.16.1.17 255.255.255.248
!
```

-A partir de la VLAN 10 hasta la VLAN 90 se configuran las direcciones IP. Como se muestra a continuación:

```
interface Vlan10
 mac-address 0040.0b9e.0801
 ip address 172.16.0.1 255.255.255.224
 ip access-group PROHIBIR in
!
interface Vlan20
 mac-address 0040.0b9e.0802
 ip address 172.16.0.33 255.255.255.224
!
 no cdp run
!
!
!
!
!
line con 0
 exec-timeout 5 0
 login local
!
line aux 0
!
line vty 0 4
 exec-timeout 5 0
 login local
line vty 5 15
 login
```

D.2 SWITCH GERENCIA

El Switch de Gerencia tiene lo siguiente configurado:

- Usuario y contraseña para consola y vty 0 4.
- Interfaces configuradas en modo de troncal para la comunicación con el Switch Distribución.
- VTP modo Client con domain “Unidas” y password “unidas”.
- Interfaces configuradas en modo de acceso para la VLAN respectiva.
- Seguridad a los puertos que estén siendo usados con “switchport port-security”.
- Los puertos que no están siendo utilizados están deshabilitados.

  Nota: La misma configuración debe ser para los demás switches de departamentos, como se estimó, a excepción de Sistemas

```
Building configuration...

Current configuration: 5657 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Gerencia
!
!
!
no ip domain-lookup
!
username admin secret 5
$1$mERr$vTbHul1N28cEp8lkLqr0f/
username monitoreo secret 5
$1$mERr$YWBjyix9xTRBr/9YX/qL80
!
!
spanning-tree mode pvst
spanning-tree extend system-id
```

-A partir de la interfaz 0/1 hasta la 0/5 se configuran en modo trunk como se visualiza a continuación:

```
interface FastEthernet0/1
 switchport trunk native vlan 90
 switchport mode trunk
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!
interface FastEthernet0/2
 switchport trunk native vlan 90
 switchport mode trunk
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!
```

-Se habilita el servicio de voz para las interfaces 0/6-0/24 como se muestra a continuación:

```
interface FastEthernet0/6
 switchport access vlan 20
 switchport mode access
 switchport voice vlan 4
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 spanning-tree portfast
!
```

```
interface FastEthernet0/7
 switchport access vlan 20
 switchport mode access
 switchport voice vlan 4
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 spanning-tree portfast
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
 login local
 exec-timeout 5 0
!
line vty 0 4
 exec-timeout 5 0
 login local
line vty 5 15
 login
!
!
!
End
```

D.3 SWITCH SISTEMAS

El Switch Sistemas tiene lo siguiente configurado:

- Usuario y contraseña para consola y vty 0 4.
- Interfaces configuradas en modo de troncal para la comunicación con el Switch Distribución.
- VTP modo Client con domain “Unidas” y password “unidas”.
- Interfaces configuradas en modo de acceso para cada una de las VLANs.
- Seguridad a los puertos que estén siendo usados con “switchport port-security”.
- Los puertos que no están siendo utilizados están deshabilitados.

```
Building configuration...

Current configuration: 5193 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Sistemas
!
!
!
no ip domain-lookup
!
username admin secret 5
$1$mERr$vTbHul1N28cEp8lkLqr0f/
username monitoreo secret 5
$1$mERr$YWBjyix9xTRBr/9YX/qL80
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
```

-Desde la interfaz 0/1 -0/5 quedarán configuradas en modo trunk, como se muestra a continuación:

```
interface FastEthernet0/1
 switchport trunk native vlan 90
 switchport mode trunk
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!
interface FastEthernet0/2
 switchport trunk native vlan 90
 switchport mode trunk
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!
```

-A partir de la interfaz 0/6 -0/24 se habilitará el servicio para voz, asegurando los puertos del equipo, como se muestra a continuación:

```
interface FastEthernet0/6
 switchport access vlan 90
 switchport mode access
 switchport voice vlan 4
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!
interface FastEthernet0/7
 switchport access vlan 90
 switchport mode access
 switchport voice vlan 4
 switchport port-security mac-address sticky
 switchport port-security violation restrict
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
```

```
!
interface Vlan1
 no ip address
 shutdown
!
!
!
!
line con 0
 login local
 exec-timeout 5 0
!
line vty 0 4
 exec-timeout 5 0
 login local
line vty 5 15
 login
!
!
!
End
```

D.4 ROUTER UNIDAS

El Router Unidas tiene lo siguiente configurado:

- Usuario y contraseña para consola y vty 0 4.
- DHCP para el rango de direcciones del servicio de VOZ.
- Más de 10 ephone creados para los teléfonos IP.
- Los puertos que no están siendo utilizados están deshabilitados.

```
Unidas# sh run
Building configuration...

Current configuration: 2514 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Unidas
!
!
!
!
!
ip dhcp pool Voz
 network 172.16.2.0 255.255.255.0
 default-router 172.16.2.1
 option 150 ip 172.16.2.1
!
!
!
ip cef
no ipv6 cef
!
!
!
!
!
!
!
!
!
!
!
no ip domain-lookup
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip address 172.16.3.3 255.255.255.240
!
interface FastEthernet0/0.4
 encapsulation dot1Q 4
 ip address 172.16.2.1 255.255.255.0
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
router rip
!
ip classless
!
ip flow-export version 9
!
!
```

```
!
!
!
!
!
telephony-service
 max-ephones 40
 max-dn 100
 ip source-address 172.16.2.1 port 2000
 auto assign 1 to 10
 auto assign 1 to 40
!
```

-Se habilita la línea telefónica y así para la cantidad de teléfonos que se quiera configurar, como se muestra a continuación:

```
ephone-dn 1
 number 200
!
ephone-dn 2
 number 201
!
```

-Se asignó automáticamente la MAC-Address de algún teléfono conectado y así se irán asignando direcciones a cada una de las líneas añadidas, como se muestra a continuación:

```
ephone 1
 device-security-mode none
 mac-address 0090.0CA2.463C
 type 7960
 button 1:1
!
ephone 2
 device-security-mode none
 mac-address 000D.BD7A.8780
 type 7960
 button 1:2
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
!
!
end
```

ANEXO E

Configuración e instalación de la máquina virtual con Windows Server 2012

Seleccionaremos el tipo de idioma, huso horario, entre otras configuraciones que corresponderán a las preferencias del administrador, una vez seleccionados estos parámetros le damos click a “Next” para continuar el proceso de instalación.

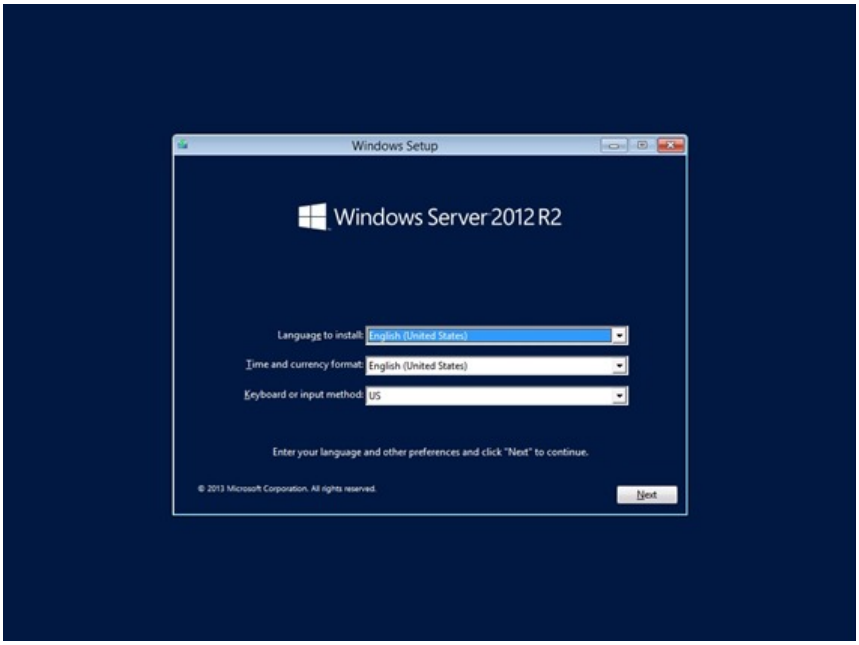


Figura. E. 1 Instalación del Windows Server 2012.

Se nos pedirá la creación de un usuario, el cual debe contener el nombre del usuario y una contraseña, es recomendable la creación de este usuario con el fin restringir el uso de Windows Server únicamente a los usuarios que conozcan estos parámetros de ingreso, normando y protegiendo el uso de la información a ser almacenada, le damos click a “Finish”.

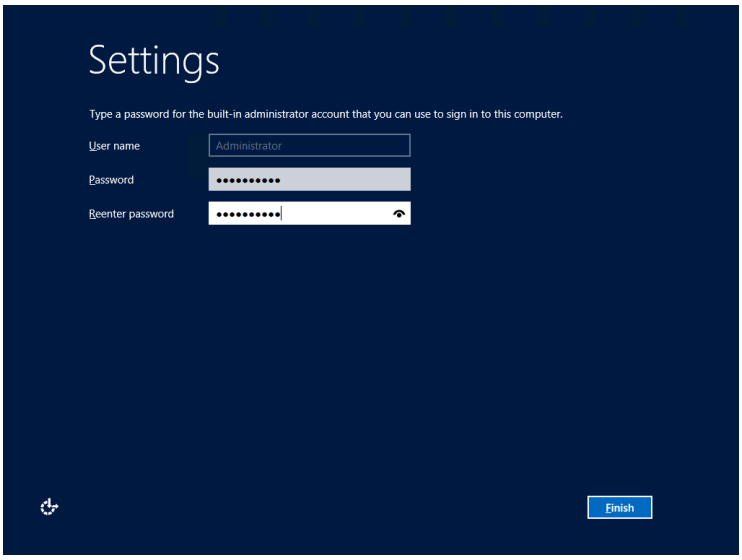


Figura. E. 2 Ingreso de Password.

Comprobación del dominio configurado, que antes de esto se instaló el rol de Active Directory Domain Services, para promover el servidor a controlador de dominio.

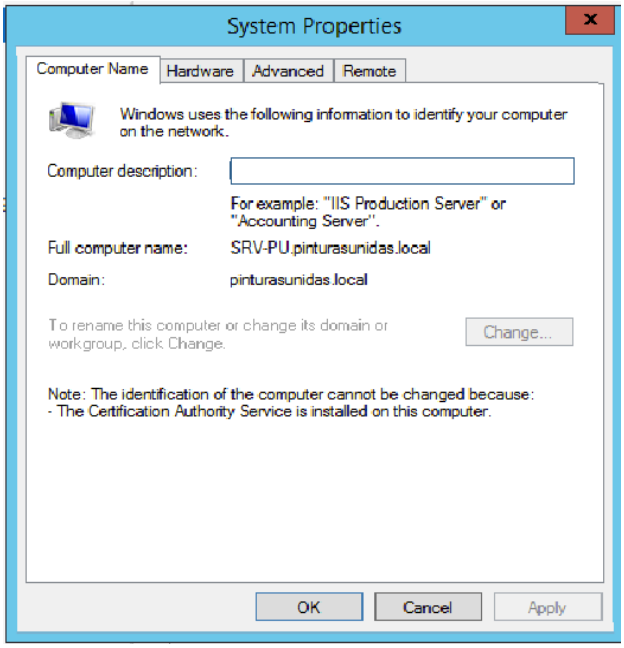


Figura. E. 3 Configuración del dominio para Pinturas Unidas.

Configuramos una dirección IP para la salida a la red WAN.

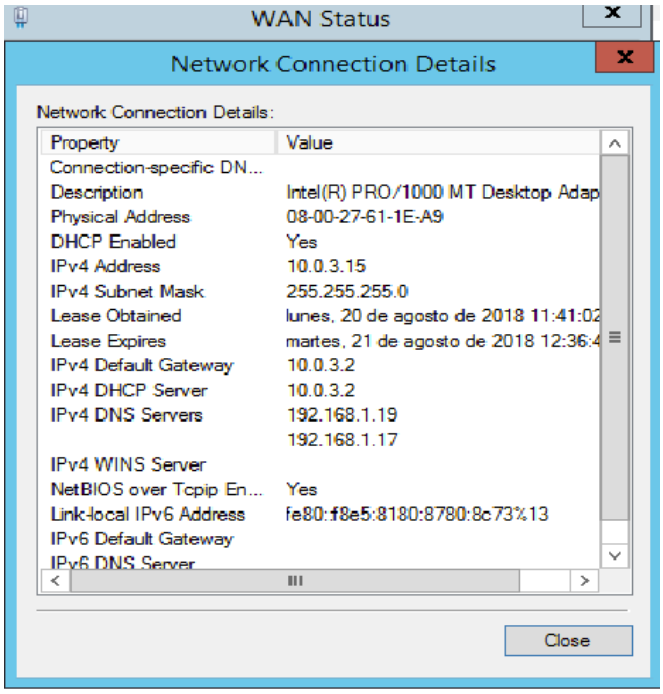


Figura. E. 4 Configuración de la red para la WAN.

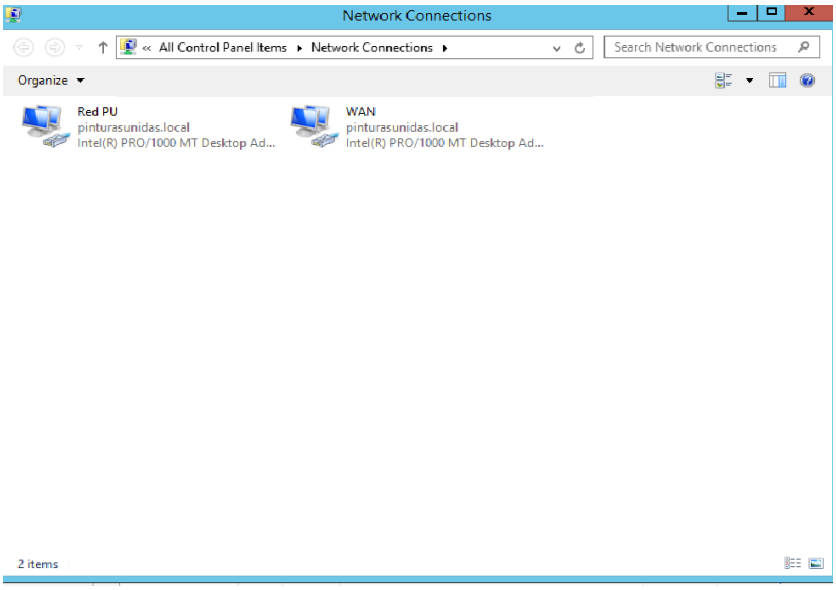


Figura. E. 5 Verificación de la red para la WAN

ANEXO F

Creación de OU y usuarios para la empresa.

En active Directory Huseras and Computers *(*Figura F.1 y Figura F.2*)*, creamos las OU que representan a cada uno de los departamentos de la empresa, con sus respectivos usuarios.

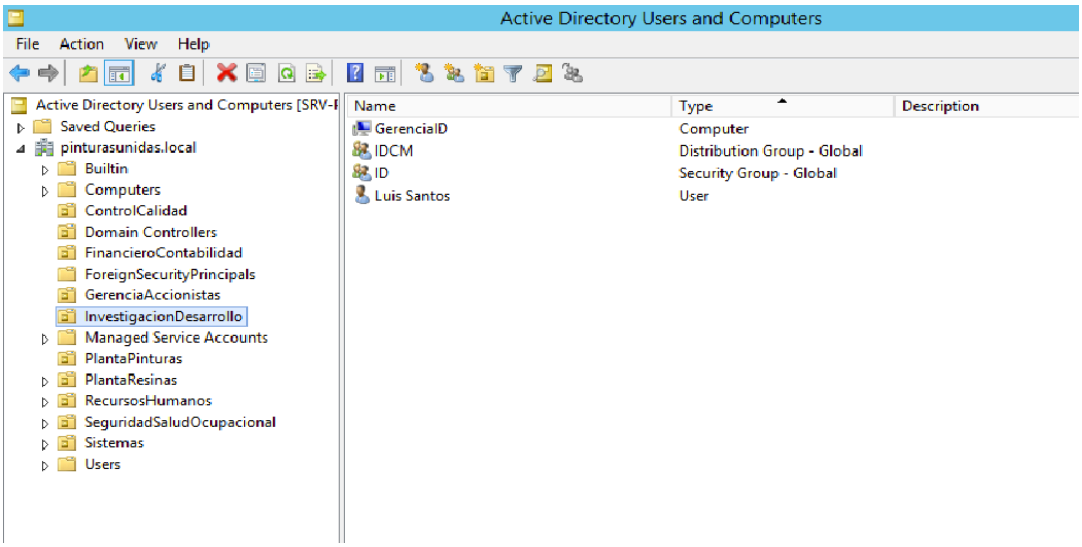


Figura. F. 1 Creación de OU y Usuarios para cada departamento de la empresa.

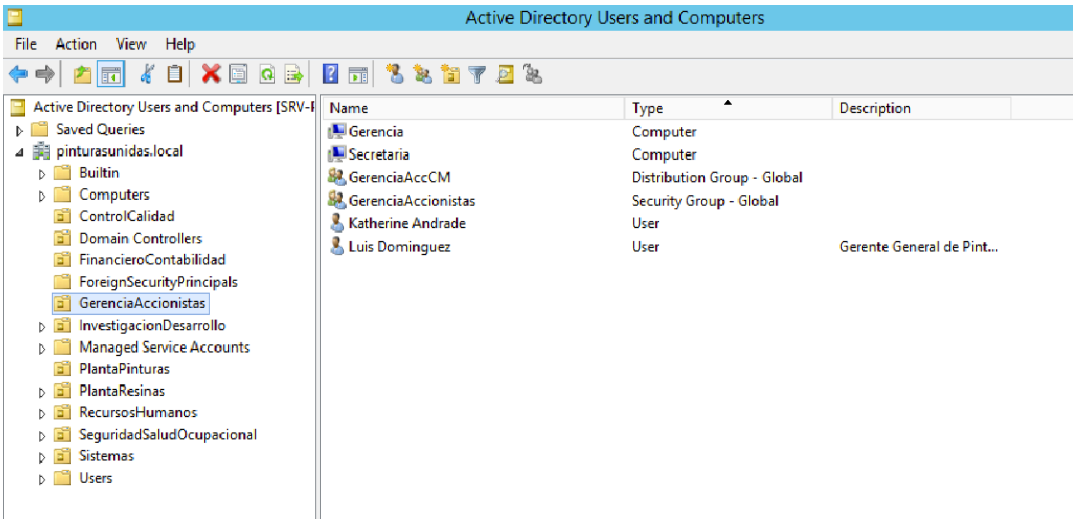


Figura. F. 2 Usuarios y OU creados para cada departamento de la empresa.

ANEXO G

Aplicación de políticas Firewall

Configuramos el bloqueo para que los usuarios de ciertos departamentos no tengan salida al internet.

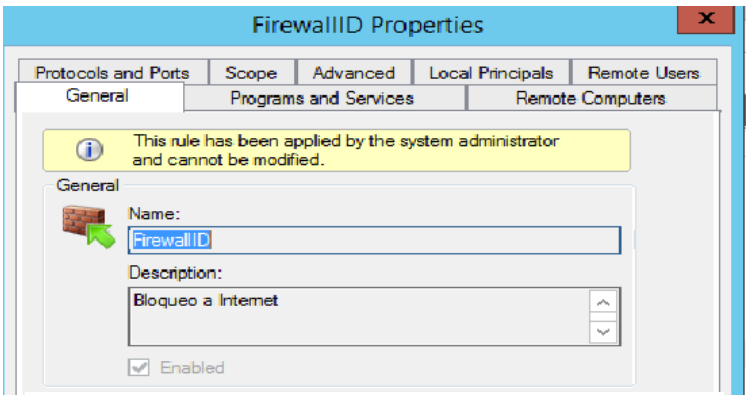


Figura. G. 1 Bloqueo de internet en departamento ID.

Se especifican los puertos, a los cuales pertenecen la salida a internet, para que sean bloqueados.

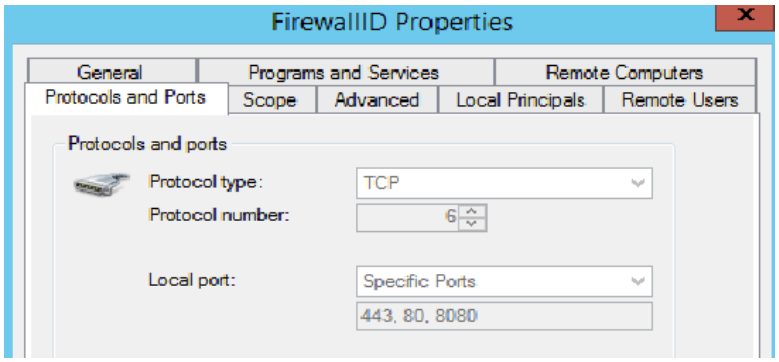


Figura. G. 2 Bloqueo de puertos de internet en departamento ID.

Ahora configuramos los servicios a los que va a acceder los departamentos, y los especificamos en la descripción.

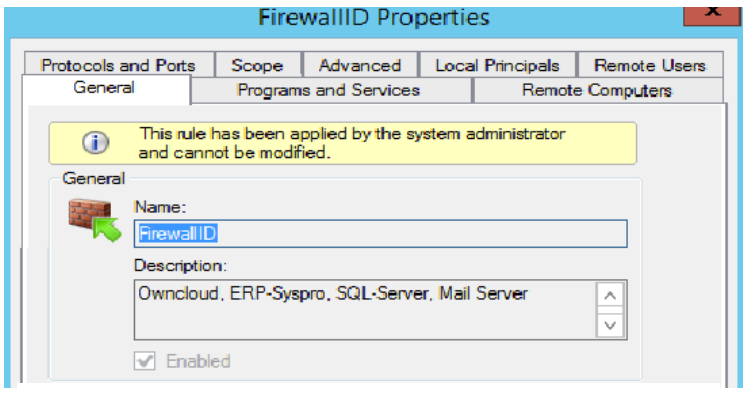


Figura. G. 3 Servicios permitidos para ID.

Y especificamos los puertos, a los cuales pertenecen cada uno de los servicios, para que puedan tener acceso los departamentos.

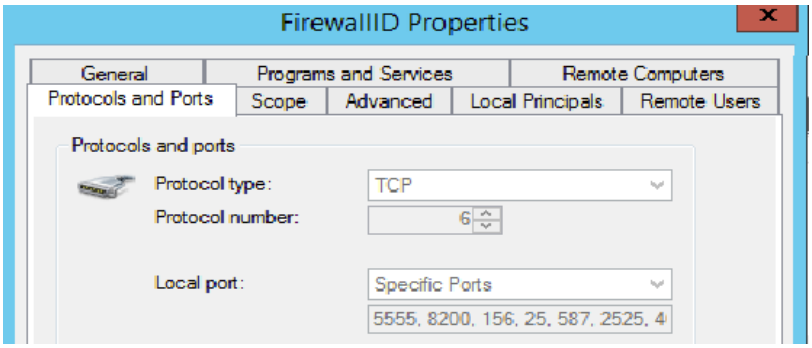


Figura. G. 4 Puertos permitidos para ID.

Configuramos los servicios que van a acceder los departamentos que tienen mayor prioridad, y los especificamos en la descripción.

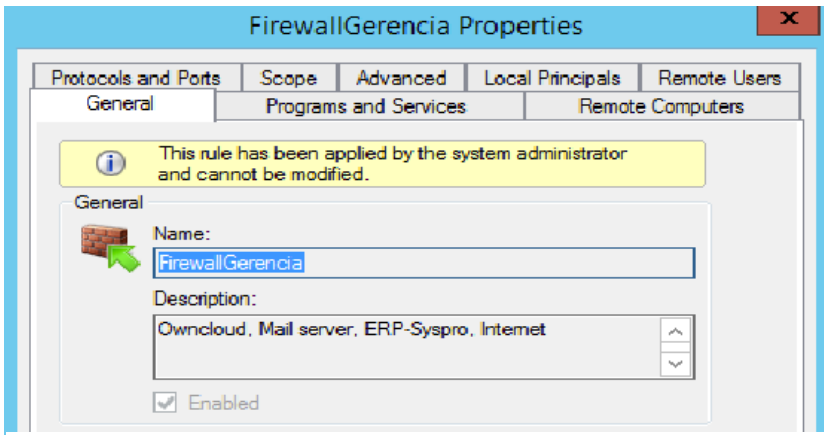


Figura. G. 5 Servicios permitidos para Gerencia.

Y especificamos los puertos, a los cuales pertenecen cada uno de los servicios, para que puedan tener acceso los departamentos.

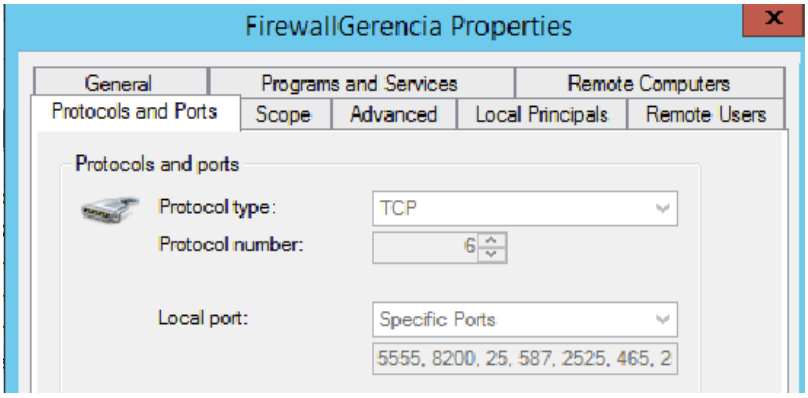
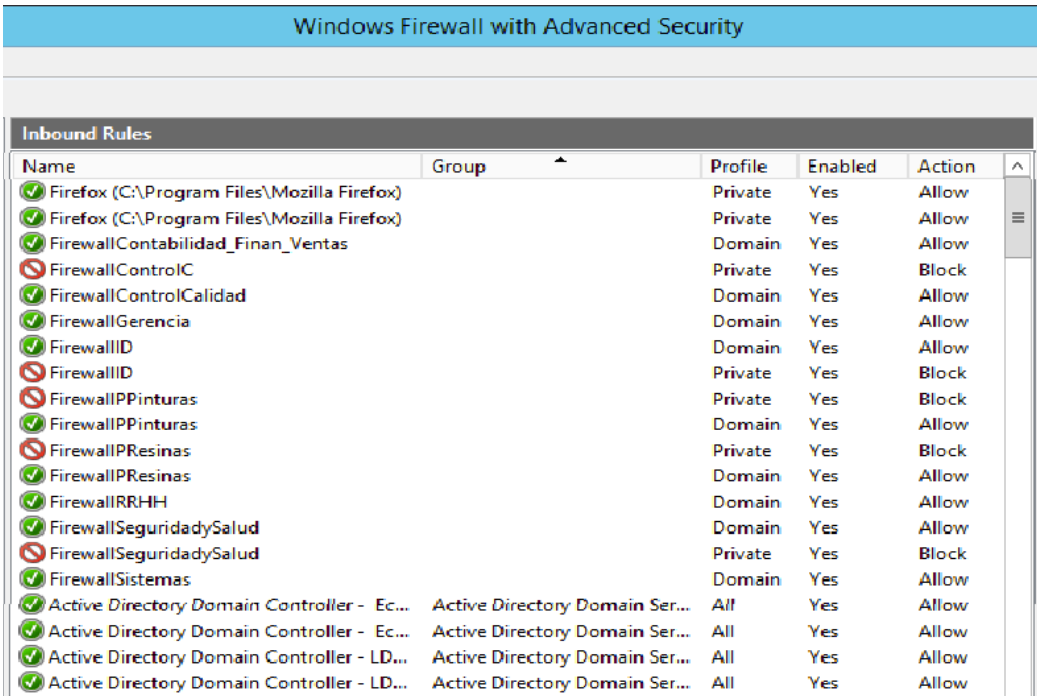


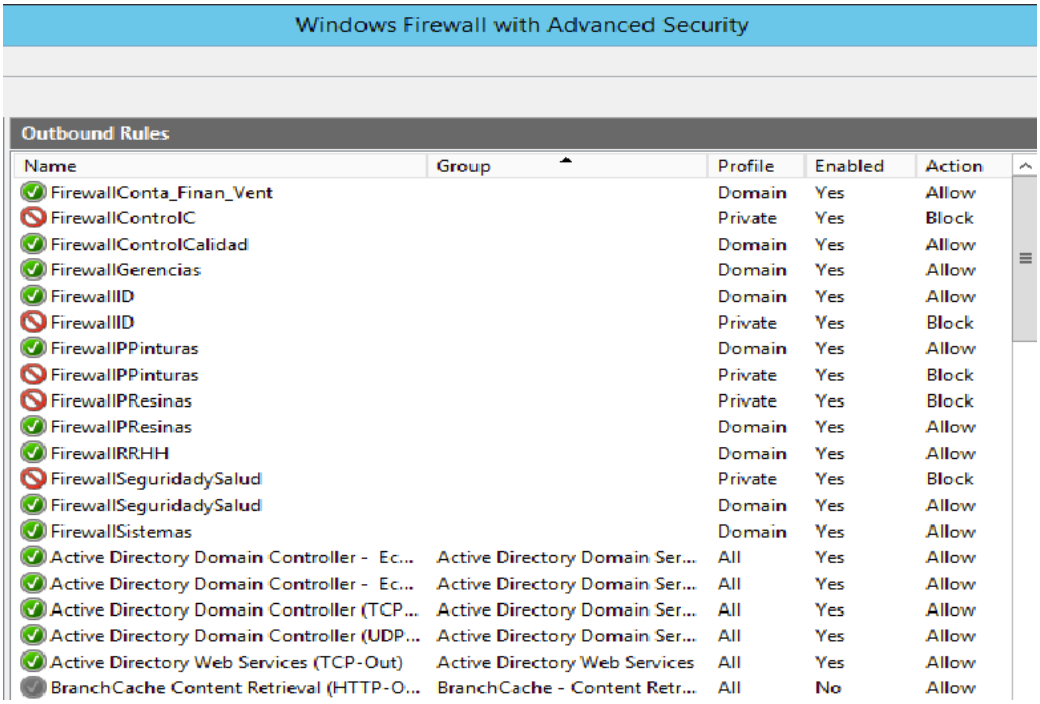
Figura. G. 6 Protocolos habilitados para Gerencia.

Podemos visualizar las reglas de entrada y salida configuradas (Figura. G.7 y Figura. G.8*)* para cada uno de los departamentos de la empresa, la cual nos indicará qué tipo de servicios pueden entrar o salir en la empresa a través de la red.



Name	Group	Profile	Enabled	Action
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow
Firefox (C:\Program Files\Mozilla Firefox)		Private	Yes	Allow
FirewallContabilidad_Finan_Ventas		Domain	Yes	Allow
FirewallControlC		Private	Yes	Block
FirewallControlCalidad		Domain	Yes	Allow
FirewallGerencia		Domain	Yes	Allow
FirewallID		Domain	Yes	Allow
FirewallID		Private	Yes	Block
FirewallPPinturas		Private	Yes	Block
FirewallPPinturas		Domain	Yes	Allow
FirewallPResinas		Private	Yes	Block
FirewallPResinas		Domain	Yes	Allow
FirewallRRHH		Domain	Yes	Allow
FirewallSeguridadySalud		Domain	Yes	Allow
FirewallSeguridadySalud		Private	Yes	Block
FirewallSistemas		Domain	Yes	Allow
Active Directory Domain Controller - Ec...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - Ec...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - LD...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - LD...	Active Directory Domain Ser...	All	Yes	Allow

Figura. G. 7 Reglas INBOUND asignadas para cada departamento.



Name	Group	Profile	Enabled	Action
FirewallConta_Finan_Vent		Domain	Yes	Allow
FirewallControlC		Private	Yes	Block
FirewallControlCalidad		Domain	Yes	Allow
FirewallGerencias		Domain	Yes	Allow
FirewallID		Domain	Yes	Allow
FirewallID		Private	Yes	Block
FirewallPPinturas		Domain	Yes	Allow
FirewallPPinturas		Private	Yes	Block
FirewallPResinas		Private	Yes	Block
FirewallPResinas		Domain	Yes	Allow
FirewallRRHH		Domain	Yes	Allow
FirewallSeguridadySalud		Private	Yes	Block
FirewallSeguridadySalud		Domain	Yes	Allow
FirewallSistemas		Domain	Yes	Allow
Active Directory Domain Controller - Ec...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller - Ec...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller (TCP...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Domain Controller (UDP...	Active Directory Domain Ser...	All	Yes	Allow
Active Directory Web Services (TCP-Out)	Active Directory Web Services	All	Yes	Allow
BranchCache Content Retrieval (HTTP-O...	BranchCache - Content Retr...	All	No	Allow

Figura. G. 8 Reglas OUTBOUND asignadas para cada departamento.