Propuesta de mejoramiento del sistema de seguridad informática para el Instituto Cristo Rey, ubicado en la ciudad de Fonseca, La Guajira

Juan Fernando Corredor Niño

Especialización en Seguridad de la Información

Fundación Universitaria Los Libertadores

15 de noviembre de 2021

Nota de aceptación

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

15 de noviembre de 2021

Tabla de Contenido

1. Descripción del problema 11

1.1 Antecedentes 11

1.2 Planteamiento del problema 13

1.3 Formulación del problema 14

1.4 Objetivos 14

1.4.1Objetivo general 14

1.4.2 Objetivos específicos 14

1.5 Justificación 15

1.6 Delimitaciones 16

2. Marco Referencial 17

2.1 Marco Histórico 17

2.1.1 Redes de telecomunicaciones. 19

2.2 Marco Conceptual 21

2.3 Marco Teórico 30

2.3.1Funciones de la administración de redes de computadoras. 30

2.3.2 Configuración y administración. 31

2.3.2Administración de la configuración para el uso de equipos en una red de computadores. 41

2.3.4 Contabilidad (administración de los usuarios) 45

2.3.4 Análisis de desempeño de la red: tráfico y servicios. 86

2.4 Marco Legal 93

2.4.1 Normatividad sobre derechos de autor y propiedad intelectual en Colombia 93

2.4.2 Políticas de seguridad 94

2.5 Marco Geográfico 109

2.5.1 Ciudad de Fonseca, La Guajira 109

2.6 Marco Institucional 110

2.6.1 Instituto Cristo Rey 110

2.7 Marco Contextual 112

3. Estado de Arte 114

4. Marco Metodológico 119
4.1 Tipo de investigación 119
4.1.1 Herramientas 120
4.1.2 Pilar 121
4.2 Tipo de estudio 122
4.3 Método de investigación 122
4.4 Fuentes de recolección de información 122
4.5 Técnicas de recolección de información 123
4.6 Fases de la investigación 124
4.7 Población y Universo 127
4.8 Muestreo 128
4.9 Variables 128
4.10 Cronograma de actividades 130
4.11 Aspectos administrativos 132
4.11.1 Presupuesto del proyecto 132
4.11.2 Costo del personal 133
4.11.3 Costo de viajes 133
4.11.4 Equipos de oficina 133
5. Resultados 136
5.1Realizar una revisión bibliográfica sobre el objeto de estudio planteado. 136
5.1.1 Principales problemas de Seguridad en los colegios 139
5.1.2 Situación mundial ataques cibernéticos 144
5.2 Realizar levantamiento de información. 146
5.2.1Observación del entorno 146
5.2.2 Mapa de red actual 150
5.2.3 Conceptualización fase de Observación 151
5.2.4 Aplicación de encuestas usuarios del Instituto Cristo Rey 151
5.2.5 Resultados Encuesta 153
5.2.6 Análisis de resultados encuesta 164
5.3 Analizar la seguridad perimetral actual para generar un plan que permita salvaguardar los activos de información mitigando el riesgo de daño, pérdida o robo. 165

5.3.1 Análisis de vulnerabilidades 165
5.3.2 Análisis de vulnerabilidades en servidores 167
5.3.3 Matriz de riesgo 168
5.4 Presentar al Instituto Cristo Rey una solución 168
5.4.1 Segmentación de redes 169
5.4.2 Firewall perimetral 178
5.4.2.1 Selección de UTM 179
4.4.2.2 Endian 3.3.0 Firewall 181
4.4.2.3 Conexiones externas seguras 189
4.4.2.4 Sistemas de control de acceso 190
4.4.2.5 Servidor de autenticación 191
4.4.2.6 Selección software para administración de Radius 193
4.4.2.7 Mapa de red actualizado 195
Conclusiones 196
Glosario de términos 199
Bibliografía 202
Anexos 204

Lista de figuras

Figura 1. Configuración y administración. 35
Figura 2. Labores que solo puede hacerse desde la cuenta del administrador 37
Figura 3. Administración de una red de computadoras en la práctica 39
Figura 4. Información simultanea 43
Figura 5. Administración de la configuración 46
Figura 6. Sistema para describir la documentación de las configuraciones 47
Figura 7. Correcta administración de las fallas en una red de computadoras 48
Figura 8. Representación de la administración de los usuarios en una red 52
Figura 9. Administración del desempeño de una red de computadores. 54
Figura 10. Servicios (Bhatti y Crowcroft 2000) 56
Figura 11. Las metas y los requerimientos de seguridad 58
Figura 12. Administración de seguridad 58
Figura 13. Ventajas del uso de las redes en los entornos de trabajo 60
Figura 14. Servicios fundamentales 60
Figura 15. Protocolo de configuración dinámica 62
Figura 16. Opciones configurables 64
Figura 17. Componentes principales 66
Figura 18. Telnet 68
Figura 19. Telnet no se recomienda para los sistemas modernos 70
Figura 20. Conexiones 73
Figura 21. Protocolo 74
Figura 22. Características 76
Figura 23. Diferentes tipos de información 78

Figura 24. Conexión de servidor 80
Figura 25. IMAP 82
Figura 26. NTLM 85
Figura 27.ANMP 87
Figura 28.Analizadores de protocolos 88
Figura 29.Planificadores. 91
Figura 30.Operación de un cortafuego 98
Figura 31.Políticas de seguridad 103
Figura 32.Esquemas y modelos de seguridad 114
Figura 33.Administración de la red de seguridad 116
Figura 34.Ciudad de Fonseca, La Guajira 117
Figura 35.Instituto Cristo Rey 118
Figura 36.Factores 126
Figura 37.Investigación mixta 127
Figura 38.Técnicas de recolección de información 131
Figura 39.Fases de la investigación 132
Figura 40.Aspectos administrativos 139
Figura 41. Principales problemas en antivirus y antimalware en Instituciones Educativas 140
Figura 42. Incidentes cibernéticos en Instituciones Educativas 141
Figura 43. Desinfección de virus en Instituciones Educativas 142
Figura 44. Uso de las redes sociales por parte de los alumnos y docentes en las Instituciones Educativas 143
Figura 41445. El uso de periféricos externos en la red 144
Figura 46. A145dministración de IT de los colegios 145

Figura 47. Países más ciberseguros 146
Figura 48. Mapa de red actual 151
Figura 49. Pregunta 1 154
Figura 50. Pregunta 2 155
Figura 51. Pregunta 3 156
Figura 52. Pregunta 4 157
Figura 53. Pregunta 5 158
Figura 54. Pregunta 6 159
Figura 55. Pregunta 7 160
Figura 56. Pregunta 8 161
Figura 57. Pregunta 9 162
Figura 58. Pregunta 10 163
Figura 59. Pregunta 11 164
Figura 60. Pregunta 12 165
Figura 61. Pregunta 13 166
Figura 62. Pregunta 14 167
Figura 63. Pregunta 15 168
Figura 64. Pregunta 16 169
Figura 65. Principios de seguridad para la segmentación de red 176
Figura 66. Tarjetas de red de servidores 187
Figura 67. Endian logo 187
Figura 68. Interface principal Endian Firewall 188
Figura 69. Topología de red firewall 189
Figura 70. Tráfico de seguridad entre zonas 190

Figura 71. Aspectos para mejorar con el montaje de firewall perimetral 191
Figura 72. Políticas de salida en firewall Endian 192
Figura 73. Logs IPS Endian Firewall 193
Figura 74. Pregunta 17 194
Figura 75. Ejemplo certificado digital emitido por Endian Firewall 195
Figura 76. Topología de red ubicada en servidor de dominio 196
Figura 77. Configuración de GPO 197
Figura 78. Topología de red ubicación de servidores Radius 198
Figura 79. Comparativo de dolo radios vs free Radius 199
Figura 80. Interfaz web dolo Radius 200
Figura 81. Mapa de red post implementación 201

Lista de Tablas

Tabla 1. Antecedentes 15

Tabla 2. Características básicas de los principales sistemas de distribución 22

Tabla 3. PSI 104

Tabla 4. Puntos a tener en cuenta 105

Tabla 5. Política de seguridad 107

Tabla 6. Concentrado de los diferentes niveles de seguridad en una red de computadoras 110

Tabla 7. Clase C1 111

Tabla 8. Propiedades 115

Tabla 9. Cronograma de actividades 138

Tabla 10. Presupuesto del proyecto 140

Tabla 11. Costo del personal 141

Tabla 12. Costo de viajes 141

Tabla 13. Equipos de oficina 141

Tabla 14. Revisión bibliográfica 142

Tabla 15. Identificación de vulnerabilidades 144

Tabla 16. Ficha técnica de encuesta 144

Tabla 17. Análisis de vulnerabilidades 168

Tabla 18. Análisis de vulnerabilidades 169

Tabla 19. Matriz de riesgo 170

Tabla 20. Segmento de red 173

Tabla 21. Sala de profesores 174

Tabla 22. Administrativo 174

Tabla 23. Sala de informática 1 175

Tabla 24. Sala informática 2 176
Tabla 25. Aula de clases 176
Tabla 26. Biblioteca 177
Tabla 27. Patio 177
Tabla 28. Visitantes 178
Tabla 29. Estudiantes 179
Tabla 30. Red de servidores 180
Tabla 31. Firewall UTM 181
Tabla 32. Ventajas y desventajas 182

Resumen

El objetivo de este proyecto es la creación de una Propuesta de mejoramiento del sistema de seguridad informática para el Instituto Cristo Rey, ubicado en la ciudad de Fonseca, La Guajira. Este objetivo es desarrollado a través de un estudio descriptivo, en el cual se hizo la recolección de la información a través de encuestas y de fuentes secundarias, terciarias públicas y privadas, bibliotecas, ministerios e internet , con el fin de ser analizada para generar posteriores resultados y conclusiones como se observa durante el desarrollo del proyecto. Dentro de los cuales cabe señalar principalmente, la deficiencia que existe en cuanto los problemas que acarrea el Instituto Cristo Rey. Como también otras variables que encausan el objeto de estudio planteado. Finalmente cabe destacar que el proyecto está conformado por cinco capítulos en los cuales se expone todo lo referente al tema propuesto, en dicha investigación.

Palabras claves: Firewall, Seguridad perimetral, segmentación, levantamiento de activos, vulnerabilidades, IDS, privilegios mínimos, GPO, AAA, segmentación de redes, institución educativa, Radius.

Abstract

The objective of this project is the creation of a proposal to improve the computer and perimeter security system for the Cristo Rey Institute, located in the city of Fonseca, La Guajira. This objective is developed through a descriptive study, in which the information was collected through surveys and secondary sources, public and private tertiary, libraries, ministries and the Internet, in order to be analyzed to generate subsequent results and conclusions as observed during the development of the project. Among which it is worth mentioning, the deficiency that exists in terms of the problems that the Cristo Rey Institute entails. As well as other variables that cause the object of study raised. Finally, it should be noted that the project is made up of five chapters in which everything related to the proposed topic in said research is exposed.

Keywords: Firewall, perimeter security, segmentation, asset lifting, vulnerabilities, IDS, minimum privileges, GPO, AAA, network segmentation, school, Radius.

Introducción

En la actualidad, la información se ha convertido en uno de los recursos más valiosos que poseen las instituciones, a su vez esta provee insumos a las aplicaciones y servicios que usan a diario los usuarios internos y externos. Por este motivo, hay una gran necesidad de observar e identificar la situación actual de seguridad, principalmente el sistema de seguridad perimetral y de defensa de la institución educativa.

Mediante la recolección de información utilizando diferentes medios; se pueden identificar hallazgos mayores y menores que comprometen la seguridad perimetral y a su vez de la información, con esto se podría analizar y evaluar a corto plazo los controles de seguridad ajustadas a los requerimientos y presupuesto del cliente.

Con los controles que se sugerirán en el desarrollo de este proyecto, se pretende minimizar el riesgo de pérdida de información y asegurarla con dispositivos, configuraciones de defensa perimetral, además de inspeccionar el uso y accesos hacia internet. Al proporcionar dichos controles se tratará de garantizar que las aplicaciones cuenten siempre con los recursos de red que necesitan y que se mitigue el impacto ante posibles ataques y pérdida de información.

A lo largo del desarrollo de esta investigación se pueden observar toda la información concerniente al objeto de estudio, ubicando la histórica, espacial y temporalmente dentro de un marco referencial, con el fin de conocer las causas en que se enmarcan la situación y las posteriores hipótesis generadas.

Es así como esta publicación está compuesta por diferentes partes que indican su relevancia dentro del proyecto y en las cuales se describe el problema , los objetivos investigados y la

justificación, en una primera parte; en una segunda parte , se localiza el cuerpo del documento que a su vez se subdivide en capítulos que enuncian los marcos histórico, teórico, conceptual, y legal , los cuales dan pie a la tercera parte en donde se explica la forma que se desarrolló el proyecto, finalizando con la última sesión en donde se muestran los resultados y conclusiones obtenidas.

Esta investigación permitirá un mayor desenvolvimiento para posteriores investigaciones y teorías que permitan el mejoramiento continuo en la Seguridad de la Información.

1. Descripción del problema

1.1 Antecedentes

Tabla 1.

Antecedentes

Antecedentes Nacionales	Colombia sufre problemas significativos de ciberseguridad, pero esas falencias no son tan críticas si se comparan con las de otros países de la región, e incluso del mundo desarrollado. El balance lo entregó Comparitech, una plataforma especializada en el análisis de servicios tecnológicos. El análisis tomó en cuenta siete categorías. Encontró, por ejemplo, que en Colombia el 12,52% de los dispositivos móviles están infectados con algún tipo de malware diseñado para entrar o destruir el sistema sin autorización del usuario. Según el análisis, en Colombia se producen el 0,5% de los ataques al software financiero con el que se pretende robar a los usuarios. En los países peor calificados, ronda el 2%.En Colombia, se registraron más de 7 billones de intentos de ciberataques durante 2020, de un total de 41 mil millones en América Latina y el Caribe.
Antecedentes Internacionales	En Japón es apenas del 1,34% pero en Nigeria del 28%. En computadores, las infecciones son mayores y, en Colombia, afectan al 16,4% de los sistemas. Al país no le fue muy bien en la calificación de su legislación, que mide qué tan actualizada está para brindar garantías de ciberseguridad. El puntaje fue de 4 sobre 10, aunque ningún país pasó de 7, ni China ni Francia, los mejor posicionados en ese ítem. Precisamente, el Gobierno de Iván Duque ha intentado modernizar la ley de las TIC en Colombia, pero sus propuestas han recibido críticas, especialmente por el trato a la televisión pública, y el Congreso las puso en lista de espera para su análisis. Comparado con los 6 países de Latinoamérica que fueron medidos, Colombia sale bien librado en el 5 puesto (de peor a mejor), solo superada por México. Incluso está mejor calificado que países europeos como Italia, Grecia o Portugal. Pero también peor que otras 21 naciones. A la luz del informe, el país tiene mucho por mejorar en materia de ciberseguridad, pero su diagnóstico no es crítico. **Botnets más antiguas siguen activas en América Latina:** las botnets Gh0st y Andromeda, también conocidas como Gamaru y Wauchos, aparecen como las más detectadas en América Latina, a pesar de que las fuerzas de ciberseguridad llevaron a cabo una importante operación de eliminación de ésta última en diciembre 2017. Nuevamente, aplicar los parches de los fabricantes y realizar actualizaciones periódicas es fundamental en términos de seguridad.
Antecedentes Locales	Bogotá, febrero de 2020 - Fortinet® (NASDAQ: FTNT), líder global en soluciones amplias, integradas y automatizadas de ciberseguridad, anunció los resultados para el cuarto trimestre de 2020 y el consolidado del año de los datos de intentos de ciberataques obtenidos por su laboratorio de inteligencia de amenazas FortiGuard Labs, que colecta y analiza diariamente incidentes de ciberseguridad en todo el mundo. Campañas con troyanos durante este período, que llevan a cabo actividades sin el conocimiento del usuario y que generalmente

	incluyen el establecimiento de conexiones de acceso remoto, la captura de entrada de teclado, la recopilación de información del sistema, descarga/carga de archivos y la colocación de otros malware en el sistema. Los activos infectados pueden realizar ataques de denegación de servicio (DoS) y ejecutar o detener procesos. El malware JS/ScrInject.B! fue el más activo de la región en ese período. **Trabajo remoto como puerta de entrada a las redes corporativas:** se ha detectado una gran cantidad de solicitudes HTTP maliciosas para aprovechar vulnerabilidades en varios productos de enrutadores domésticos que podrían permitir a los atacantes ejecutar comandos arbitrarios. Esto puede ser una tendencia, ya que más personas trabajan desde sus hogares, con menos protección y más acceso a los datos corporativos. **Gran ola de intentos de explotar vulnerabilidades:** se detectaron numerosos intentos de ejecución remota de código contra ThinkPHP y PHPUnit, un marco web utilizado por una gran cantidad de desarrolladores web. La vulnerabilidad ThinkPHP se reveló en 2018 y permite a los atacantes obtener acceso al servidor e instalar software malicioso. Mantener los servidores actualizados ayuda a reducir el riesgo de exploits. Por lo tanto, si está utilizando ThinkPHP versión 5 o anterior, debe aplicar la última actualización o parche del proveedor. **Las botnets apuntan a dispositivos IoT:** la botnet Mirai, dirigida a dispositivos IoT, se ha vuelto muy robusta y muy utilizada a lo largo de los años, y ha ganado un interés cada vez mayor por parte de los atacantes que apuntan a vulnerabilidades más antiguas en productos de IoT para el mercado consumidor. En los últimos meses, Mirai se ha vuelto más fuerte, más rápida, más resistente y más evasiva, agregando otras armas cibernéticas a su arsenal como la explotación de vulnerabilidades encontradas en servidores web. Los ciberdelincuentes son conscientes de que los dispositivos de IoT están menos protegidos y se aprovechan de eso.

Nota: La tabla expone los antecedentes Nacionales, Internacionales y Locales. Tomado de Infobae (2021), Acis (2020), Semana (2021).

1.2 Planteamiento del problema

Bajos o nulos controles de seguridad junto con la exposición de la información crean la necesidad de tener controles de seguridad establecidos para garantizar en mayor medida el buen funcionamiento de la infraestructura tecnológica de la institución. A la fecha el Instituto Cristo

Rey no ha implementado alguna mejoría notable o aceptable a su protocolo de seguridad cibernética debido a no disponer con los recursos suficientes y asesoría adecuada, por tal motivo, no conoce todos los riegos a los que se encuentran expuestos ni a los beneficios que la mejoría del sistema de seguridad aportaría al mismo.

La institución cuenta con salas de informática, salones, servicio de correo, software contable, zonas Wifi, sistema de notas, registra aproximadamente 600 alumnos en la cual el 80% utiliza infraestructura tecnológica. Múltiples riesgos de seguridad están latentes y se presentan en la organización. Lo más prioritario es detectarlos para evitar incidentes de seguridad graves, por otro lado, hay 86 personas de la parte administrativa la cual en gran parte utiliza y tiene contacto con infraestructura tecnológica, ya sea para gestionar sus correos o para administrar el software contable siendo este vital para el funcionamiento del Instituto Cristo Rey.

Basados en la información que se entregó por parte de la directiva de la institución, la plataforma tecnológica actual del Instituto Cristo Rey no tiene los controles de seguridad informática apropiados, causando que puedan existir conexiones no autorizadas, infección por programa maligno, robo o pérdida de información, comprometiendo la integridad, la disponibilidad y la confidencialidad de la información que se almacena o crea.

1.3 Formulación del problema

¿Cómo crear un plan de mejoramiento del sistema de seguridad informática y perimetral para el Instituto Cristo Rey, ubicado en la ciudad de Fonseca, La Guajira?

1.4 Objetivos

1.4.1Objetivo general

Creación de una Propuesta de mejoramiento del sistema de seguridad informática para el Instituto Cristo Rey, ubicado en la ciudad de Fonseca, La Guajira.

1.4.2 Objetivos específicos

1. Realizar una revisión bibliográfica sobre el objeto de estudio planteado.
2. Realizar levantamiento de información por medio de observación del estado actual de la infraestructura tecnológica de la institución con base en planos, fotografías, encuestas y mapas de red. Con esto Identificar vulnerabilidades y riesgos de seguridad perimetral que exponen los activos de información.
3. Analizar la seguridad perimetral actual para generar un plan que permita salvaguardar los activos de información mitigando el riesgo de daño, pérdida o robo.
4. Presentar al Instituto Cristo Rey una solución, mediante controles y técnicas de defensa cibernética, resguarden y mitiguen los riesgos de pérdida o robo de activos críticos de información de la institución, con esto cubrir los aspectos mínimos de seguridad perimetral.

1.5 Justificación

El Instituto Cristo Rey sufrió muchos problemas a lo largo de los años, información (notas) perdidas de los cuales fueron afectados alrededor de 37 estudiantes en diferentes cursos de nivel bachillerato, dicho suceso ocurrió hace 5 años por lo cual se tuvo que optar por buscar registros de profesores para poder reemplazar dicha perdida. El uso indebido de los equipos informáticos en el

cual se presentó un incidente de seguridad donde un malware tipo rasomware, cifró archivos importantes, encriptando información que se encontraban en algunos equipos de la oficina y un File Server en el periodo de 2020-1. Mediante el análisis del estado actual de la infraestructura tecnológica y la propuesta de mejoramiento planteada, se buscará que la alta dirección tome consciencia de los riesgos que conlleva no implementar controles mínimos de seguridad en la institución. La intención será la defensa del perímetro de red, iniciando desde el exterior hasta llegar al datacenter donde se almacena y procesa la información, en estas zonas se deberán aplicar controles de seguridad.

1.6 Delimitaciones

Delimitación Operativa: Se pueden presentar algunos inconvenientes al momento de recaudar datos, por el tema de la vulnerabilidad de la misma. Para ello se tendrán en cuenta otras alternativas que determine el objeto de estudio planteado.

Delimitación Conceptual: En el presente proyecto principalmente se va a diseñar y analizar una revisión documental sobre los antecedentes referentes al objeto de estudio del Instituto Cristo Rey.

Delimitación Geográfica: El proyecto se desarrollará según los datos e información recolectada a través del trabajo de campo del Instituto Cristo Rey, ubicado en la ciudad de Fonseca, La Guajira.

Delimitación Temporal: El objeto de la investigación se desarrollará según las pautas y tiempos de la Universidad.

2. Marco Referencial

2.1 Marco Histórico

La industria de la información digital (o electrónica) se ocupa de la producción y distribución de información por medio de un soporte digital, ya sea magnético u óptico sus orígenes se remontan a la década de 1970 en los Estados Unidos, y unos diez años más tarde empieza a extenderse en Europa, desde entonces y de modo progresivo, se ha ido consolidando como complemento o alternativa, según los casos, a la información registrada sobre papal.

El sector de la información digital presenta un ciclo de producción y distribución más complejo y diversificado que el existente en la industria editorial tradicional porque incluye algunos agentes que no existen en el ámbito del a edición impresa y se ve alterado el papel ejercido por otros, la tabla que se presente a continuación intenta sintetizar cuales son los actores que forman parte de esta cadena, los objetos de los que se ocupan y las funciones que realizan.

Tabla 2.

Características básicas de los principales sistemas de distribución

Parámetros	Formato web	En línea ASCII	Edición óptica
Tipo de información	Texto, sonido, gráficos, imagen fija, imagen animada.	Text ,gráficos muy sencillos	Texto, sonido, gráficos, imagen fija, imagen animada.
Forma de difusión	Red de transmisión de datos.	Red de transmisión de datos.	Autonomía respecto de la red de telecomunicaciones
Usuarios	Gran público como sectores especializados y profesionales.	Sectores muy especializados, investigación negocios y finanzas.	Gran público como sectores especializados y profesionales.
Forma de consulta	Lenguaje de interrogación simple .Menús, enlace hipertextuales.	Lenguaje interrogación complejo.	Lenguaje de interrogación simple .Menús, enlace hipertextuales.
Variables de facturación	Muchos servicios gratuitos, en algunos casos, tiempo de uso número de documentos consultados.	Tiempo de uso de información consultada	Precio fijo independiente del uso
Formas de pago	Facturación del proveedor de acceso a internet según tiempo de utilización, y cuando procede como facturación del Servicio de Información.	Factura del proveedor de servicio previo contrato.	Suscripción a precio por unidad compra el número.
Equipos necesarios	Microordenador, módem, línea telefónica y acceso a internet.	Microordenador, modem ,línea telefónica, acceso a red de datos	Micro ordenador y lector de discos ópticos.
Fecha de aparición	Principios de la década de 1990.	Principios de la década de 1970.	1985 (cederrón)

Nota: La tabla expone las características básicas de los principales sistemas de distribución teniendo en cuenta los parámetros formatos web edición óptica y en línea. Tomado de Falgueras (2001).

Los actuales sistemas de producción y distribución están permitiendo que los autores se ocupen o solo de la creación de originales, sino que empiecen a abordar también seriamente el proceso de producción y distribución de sus textos cada vez es más frecuente de que publiquen en la red, se trata de empresas, organizaciones o instituciones que disponen de alguna información o servicio que quieren ofrecer telemáticamente al público de forma gratuita o a cambio de alguna compensación económica, los primeros proveedores solían ofrecer exclusivamente servicios de información (es decir, no ofrecían servicios de comunicaciones ni de transacciones) así pues , dedicaban a recopilar y analizar información en algún ámbito especializado con la biomedicina, la química, las artes y la cultura, etc. o también información de carácter general dentro de esta categoría de proveedores se puede encontrar empresas y organismos de sectores diversos como empresas de análisis de tratamiento documental de la información.

2.1.1 Redes de telecomunicaciones.

Los notables avances conseguidos en este campo han propiciado el gran desarrollo experimentado por la información digital en los últimos veinte años , gracias a las redes de telecomunicaciones resulta rápido y simple poder acceder a depósitos de información que se encuentren en cualquier parte del mundo ; intentar hacer una breve caracterización técnica de las redes de telecomunicaciones implica describir su tipología básica; si seguimos un orden cronológico y de importancia esto equivale a hablar de las siguientes redes :

RTB Red telefónica básica.

También se conoce como red telefónica conmutada y aún es la red más extendida, funciona basándose en un cable que contiene hilos de cobre en su interior las líneas están unidas entre sí por centralitas y se van remitiendo hasta llegar a domicilios de los usuarios. Es analógica porque transmite en forma de impulsos eléctricos; las vibraciones de nuestra voz, aunque sus orígenes y desarrollo van íntimamente ligados a la transmisión de voz, aunque sus orígenes y desarrollos van íntimamente ligados a la transmisión de voz, también es posible enviar datos es decir comunicar entre sí dos ordenadores lo que se consiguió a medida de la década de 1950. En este caso es necesario el concurso de un módem que se ocupa de convertir la señal analógica en digital y viceversa.

RTD red de transmisión de datos.

A partir de la década de 1970, la mayoría de los países occidentales comenzó a crear redes específicas para la transmisión de datos que funcionan con el sistema de conmutación de paquetes. Hasta este momento la red telefónica era la más importante y utilizada.

RDSI Red digital de servicios integrales.

La red digital de servicios integrados trabaja también sobre la base de cables de cobre, aunque en este caso el cableado es más grueso, pero con la capacidad de enviar y recibir datos a mayor velocidad de conexión de hasta 128 kbps.

2.2 Marco Conceptual

Antivirus: programas que buscan prevenir, detectar y eliminar distintos tipos de malware que puedan llegar al sistema, si no nos importa pagar, por menos de 50 euros al año podemos obtener antivirus de gran calidad desarrollados por Mc Affe, Panda, Norton, Kaspersky,Avira, Avasta o Panda (Lopez,2015,p.32).

Antispyware: su finalidad es combatir los llamados programas espía, que se dedican a recopilar información de nuestros equipos y enviársela al atacante, también pueden realizar otra tarea que no son propiamente espías, como la muestra continua de *pop-up* redirigir solicitudes de páginas o cambios en la configuración del sistema Malware bytes Anti-Malware o SUPER Antispyware, como *software de pago, Y Súper Antispyware,* Windows Defender o Spybot Search and Destroy, como software libre están considerados algunos de los mejores antispyware del mercado (Ramírez, 2016, p. 05).

Firewall: software que controla las conexiones que salen y entran en mi equipo, evitando que alguien no autorizado entre en el sistema, ZoneAlarm y ComodoFierewll son los reyes indiscutibles en el mercado de los firewalls, tanto en sus versiones de pago como las gratuitas.

Antiadwere: se emplea para evitar la acción de los programas de publicidad computacional que generalmente basan su funcionamiento en la aparición de *pop-up*, cambio de páginas de inicio y los motores de búsquedas de los navegadores o la instalación en los mismos de barra de herramientas o de búsqueda, AdwCleaner y AT-Destroyer son dos buenas herramientas dedicadas a este fin, aunque la mayoría de las mencionadas en el apartado del *antispyware* también cumplen la misma función. (Sandoval, 2016, p.12).

Antispam: herramientas utilizadas para prevenir el correo basura, SPAMfighter o Spamihilator se pueden encontrar de forma gratuita por internet, aunque la mayoría de gestores de correo actuales ya incorporan sus propios sistemas internos de *antispam*.

No siempre es necesario instalar una herramienta distinta para cada una de estas protecciones, ya que en la actualidad las compañías de seguridad tienden a ofrecer paquetes que incluyen varias de ellas juntas como solución combinada (Contreras, 2016, p.26).

Adware: del inglés advertising (publicidad) y were (programa), concepto que engloba a todos aquel *software* que se encarga de mostrar de forma automática publicidad en internet en diferentes formatos: dentro de una página, con ventanas emergentes, durante instalaciones.

Algoritmo de cifrado: conjunto de instrucciones u operaciones que, junto con una clave de cifrado, se llevan a cabo sobre un mensaje legible para encriptarlo (Borghi, 2020,p.31).

Back –up: anglicismo sinónimo de *copia de seguridad.*

Banner: enlaces publicitarios incluidos dentro de páginas web, suelen presentarse en forma de imágenes o animaciones que buscan llamar la atención del usuario para que pinche en ellos y redirigir su tráfico hacia la web del anunciante.(Rodríguez, 2016,p15).

Bluebugging: ataque de spam a través de la conexión *bluetooth* de un terminal.

Bluesnarfing: ataque sobre dispositivos móviles consistente en las escuchas no autorizadas de conversaciones telefónica, el hacheo del manos libres *bluetooth* que se esté empleando para ello.

Bluetooth: tecnología de comunicación inalámbrica de corto alcance muy extendida en dispositivos electrónicos móviles.

Bug: errores, de cualquier tipo, que incluyen los programas informáticos y que provocan un funcionamiento incorrecto de la aplicación, los desarrolladores de software suelen reparar estos fallos en sus productos mediante las actualizaciones que implementan según se van descubriendo. (Zuluaga, 2019,p.17).

Chat: tecnología de comunicación instantánea entre usuarios mediante el uso de un software y una conexión a una red, generalmente internet.

Ciberbullying: delito telemático consistente en la acción de ejercer acoso psicológico entre menores a través de medios telemáticos si el caso fuera entre adultos se considera ciberacoso: y si fuera entre un menor y un adulto se denomina *grooming*.

Cifrar (o enccriptar) **:** procedimiento que emplea un algoritmo de cifrado y una clave para transformar un mensaje en otro incomprensible, el mensaje generado podrá ser descifrado por aquel que tenga la clave de descifrado, que podrá, ser la misma que la de cifrado o no.

Clave de cifrado: conjunto de caracteres que se emplea junto con un algoritmo de cifrado para encriptar un mensaje.

Control parental: procedimiento que busca impedir o limitar el acceso de los menores a determinados contenidos en Internet no apropiados para su edad.

Cookies: pequeños programas informáticos enviados por las páginas web y almacenados en los ordenadores de los usuarios, unas de sus principales misiones es recabar información sobre los hábitos de navegación, normalmente con fines publicitarios, aunque pueden ser empleados para ataques como *spyware,* por lo que pueden llegar a ser un peligro para la privacidad. (Viloria, 2018, p.16).

Crack: código de software creado para actuar sobre otro programa y modificar su comportamiento sin la autorización del desarrollador original, son muy empleados ara piratear aplicaciones de pago, saltándose las restricciones de las mismas y permitiendo su uso libre.

Creepwere: tipo de malware cuyo objetivo es tomar el control de formar remota de la cámara web o el micrófono de un equipo para así poder grabar imágenes o sonidos sin que el propietario del ordenador sea consciente de ello.(Porras, 2017, p.45).

Firewall: dispositivo, ya sea hardware o software, que controla los accesos a un determinado sistema o red, permitiendo aquellos que son aceptados y bloqueados los que no lo son.

Firmware: programas informáticos que se encarga de controlar circuitos electrónicos de algún dispositivo, normalmente va integrado en los propios circuitos hardware y gestiona que el dispositivo funcione correctamente.

Freeware: programa informático que se distribuye de forma gratuita para su uso durante un tiempo limitado o bajo unas determinadas condiciones, suele emplearse como prueba del software libre, distribuido sin limitaciones de forma gratuita, aunque por su terminología inglesa pueda llevar a confusión.(Arias,2019,p.19).

Fuerza bruta: ataque que busca obtener una clave (de acceso, de cifrado..) probando todas las combinaciones posibles que puede tener hasta dar con la correcta.

GPS: del inglés global positioning Sytem , sistema que, mediante una red de satélites, permite la localización en cualquier parte de la Tierra de una persona o de un objeto con una precisión de hasta centímetros.(Palma,2018,p.89).

Crooming: delito telemático que consiste en el engaño de un adulto hacia un meno con el objetivo de ganarse su confianza y poder realizar algún tipo de abuso sexual sobre el mismo.

Hozx: bulo son mensajes, a través de correo electrónico redes sociales, etc., que alertan de falsas alarmas de cualquier tipo, y que se intenta extender a la mayor cantidad de usuarios, posibles con el objetivo de conseguir cuentas activas, engañar o molestar a los usuarios.

Informática forense: ciencia basada en la aplicación de técnicas científicas y analíticas sobre equipos informáticos para detectar o investigar ataques sobre los mismos.

IP (Dirección): número que identifica un dispositivo dentro de una red cuando un ordenador se conecta a Interne, se le asocia una dirección IP para saber dónde se debe enviar los paquete de los que sea destinatario, se puede saber quién ha realizado alguna acción determinada en la red gracias a este parámetro.(Blanco, 2019,p.65).

ISP: del inglés internet Service Provider, es la compañía con la que contratamos nuestro acceso a la red.

Keygen: software generador de claves de registro ara ser empleadas con programas de pago, que sustituye la clave entregada al pagar por él, y permite el uso de la aplicación de forma libre e ilegal.

Keylogger : tipo de software o dispositivo hardware cuyo objetivo es guardar las pulsaciones de teclado que se realiza en el equipo sobre el que está instalado, para transmitirlas después al atacante es una forma muy empleada en el robo de credenciales de acceso a cuentas de sesión.

Login: anglicismo empleado como sinónimo de entrar, es el proceso de inicio de sesión o de entrada a algún servicio o sistema informático a través de credenciales de acceso (nombre de usuarios y contraseñas).

MAC (Dirección): del inglés Media Access Control, también denominada dirección física, es una serie de caracteres alfanuméricos que identifica de forma única a una tarjeta o dispositivo que hay en el mundo.

Malwere: Todos aquel programa informático que tiene como objetivo realizar algún efecto dañino en el equipo sobre el que actué, ya sea destruir información, espiar y recabar información o simplemente perjudicar el correcto funcionamiento de la máquina. Incluye virus informáticos, troyanos, gusano, Edward, spyware.

Marquet: Mercado***,*** se entiende por Marquet aquellos sitios web que permiten la descarga de aplicaciones para dispositivos móviles. Cada sistemas operativo tiene el suyo propio donde se controla la veracidad del software que ellos se cuelga, por lo que siempre se debe acudir a estos y no a otros markets alternativos. (Castejon, 2019,p.09).

Metadatos: Son datos que describen otros datos otros datos o archivos de datos. Suelen representar diferentes propiedades de un archivo como la fecha de creación, de la última modificación o el autor. En el caso de las fotografías pueden indicar el lugar y el momento en los en los que fueron tomadas, o el modelo de teléfono móvil o de cámara digital con que fueron hechas. (Arango, 2017, p.87).

NFC: Siglas en inglés para comunicación en Campo Cercano. Es una tecnología de comunicación inalámbrica de muy corto alcance, muy popular actualmente en los dispositivos móviles para procesos de pago.

P2P: Del inglés peer to peer, red de pares en español. Es una red de ordenadores en la que no existe una arquitectura cliente- servidor como tal, sino que cada usuario que puede hacer las veces de ambos (cualquiera puede enviar o recibir datos). Permite el intercambio libre de información entre todos los nodos de la red.

Password: Anglicismo sinónimo de contraseña

Phising: También conocido como suplantación de identidad. Es un tipo de delito telemático, en el cual se consigue información confidencial mediante ingeniería social para posteriormente hacerse pasar por la persona o la empresa suplantada, y llevar a cabo acciones constitutivas de delito.(Ortega, 2016,p.11).

PIN: De las siglas en ingles personal identificación number o número de identificación personal. Es un tipo de contraseña, formada por una serie de dígitos (normalmente cuatro) que se suelen emplear en tarjetas de crédito o en tarjeta SIM de telefonía móvil.

Pluggin: Programa informático que completa a un segundo añadiéndole nuevas funcionalidades. Son muy habituales los pluggins de juegos o de aplicaciones instalados en los navegadores web.

POP-UP: Ventanas emergentes que suelen utilizarse en entornos web para diferentes fines, normalmente sin que el usuario lo haya solicitado. Su uso más habitual es mostrar publicidad en muchas páginas. (Tamayo, 2018, p.48).

QR (código): Del inglés, Quick responde code. Esta compuestos de una matriz de puntos bidimesional. Viene a sustituir a los códigos de barras tradicionales, permitiendo una lectura o alta velocidad para dirigirnos a un sitio web.

Router: Dispositivos electrónico que se encarga de la conectividad de una red. Al instalar una conexión de acceso a internet en nuestros hogares, este aparato es el que encarga de mandar los datos a nuestro ordenador (cuando descargamos algo de la red) o enviarlos hacia internet (si estamos subiendo información).

SCAM: Estafa. En el ámbito de la ciberseguridad, se emplea para definir los correos electrónicos que esconden un intento de estafa de algún tipo, normalmente de phising.

Sexting: Es él envió de material con contenido sexual, fotos y videos generalmente, del propio remitente a otras persona.

SMS: Servicios de mensajes cortos de telefonía. Servicios disponibles en los teléfonos móviles, actualmente en desuso debido a la aparición de aplicaciones gratuitas de mensajería instantánea en los terminales inteligentes, como puede ser el casco de whatsapp.

SPAM: Correos no deseados que recibe un usuario sin saberlos solicitado. Suelen enviarse de forma masiva a través de listas de correos electrónicos. Su finalidad principal es la publicitaria, aunque puede ser empleados para seguir información de usuarios a los que dirigir ataques que atente contra su seguridad digital.

Spyware: Tipo de malware cuyo objetivo es la recopilación de información sensible del ordenador donde está instalado y de los usuarios que lo utilizan, y posteriormente trasmitirla al atacante sin el conocimiento de la víctima. (Galán, 2017, p.22).

Sniffer: Programas informático que capta el tráfico de información que genera un ordenador con los dispositivos que tiene conectados, e incluso puede registrar la actividad del propio equipo, son muy empleados en técnicas de hacking para obtener los datos que se transmite entre el ordenador y el router.(Cedeño,2017,p.29).

SSID: Serie de caracteres alfanuméricos que proporcionan un nombre a una red inalámbrica para poder distinguirla del resto.

URL: Del inglés Uniform Resource Locator en nuestro ámbito se refiere a los caracteres que identifican a un sitio web dentro de la red, es decir, la dirección que escribimos en el navegador para acceder a él.

USB: Del inglés Universal Serial Bus o Bus Universal de Serie, es una estadar industrial de conectores de dispositivos electrónicos y periféricos de ordenador, está muy extendido en la actualidad, y la gran mayoría de pendrive y discos duros de almacenamiento externo funcionan bajo esta tecnología.

Webmaster: Del inglés web y master, es el encargado del desarrollo y/o mantenimiento de un sitio web; según cada caso en particular, puede estar referido al funcionamiento y la operatividad de la web, al contenido que se muestra en la misma, o ambos aspectos simultáneamente.(Pizano, 2020,p.19).

2.3 Marco Teórico

2.3.1Funciones de la administración de redes de computadoras.

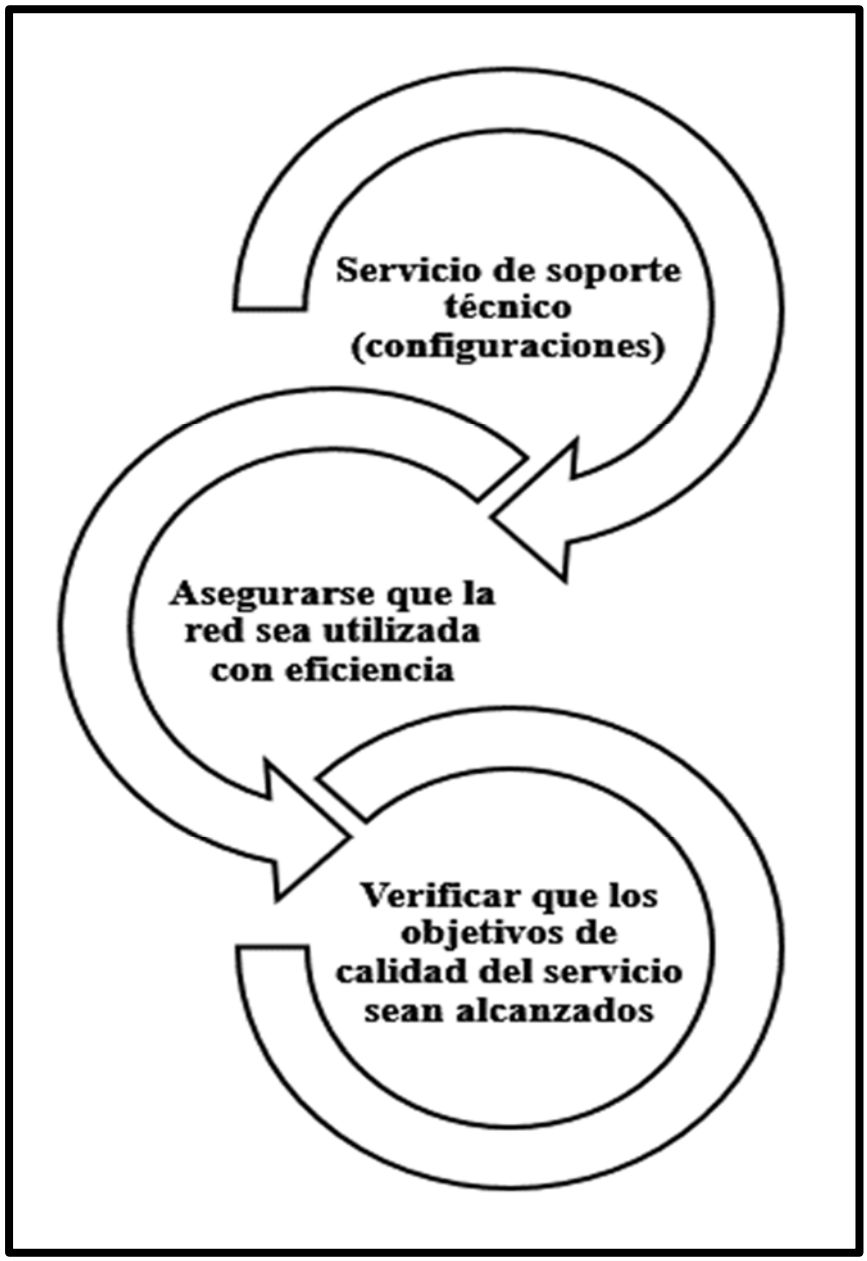
Mencionan López (2015) que la administración de redes es una profesión muy demandada, la proliferación de las redes informáticas y las consecuencias en el uso y abuso , ha hecho que la administración de redes, se conviertan en una tarea imprescindible para la organizaciones (empresas, industrias, corporativos, dependencias, o instituciones) la administración de redes informáticas se vincula con la tecnología de la información (TI); esta última se relaciona con el diseño, el desarrollo , la implementación , el soporte y la administración de hardware , software, y los sistemas informáticos en red, los profesionales de TI poseen un amplio conocimiento sobre sistemas de computación y sistemas operativos; además gozan de las capacidades necesarias para llevar a cabo la administración de red.

2.3.2 Configuración y administración.

La configuración comprende las funciones de monitoreo y mantenimiento del estado de la red, las cuales incluyen.

Figura 1.

Configuración y administración.

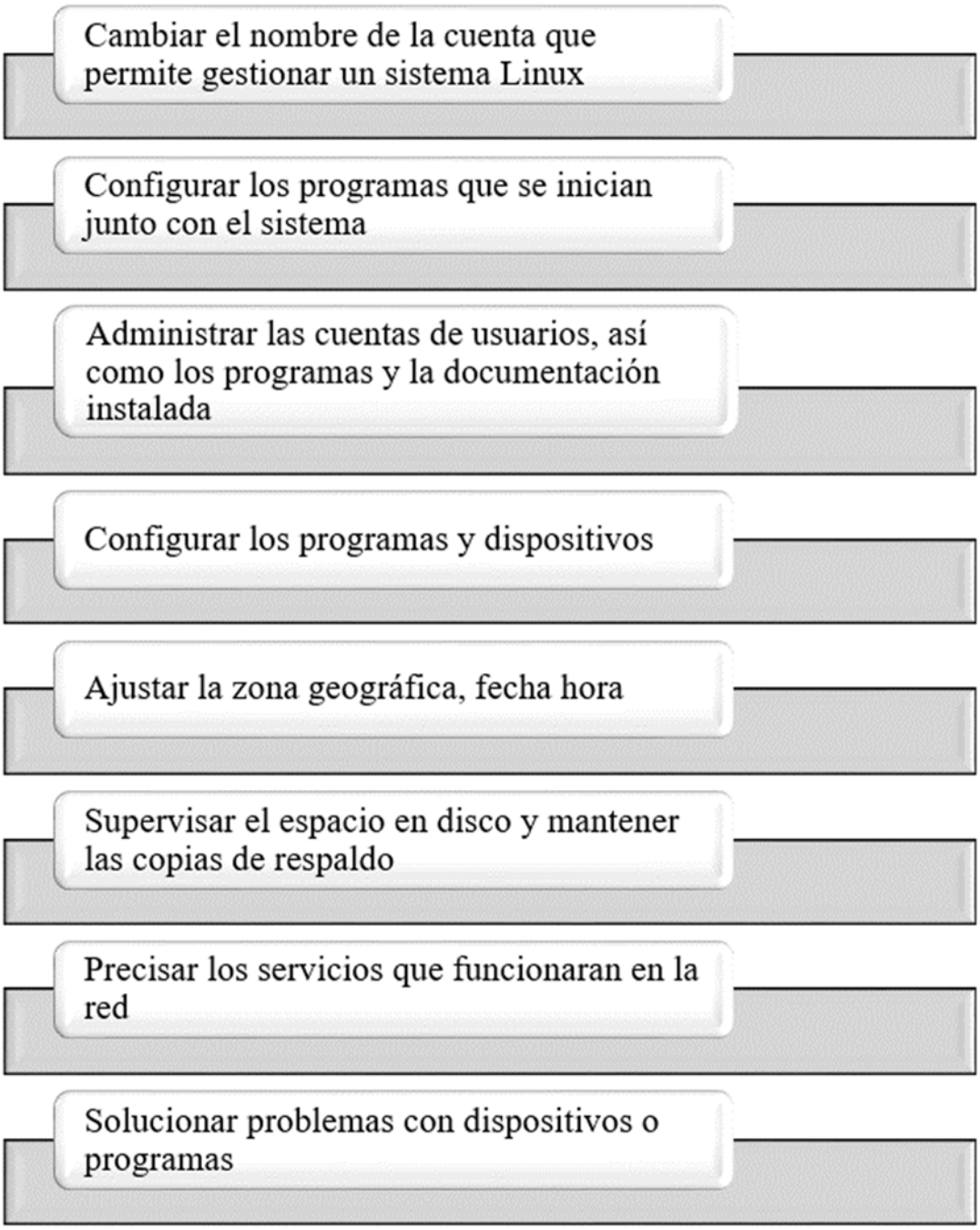


Un administrador de red sirve a los usuarios de distintas formas, crea espacios de comunicación, atiende sugerencias, mantiene a tiempo y en buena forma las herramientas requeridas, vigila el adecuado funcionamiento del hardware y software de las computadoras y redes a su cargo, también se ocupa de la documentación que describe la red; respeta la privacidad de los usuarios y promueve el buen uso de los recursos (Bertsekasy Gallager, 1992,p.1); a cambio de tantas responsabilidades , la recompensa es el buen funcionamiento de la red como un medio que vincula a las personas a través del uso de las computadoras y los programas como herramienta para agilizar algunas labores que dan tiempo y eficiencia para la productividad personal.

Afirma Rodríguez (2019) que de igual forma, el administrador de la red debe conocer las reglas de root (en sistemas operativos del tipo UNIX, es el nombre convencional de la cuenta de usuario que posee todos los derechos en todos los modos , mono o multiusuarios); que también es llamado súper-usuario o la cuenta del administrador, el root puede hacer muchas cosas que un usuario común no puede , como cambiar el dueño o los permisos de los archivos y alcanzar a puertos de numeración pequeñas , no es recomendable utilizar el usuario root para una simple sesión de uso habitual porque se pone en riesgo el sistema al garantizar acceso privilegiado a cada programa en ejecución ; por ello, es preferible usar una cuenta normal y el comando sur para acceder a los privilegios de root de las máquinas que se administra dado que puede configurar servicios y establecer políticas que afectará a los usuarios de la red ; algunas de las labores que solo puede hacerse desde la cuenta del administrador son:

Figura 2.

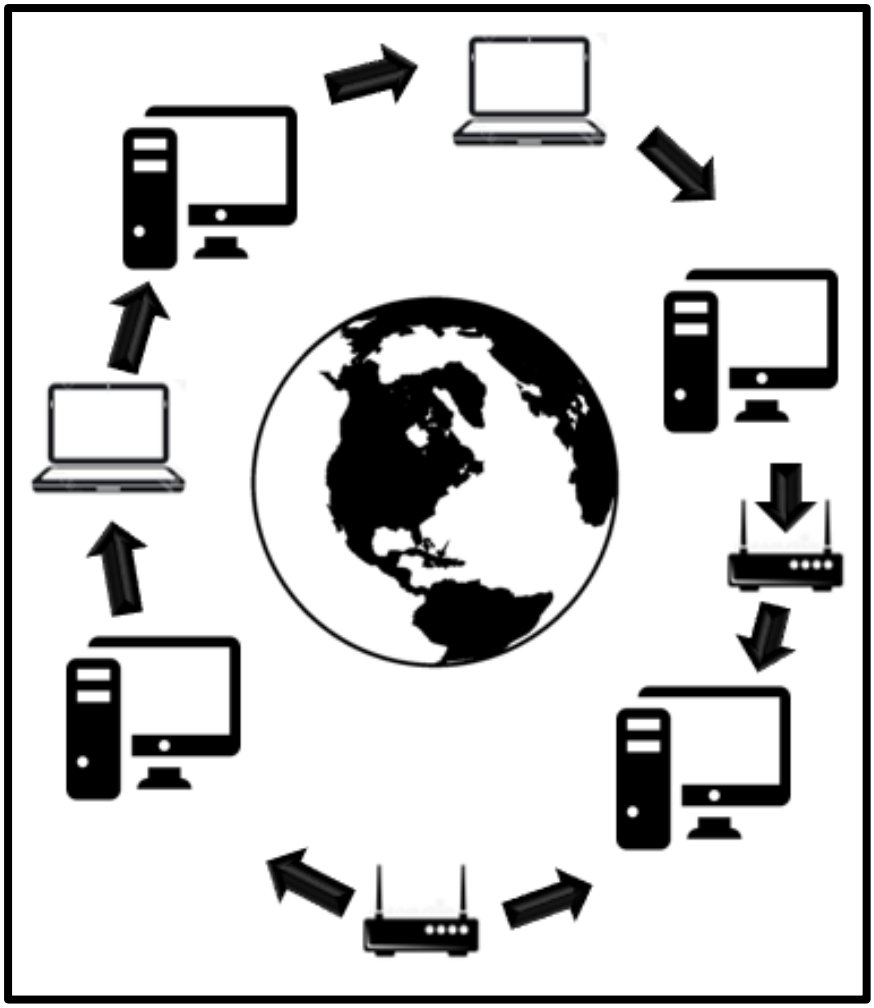
Labores que solo puede hacerse desde la cuenta del administrador



Analiza Pedraza (2020) que finalmente en este contexto el término “monitoreo” describe el uso de un sistema que revisa constantemente una red de computadoras en busca de componentes defectuosos o lentos para luego informar cual la problemática y dar solución a la misma (Bhatti y Crowcroft, 2000). La administración de redes es un subconjunto de funciones; mientras que un sistema de detección de intrusos monitorea una red por amenazas externas, otro monitorea en busca de problemas causados por la sobrecarga en la infraestructura y fallas en los servidores.

Figura 3.

Administración de una red de computadoras en la práctica



Concuerda Ruiz (2019) que para determinar el estatus de un servicio web, software de monitoreo envía con periodicidad particiones del protocolo de transferencia de hipertexto (HTTP, hipertexto transfer Protocol),con el objetivo de obtener paginas para un servidor de correo electrónico y después enviar mensajes mediante el protocolo SMTP, los cuales posteriormente serán retirados mediante IMAP (internet message Access protocl) o POP3 (protocolo post office), por lo general los datos evaluados son tiempo de respuesta y disponibilidad optime, aunque también se obtienen estadísticas con consistencia y fiabilidad que han ganado popularidad.

Menciona (2018) que la monitorización del servidor puede ser interna por ejemplo se comprueba su software o externa revisión manual, en ambas se verifican características como el uso del procesador y la memoria el rendimiento de la red, el espacio libre en disco y las aplicaciones instaladas; a lo largo de este proceso se comprueban también los códigos HTTP enviados del servidor (refinados en la especificación HTTP RFC2616) que son la formas rápida de comprobar el funcionamiento ; a continuación se dan ejemplos de las herramientas de monitoreo más utilizadas:

Tcodumo: Permite monitorear a través de comandos de la consola de LINUX, todos los paquetes que atraviesan la interfaz indicada, a la ir de los múltiples filtros, parámetros y opciones, tecpdump ofrece infinidad de combinaciones filtros, para monitorear, como el tráfico que ingresa de una IP, un servidor o una página determinada, se puede solicitar el tráfico de un puerto especifico o pedirle que muestre todos los paquetes cuyo destino sea una dirección MAC determinada.

Wireshark: sniffer captura las tramas y paquetes que pasan a través de una red; cuenta con todas las características estándar de un analizador de protocolos y posee una interfaz gráfica fácil de manejar, se usa con frecuencia en Ethernet aunque es compatible con otras redes.

Hyperic: aplicación que posibilita administrar infraestructuras virtuales, físicas y en la nube. Este programa autodetecta muchas tecnologías y cuentas con dos versiones; una open source y una comercial, algunas de sus características son la optimización para ambientes virtuales que integran vCenter y vSphere también cuenta con capacidad para funcionar en 75 componentes comunes como base de datos en dispositivos y servidores de red y detecta de forma automática los componentes de cualquier aplicación virtual.

Nagios: sistema de monitoreo que concede a cualquier empresa identificar y resolver errores críticos antes de que afecten los procesos de negocios, en caso de un error, la aplicación se encarga de alertar al grupo técnico para que rápidamente sea resuelto sin afectar a los usuarios finales.

Manifiesta Cruz (2017) que la evolución y tendencia de las herramientas de monitoreo de redes establecen retos a los ejecutivos de la Tecnología de la Información (TI) como mostrar los datos de su operación para que los ejecutivos de la organización dispongan de elementos suficientes para reconocer y fomentar la importancia de la tecnología como un componente habilitador del negocio .Dicha evolución se ha alimentado mediante la llegada de protocolos más avanzados de visualización de trafico como Netfow, Jtlow, Cftow, Sfrow, IPFIX o Neststream; el propósito hoy en día es tener una perspectiva global de "todo" del proceso de negocios involucrados Held 2010; de hecho a media que han avanzado las tecnologías, e ha atravesado por diferentes etapas en el monitoreo de redes las cuales se enumeran a continuación:

Primera generación: aplicación propietarias para monitoreo dispositivos activos o inactivos, la industria ha desarrollado un sinfín de herramientas para tratar de presentar los recursos de una forma amable y en tiempo real, estas presentan los elementos a través de un código universal de colores:

-***Verde:*** todo funciona en orden.

-***Amarillo:*** detección de algún problema temporal que no afecta la disponibilidad; sin embargo, se deben realizar ajustes para no perder la comunicación.

-***Anaranjado:*** el problema se ha hecho persistente y requiere pronta atención para evitar afectaciones a la disponibilidad.

-***Rojo:*** el dispositivo se encuentra fuera de servicio en ese momento y requiere acciones inmediatas para su restablecimiento.

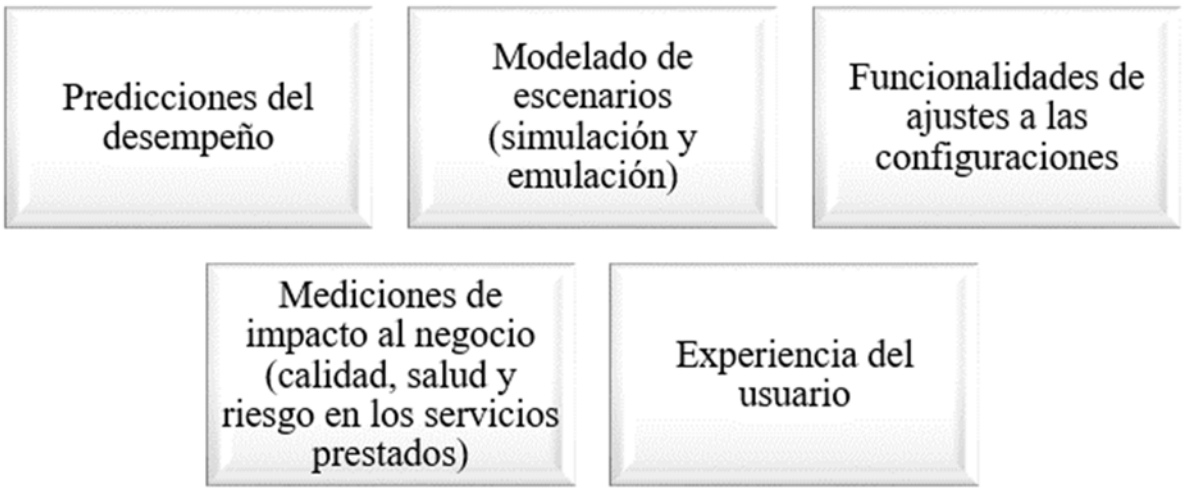
Segunda generación: Aplicación de análisis de parámetros de operación a profundidad por medio de estos, las herramientas realizan un análisis detallado con el fin evaluar los estados de los componentes dentro de los dispositivos (microprocesador, memoria, espacio de almacenamiento, paquetes enviados recibidos, broadcast, unicast, multicast, etc.) de manera que es posible de ajustar los parámetros y establecer los niveles de servicios del dispositivo, este tipo de aplicaciones se apoyan en sniffers y en elementos físicos distribuidos conocidos como probadores (probes), cuya función es, exclusivamente colectar, estadísticas de tráfico, controladas desde una consola central.

Tercera generación: aplicación de análisis punta a punta con enfoque al servicio con mayores niveles de información sobre los dispositivos se tienen elementos adicionales de análisis, pero aun no existen suficientes parámetros para tomar decisiones. Esta generación de aplicaciones con enfoque transaccional captura flujos de tráfico e identifica cuello de botella y latencias a lo largo de los conexiones que existen entre los componentes de un servicio, entregado información acerca de "la salud" de este; además logra conectar todas las partes de manera más eficiente; en dicho caso, cada dispositivo sabe cuándo se debe informar a otro sin afectarlo en sus tarea, esto para no generar , una sobrecarga de información, lo cual significa que existe una toma de decisiones con enfoque de repercusión, generada en los negocios.

Cuarta generación: la personalización de indicadores de desempeño de los procesos de negocio llevando el crecimiento de las soluciones tecnológicas a los requerimientos de las organizaciones actuales dentro de las cuales están aquellas que monitorean el Desempeño de Aplicaciones (APM, Application Performace Management), donde convergen elementos de tecnología (Backend) con los sistemas de los que forman parte para llevar a cabo, las transacciones que impulsan los procesos de negocios (Frontend); en otras palabras, es un análisis de punta a punta el potencial de estas herramientas permite tener información simultanea de :

Figura 4.

Información simultanea



En resumen, el término “configuración” tienen un significado diferente dependiendo del contexto en que sea utilizado, aun dentro del diseño y la operación de las redes de computadoras (Held 2010) una configuración puede ser:

1. Una descripción de un sistema distribuido basado en la ubicación física y geográfica de los recursos la cual incluye la manera en que se encuentran interconectados además de la información sobre las relaciones lógicas, estas pueden basarse en diferentes puntos

de vista (organizacional, administrativo, etc.), o en aspectos relacionados con la seguridad,

2. Un proceso para manipular la estructura del sistema distribuido donde se establecen o modifican paramentos que controlan la operación y ajustan el ambiente requerido para su funcionamiento normal,
3. El resultado de un proceso de ordenamiento donde el sistema genera un conjunto de ciertos valores de los parámetros característicos para la operación normal del recurso.

Confirma Arias (2017) que para los enlaces conectados a los encomiadores (interfaces, ancho de banda), para máxima cuota de los usuarios etc., los siguientes aspectos se presentan en relación con el proceso de la configuración., donde las herramientas que ayudan a disponer los componentes son:

Lugar : una configuración puede hacerse en el mismo dispositivo o realizarse de forma remota; por ejemplo, por medio de un servidor DHCP, el sistema que se configura no siempre es compatible desde el equipo (servidor remoto) a configurar esto puede deberse a razones técnicas, de organización o seguridad.

Almacenamiento: la configuración puede almacenarse en NVRAM(Nonvolatile Ranbdom Access Memory) en disco duros, en un boot Servet para ser invocado a través de los protocolos adecuados o incluso, es posible que se recargue a través de la red.

Validez: una configuración estática es aquella donde cada reconfiguración implica interrumpir la operación del componente (apagar y prender el sistema o reiniciar) una dinámica, por otra parte, permite hacer cambios mientras al componente opera.

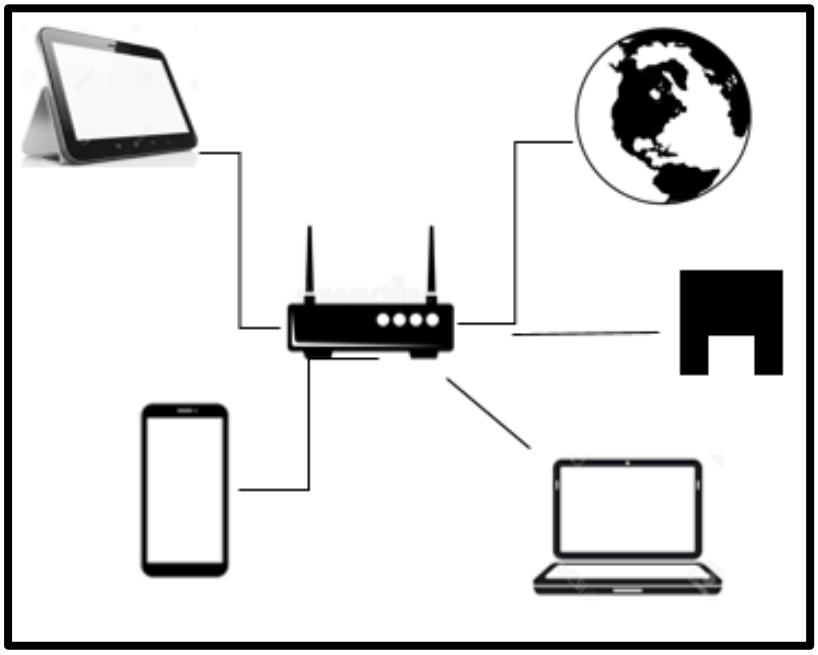
Interfaz de usuarios del configurador: la calidad de la interfaz de usuarios depende de la magnitud de los parámetros que pueden ser modificados con rapidez o aplicados al mismo tiempo a varios dispositivos, el sistema de configuración y la documentación de esta deben estar protegidos de uso no autorizado (con contraseña, en áreas físicas restringidas, con seguridad de protocolos de configuración etc)

La administración de la configuración implica establecer parámetros, definir valores de umbral (threshold), determinar filtros, asignar nombres a los objetivos administrados, proveer la documentación necesaria y cambiar las configuraciones cuando sea necesario.

2.3.2Administración de la configuración para el uso de equipos en una red de computadores.

Figura 5.

Administración de la configuración para el uso de equipos en una red de computadores.

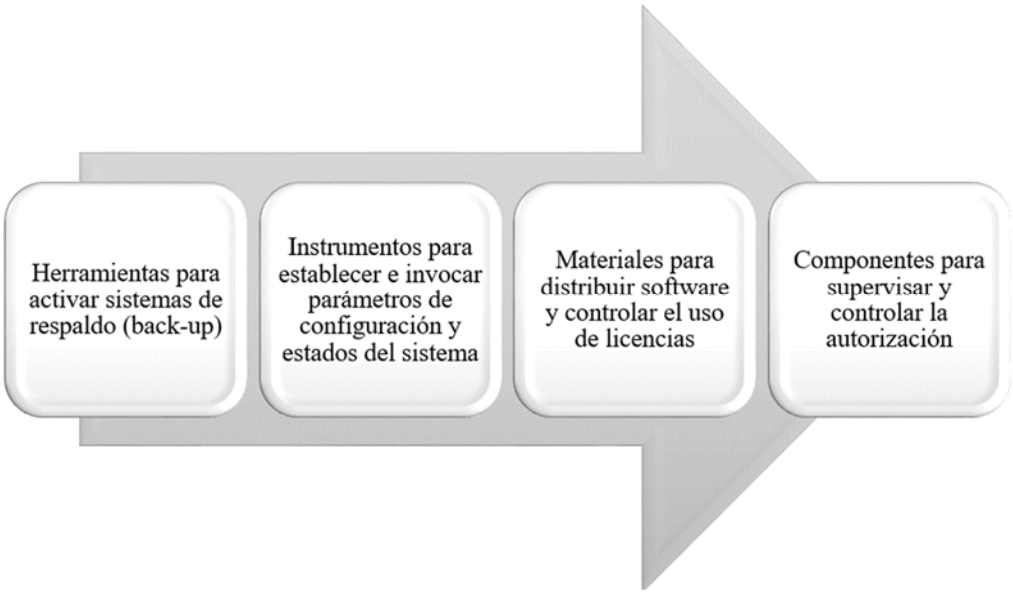


2.3.3 Sistema para describir la documentación de las configuraciones o bases de datos maestras.

Elementos para generar mapas de la configuración de una red, es decir el uso de MRTG (multi router traffic grapher) que en la práctica e un recopilador de datos del tráfico de la red, para supervisar la red, o también el uso de Nagios que es un sistema de monitorización de redes.

Figura 6.

Sistema para describir la documentación de las configuraciones o bases de datos maestras.



Fallas.

La administración de las fallas se relacionan con la detección, aislamiento y eliminación de comportamientos anormales del sistema ; la identificación y seguimiento de estas es un problema operacional importante en todos los sistemas de procesamiento de datos (Lin y Costello, 2004,p.3) ; en comparación con sistemas no conectados a una red , la administración de fallas en redes de computadoras y sistemas distribuidos es más difícil por una diversidad de razones que incluyen entre otras, el mayor número de componentes involucrados, la amplia distribución física

de los recursos, la heterogeneidad de los componentes de hardware y software así como las diferentes unidades de la organización involucradas.

Una falla puede ser definida como una desviación de las metas operacionales establecidas con respecto en las funciones del sistema o los servicios, los mensajes sobre las fallas son dados a conocer por el mismo componente o por los usuarios del sistema, algunas delas fuentes más frecuentes de errores son:

- Los elementos que conforman los enlaces (cables UTP o de fibra óptica, líneas dedicadas a canales virtuales entre otros).

Figura 7.

Correcta administración de las fallas en una red de computadoras

-El sistema de transmisión (transceivers, concentradores, switches, servidores de acceso, encamiandores)

-Sistema final (clientes o servidores)

-El software de los componentes.

- La operación incorrecta por parte de los usuarios y los operadores.

Analiza Duran (2019) aunque la función de la administración de las fallas es detectar y corregir con rapidez los errores para asegurar un alto nivel de disponibilidad de un sistema distribuido y los servicios que presenta por otro lado las tareas son:

1. Monitoreo del sistema y la red
2. Respuesta y atención a alarmas.
3. Diagnóstico de las causas de la falla
4. Establecer la propagación de errores.
5. Presentar y evaluar medidas para recuperarse de los errores.
6. Operación de sistemas de etiquetación de problemas (TTS,Trouble Tickets Systems)
7. Proporcionar asistencia a usuarios (Help Desk).

Además, las siguientes capacidades técnicas pueden ayudar en el análisis de fallas:

1. Autoidentificación de los componentes del sistema.
2. Realización de pruebas, por separado, con los componentes del sistema.
3. Facilidades de seguimiento (tracing)
4. Disposición de una bitácora (log) de errores.
5. Hacer eco de los mensajes en todas las capas del protocolo.
6. Posibilidad de revisar los vaciados (dumps) de memoria.
7. Métodos para generar errores a propósito en ambientes predefinidos para el sistema.
8. Posibilidad de iniciar rutinas de autoverificación y transmisión de datos de prueba a puertos específicos (tés de loops, tés remotos), al igual que pruebas de asequibilidad con paquetes ICMP (ping o traceroute).

9. Establecer opciones para valores de umbral.
10. Activación de reinicios planificados (dirigidos a puertos, grupos de puertos o componentes específicos).
11. Disponibilidad de sistema para realizar tests especiales (osciloscopios, refractómetros, probadores de interfaces, analizadores de protocolos monitoreadores de hardware para supervisión de líneas)
12. Soporte de mecanismos de filtraje para mensajes de fallas o alarmas y correlación de eventos para reducir el número de eventos relevantes y para análisis de las causas de los problemas.
13. Interfaces de herramientas de administración de fallas a sistemas de etiquetación de problemas y soportes técnicos o ayuda al usuario (help desk); es decir, propagación automática de notificaciones y correcciones de fallas.

2.3.4 Contabilidad (administración de los usuarios)

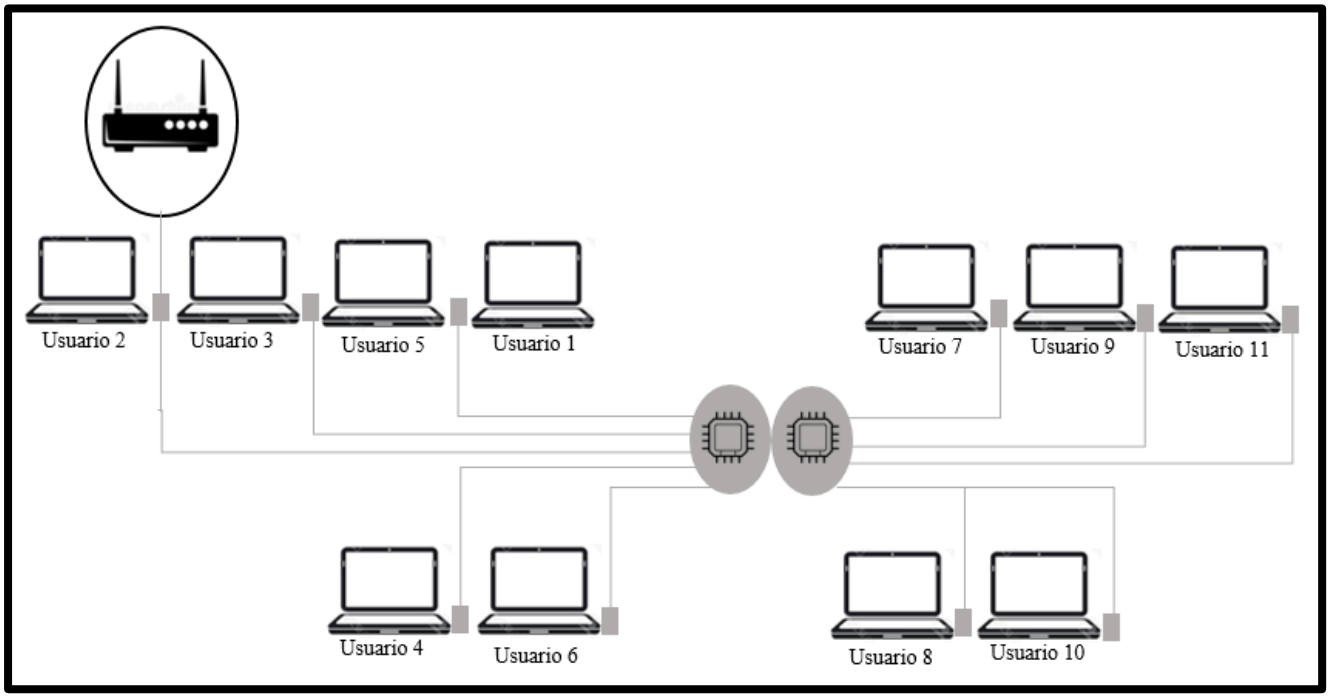
La administración de los usuarios comprende tareas como la gestión de los nombres y las direcciones, servicios relacionados con directorios y permisos para el uso de los recursos, así como de contabilidad, pues existen costos asociados al proporcionar servicios de comunicaciones que deben ser informados a los usuarios (cargos de acceso y de utilización).

Las estrategias y procedimientos para la asignación de costos no puede ni deben ser establecidos rígidamente por un sistema de contabilidad; además, es importante que su administración sea capaz de ajustarse a los lineamientos de una política dada (Chen y Nahrstedt 1998).

La administración de la contabilidad también incluye la recopilación y cuidado de estadísticas de uso, definición de unidades de contabilidad, asignación de cuentas y costos, mantenimiento de bitácoras de contabilidad, establecimientos y monitoreo de las costas concedidas y, finalmente, definición de políticas de contabilidad y tarifas que permitirán generar facturas y cargos a los usuarios.

Figura 7.

Representación de la administración de los usuarios en una red



Estipula Fonseca (2020) cuando se implementa el sistema de contabilidad, que enfoque se utilizara para recopilar los parámetros de contabilidad y como serán distribuidos los costos, es una decisión administrativa que puede ser influenciada por políticas de la organización, entre más sutil sea el enfoque, más complicado e intensivo en costos es el procedimiento de contabilidad (p.13).

Los parámetros “de uso” utilizados para calcular los costos incluyen la cantidad de paquetes o bytes transmitidos, la duración de la conexión , el ancho de banda, la calidad del servicio

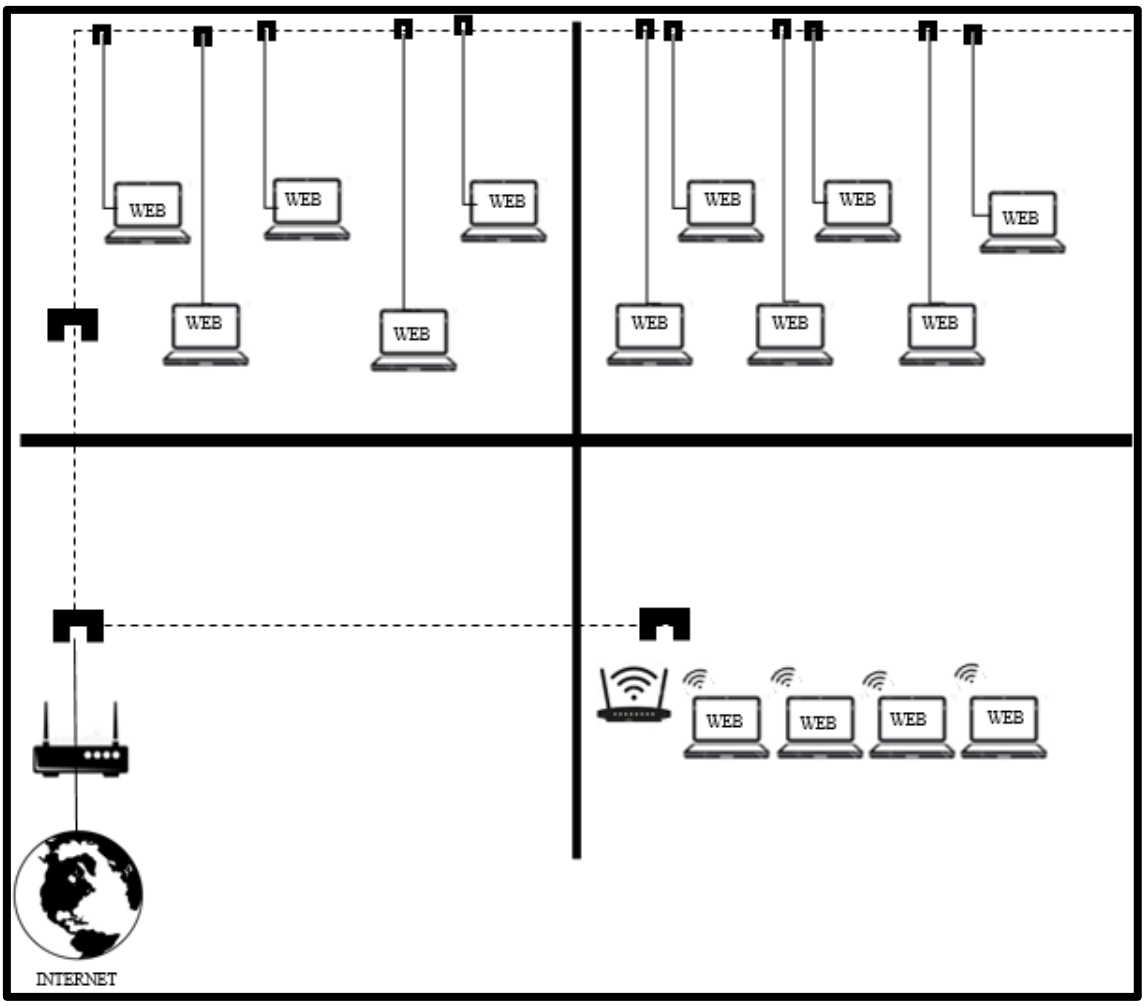
.S (Quality of service) la conexión la localización de los participantes en la comunicación , los costos para servidores y el de productos de software (control) de lincias además de los costos variables, también se tiene en cuenta los fijos espacios de oficina, mantenimiento , depreciación de muebles y equipos , etc.

Desempeño: en términos de los objetivos (muy concretos y específicos), la administración del desempeño se entiende como una continuación sistemática de la administración de fallas mientras que esta última es la responsable de asegurar que una red de comunicaciones o un sistema distribuido solamente opera, la segunda busca que el sistema como un todo, se comporte bien; es decir, se enfoca en la calidad del servicio.

La calidad del servicio es un mecanismo para establecer una interfaz que permita "negociar" ente el proveedor y el cliente; su importancia se incrementa a medida de que más relaciones ente estos se involucran en la implementación de redes corporativas, o de sistemas distribuidos (Tompros y Denazis 2007) entonces, la interfaz de servicios es definida por las siguientes características:

Figura 8.

Administración del desempeño de una red de computadores.



1. Especificación del servicio y del tipo de este (determinístico, estadístico, si mejor posible).
2. Definición de los parámetros de Q, S relevantes con valores cuantificables incluyendo los de uso, promedio y limite, entre muchos otros.
3. Establecimiento de las operaciones de monitoreo.
4. Descripción de reacciones a cambios de los parámetros de Q, S.

Sin embargo, es difícil y no siempre posible proporcionar una definición, completa de un interfaz de servicios sobre la base de los escritos antes que tienden a aparecer las siguientes situaciones:

Problemas en el mapeo vertical Q,S.: gracias a que los sistemas de comunicación son sistemas por capas, los parámetros de Q,S específicos a la capa N tiene que ser mapeados de dicha manera (N+1) °(N-1) por ejemplo un parámetro de la Q,S orientada a la aplicación (en este caso, calidad de transmisión de voz) se debe mapear a la Q,S dependiente de la red, (jitter) las jerarquías de Q,S aún no están definidas por completo para todos los protocolos o servicios, esta situación se exacerba cuando los servicios de diferentes capas se proveen por distintos proveedores (carriers).

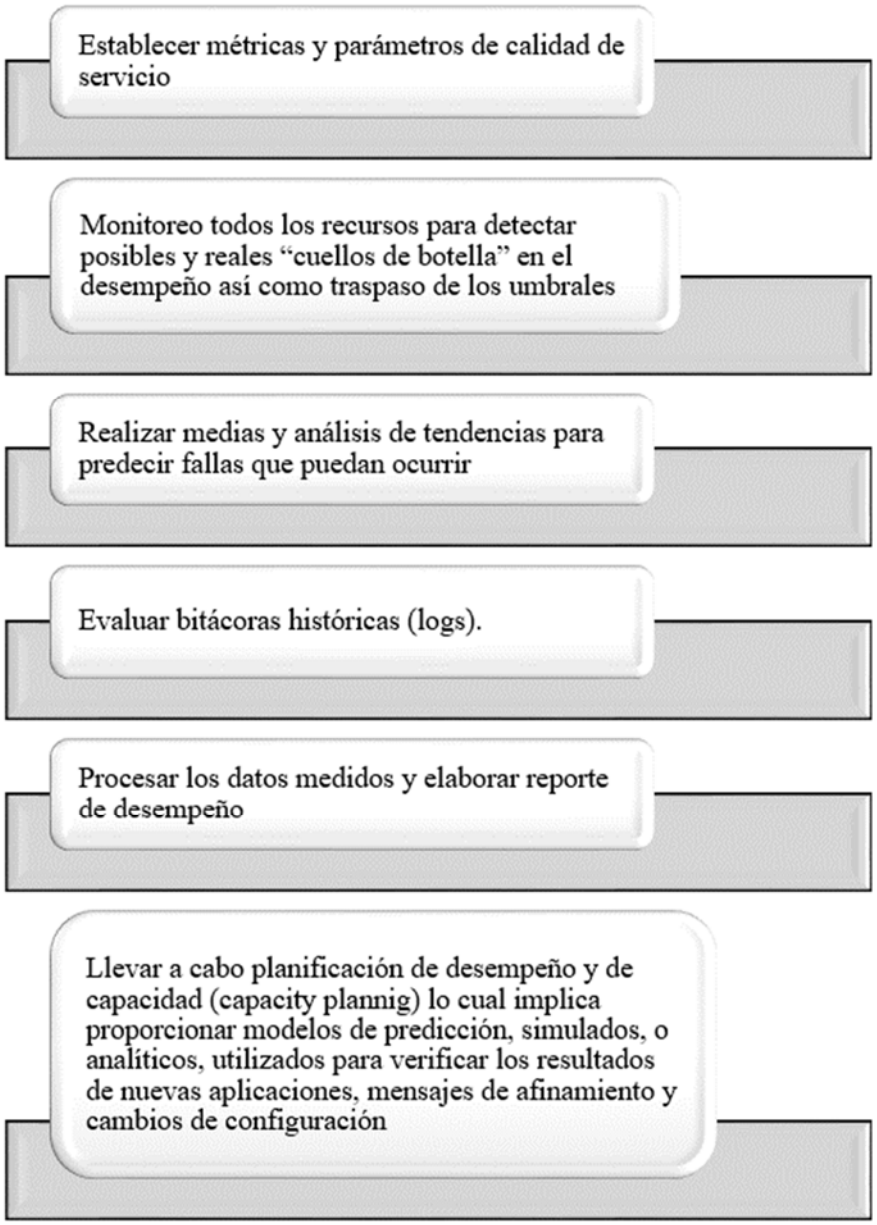
Problemas en el mapeo horizontal de Q,S: si más de un proveedor participa en una red corporativa, el resultado puede ser la concatenación de diferentes subredes o secciones de troncales, que son utilizadas para proveer un servicio con calidad uniforme entre dos usuarios, se asume que cada carrier tiene implementadas las mismas características de calidad de servicios, o al menos ,utiliza protocolos de negociación de Q,S de reservación de recursos o administración estandarizados, cuanto más complejo sea el servicio, menos probables es que se reúnan estos requisitos.

Métodos de medición: la forma óptima para calcular la Q, S seria aplicar métodos de medida basados en cantidades visibles en la interfaz de servicios ante que utilizar un análisis de la tecnología suministrada por el proveedor, pues esta puede cambiar rápidamente y, además, las cantidades de medidas no son de interés del cliente, por ello, para el deben ser convertidas a los parámetros de Q, S.

Expresa Cruz (2019) que en resumen, la administración del desempeño incorpora toda la medida requeridas para asegurar que la calidad del servicio (Q, S) cumpla con un contrato de nivel de servicios (Bhatti y Crowcroft 2000) esto incluye:

Figura 9.

Servicios (Bhatti y Crowcroft 2000)



Seguridad: la seguridad se relación con los sistemas distribuidos y los recursos de la compañía que "vale la pena" proteger como la información, la infraestructura de tecnologías de la información (ITI) y los servicios, los cuales se encuentran expuestos a amenazas o al uso inadecuado , las medias de seguridad son necesarias para prevenir daños y pérdidas , así como para establecer acciones que busquen "enfrentar " las amenazas y riesgos obtenidos como resultados de los análisis de seguridad del sistema en red (Anderson, 2008); los cuales, por lo regular derivan de:

Ataques pasivos: Robo de información lleva a cabo de forma oculta y a través del análisis de tráfico de la red.

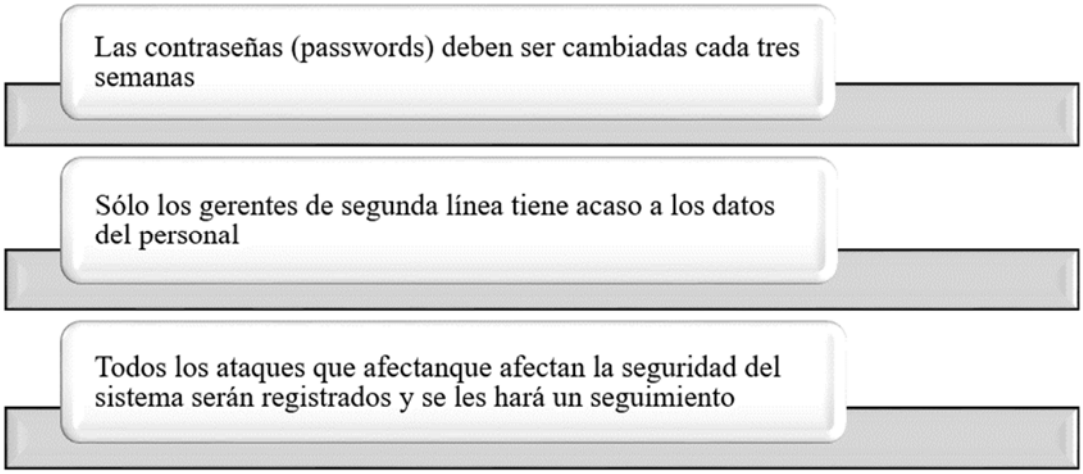
Ataques activos: Accesos no autorizados, por medio de elementos como virus, tras lo que se lleva a cabo, por ejemplo, suplantaciones de usuarios, traducidas en una manipulación de secuencias de mensajes, manejo de los recursos al recargar su uso, reconfiguración no autorizada, reprogramación de sistemas, etcétera.

Mal funcionamiento de los recursos. Comportamiento inapropiado o deficiente y respuestas de operación incorrectas.

Las metas y los requerimientos de seguridad se establecen a partir de análisis de amenazas y de los valores que necesitan protección (Berghel, 2001, p.3). Las políticas de seguridad definidas podrán identificar los requerimientos de seguridad; algunos ejemplos son:

Figura 10.

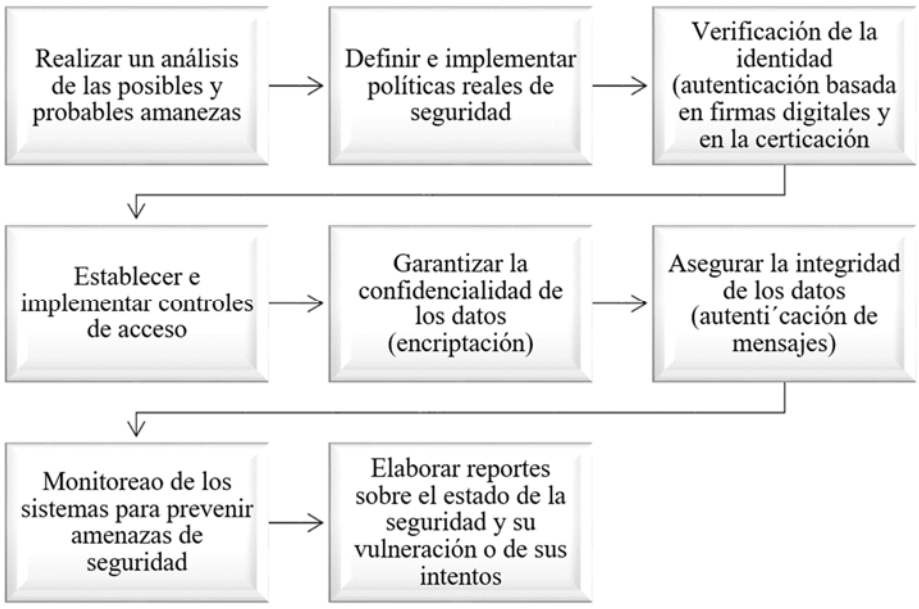
Las metas y los requerimientos de seguridad



Confirma Guevara (2017) que dichas políticas sirven como marco de referencia para los servicios de seguridad necesarios y su implementación; por ello, la administración de seguridad comprende los siguientes puntos:

Figura 11.

Administración de seguridad



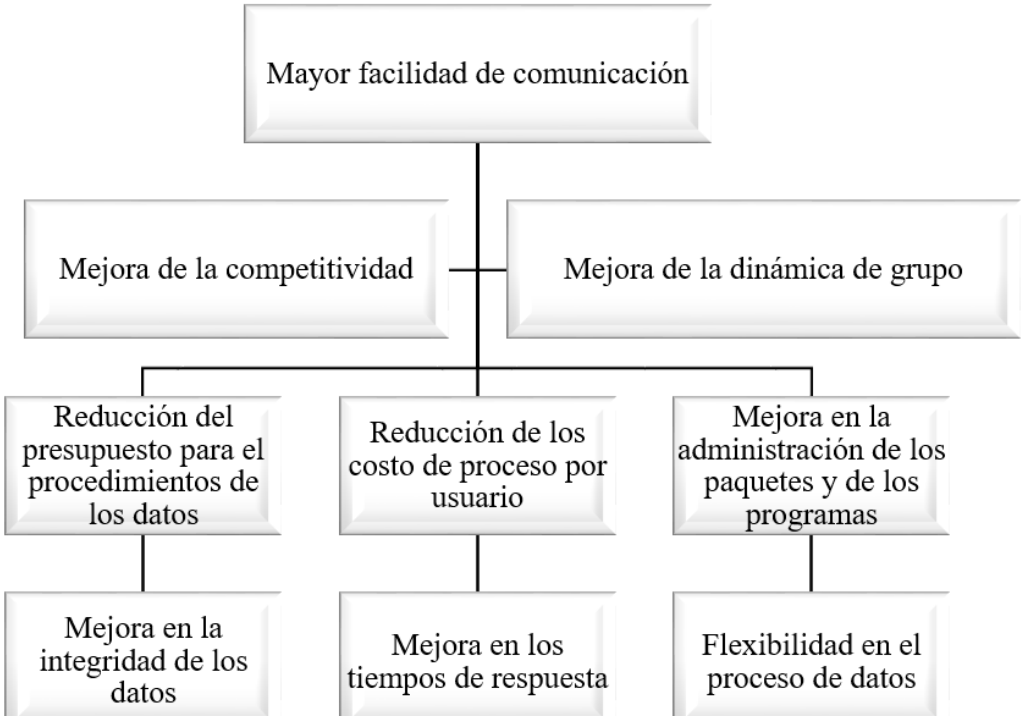
Podría asumirse que un conjunto de procedimientos de seguridad reconocidos, cuya mayor parte está disponible como software de dominio público, ya existe en el área de administración de

seguridad. El principal problema es encontrar la forma correcta de incorporarlos a una arquitectura de la administración y de controlarlos de una manera uniforme dentro del marco de las políticas de seguridad.

La finalidad de los servicios de una red de computadoras es que los usuarios del sistema informáticos de una organización puedan hacer un mejor uso de estos, enriqueciendo de este modo el rendimiento global de la organización. Así las organizaciones contienen una serie de ventajas del uso de las redes en los entornos de trabajo como son:

Figura 12.

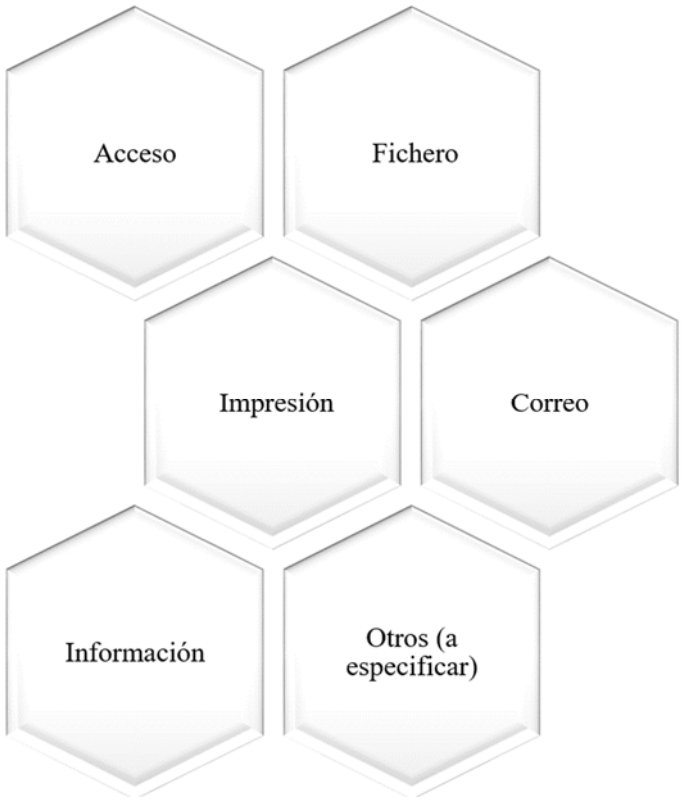
Ventajas del uso de las redes en los entornos de trabajo



Para que todo esto sea posible, la red debe presentar una serie de servicios fundamentales a los usuarios como:

Figura 13.

Servicios fundamentales



Concuerda Turbay (2016) aumentar la prestación de los servicios de la red, se requiere que existan sistemas en la red con capacidad para actuar como servidores. Los servidores y los servicios de red se basan en los sistemas operativos de la red (los cales pueden ser centralizados). Un sistema operativo de la red es un conjunto de programas que permiten y controlan el uso de dispositivos de red, por múltiples usuarios. Estos programas interpretan las peticiones de servicios de los usuarios, y las dirigen a los equipos servidores adecuados. Por ello, el sistema operativo de red le permite a esta, ofrecer capacidades de multiproceso y multiusuario.

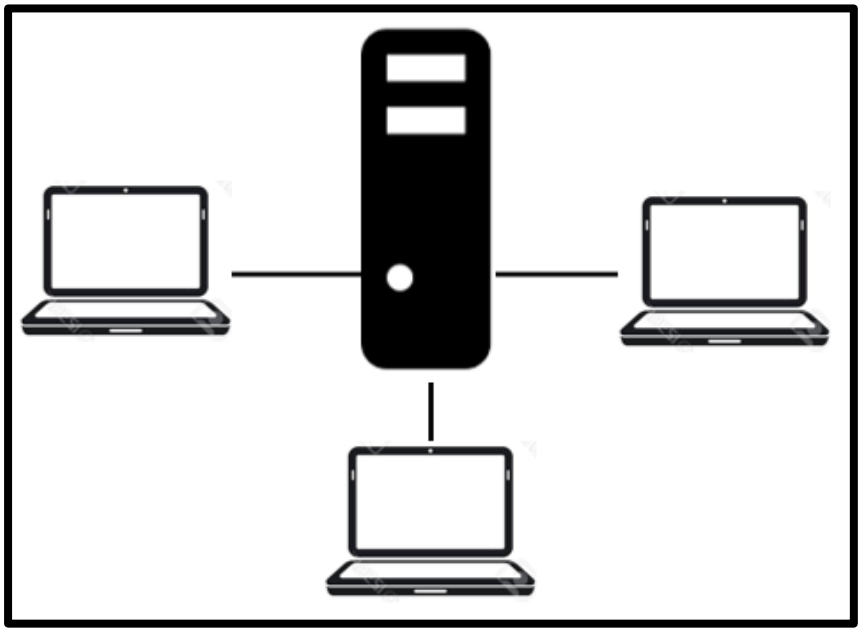
DHCP: El protocolo de configuración dinámica de host o DHCP (Dynamic Host Configuración Protocol) permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor que por lo regular

el servidor posee una lista de direcciones IP dinámicas que se asignan a los clientes, sabiendo en todo momento quien ha estado en posición de cada una, cuanto tiempo la ha tenido y a quien ha sido concedida después. DHCP se estableció como una extensión del protocolo Bootstrap (bootp), el cual fue extendido porque se requería intervención manual para completar la información de configuración en cada cliente sin proporcionar un mecanismo para la recuperación de las direcciones IP en desuso. En la actualidad, este sea mantiene como el estándar para redes IPv4.

En octubre de 1993, este protocolo se publicó por primera y su implementación actual se encuentra en el estándar RFC 2 131, aunque de forma original, se definió bajo 1 531; para DHCPv6 se publica el estándar FRC 3 315, aunque 3 633 le añadió un mecanismo de delegación de prefijo (Joel, 2002).

Figura 14.

Protocolo de configuración dinámica



DHCPv6 se amplió más para proporcionar información a los clientes con la configuración automática de direcciones son estado en el RFC 3 736. El protocolo BOOTP, a su vez, fue definido

por primera vez en el 951 como un reemplazo para la solución de direcciones inversa o RARP (Reverse Address Resolution Protocol). La principal motivación para dicha situación fue que este último era un protocolo de la capa de enlace de datos, lo cual hizo más difícil su aplicación en muchas plataformas de servidores y requería uno presente en cada enlace de red individual.

BOOTP introdujo la innovación de un agente de retransmisión, lo que permitió el envío de paquetes BOOTP fuera de la red local utilizando enrutamiento IP estándar, por lo que un servidor central podría servir de anfitrión en muchas subredes IP (Croft, 2005,p.13).

El DHCP permite al administrador supervisar y distribuir de forma centralizada las direcciones IP necesarias, así como asignar y enviar en automático una nueva, si el dispositivo es conectado de asignación de direcciones IP:

Asignación manual o estática: se proporciona una dirección IP a una maquina determinada; suele utilizarse cuando se requiere controlar la asignación de dirección IP a una maquina determinada; suele utilizarse cuando se quiere controlar la asignación de dirección IP a cada cliente y , a la par, evitar que se conecta clientes no identificados.

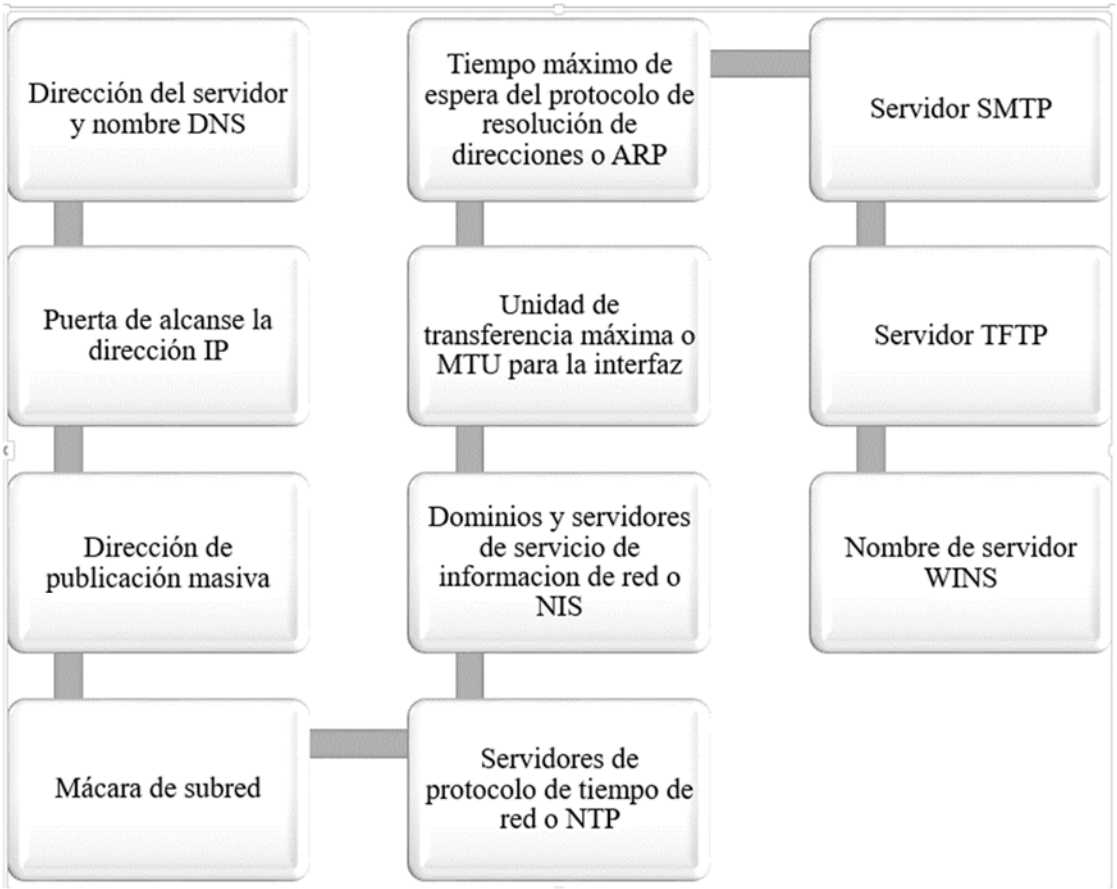
Asignación automática: Determina una dirección IP a una maquina cliente la primera vez que hace la solicitud al servidor DHCP y hasta que el cliente la libera. Se utiliza cuando el número de clientes no varía demasiado.

Asignación dinámica: es el único método que permite la reutilización dinámica de las direcciones IP. El administrador de la red determina un rango de estas y cada dispositivo conectado a la red está configurado para solicitar la suya al servidor cuando la tarjeta de interfaz de red se inicializa. El procedimiento usa un concepto muy simple en un intervalo de tiempo contable; esto facilita la instalación de nuevas máquinas-clientes a la red.

Algunas implementaciones de DHCP puede actualizar el sistema de nombres de dominio o DNS (Domain Name System), asociado con los servidores para reflejar las nuevas direcciones IP mediante el protocolo de actualización de DNS establecido en RFC 2 136 (versión en inglés). Dichas opciones configurables están definidas en RFC 2 132 (versión en inglés) y se presentan a continuación.

Figura 15.

Opciones configurables



DNS: Al explicar las características del DND, se debe establecer que un nombre de dominio consiste en dos o más partes, técnicamente etiquetadas, separadas por puntos cuando son escritas en forma de texto. Por ejemplo, el punto final separa la etiqueta de la raíz de la jerarquía,

aunque por lo general, se omite por ser puramente formal. Una muestra de nombre de dominio coreccto o FQDN (Full Qualified Domain Name).

A la etiqueta ubicada más a la derecha se llama dominio de nivel superior (LTD, Top Level Domain), como “.com” en www.ejemplo.com u”.org” en es. Wikipedia.org cada etiqueta A la izquierda especifica una subdivisión o subdominio. Finalmente, la parte más a la izquierda expresa el nombre de la máquina (hostname); por ejemplo, El dominio es. Wikipedia. Org tendría el nombre de la máquina "es" , aunque en este caso no se refiere a una máquina física en particular. Teoría, esta subdivisión puede tener hasta 127 niveles, y es posible que cada etiqueta contenga hasta 63 caracteres restringidos para que la longitud total nombre del dominio no exceda los 255, aunque en la práctica los dominios son casi siempre cortos; estos deben comenzar con una letra y tienen "-" cómo único símbolo permitido.

Manifiesta Ayala (2017) que una vez establecido esto, cabe mencionar que el sistema de nombres de dominio (DND, Domain Name Sytem) nació de la necesidad de recordar fácilmente los nombres de todos los servidores conectados a internet, pues la empresa estadounidense hosts, que contenía todos los nombres de dominio conocidos, el crecimiento explosivo de la recta uso que esto no resultará práctico, por lo que en el 1983, Paul V. Mockapetris público los RFC 882 y 883 defendiendo lo que hoy en día ha evolucionado hacia el DNS moderno.

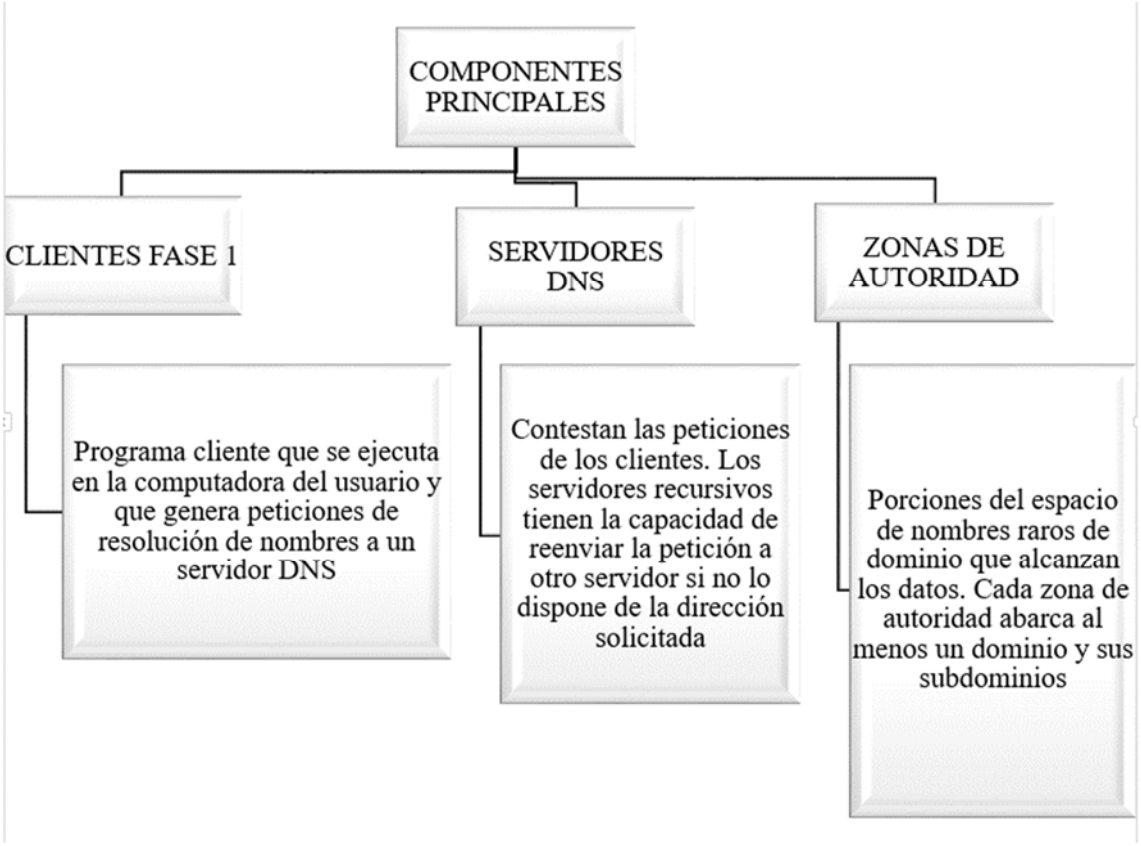
El DNS Se asocia a información variada con nombre de dominios asignados a cada uno de los participantes. Su función más importante es traducir nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red y enfocado el propósito de localizarlos y direccionar los a todo el mundo (Anderson, 2008).

Otro de sus usos más comunes son las sin nación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada uno. Por ejemplo, si la dirección IP del sitio FTP (File Transfer Protocol) de prox.mx es 200.64.128.4, La mayoría de la gente llega este equipo especificando ftp. prox.mx y no la IP, Pues, además de ser más fácil de recordar, qué más fiables; sin embargo, la dirección numérica podría cambiar por muchas razones, sí que tenga que modificarse el nombre.

Para la operación práctica del sistema DNS se utilizan tres componentes principales:

Figura 16.

Componentes principales



Analiza Santos (2018) que en el mundo real en DNS funciona de la siguiente forma: los usuarios, por lo general, no se comunican de manera directa con el servidor, sino que la resolución de nombres se hace de forma transparente por las aplicaciones del cliente

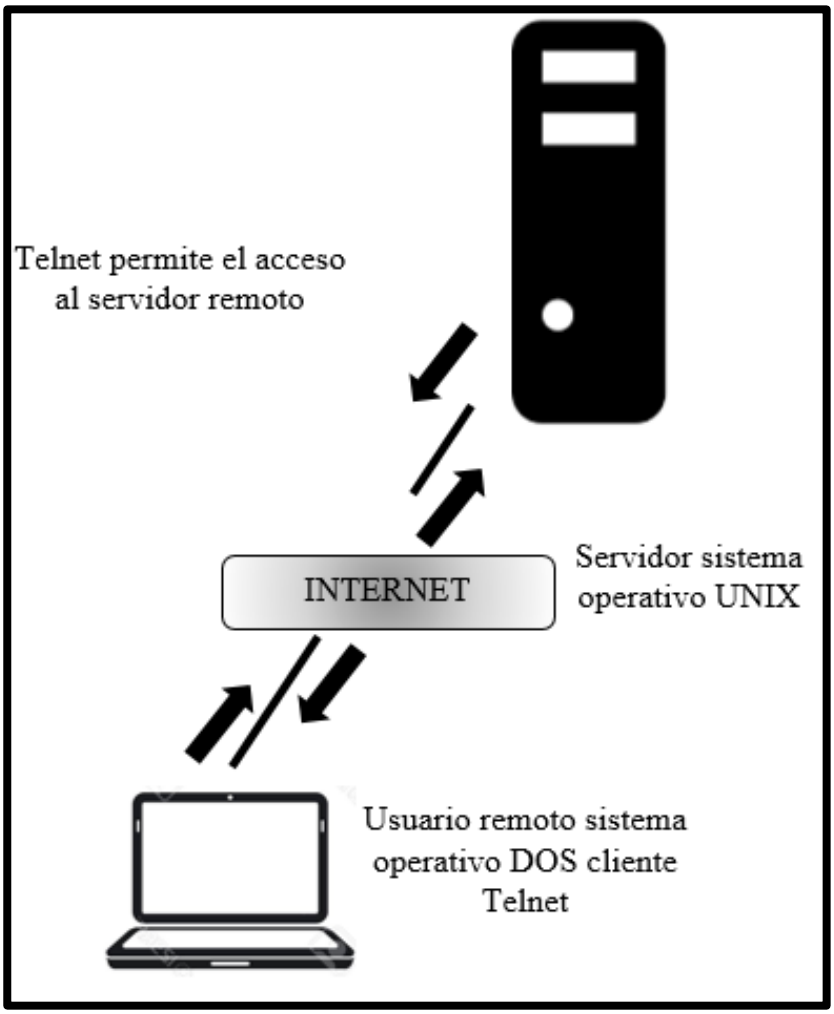
(Por ejemplo, navegadores, cliente de correo y otras usadas en internet).

La mayoría de los usuarios domésticos utilizan como servidor DNS el proporcionado por su proveedor de internet, dónde la dirección de servidores puede ser ajustada de forma manual o automática mediante DHCP. Otros casos, el administrador de red tiene configurado sus propios servidores DNS. En cualquiera de las dos situaciones los servidores DNS reciben la petición busca en primer lugar verificar si disponen de la respuesta en la memoria caché, puede ser así, sirven; en caso contrario, iniciarían la búsqueda de manera recursiva. Una vez encontrada la respuesta, el servidor DNS guardara el resultado en su memoria caché para futuros usos y devuelve el resultado.

Telnet: (telecomunicación Network) Es el nombre de un protocolo de red que permite viajar a otra máquina para manejarlos de manera remota como si se estuviera sentada delante de ella; también se trata del programa informático que implementa el cliente. Para que la conexión funcione, cómo en todos los servidores de internet, la máquina de la que se accede debe tener un programa especial que reciba y gestione las conexiones (Braden, 1989). El puerto que se utiliza de manera común en 2,3.

Figura 17.

Telnet



Telnet Solo sirve para acceder en modo terminal; es decir, sin gráficos, pero es una herramienta muy útil para arreglar fallas a distancia y para consultar datos personales en máquinas accesibles por la red. Además, se ha utilizado (y aún hoy se puede ocupar en su variante SSH) para abrir una sesión cuando una máquina UNIX, de modo que múltiples usuarios se conecten, Abraham sección y puedan trabajar a través de esta.

A pesar de sus beneficios, el mayor problema de telnet en la seguridad porque todos los nombres de usuario y contraseñas necesarias para entrar en las máquinas viajan por la red como

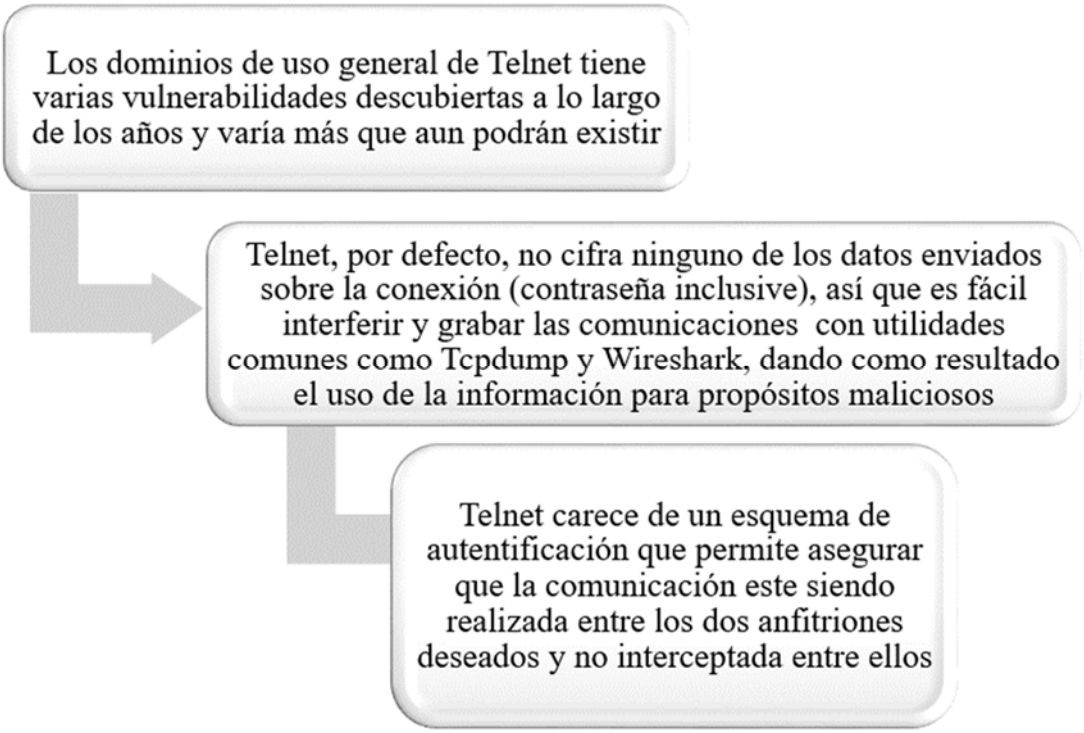
texto plano, lo cual facilita que cualquiera que expide el tráfico pueda obtener dichos datos; por esta razón, dejó de usarse telnet hace unos años cuando apareció y se popularizó el SSH. Algunos clientes de tener son m telnet, NetRunner, Putty o Zoc.

Hoy en día, este protocolo también se usa para llegar al sistema de tablón de anuncios o BBS (Bulletin Boar Sytem) que al principio era accesible con solo un módem a través de la línea telefónica. Para acceder a un BBS mediante telnet es necesario un cliente que proporciona soporte a gráficos ANSI y los protocolos de transferencia de ficheros.

En 1969 se desarrolló telnet, la mayoría de los usuarios de computadoras en la red estaba en los servicios informáticos de instituciones académicas o en grandes instalaciones de investigación privada y de gobierno. En este ambiente, la seguridad no fue una preocupación hasta después de la explotación de ancho de banda de los años 90 del siglo xx, pues con la subida exponencial del número de gente con acceso a internet y por ende, el aumento en usuarios que procurarán ingresar maliciosamente a los servidores de otras personas, telnet dejó de ser recomendado en redes con conectividad a internet. En resumen, se hace necesario destacar tres razones principales por las cuales telnet no se recomienda para los sistemas modernos desde el punto de vista de la seguridad:

Figura 18.

Telnet no se recomienda para los sistemas modernos



Estos defectos han causado el abandono y depreciación del protocolo Telnet rápidamente a favor de uno más seguro y funcional como SSH lanzado en 1995, este proporciona toda la utilidad presente en Telnet, pero agrego el cifrado fuerte para evitar que los datos sensibles sean interceptados y la autentificación mediante llave publica para asegurar que el equipo remoto sea realmente el autorizado; con base en esto, los expertos en seguridad computacional como el Instituto SANS (Sysadmin audit, networking and security institute) ,para ejecutar programas para las conexiones remotas sea descontinuado bajo cualquier circunstancias normal (Braden, 1989,p.3).

SSH: SSH (Secure Shell) o interprete de ordenes seguro, es el nombre de un protocolo y del programa que lo implementa, el cual sirve para acceder a maquinas remotas a través de una red, permite manejar por completo la computadora mediante un intérprete de comandos, así como

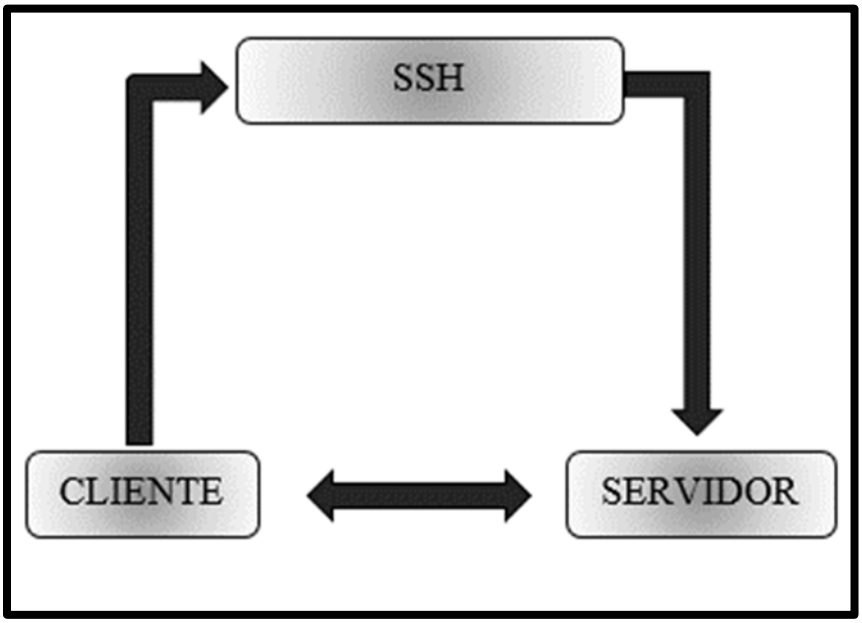
redirigir el tráfico de “X” para ejecutar programas gráficos si se tiene un servicio “Y “corriendo en sistema Unix Y Windows. Además SSH permite copiar datos de forma segura, como simular sesiones FTP cifradas y gestionar claves RSA, es el primero y más utilizado algoritmo de este tipo , valido tanto para cifras como para firmar digitalmente; la seguridad de este radica en el problema de la factorización de números enteros pues los mensajes enviados se representan mediante números y el funcionamiento se basa en el producto conocido de dos números primos grandes elegidos al azar y mantenidos en secreto para no escribir claves al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH ; en la actualidad, estos primos son del orden de 10^{200} y se prevé que dicho tamaño crezca con el aumento de la capacidad de cálculo de las computadoras.

Al principio solo existían los r comandos, que se basaban en el programa alogin , el cual funciona de forma similar a Telnet, la primera versión del protocolo y el programa eran libres y los creo un finlandés llamado Tatú Ylon, pero su licencia fue cambiando y termino apareciendo la compañía SSH Communication Security , que lo ofrecía de manera gratuita para uso doméstico y académico, pero exigía el pago a otras empresas , en 1997, dos años después de que se creara la primera versión, se propuso como borrador en la IETF , en español llamada Grupo de Trabajo de Ingeniera Abierta Abrasom 2000; por otro lado principios de 1999 se empezó a escribir una versión que se convertiría en la implementación libre por excelencia llamada Open SSH de open BSD, en la actualidad existen dos versiones de SSH ; la primera utiliza muchos alegorismos de cifrados potentados y es vulnerable a un agujero de seguridad que potencialmente permite a un intruso insertar datos en la corriente de comunicaciones , la segunda versión suite Apenas bajo Red Hat Enterprise Linux que tiene un algoritmo de intercambio de claves mejorado que no es

vulnerable al agujero de seguridad de la versión 1; sin embargo, esta también soporta las conexiones de la primera.

Figura 19.

Conexiones

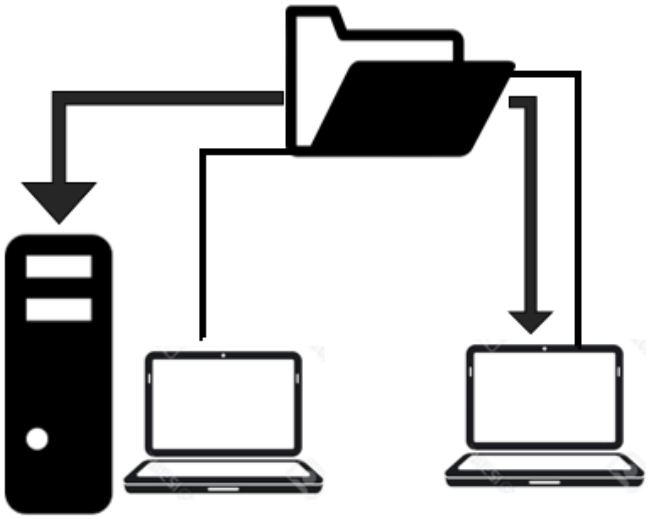


FTP Y TFTP: FTP (File Transfer Protocol) es un protocolo de red de transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol) basado en la arquitectura cliente-servidor, independiente al sistema operativo utilizado en cada equipo, el servicio FTP es ofrecido por la capa de aplicación del modelo de capas de red TCP/IP al usuario, utilizado los puertos de red 20 y 21. Un problema básico de FTP es que está pensando para ofrecer la máxima velocidad en la conexión pero no la máxima seguridad porque todo el intercambio de información (desde el login y el pssword del usuario en el servidor hasta la transferencia de cualquier archivo) se realiza en texto plano sin ningún tipo de cifrado con lo que un posible atacante puede capturar este tráfico, acceder al servicio y/o apropiarse de los archivos transferidos , para solucionar dicha situación son de gran utilidad aplicaciones como SCP y SFTP , incluidas en el servicio SSH y quien permiten transferir archivos cifrando toda la actividad; en el

modelo de intérprete de protocolo de usuarios inicia la conexión de control en el puerto 21 (Tanenbaum, 2006,p.2) .

Figura 20.

Protocolo



El funcionamiento de FTP es el siguiente: las ordenes estándar las genera la IP de usuarios y se transmite al proceso del servidor a traver de la conexión de control como respuesta a las órdenes, las cuales especifican parámetros como puerto, modo de transferencia, tipo de representación y estructura; así como la naturaleza de la operación sobre el sistema de archivos como almacenar, recuperar, añadir, borrar etc. También de transferencia de datos (DTP Dynamic trunking protocol) de usuarios, u otro en su lugar , debe esperar q que el servidor inicie la conexión al puerto de datos especificando para transferirlos en función de los parámetros determinados; también hay que destacar que la conexión de datos es bidireccional; es decir que se puede usar simultáneamente para evitar y recibir, esta al principio tenía un problema la localización de los servidores en la red,es decir, el usuario que quería descargar algún archivo mediante FTP debía conocer en que maquina estaba ubicado en ese momento, la única herramienta de búsqueda de

información que existía era Gopher (ósea literalmente “lanzarse sobrfe la información) con todas sus limitaciones , se trata de un servicio cuyo objetivo es la localización de archivos a partir de título, el cual consiste en un conjunto de menús de recursos ubicados en diferentes maquinas intercomunicadas cada una sirve un área de información, pero la organización interna permite que todas ellas funcionen como si se tratase de una sola, de acuerdo con esto; el usuario navega a través de menús hasta localizar la información buscada y descote exactamente de qué maquina se está descargado; con la llegada de internet los potentes motores de búsqueda como Google dejaron de lado el servicio Gopher y la localización de los servidores FTP paso a ser un problema olvidado.

Antes de cada nueva transferencia , tanto en el modo activo como en el pasivo, el cliente debe enviar otra vez un comando de control, tras lo que el servidor recibirá esa conexión de datos en un nuevo puerto aleatorio (si está en modo pasivo) o por el puerto: por otro lado , en el protocolo FTP existen dos tipos de transferencia en ASCII y binarios, es muy importantes conocer estos, pues si no se utilizan las operaciones adecuadas puede destruir la información del archivo, por ello al ejecutar las aplicaciones FTP se debe utilizar uno de estos comandos (o poner la correspondiente opción en un programa con interfaz gráfica)

Tipo ASCII: adecuado para transferir archivos que solo contengan caracteres imprimibles (los archivos ASCII no son archivos resultantes de un procesador de texto) por ejemplo paginas HTML (hipertexto markup lenguaje) pero sin las imágenes que puedan contener.

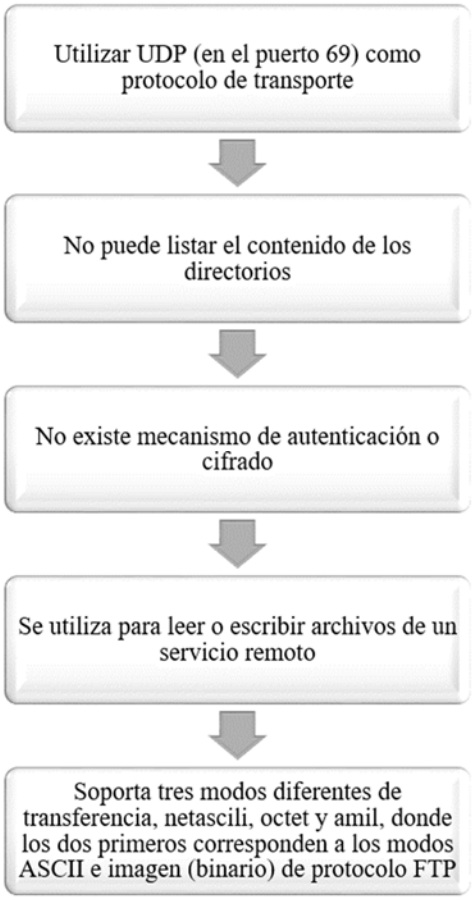
Tipo binario: usado cuando se trata de archivos comprimidos ejecutables para computadoras personales, imágenes y archivos de audio, entre otras aplicaciones.

Por otro lado TFTP son las siglas en ingles de Trivial File Transfer Protocol que significa protocolo de transferencia de archivos trival; el cual consiste en una versión básica de FTP sin

embargo, TFTP a menudo se utiliza para enviar pequeños archivos entre computadoras en una red, algunas de sus características son:

Figura 21.

Características



Puestos que TFTP utiliza UDP , no hay una definición formal de sesión, cliente y servidor aunque se considera servidor a aquel que abre el puerto , y cliente a quien se conecta sin embargo, cada archivo transferido vía TFTP constituye un intercambio independiente de paquetes , en el cual existe una relación cliente- servidor informal; la maquina A que inicia la comunicación envía un paquete de petición de lectura RRQ y el modo de transferencia posteriormente esta última

responde con un paquete de confirmación ACK, que también sirve para formar acerca de puertos al que tendrá que enviar los paquetes restantes la B, la maquina origen envía todos los datos numerados a la de destino , excepto el ultimo que contiene 512 bytes de datos ; entonces esta responde con paquete ACK numerados para todos los paquetes de datos, donde el ultimo debe contener menos de 521 bytes de datos , si el tamaño de archivo transferido es un múltiplo exacto de este valor, obtiene como respuesta del origen el envío de un paquete final que contiene 0 bytes de datos.

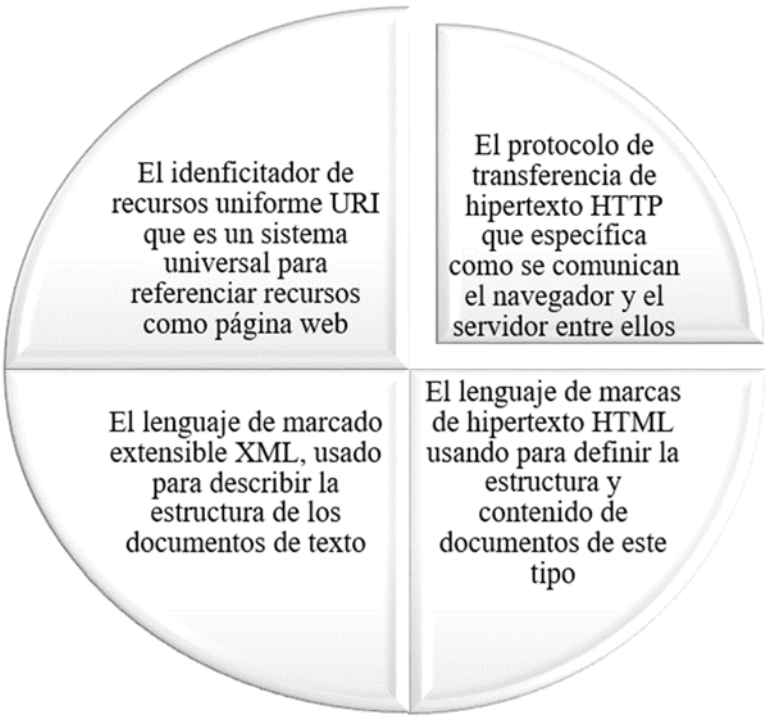
WWW: HTTP y HATTPS

En la información la red informática mundial (WWW, Word W de Web), comúnmente conocida como web, es un sistema de distribución de documentos de hipertexto o hipermedicos interconectados y accesibles vía internet, con un navegador web, suaviza sitios compuestos de páginas que pueden contener textos, imágenes, videos u otros, contenidos multimedia; además puede navegar a través de estos usando hiperenlaces. Entre marzo de 1989 y diciembre de 1990 , el británico Tim Bernes - Lee con ayuda del belga Robert Cailliau desarrollaron la web por mientras trabajaban en el Centro Europeo de Investigación Nuclear CERN en Ginebra , para vincular y acceder a información de diversos tipos como una red de nodos en que el usuario puede navegar; el funcionamiento de WWW ,es el siguiente el primero paso consiste en traducir la parte del nombré del servidor de la URL en una dirección IP usando HNS lo siguiente es enviar una petición HTTP al servidor web solicitando el recurso, en el caso de una página web típica, primero se solicita el texto HTML , que de inmediato es analizando por el navegador busca y establece la página y como se describe en el código HTML, el CSS y otros lenguajes web al final se incorporan las imágenes y otros recursos para producirle la página completa que el usuario despliega en la pantalla (Berners- Lee ; Ciliau; Loutonen; Nielsen y Secret 1994). Desde 2007 mantienen los

siguientes y otros estándares que permiten a las computadoras de la web almacenar y comunicar con eficacia los diferentes tipos de información (Berners, 2009, p.3).

Figura 22.

Diferentes tipos de información



Aunque la existencia y uso de la web se basa en tecnología material que tiene a su vez algunas desventajas , esta información no utiliza recursos físicos como las bibliotecas o la prensa escrita, razón por la cual su propagación vía internet no está limitada por el movimiento de volúmenes físicos o por copias manuales o materiales de datos, gracias su carácter virtual puede ser buscada fácil, eficaz y más rápido de lo que una persona podría recabarla por si misma a través de un viaje , correo, teléfono o celular o cualquier otro medio de comunicación que existe actualmente

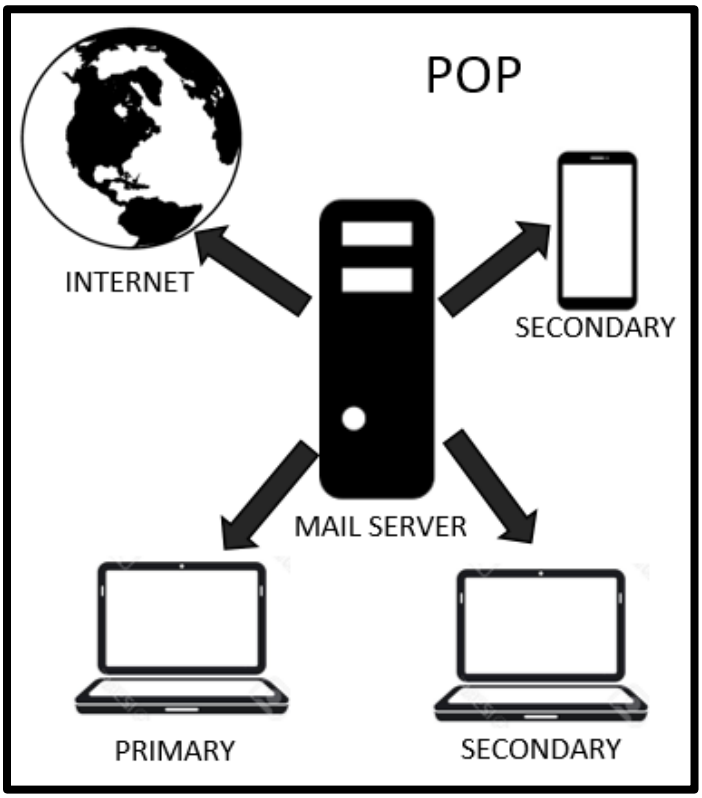
POR: En informática se utiliza el protocolo de oficina de correo POP (pos office

Protocol de novel de aplicación en el Modelo OSI utilizado para obtener mensajes de correo electrónico almacenados en un servidor remoto ; las versiones de este protocolo POP, informalmente conocido como POP1y POP2,se han quedado obsoletas debido a las ultimas de POP3, en general cuando se hace referencia al termino POP se refiere directamente al POP3 dentro de contexto de protocolos de correo electrónico ; por otro lado POP3 está diseñado para recibir correos no para enviarlo , lo que permite a los usuarios con conexiones intermitentes o muy lentas (como aquellas por modem),descargan su correo electrónico mientras tengan conexión para revisarlo posteriormente incluso estando desconectado cabe mencionar que la mayoría de los clientes de correo incluyen la opción de dejar los mensajes en el servidor por lo que un cliente que utilice POP3 se conecta , obtiene todos los mensajes, los almacena en la computadora del usuario como mensaje nuevos , los elimina del servidor y finalmente se desconecta.

La mayoría de las ordenes de POP3 identifican los mensajes dependiendo de su número ordinal en el servidor de correo, estos generan problemas cuando un cliente pretende dejar los mensajes en el servidor, pues los que tienen un numero cambian de una conexión de servidor a otra.

Figura 23.

Conexión de servidor



Los clientes que utilizan la opción de dejar mensajes en el servidor por lo general utilizan UIDL (Unique Identification Listing), el cual proporciona un mecanismo que evita los problemas numéricos: el servidor le asigna una cadena de caracteres única y permanente al mensaje; cuando un cliente de correo compatible con POP3 se conecta al servidor utiliza la orden UIDL para obtener el mapeo para determinar qué mensaje se deben descargar y cuales guardar al momento de la descarga. Al igual que otros viejos protocolos de internet, POP3 utilizaba un mecanismo de firmado sin cifrado. La transmisión de contraseña de POP3 en texto plano aún se da.

En la actualidad, POP3 cuanta con diversos métodos de autenticación que ofrecen una diversa gama de niveles de protección contra los accesos ilegales al buzón de correo de los usuarios. Uno de estos es APOP, el cual utiliza funciones MD5 para evitar los ataques de

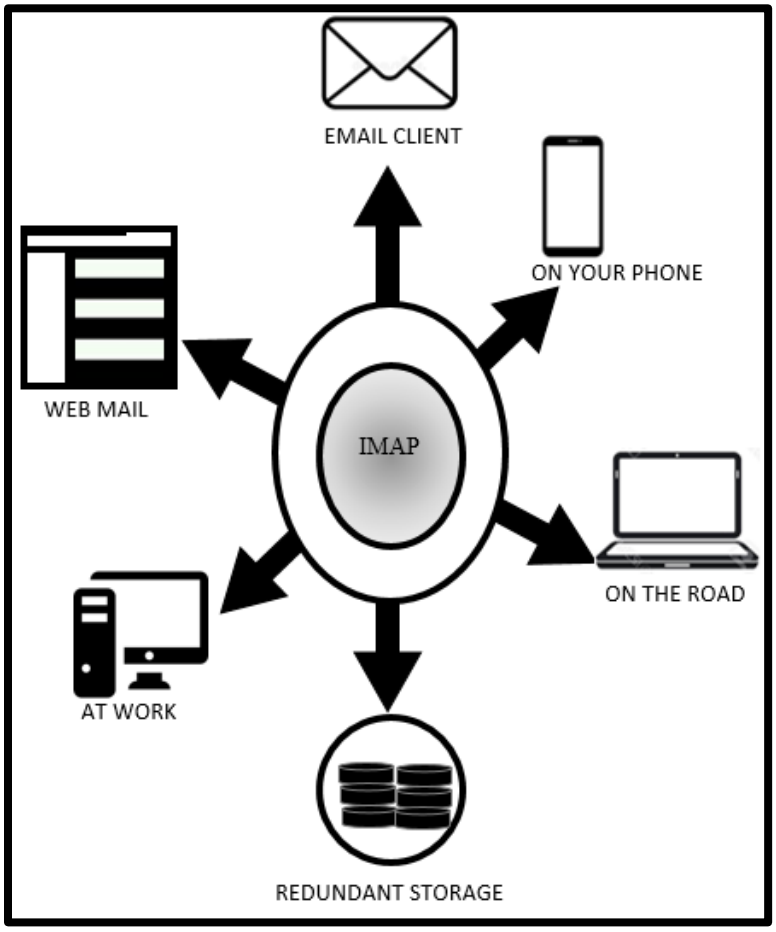
contraseñas. Mozilla, Eudora, Novell Evolution, así como Mozilla Thunderbird, implementa funciones APOP.

IMAP: (Internet Message Access Protocol) es un protocolo de aplicación que permite el acceso a mensajes almacenados en un servidor. Mediante este se puede tener acceso al correo electrónico desde cualquier equipó que tenga una conexión a internet.

IMAP tiene varias ventajas sobre POP como especificar carpetas del lado del servidor, visualizar los mensajes de manera remota sin descargarlos y permite los modos de operación" conectado" y "desconectado". Los clientes de correo electrónico que utilizan IMAP dejan los mensajes en el servidor hasta que el usuario los elimine, de forma directa. Esto y otros factores hacen que la operación de IMAP permita a múltiples clientes acceder al mismo buzón de correo.

Figura 24.

IMAP



La versión 4 revisiones 1 (IMAP4rev1) está definida por el RFC 3 501; es decir, en 1986 IMAP fue diseñado por Mark Cispin como una alternativa moderna a POP.

Todos los servidores y clientes de correo electrónico están virtualmente soportados por IMAP y POP3, aunque en algunas cosas hay interfaces específicas del fabricante.

Amanera de ampliación, algunas de las características importantes que diferencian a IMAP y POP3 son:

Soporte para la conexión de múltiples clientes simultáneos a un mismo destinario

El protocolo POP3 supone que el cliente conectado es el último dueño de una cuenta de correo, en contraste, el protocolo IMP4 permite acceso simultáneo a múltiples clientes y les proporciona ciertos mecanismos para que se detecten los cambios hechos a un buzón de correo por usuario concurrentemente conectados

Soporte para acceso a partes MIME de los mensajes y obtención parcial

Casi todo el correo electrónico de internet es transmitido en formato MIME, el protocolo IMP4 permite a los clientes obtener por separado cualquier parte MIME individual, así como conseguir porciones de las partes individuales a los mensajes completos, lo cual es más seguro.

Soporte para que la información de estado del mensaje se mantenga en el servidor

A través de la utilización de señales definidas en el protocolo IMP4, de los clientes se puede vigilar el estado del mensaje; por ejemplo si este ha sido o no leído, respondido o eliminado, las señales se almacenan en el servidor, de manera que varios clientes conectados al mismo correo en diferentes tiempo puedan detectar los cambios hechos por otros clientes; el soporte para múltiples buzones de correo también le permite al servidor proporcionar acceso a los directorios públicos y compartidos .

Soporte para búsquedas de parte del servidor

IMP4 proporciona un mecanismo para que los clientes pidan al servidor que busque mensajes de acuerdo con cierta variedad de criterios, este mecanismo evita que se descarguen los mensajes de su buzón, agilizando las búsquedas.

Soporte para un mecanismo de extensión definido

Como reflejo de la experiencia en versiones anteriores de los protocolos de internet IMAP define un mecanismo explicito mediante el cual puede ser extendido.

Se han propuesto muchas extensiones de IMP4 de uso común, un ejemplo es el IMAP IDLE, que permite al servidor avise al cliente cuando ha llegado un nuevo mensaje de correo y estos se sincronicen, para realizar la misma tarea sin dicha extensión al cliente deberá conectar periódicamente al servidor para revisar si hay mensajes nuevos.

SASL: Finalmente SASL que es en español se define como la capa de seguridad y autenticación simple es autorización en protocolos de internet este los separa de la aplicación permitiendo en teoría, usar el soportado por cualquier aplicación que utilice SASL. A pesar de que solo maneja la autenticación (y se requieren otros mecanismo como TLS para cifrar el contenido que transfiere, SASL proporciona medios para un uso negociado del mecanismo elegido, las especificaciones originales fueron editadas por John Meyer en el RFC 2222 pero quedo obsoleto por el 4422, editado Por Alexey Melnikov y Kurt Zeileng.

Los mencionados mecanismos se modelan como una sucesión de retos y respuestas estas incluyen:

Esternal: la autenticación esta implica en el contexto (por ejemplo para protocolos que usan (Psec i TLS).

Anonymous: para el acceso de invitados sin autenticar.

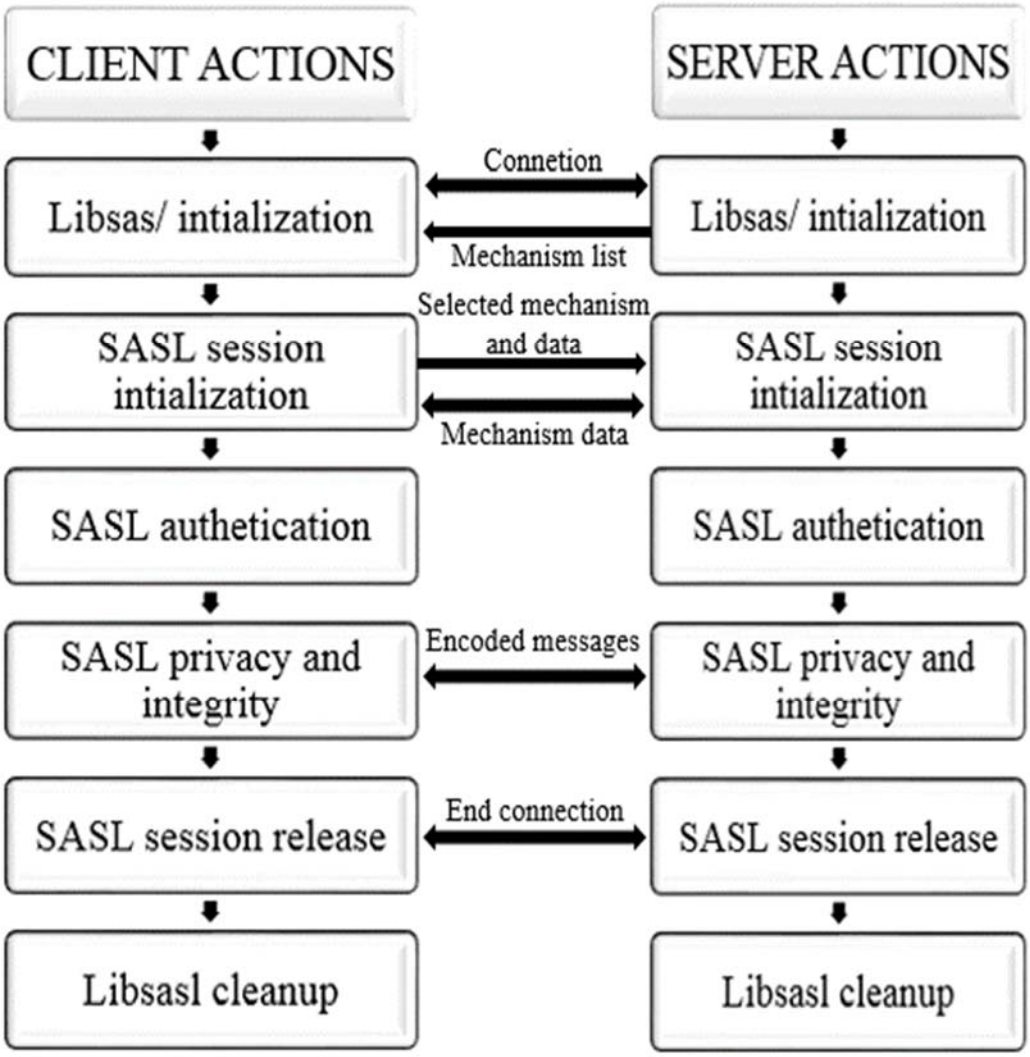
Plain : un mecanismo de contraseña simple en texto plano.

Otp: para el sistema que evoluciono de S/KEY y se encuentra definido en RFC 2289.

NTLM: en una red de Windows, NT LAN Manager (NTLM), es un conjunto de protocolos de seguridad Microsoft que proporciona, autenticación, integridad y confidencialidad a los usuarios NTLM es el sucesor del protocolo de autenticación en Microsoft LAN manager (LANMAN) un producto anterior de Microsoft.

Figura 25.

NTLM



Protocolo de administración de red (SNMP)

El protocolo simple de administración de red (SNMP, simple network management protocol) facilita el intercambio de información de gestión entre dispositivos y permite supervisar el funcionamiento de la red, buscar y resolver sus problemas y planes su crecimiento , las versiones de (SNMPv3) posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad, sin embargo, no ha sido por completo aceptado en la industria, una red administrador a través de SNMP se compone de tres elementos claves:

Dispositivos administrativos: son los que se encargar de recoger y almacenar información la cual es puesta a disposición de los sistemas administradores de red NMS los dispositivos administradores a veces llamados elementos de red.

Agentes: los módulos son de software de administración de red poseen un conocimiento local de información (memoria libre, número de paquetes IP recibidos, rutas, etc.) la cual es traducida a un formato compatible y memoria requeridos para la administración de la red.

Sistemas administradores de red (NMS, Network Management station): ejecutan aplicaciones que supervisan y controlan los dispositivos administrados los NMS proporcionan el volumen de recursos de procesamiento y memoria requeridos para la administración de la red, uno o más deben existir en cualquier red administrativa.

Por su parte, los dispositivos administrados son supervisados y controlados usados cuando comandos SNMP básicos:

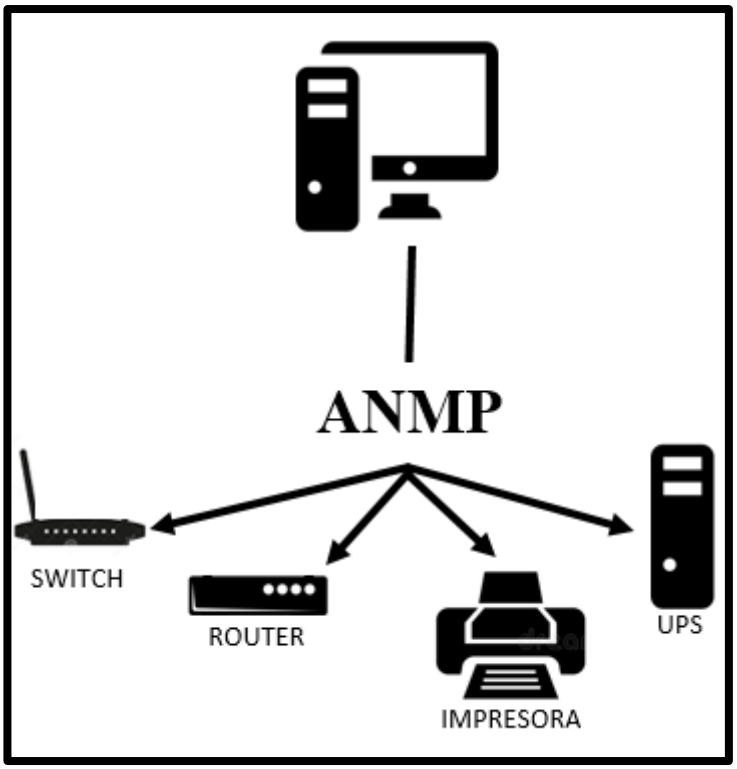
Comando de lectura: usado para supervisar elementos de red, el NMS examina diferentes variables que son mantenidas por los dispositivos administrativos.

Comando de escritura: se utiliza para controlar elementos de red, el NMS cambia los valores de las variables almacenadas dentro de los dispositivos administrativos.

Comando de notificación: sirve para reportar eventos en forma asíncrona a NMS cuando cierto tipo de eventos ocurre un dispositivo administrado envía un aviso.

Figura 26.

ANMP

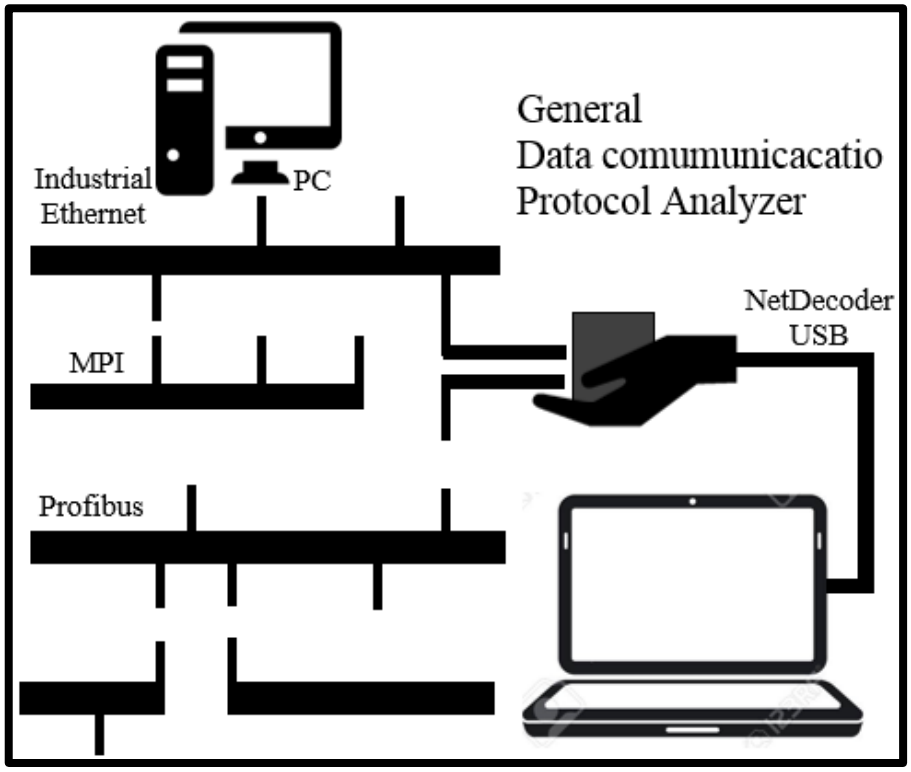


Analizadores de protocolos

Un analizador de protocolo es una herramienta que sirve para desarrollar y depurar los protocolos y las aplicaciones de red, este permite a la computadora capturar diversas tramas de red para analizarlas, ya sea en tiempo red o después de haberlas capturado, lo cual significa que se puede reconocer que la trama capturada pertenece a un (Bertsekas y Gallager 1992) de esta forma el usuario puede ver todo aquello que un momento concreto está circulando por la red analizada.

Figura 27.

Analizadores de protocolos



Otros usos de los analizadores de protocolos son:

1. Examinar y soportar demandas de nuevas aplicaciones (como VoIP).
2. Obtener mayor efectividad de la red al analizar todo lo que pasa por ella y detectar problemas concretos.
3. Verificar redes remotas sin necesidad de realizar largos viajes.
4. Observar y monitorear varias redes a la vez.

Expresa Gutiérrez (2019, p.58) Que hay diversos tipos de analizadores de protocolos disponibles en el mercado peo en general, son productos bastantes caros, el precio depende de la capacidad de análisis, de la tecnología de red soportada y de si se trata de software o hardware, algunos ejemplos de analizadores de protocolos son:

Appsniffing: cuenta con una poderosa interfaz gráfica que permite diagnosticar rápidamente problemas y anormalidades de la red, se caracteriza porque la captura puede ser efectuada tanto en el disco como en la memoria además de que el análisis de datos, y uso de filtros puede ser efectuados en tiempo real y porque permite estadísticas globales, así como un análisis TCP .

Productos observer (expert observer, obsrver, suite, observer probes etc.) : sirve para Ethernet, inalámbrico 802.11ba Token Ring y FDDI observa mide, captura y predice tendencias de sus redes, se ejecuta en el ambiente Windows y monitorea y sirve como herramienta para resolver problemas que se presentan en las redes.

Super agent: solución número uno para realizar la monitorización, establecer las tendencias y solucionar los problemas del rendimiento de aplicaciones permite ver con precisión

y detalles los tiempos de respuestas del usuario final por toda la empresa y de todas las aplicaciones de TCP sin la necesidad de usar extremos ni sondas distribuidas.

OptiView Console: consola de funcionamiento centralizado de optiviw con función de acceso remoto que detecta rápidamente y supervisa de forma continua los dispositivos de red, al mismo tiempo que documenta su conectividad.

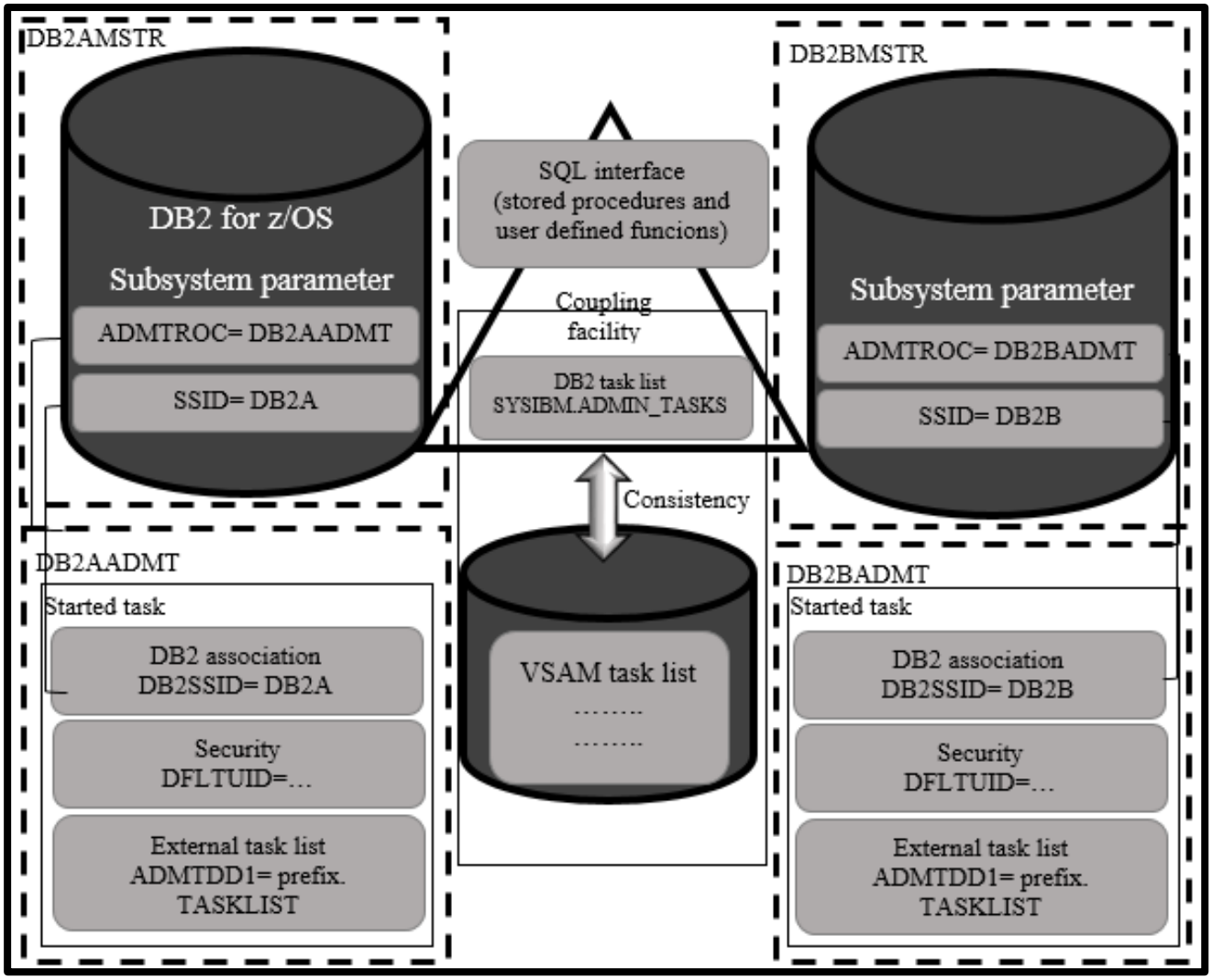
OptiView Protocol Expert: aplicación basada en Windows que ofrece análisis de protocolos autónomos para paquetes capturados de Workgroups Analyzer Link Analyzer e Integrated Network Analyzer de Optiview.

Planificadores.

El planificador (Schedule) es un componente funcional muy importante de los sistemas operativos multitarea y multiproceso que es esencia en los sistemas operativos de tiempo real, la cual su función del planificador consiste en repartir el tiempo disponible de un microprocesador entre todos los procesos disponibles para ejecución (Bournoure 2006, p.12). Todo sistema operativo gestiona los programas mediante le concepto de proceso de ahí la necesidad de que una parte del sistema operativo gestione, de una manera equi8tativa, cual debe ejecutarse en cada momento para hacer un uso eficiente del procesador, esto se consigue de dos maneras, simple con ayuda del propio hardware:

Figura 28.

Planificadores.



- Cuando expira un temporizador, que se activa a intervalos regulares de tiempo.
- En intervalos cortos, generalmente cada 250 milisegundos.
- Cuando el programa solicita una operación de entrada/salida, dado que este no puede continuar hasta que aquella termine, momento idea la para ejecutar otro, en ambos caos el control del microprocesador pasa a manos del planificador gracias a que el hardware genera una interrupción; en este proceso de expulsión se guarda

el estado de ejecución del programa, llamado contexto, todo esto apenas dura unos procos milisegundos.

Explica Monfasani (2018) que gracias a que el tiempo del microprocesador se reparte entre todos los procesos en intervalos muy cortos, la computadora ofrece la sensación de que estos encuentran ejecutándose a la vez; cuando una computadora tiene varios microprocesadores, este esquema se repite para cada microprocesador.

Los niveles de planificación están basados en la frecuencia con la que se realiza cada uno en los sistemas operativos de propósitos generales existen tres tipos de planificadores:

Planificador a corto plazo: es el más importante, que en ingles se denominan despachar o short term scheduler.

Planificador a mediano plazo: en inglés midterm scheduler relacionado con aquellos proceso que no se encuentran en la memoria principal, su misión es mover procesos entre memoria principal y disco (lo que se conoce com swpping).

Planificador a largo plazo: en inglés, logterm Schedule, que es el encargado de ingresar nuevos proceso al sistema y también de finalizarlos; por otro lado, existen dos tipos de algoritmos de calendarización o políticas de planificación:

Expropiativos: Asignan tiempo de ejecución a cada proceso después del cual se calendariza otros gasta que cada uno acabe el trabajo, también expulsan un proceso en ejecución, si llega otro de mayor prioridad que necesita ejecutarse.

No expropiativos: permiten que se ejecute el proceso hasta que acabe el trabajo; es decir, una vez que les llega el turno, no dejaran libre al procesador hasta que termine o se bloqueen.

2.3.4 Análisis de desempeño de la red: tráfico y servicios.

Reporta Maíllo (2017, p.49). En cuanto a la arquitectura de rendimiento de una red describe la forma en que los usuarios aplicaciones, dispositivos y redes logran cumplir con los requerimientos de rendimiento que fueron establecidos en el momento en que se planifico la red, por otra parte, dentro de los niveles de análisis y diseño de redes se encuentran la arquitectura de rendimiento (Haliivuori, 2000), en una red es de suma importancia mantener niveles óptimos en estos componentes ya que los diferentes flujos de información generados por los usuarios , dispositivos o aplicaciones pueden verse muy afectados en sus actividades debido a variaciones de los niveles de rendimiento; se entiende entonces por arquitectura de rendimiento , y el conjunto de mecanismos que se utilizan para configurar; opera, gestionar, disponer y enlistar los recursos en la red que soportan los tráficos de flujo de información, la capacidad se puede definir genéricamente, como la habilidad que tiene el sistema para lograr la transferencia de información a través de la red, al término de capacidad se le liga con otros como:

Ancho de banda: Capacidad que tiene un red para transmitir datos; por lo regular, se refiere a la cantidad de estos que se pueden transferir en determinado momento a través de la red, medidos e bits, por segundo (bit/s) o en sus múltiplos.

Throughpt: se refiere a la tasa promedio de datos o de mensajes que han sido transferidos con éxito y sin errores en la red de un nodo a otro.

Goodupu: cantidad de bits de información utilizables que se envía en la red a un destino determinado por unidad de tiempo.

Retardo: cantidad de tiempo que se toma la transferencia de una unidad de información a través del sistema, desde un origen hasta un destino, los usuarios que utilizan aplicaciones que corren en tiempo real o interactivas, esperan que el retardo en la red sea mínima.

Seguridad básica.

Describe Martínez (2019, p.89) En cuanto a la seguridad a nivel informático significa que el sistema esa libre de peligro, daño o riesgos (Kaufma, Periman, y Speciner , 2002) , el objetivo de establecer la seguridad básica en la red de computadores es mantener la integridad , disponibilidad y confidencialidad de la información de la red para que la organización mantenga la continuidad en sus procesos; cuando se habla de integridad, se quiere decir que los objetivos del sistema solo pueden ser modificados por personas autorizadas y en forma controlada, por otro lado, la disponibilidad significa que los objetos del sistema deban permanecer accesibles a dichas personas; por último , la confidencialidad en el sistema se presenta cuando la información contenida en este no es brindada a entidades externas, para alcanzar este último objetivo se debe plantear y definir lo siguiente: los recursos se quieren proteger dentro de una red? Qué medidas y herramientas se deben implantar para alcanzar un óptimo nivel de seguridad sin perder de vista la relación costo- beneficio, una vez definido estos puntos, pueden diseñarse las políticas de seguridad adecuadas para implementar en la organización y crear un perímetro de defensa que permita proteger las fuentes de información, las normas de control interno que conforman las medidas de seguridad para sistema interactivos y procesos en redes privadas se dividen en seguridad lógica y física, donde los recursos que se han de proteger básicamente son hardware, software y datos; para los tres elementos a proteger existen cuatro tipos de amenazas:

Interrupción: cuando un objeto del sistema se pierde y queda inutilizable o no disponible.

Intercepción: cuando un elemento no autorizado consigue un acceso a un determinado objeto del sistema.

Modificación: cuando se altera algún objeto del sistema una vez adentro de este.

Fabricación: cuando se cambia algún objeto del sistema por otro de aspecto igual pero con un objetivo distinto. Sin embargo, se debe tener en cuenta que cuando se hace referencia a seguridad en redes, el bien más preciado a proteger es la información que circula por ellas.

Los elementos de seguridad.

Confirma Walter (2019, p.92) Que dentro de las medidas de seguridad con relación en los equipos se pueden establecer los que se describirán a continuación:

Cortafuegos (firewall) sistema de defensa lógico y físico basado en el hecho de que todo el tráfico de entrada o salida a la red , debe pasar sin excepción por un sistema de seguridad capaz de autorizar, denegar y tomar nota de aquello que ocurre, el concepto de cortafuego(firewall) genera controversias, por lo que se define junto con las normas, los procedimientos y las herramientas que se utilizan con el objetivo de mantener la integridad , la operatividad y la privacidad de la información manejada por las computadoras (Terán Pérez , 2010).

El contrafuegos tienen que detectar puntos débiles y monitorear en lapsos de tiempo cortos el estado y seguridad de la red, generando informes en tiempo real, el responsable de diseñar e implementar las políticas de seguridad para una red privada debe ser un integrador, o sea, el administrado de los recursos informáticos de la empresa quien requiere los datos y valor para considerar los puntos planteados a continuación:

1. Quienes deben acceder solo para consultas sin actualizar ni modificar datos.
2. Quienes pueden consultar y actualizar datos.
3. Quienes pueden realizar ciertos procesos.
4. Que se debe filtrar.
5. Definir las condiciones de validación por software y hardware a la par de que controla los accesos y la salida de datos de la red al exterior.
6. Determinar las condiciones complementarias de seguridad para los nombres y claves; por ejemplo preguntas, tarjetas magnéticas, contraseñas, etc.
7. Establecer las formas de encaminar los datos que se agregan en las consultas para los usuarios que están de otro lado de los cortafuegos.
8. Saber que cortafuegos es virtual.
9. Control de los vínculos físicos.

A pesar de las múltiples ventajas de unos cortafuegos, este también tienen algunas debilidades como:

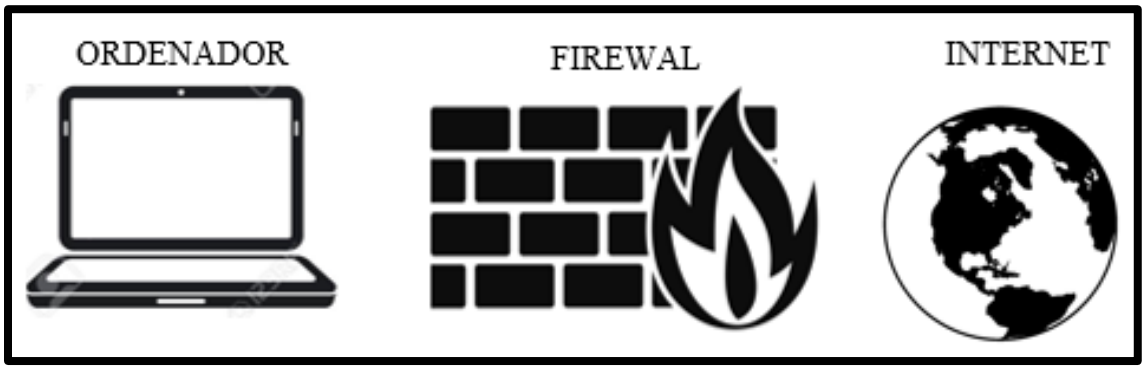
1. No puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación.
2. No es posible protegerse de las amenazas a que se somete por traidores o por usuarios inconscientes.
3. No puede prohibir que los espías corporativos copien datos sensitivos en discos, en memorias USB o tarjetas PCMCIA y los sustraigan del edificio.
4. No puede garantizar protección contra ataques de ingeniería social.
5. No puede protegerse contra los ataques posibles a la red interna por virus informáticos a través de archivos y de software obtenidos desde internet, pues al

momento de querer comprimir o descomprimir archivos binarios los cortafuegos de internet no puede contar con un sistema preciso de verificación para cada tipo de virus que se puedan presentar.

6. Finalmente el cortafuegos de internet no puede proteger contra los ataques posibles en la transferencia de datos, estos ocurren cuando datos inocuos son enviados o copiados a un servidor interno y son ejecutados facilitando un ataque.

Figura 29.

Operación de un cortafuego



Proxy o servidor de defensa: el proxy es un software que se instala en una computadora personal conectada a una red local, de preferencia exclusiva para este uso, la cual se busca que funcione como una puerta lógica ; al servidor proxy pueden acceder los clientes, los posibles clientes o clientes virtuales, los proveedores o las instituciones financieras; siempre y cuando este protegidos en cuanto a la ubicación de los datos alojados, pues es necesario monitorear la red y su desarrollo para que no lleguen a los elementos protegidos.

Por lo regular, se trata de un programa que trabaja con servicios externos en nombre de clientes internos; estos se comunican con los servicios que a su vez transmite las solicitudes

aprobadas a cada uno de ellos para después enviar las respuestas al servidor y de este a los clientes

. **Pasarelas (Gateway) a nivel de aplicación**

El Gateway se caracteriza por ser un dispositivo que filtra datos (Terán Pérez, 2010) como los puentes (bridges) o Reuters , las pasarelas en el nivel de aplicación permiten al administrador de red la implementación de una política de seguridad estricta, pues se instala un servicio proxy para cada aplicación deseada.

Encaminado (router) paquetes

El router toma las decisiones de negar o permitir el paso de cada uno de los paquetes de datos que son recibidos este examinar cada datagrama para determinar si corresponda a uno de sus paquetes filtrados y si ha sido aprobados por sus reglas; de ser así, se permite el paso del paquete, el cual será desplazado de acuerdo con la información de la tabla de ruteo en el cambio si las reglas niegan el paso, el paquete es descartado, el router de filtrado es por lo general , transparente a los usuarios finales y a las aplicaciones por lo que se requiere entrenamiento o software especializado que necesite ser instalado en cada uno de los servidores (Terán Pérez

, 2010).

2.4 Marco Legal

2.4.1 Normatividad sobre derechos de autor y propiedad intelectual en Colombia

Según la Constitución Política de Colombia la ley 23 de (1982) Sobre los Derechos de Autor establece que:

Articulo 1 Los autores de obras literarias, científicas y artísticas gozarán de protección para sus obras en la forma prescrita por la presente ley y, en cuanto fuere compatible con ella, por el derecho común. También protege esta ley a los intérpretes o ejecutantes, a los productores de fonogramas y a los organismos de radiodifusión, en sus derechos conexos a los del autor. 2.2

Articulo 2 Los derechos de autor recaen sobre las obras científicas, literarias y artísticas las cuales se comprenden todas las creaciones del espíritu en el campo científico, literario y artístico, cualquiera que sea el modo o forma de expresión y cualquiera que sea su destinación, tales como: los libros, folletos y otros escritos (…)

Por otro lado la Ley 44 de (1993) expone:

Artículo 6 Todo acto en virtud del cual se enajene el Derecho de Autor, o los Derechos Conexos así como cualquier otro acto o contrato vinculado con estos derechos, deberá ser inscrito en el Registro Nacional del Derecho de Autor como condición de publicidad y oponibilidad ante terceros.

2.4.2 Políticas de seguridad

Una política de seguridad es " un conjunto de requisitos definidos por los responsables de un sistema, qué indica en términos generales qué está y que no se permite en el área de seguridad durante la operación general del sistema" (Villalón, 2010, p.12).

Por otro lado, la RFC 1 244 establece una política de seguridad cómo " una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán".

La política se refleja en una serie de normas, reglamentos y protocolos a seguir, dónde se determinan las medidas a tomar para proteger la seguridad del sistema; pero ante todo, "una política de seguridad es una forma de comunicarse con los usuarios. Por lo que siempre hay que tener en cuenta que la seguridad comienza y termina con las personas (Spafford, 2000, p.6); tanto, está debe:

Holística (todos los objetos revelados con la misma): No tiene sentido proteger el acceso con una puerta blindada, sí ahí está no se ha cerrado con llave.

Adecuarse a las necesidades y recursos: No es necesario el quirir una caja fuerte para proteger un lápiz.

Ser atemporal: El tiempo en el que se aplica no debe influir en la eficiencia y eficiencia

Definir estrategias y criterios generales a adoptar en distintas funciones y actividades: En dónde se conocen las alternativas ante circunstancias repetidas.

Cualquier política de seguridad debe considerar los elementos claves de seguridad: La integridad, disponibilidad, privacidad, control, autenticidad y utilidad.

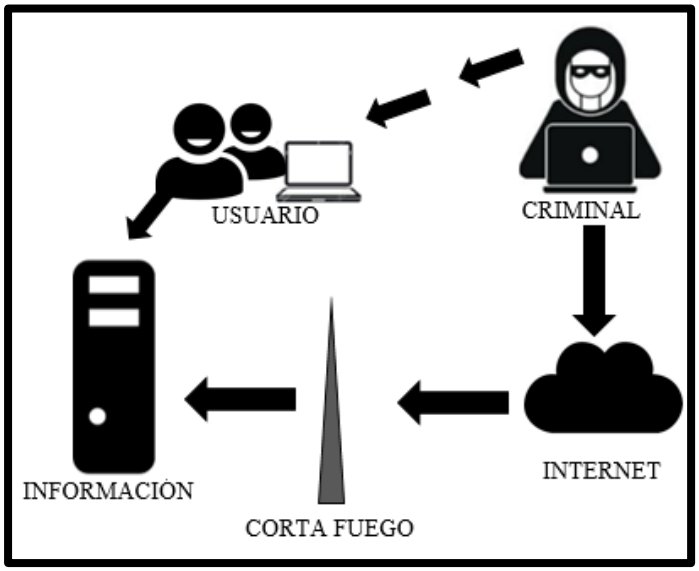
No debe tratarse de una descripción técnica de mecanismo de seguridad y de una expresión legal que involucre sensaciones alas conducta de los empleados: Es más bien, una descripción de lo que se desea proteger y él porque de ello.

Hoy es imposible hablar de un sistema 100% seguro, porque el costo de esto sería muy alto, debido a que todos los sistemas (físicos y lógicos) son vulnerables.

Algunas organizaciones gubernamentales y no gubernamentales, nacionales y también internacionales han desarrollado documentos, directrices y recomendaciones que orientan en el uso adecuado de las nuevas tecnología para obtener el mayor provecho y evitar el uso indebido de estas, lo cual puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

Figura 30.

Políticas de seguridad



Debe dejarse muy claro que la seguridad informática no tiene una solución definitiva, sino que es y será el resultado de la innovación tecnológica por parte de aquellos que son los responsables del sistema. En palabras de Ardita (2001):

Una política de seguridad funcionó muy bien en los Estados Unidos de América, pero cuando esos manuales se llevaron a América Latina, todo fue un fiasco. Armar una política de procedimientos de seguridad en una empresa cuesta entre 150 y $350 y sin resultado. La razón es posible por qué es un manual que llevado a la implementación nunca se realiza. Es muy difícil armar algo global, por lo que siempre se trabaja en un plan de seguridad real las políticas y los procedimientos por un lado y la parte física por el otro.

Para continuar hará falta definir algunos conceptos aplicados en la definición de las políticas de seguridad informática (PSI):

Tabla 3.

PSI

DECISIÓN	Elección de un curso de acción determinado entre varios posibles.
PLAN	Conjunto de decisiones que definen cursos de acción futuras y los medios para conseguirlos. Consiste en diseñar un futuro deseado y La búsqueda del mundo de conseguirlo.
ESTRATEGIA	Conjunto de decisiones que se toman para construir políticas, metas y programas.
POLÍTICAS	Definiciones establecidas por la dirección que determina criterios generales y adoptar en distintas funciones y actividades donde se conocen las alternativas ante circunstancias repetidas.
META	El objetivo cuantificado en valores predeterminados, procedimiento definición detallada de pasos a ejecutar para desarrollar una actividad determinada.
NORMA	Forma en que se realiza un procedimiento o proceso
PROGRAMA	Secuencia de acciones interrelacionadas y ordenadas en el tiempo que se utilizan para coordinar y controlar operaciones.
PROYECCIÓN	Predicción del comportamiento futuro basándose en el pasado sin el agrado de apreciaciones subjetivas.
PRONÓSTICO	La predicción del comportamiento futuro en el agregado de hechos concretos y conocidos que se prevé, influirán en los acontecimientos futuros.
CONTRO	Capacidad de ejercer o dirigir una influencia sobre una situación dada o hecho; es una acción tomada para hacer un hecho conforme a un plan.
RIESGO	Proximidad o posibilidad de un daño o peligro; o sea, cada uno de los imprevistos, hechos desafortunados que pueden tener un efecto adverso.

Una vez establecida estás definiciones, es importante establecer que para crear una estrategia adecuada es conveniente pensar en una política de protección en los distintos niveles que está debe abarcar y que no son ni más ni menos que los estudiados hasta aquí: física, lógica, factor humano y la interacción que existe entre todos estos factores.

En cada caso considerado, el plan de seguridad debe incluir una estrategia proactiva y otra reactiva (Benson, 2011). A continuación, se define en qué consiste cada una de ellas:

Estrategia proactiva (proteger y proceder) o de previsión de ataques: Conjunto de peso que ayuda a reducir el mínimo la cantidad de puntos vulnerables existente en las directivas de seguridad y que ayuda a desarrollar óptimamente planes de contingencia. La determinación del daño que un ataque va a aprovechar con un sistema y las debilidades y puntos vulnerables explotados durante este ayudará a desarrollar está estrategia

Estrategia reactiva (perseguir y procesar) o estrategia posterior al ataque: Ayuda al personal de seguridad evaluar el daño que ha causado el ataque, a repararlo o a implementar el plan de contingencia desarrollado en la estrategia proactiva, así como a documentar y aprender de la experiencia y a conseguir que las funciones comerciales se normalicen lo antes posible.

Con respecto a la postura que puede adaptarse ante los recursos compartidos tenemos los siguientes puntos a tomar en cuenta:

Tabla 4.

Puntos para tener en cuenta

Lo que no se permite expresarte está prohibido	Significa que la organización proporciona una serie de servicios bien determinados y documentados y cualquier otra cosa está prohibida.
Lo que no se prohíbe expresamente está permitido	Significa que, a menos de que se indique expresamente que cierto servicio no está disponible, todos los demás sí lo estaban.

Estás posturas constituyen la base de todas las demás políticas de seguridad y regulan los procedimientos puestos en marcha para implementarlas. Se dirigen a describir qué acciones se toleran y cuáles no. En la actualidad y "gracias" alas cada día más repetitivas y eficaces acciones que atenta contra los sistemas informáticos, los expertos se inclinan por recordar la primera política.

Finalmente, las políticas de seguridad informática (PSI) surgen como una herramienta organizacional para concientizar a cada uno de los integrantes de una entidad sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

De acuerdo con lo anterior, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

Grupo de elaboración de políticas para la seguridad informática:

Las políticas de seguridad informática tienen por objetivo fundamental, establecer las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de la tecnología de información (equipos de cómputo, sistema de información, redes, voz y datos) y de las personas que interactúan, haciendo uso de los servicios asociados a ellos, y se aplican sin excepción alguna, a todos los usuarios de cómputo de las empresas.

Las políticas de seguridad se elaboran de acuerdo con el análisis de riesgo y de vulnerabilidades en la dependencia de "las empresas". Por consiguiente el alcance de estas políticas se encuentra sujeto a "las empresas" las políticas son aplicables sin excepciones a todos los empleados de planta, los contratistas, los consultores, los colaboradores eventuales y otros empleados de "las empresas" incluyendo a todo el personal externo que cuente con un equipo conectado a la red de la organización. De igual manera, las políticas son aplicables también a todo el equipo y servicios (propietarios o arrendados) que de alguna manera tenga que utilizar local o remotamente la red a los recursos tecnológicos de las empresas; así como de los servicios e intercambios de archivos y de programas.

Así la elaboración de las políticas de seguridad, se fundamentan bajo la norma ISO/ IEC 17799, Además han sido planteadas, analizadas y recibidas con el objetivo de no contravenir con la garantía básica de los usuarios, y no pretende ser una "camisa de fuerza", imagen muestra una buena forma de operar los sistemas con seguridad, respetando en todo momento, los estatutos y los reglamentos internos de la empresa con dicha política de seguridad, se pretende garantizar:

Tabla 5.

Política de seguridad

El control de acceso (aplicaciones, base de datos, área del centro de cómputo o las sedes de " las empresas" filiales)
En el resguardo de la información
La clasificación y el control de los activos
La gestión de las redes (tanto de procedimiento de datos, cómo de transmisión de los mismos)
La gestión de la continuidad del negocio
La seguridad de la información en los puestos de trabajo
Los controles de cambios
La protección contra la instrucción en el software de los sistemas de información
El monitoreo de la seguridad
La identificación y la autenticación de los usuarios de los sistemas de información
La utilización de los recursos de seguridad
Las comunicaciones
La privacidad

Niveles de seguridad

Las políticas de seguridad informática (PSI) contribuyen las alarmas y compromisos compartidos en la organización que le permiten actuar proactivamente ante situaciones que comprometen la integridad. Por lo tanto, deben componer un proceso continuo irreal inventando qué observe la concientización, los métodos de acceso a la información, el monitoreo de cumplimiento y renovación, la aceptación de las directrices y la estrategia de implementación que lleven a una formulación de directivas institucionales que logran aceptación general (Bird, Gopal, Herberg, Kutten, Molva y Yung, 1993). Sin embargo, las políticas por sí sola no se tratan de una garantía para la seguridad de la organización; está debe responder a intereses y necesidades organizacionales basadas en la visión de negocio que lleven a un esfuerzo conjunto de sus actores para administrar los recursos y reconocer en los mecanismos de seguridad informática los factores que facilitan la formalización y materialización de los compromisos adquiridos con la organización.

Figura 31.

Seguridad

La tabla muestra los diferentes niveles de seguridad que las políticas de seguridad consideran en una red de computadores.

Tabla 6.

Concentrado de los diferentes niveles de seguridad en una red de computadoras

Concentrado de los diferentes niveles de seguridad en una red de computadoras	
Nivel de seguridad	Descripción
Nivel D1	El sistema entero no es confiable
Nivel C1	Protección de hardware
Nivel C2	Resuelve problemas del nivel C1 y C2
Nivel B1	Protección de seguridad y etiqueta
Nivel B2	Protección estructurada
Nivel B3	Dominio de seguridad
Nivel A	Diseño verificado

A continuación, se desarrollan cada una de las diferentes categorías de los niveles de seguridad, de acuerdo con la tabla.

Nivel D1: Muestra solo una división que se encuentra reservada para los sistemas que han sido ya evaluados y no cumple con ninguna especificación de seguridad; con estos no hay protección para el hardware, el sistema operativo es inestable y no hay autentificación con respecto a los usuarios y a sus derechos en el acceso a la información. MS-DOS y System 7.0 Macintosh responde este nivel.

Nivel C1 (protección discrecional): Se requiere la identificación de los usuarios para el acceso a distinta información. Causar yo puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quién tiene control total. Muchas de las tareas cotidianas de administración del sistema solo pueden ser realizadas por este superusuario, quién tiene la gran responsabilidad en la seguridad. Con la filosofía del actual de centralización de los sistemas de cómputo, no es raro que en una organización se encuentre dos o tres o más personas cumpliendo este rol; esto en la práctica, es un problema, pues no hay forma de

distinguir entre los cambios que hizo cada uno. A continuación, se enumeran los requerimientos mínimos que debe cumplirse en la clase C1:

Tabla 7.

Clase C1

Acceso de control discrecional (distinción entre usuario y recursos)	Se podrán definir grupos de usuarios (con los mismos privilegios) y grupos de objetos (archivos, directorios, discos) sobre los cuales podrán actuar los primeros
Identificación y autenticación	Se requiere que un usuario se identifique antes de comenzar a ejecutar acciones sobre el sistema. El dato de un usuario no podrá ser accedido por un usuario sin autorización y sin identificación

Nivel C2 (protección de acceso controlado): Este subnivel fue diseñado para solucionar las debilidades del C1. Cuenta con características adicionales que crean un ambiente de acceso controlado. Se debe llevar una auditoría de acceso e intentos fallidos de acceso a los objetos. Se tiene la capacidad de restringir aún más la actividad de los usuarios a que ejecuten ciertos comandos obtenga acceso a determinados archivos; además de permitir o denegar datos a usuarios en concreto con base no solo a los permisos, sino también en los niveles de autorización. Dicha Victoria es utilizada para llevar registros de todas las acciones relacionadas con la seguridad; por ejemplo, las actividades afectadas por el administrador de sistema y los usuarios.

La mayor desventaja reside en los recursos adicionales requeridos por el procesador y el subsistema de discos. Los usuarios de un sistema C2 tienen la autorización para realizar algunas tareas de gestión de este sin necesidad de ser administradores.

Por su parte, permite llevar mejor cuenta de las tareas relacionadas con la administración del sistema, ya que es cada usuario quién ejecuta el trabajo.

Nivel B1 (seguridad etiquetada): Dichos subnivel es el primero de los tres con qué cuenta el nivel B. Soporta seguridad multinivel como la secreta y la Ultra secreta. Se establece que el dueño del archivo no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio. A cada objeto del sistema se le asigna una etiqueta con un nivel de seguridad jerárquico (de alto secreto o de secreto, reservado) y con ciertas categorías (contabilidad, nóminas, ventas, etcétera). Traducir yo que accede a un objeto debe poseer un permiso expreso para hacerlo y viceversa; es decir, traducir yo tiene sus objetos asociados. También se establecen controles para limitar la propagación de derecho de acceso a los distintos objetos.

Nivel B2 (Protección estructurada): Requiere qué es etiqueta de cada objeto de nivel superior por ser "padre" de una inferior. La protección estructurada es la primera que empieza a referirse al problema de un objeto a nivel más elevado de seguridad en comunicación con otro a nivel inferior. Así, por ejemplo, un disco duro será etiquetado por almacenar archivos que son accedidos por distintos usuarios. El sistema es capaz de alertar a los usuarios y sus condiciones de accesibilidad y seguridad son modificadas; y el administrador es el encargado de fijar los canales de almacenamiento y ancho de banda a utilizar por aquellos.

Nivel B3 (Dominio de seguridad): Refuerza los dominios con la instalación del hardware; por ejemplo, el de administración de memoria se usa para proteger el de seguridad de acceso no autorizado a la modificación. Existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las admite y las niegas según las políticas de accesos que se hayan definido con atención. Todas las estructuras de seguridad deben ser lo suficientemente pequeñas como para permitir análisis y pruebas ante posibles violaciones.

Este nivel requiere que la terminal del usuario se conecta al sistema de manera segura. Además, cada uno tiene asignado los lugares y objetos a los que puede acceder.

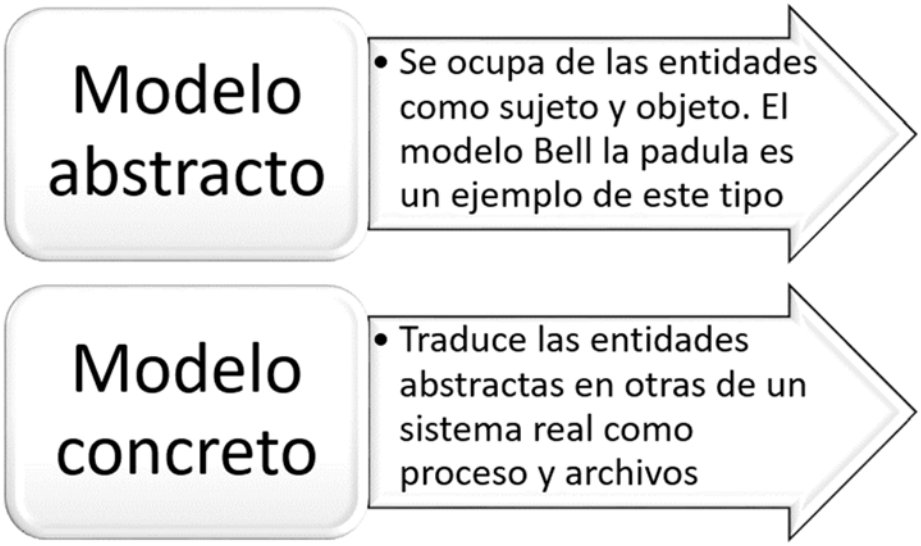
Nivel A (Diseño verificado): Es el nivel más elevado; incluye un proceso de diseño, control y verificación mediante métodos formales (matemáticos) para asegurar la totalidad de los procesos que realiza un usuario sobre el sistema. Para llegar a este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse. El diseño requiere ser verificado de forma matemática y también se debe realizar análisis de canales encubiertos y de distribución confiable. En conjunto, el software y el hardware son protegidos para evitar infiltraciones ante traslados o ante movimientos del equipamiento.

Esquemas y modelos de seguridad

"modelo de seguridad en la presentación formal de una política de seguridad. El modelo debe identificar el conjunto de reglas y prácticas que regulan como un sistema maneja. Protege y distribuye información delicada" (López Barrientos y Quezada Reyes, 2006). De acuerdo con esto, los modelos se clasifican en:

Figura 32.

Esquemas y modelos de seguridad



Esquemas y modelos de seguridad: Además, dichos modelos sirven para tres propósitos en la seguridad informática:

1. Prever un sistema que ayude a comprender los diferentes conceptos. Los modelos diseñados para este propósito usan diagramas, analogías, cartas. Un ejemplo en la matriz de acceso
2. Proveer una representación de una política general de seguridad formal y clara
3. Expresar la política exigida por un sistema de cómputo específico

Para determinar si un modo de acceso específico está permitido, se compara la acreditación de un sujeto con la clasificación del objeto (de manera precisa, la combinación de la clasificación y el conjunto de comportamientos). El esquema de clasificación acreditación se expresa en términos de un retículo.

El modelo define dos reglas de control de acceso mandatorio (MAC) y una regla de control de acceso discrecional (DAC) con tres propiedades:

Tabla 8.

Propiedades

Propiedad de seguridad simple	Un sujeto de un determinado nivel de seguridad no puede leer un objeto perteneciente a otro más alto
Propiedad estrella	(También llamada propiedad de confinamiento). Un sujeto de un determinado nivel de seguridad no puede escribir un objeto perteneciente a otro más bajo
Propiedad de seguridad discrecional	Se utiliza una matriz de acceso para especificar el control de acceso discrecional

Por medio del modelo Bell lapadula, los usuarios pueden crear contenido solo en su nivel de seguridad y por encima; es decir, los investigadores en el nivel secreto para crear archivos secretos o súper secretos, pero no archivos públicos. De forma inversa, los usuarios pueden ver solo contenidos de su propio nivel inferior.

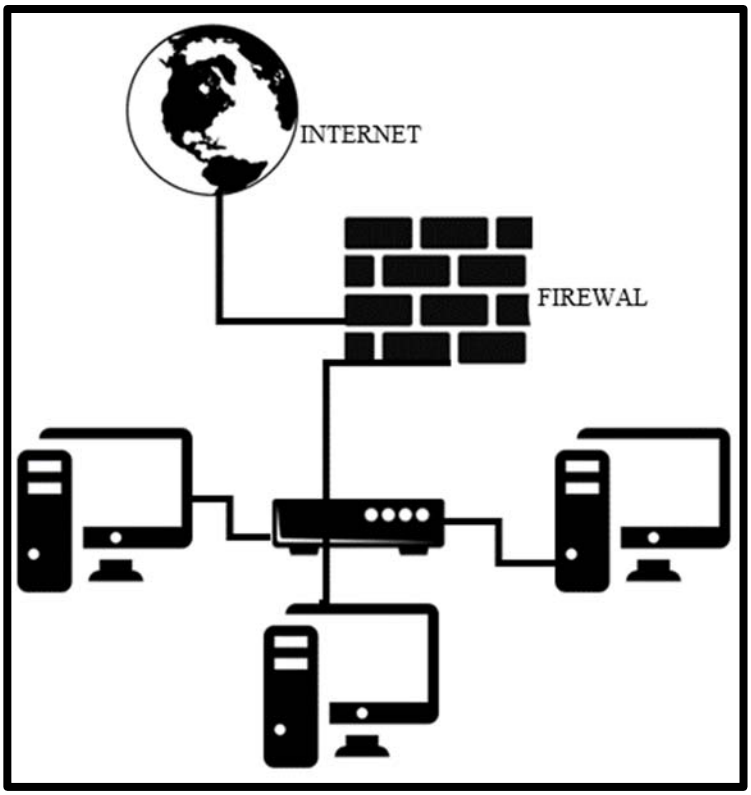
El principio de tranquilidad del modelo de Bell lapadula Establece que la clasificación de un sujeto u objeto no cambia mientras se encuentre referenciada hay 2 formas para este principio: la fuerza establece que los niveles de seguridad no cambian durante la operación normal del sistema y la débil determina qué los niveles de seguridad no cambian de ninguna manera; por lo tanto nunca violaran la regla de una política de seguridad.

La promoción de una cultura de seguridad requiere tanto un liderazgo fuerte como una participación amplia para garantizar que se le otorgue un carácter de prioritario a la planificación y administración de la seguridad. Así como la comprensión de la necesidad de que sea plena entre todos los principiantes. Los aspectos de seguridad deberían ser objeto de interés y responsabilidad

a todos los niveles de la administración de la red de seguridad, la empresa, así como para todos los participantes.

Figura 33.

Administración de la red de seguridad

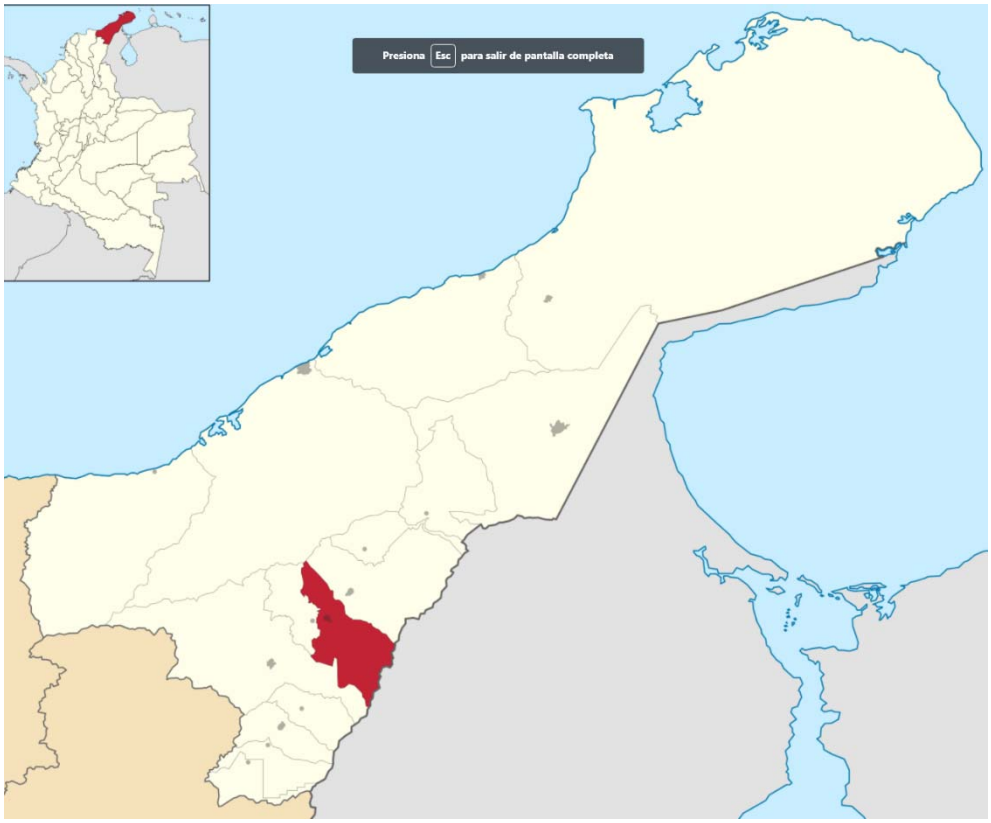


2.5 Marco Geográfico

2.5.1 Ciudad de Fonseca, La Guajira

Figura 34.

Ciudad de Fonseca, La Guajira



Nota: La figura expone la ubicación geográfica donde se desarrolló la investigación y por ende del trabajo de campo teniendo en cuenta los objetivos planteados en el objeto de estudio. Tomado de Alcaldía de Fonseca (2021).

Según Alcaldía de Fonseca (2021) es un municipio colombiano ubicado en el departamento de La Guajira, sobre una depresión en el valle del río Ranchería que atraviesa el municipio de oeste a este, entre la Sierra Nevada de Santa Marta y la Serranía del Perijá. Es importante destacar que el Instituto Cristo Rey, está ubicado en la Calle 13 N 3 45 SDA A Barrancas, Fonseca, la Guajira,

en al cuales se aplicaron los instrumentos de recolección de información por medio del trabajo de campo.

2.6 Marco Institucional

2.6.1 Instituto Cristo Rey

Las Fundadoras del Instituto Cristo Rey han sido incluidas en el libro de empresarios exitosos, testimonio vivo de emprendimiento escrito por el Doctor José Ceferino Nieves Orozco que incluye en su libro 42 empresas exitosas en el Cesar y La Guajira donde aparecen Gala García Brito y Blanca fuentes de Aragón con sus respectivas biografías (Instituto Cristo Rey, 2021, p.1).

Amigas inseparables egresadas de la normal de señoritas de Santa Marta, han dedicado toda su vida a la educación de la comunidad fonsequera inicialmente en la institución educativa Vicente Roig y Villalba(Instituto Cristo Rey,2021,p.1).

Por causas adversas tuvieron que separarse por asuntos de familias y laborales decidiendo al reencontrarse trabajar por la construcción de un ambiente educativo más sano y menos limitado a las condiciones burocráticos de los gobiernos de turno. Fue así cuando el 13 de febrero del año de 1986 abrieron las puertas del Instituto Cristo Rey en Fonseca la Guajira propendiendo por una mejor educación que llenara las expectativas de familias que buscaban la calidad en un servicio tan rezagado por el olvido en esta parte del país(Instituto Cristo Rey,2021,p.1).

Desde el lanzamiento de la primera promoción de bachilleres en el año de 1991 se ha venido demostrando que esos esfuerzos han dado los resultados previstos posicionando al Instituto Cristo Rey en los más altos estándares de calidad a nivel regional lo cual las ha hecho merecedoras de varios reconocimientos y que sean catalogadas como empresarias exitosas como lo expresa el autor José Ceferino Nieves en su más reciente libro “empresarios exitosos, testimonio vivo de

emprendimiento" el cuál es una obra bibliográfica que reúne a los principales personajes que contribuyen al desarrollo económico y social de la región con empresas que continúan vigentes a través de la innovación y son generadoras de empleo y sostenibilidad(Instituto Cristo Rey,2021,p.1).

2.7 Marco Contextual

Partiendo de las necesidades presentadas por la institución se procederá con el análisis de vulnerabilidades de seguridad perimetral, esto permitirá generar la propuesta de mejora a entregar. Los conocimientos que aplicaremos para llegar a dicha propuesta parten de las bases del área de seguridad informática en la ingeniería de sistemas y telecomunicaciones. Empezaremos el proceso con un levantamiento de activos, que consiste observar y hacer una lista de todos los recursos con los que cuenta la Institución. Una vez se tiene este pasamos al proceso de clasificación, que tiene como objetivo segmentar los activos para determinar los controles específicos que deben ser aplicados, la determinación de los controles que se aplican se hace también teniendo en cuenta un análisis diferencial de los activos, estudiando cada uno a fondo para identificar las falencias que presenten. Todos estos procesos son el conjunto necesario que fundamentan el plan de mejora a desarrollar y que permita motivar y convencer a todos sus directivos de lo necesario que es contar con un estudio con estas características, que les brinda la información sobre sus activos y de cómo protegerlos.

En nuestra propuesta impulsaremos a implementar principalmente los siguientes aspectos de los sistemas de seguridad:

Controles de acceso: La información contenida en los servidores de la institución es de carácter privado y su uso, destrucción o divulgación no autorizada conlleva a sanciones legales, es por eso por lo que es necesario asegurar la información, se deben establecer políticas de acceso.

Permisos por roles y perfiles: Se debe contar con un sistema de directorio activo que permita la segmentación de permisos de acceso a la información por roles y perfiles de acceso, dependiendo el área al cual pertenezca el empleado, permitiendo definir el manejo ya sea de escritura, lectura o ambas dado el caso.

Aseguramiento de sistemas operativos: Es una herramienta práctica que a futuro permite minimizar inconvenientes, algunas ventajas que ofrece el Hardening y una de las más importantes es la disminución de incidentes de seguridad. También se busca mejorar el rendimiento de los dispositivos tras eliminar cargas inútiles en el sistema como programas y servicios que vienen instalados por defecto.

Aseguramiento de la red: Asegurar por medio de controles de configuración la red interna. Para realizar dicho aseguramiento se tomará como base el modelo OSI que nos permitirá identificar las diferentes capas y con esto establecer un control de aseguramiento a la red partiendo desde la parte de aplicación desde la parte más importante hasta la capa física.

3. Estado de Arte

En el entorno de las redes de computadoras, un objetivo prioritario es entender la situación de un medio ambiente interconectado en el ámbito de los negocios para fomentar la seguridad informática es decir, en este punto se debe presentar a los usuarios/clientes del sistema de panorama general , considerando las implicaciones económicas y estratégicas para las empresas actuales.

Igualmente es primordial identificar los aspectos relevantes sobre la vulnerabilidad de los sistemas informáticos y conocer la funciones, métodos y procedimientos que se emplean para la creación de los esquemas de seguridad para que sea posible actualizar y formar especialistas en seguridad informática que desarrollan habilidades en el planteamiento en soluciones factibles de administración, diseño gestión y operación de sistemas de seguridad.

Muchos son los peligros a los que están expuestas una organización, en la última década los delitos informáticos han acaparado atención especial ocasionando pedidas económicas multimillonarias en 2020, se batió un triste record de generación de software nocivo con cerca de 30 millones de nuevas muestras.

Por otro lado, datos de ese mismo año establecieron que las organizaciones recibieron un ataque de software malicioso cada tres segundos, lo cual representa 300.000 ataques diarios de este tipo a nivel mundial; cifras que han aumentado hasta la actualidad (Rico, 2020, p.145).

Hoy en día, las personas que participan en estos actos delictivos son cada vez más profesionales además cuenta con significativos cursos financieros y una amplia experiencia en Tecnología de la información y delas Comunicaciones (TIC), herramientas que los hace capaces

de atacar a las organizaciones sin discriminación alguna, sin importar el tamaño o el giro de esta, hace años , los ataques eran generalizados y su objetivo radicaba en causar solo daño al equipo de cómputo o la red de computadoras.

En la actualidad, el interés principal de los delincuentes cibernéticos está enfocado al robo de información secreta o confidencial de una organización especifica (lo que se ha llamado ataque dirigido considerado uno delos tipo más peligrosos de amenazas), la filtración de esa formación estratégica, confidencial o secreta genera perdías importantes.

Según información recopila por analistas de B2B internacional y Kaspersky dichos incidentes pueden llegar a costarle a una organización hasta dos millones de euros en promedio, de esa cantidad, 1.7 millones, se relacionan al incidente en forma de pérdidas derivadas de filtraciones criticas de datos, interrupción de la operación empresarial y gastos pro servicios especializados de reparación.

Además, las organizaciones enfrentan un costo aproximado de 200.000 en euros por las medidas que deben implantar para impedir que esas acciones de intrusión y robo de información se presenten al actualizar software y hardware , contratar y capacitar al personal por su lado, las pérdidas provocadas por ataques dirigidos a las pequeñas y medianas empresas (PUME) son notablemente más bajas, aunque el monto financiero sigue siendo alto alrededor de 88.00 euros de los cuales de 68.000 euros están destinados a la reparación del ataque ,mientras que el resto se dirige a las prevención de posibles daños en el futuro inmediato.

Para los criminales cibernéticos, las empresas que se convierten en el blanco perfecto son aquellas que no protegen sus recursos informáticos, ni colaboradores tanto dentro como fuera de la organización , en especial , las instituciones donde el uso de dispositivos inteligentes ha crecido

sin control ni se han implantado estrategias y medidas de seguridad; por ejemplo la policía cibernética mexicana ha recibido más de 19 mil denuncias relacionadas con algún tipo de amenaza informática, de las cuales 55% corresponde a reportes de software malicioso y 40% se relaciona con el reclamo de fraudes derivaos al comercio electrónico, la ciudad de México así como las regiones de Puebla, Nueva León , Jalisco y el Estado de México se encuentran ente las entidades mexicanas que han registrado la mayor cantidad de estos actos delictivos (Rico,2020,p. 146).

A medida de que el rendimiento y las funciones en los lugares de trabajo, educación y ocio, se aproximan al uso de las computadoras de escritos y portátiles, se hace todavía más fácil diseñar y propagar los programas maliciosos para dichos dispositivos móviles, pues , de acuerdo con un estudio realizado por Kaspersky en 2020 , se detectaron 145.000 nuevos programas de índole maliciosa tal solo para dispositivos móviles (el doble que se reporta en 2019), cuyo principal objetivo era robar dinero a los usuarios, por eso es muy importante destacar que el crecimiento de las publicidad como amenaza para los usuarios móviles se triplico en el último año , donde uno de cada cinco avisos web en los Smartphone redirecciona hacia programas maliciosos para dichos dispositivos según reporta la empresa Blue Coat Systems, la cual indica que los anuncios web han superado incluso a la pornografía como la forma más común en que las personas se encuentran ante una amenaza de software malicioso aunque esta no alcanza ni 1% de todo el contenido solicitado, en comparación, los anuncios de internet registran 12% de contenido solicitado con 20% de tasa de infección.

Los datos significan que hoy en día el usuario es el eslabón más débil que existe en la cadena de la seguridad porque los sistemas protegen a los teléfonos, celulares pero no a las personas que inadvertidamente dan acceso a los ataques atreves de trucos burdos y bastante

trillados como el otorgamiento de “premios “o la descarga de aplicaciones no autorizados por tiendas oficiales.

Internet denominada también como la red de rede, se ha convertido en un fenómeno que ha revolucionado la sociedad en la última década en especial en la pandemia donde más se ha utilizado por la necesidad de trabajo, en la actualidad tanto las organizaciones como las personas a nivel mundial utilizan las computadoras envían y reciben correos electrónicos comparten información de4 manera local o a nivel mundial realizan operaciones y transacciones ; ofrecen productos, bienes y servicios y encuentran soluciones a sus requerimientos , es así que la información se vuelve algo muy preciado tanto para los usuarios como para los intrusos por ello se debe tener una serie de precauciones para evitar que alguien no deseado busque datos relevantes en la información delas organizaciones y las personas como presa fácil de extorsiones , fraudes y pérdidas irreparables (Anderson, 2020,p.147).

De los muchos factores que han convergido en este nuevo fenómeno para catapultarlo de forma masiva a la sociedad actual, se pueden destacar tres principales:

Figura 36.

Factores

Desde un punto de vista sociológico, en cualquier grupo social un cierto porcentaje de la población posee conductas malévolas en 2020, internet alcanzo más de 500 millones de computadoras conectadas, sumando un total estimado de un billón de usuarios en todo el mundo, si tan solo 1% de la población pertenece a dicho sector, se tiene casi un millón de posibles atacantes (Anderson, 2020, p.147).

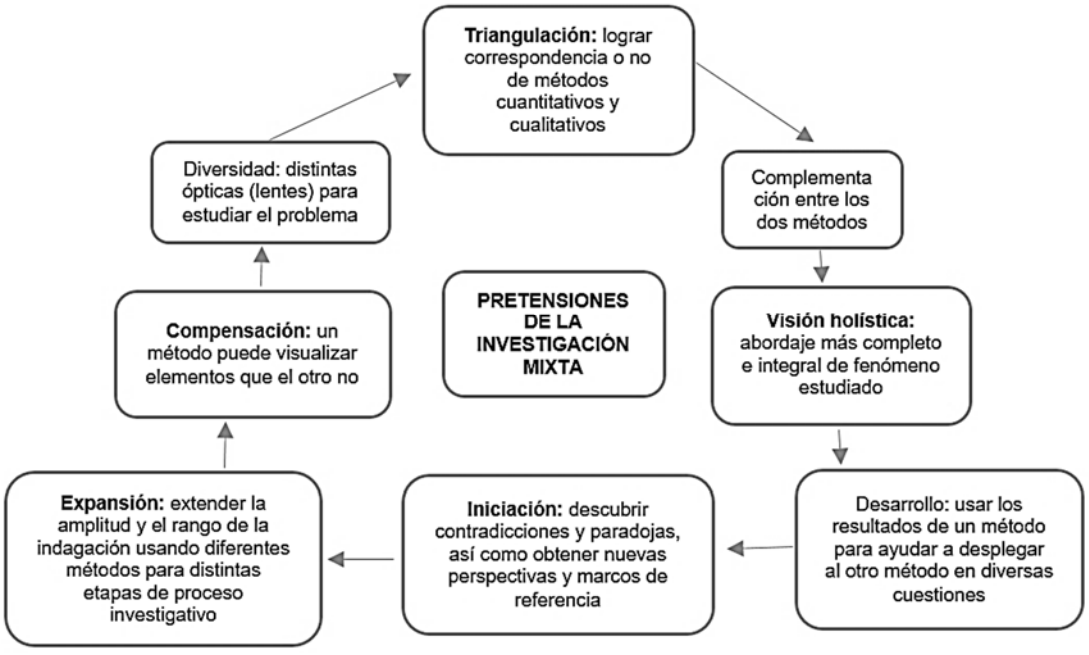
4. Marco Metodológico

En el actual apartado se define el alcance que tiene la actual investigación, y determina la forma en que se realiza, como también elementos relacionados e implementados para la metodología utilizados para el desarrollo de la investigación, de igual forma se dará una explicación de las fases que se involucraron en la recolección de los datos, el diseño de la propuesta y el análisis de los resultados para llegar finalmente a la generación de las conclusiones de la investigación. Tal como se explica a continuación.

4.1 Tipo de investigación

Figura 37.

Investigación mixta



Teniendo como base en el estado del arte la Metodologías MARGERIT para gestionar los riesgos de la información. Esta metodología fue creada por el consejo superior de administración electrónica con una actualización en el año 2012 para su versión número Tres.

1. Determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de qué perjuicio o coste supondría su degradación.

2. Determinar a qué amenazas están expuestos aquellos activos.

3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.

4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia de la amenaza.

4.1.1 Herramientas

Por lo general los análisis de riesgo conlleva considerar una gran cantidad de activos, y a cada uno de estos les corresponde un sinnúmero de amenazas y salvaguardas, por ello resulta un arduo trabajo manipular tal magnitud de información y es por esta razón que se han desarrollado herramientas de apoyo de análisis de riesgos que cumplen ciertos requisitos:

1. Permiten trabajar con un conjunto amplio de activos, amenazas y salvaguardas.
2. Permiten un tratamiento flexible del conjunto de activos para asemejar al modelo real de la organización.
3. Demostrar resultados cercanos a la realidad.

4.1.2 Pilar

"Procedimiento Informático Lógico para el Análisis de Riesgos" es una herramienta desarrollada para soportar el análisis y la gestión de riesgos de sistemas de información siguiendo la metodología MAGERIT Creado por el Centro Nacional de Inteligencia, actualmente se encuentra disponible la versión 6.2.6.

Analiza los riesgos en varias dimensiones:

a. Confidencialidad, integridad, disponibilidad, autenticidad y
b. Trazabilidad. Para tratar el riesgo se proponen: salvaguardas

O contramedidas, normas y procedimientos de seguridad.

Esta herramienta soporta las fases del método MAGERIT:

a. Caracterización de los activos: identificación, clasificación, dependencias y valoración
b. Caracterización de las amenazas
c. Evaluación de las salvaguardas

Evalúa el impacto y el riesgo, acumulado y repercutido, potencial y residual, presentándolo de forma que permita el análisis de por qué se da cierto impacto o cierto riesgo. Las salvaguardas se califican por fases, permitiendo la incorporación a un mismo modelo de diferentes situaciones temporales. Se puede incorporar el resultado de los diferentes proyectos de seguridad a lo largo de la ejecución del plan de seguridad, monitorizando la mejora del sistema. Pilar presenta los resultados en varias formas, ya sea en informes RTF, gráficas o tablas que se pueden agregar a una hoja de cálculo, logrando elaborar diferentes tipos de informes y presentaciones de los resultados.

Finalmente, la herramienta calcula calificaciones de seguridad respecto a normas ampliamente conocidas, como son UNE-ISO/IEC 27002:2009: sistemas de gestión de seguridad, RD 1720/2007: datos de carácter personal y RD 3/2010: Esquema Nacional de Seguridad. Cabe destacar que esta herramienta incorpora tanto los modelos cualitativos como cuantitativos, logrando alternarse entre estos para extraer el máximo beneficio de las posibilidades teóricas de cada uno de ellos" (Molina &Miranda, 2017, p.3-4)

4.2 Tipo de estudio

Basado en un estudio descriptivo, ya que se ocupa de la descripción de las características que identifican los diferentes elementos y componentes, y su interrelación, permitiendo aclarar términos y de delimitar hechos relacionados con el problema. Además este tipo de estudio posibilita el establecer características demográficas de la población investigada, identificar el comportamiento y conducta con qué procede, a través de la construcción de un marco teórico, que facilita su posterior análisis, sin llegar a controlar el fenómeno, según se da naturalmente, pues es de gran envergadura.

4.3 Método de investigación

El tipo de método utilizado se encuentra ligado al tipo de estudio que se desarrolla en esta investigación; bajo esta premisa el método desarrollado, es el método de análisis, puesto que conoce la realidad objetivamente, identificando las partes que conforman el todo (Objeto de estudio), y permitiendo conocer las causas y efectos de las mismas.

4.4 Fuentes de recolección de información

Se utilizó unas fuentes primarias, tal como el Instituto Cristo Rey. Por otro lado las fuentes secundarias utilizadas, se encuentran las siguientes:

1. Dirección y Coordinación Instituto Cristo Rey
2. ADALID
3. 2Secure S.A.S.

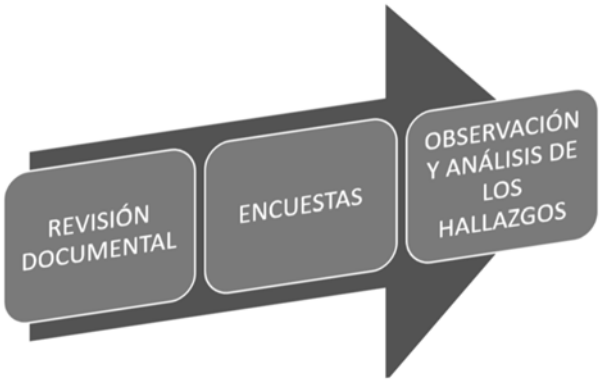
Finalmente las fuentes terciarias utilizadas fueron:

1. Biblioteca Nacional
2. Biblioteca Pública El Tintal Manuel Zapata Olivella
3. Bibliored
4. Internet, Páginas web, debidamente mencionados en la ciber grafía.

4.5 Técnicas de recolección de información

Figura 38.

Técnicas de recolección de información



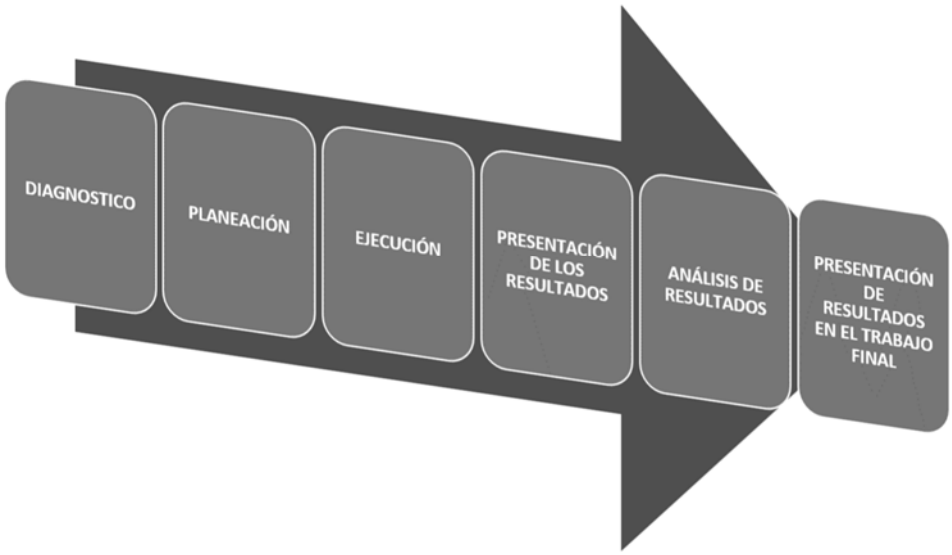
Básicamente se utilizaron 3 instrumentos; el primero es la revisión documental, la cual consistió en la consulta de libros, boletines, revistas, páginas web entre otros medios. En cuanto al segundo instrumento se realizó por medio del trabajo de campo, una serie de encuestas al personal del Instituto Cristo Rey. Es importante destacar que por medio del consentimiento informado se logró enviar el link a la muestra obtenía, para esta técnica de recolección de información.

Finalmente el tercer instrumento consistió en la observación y análisis de los hallazgos obtenidos a través del trabajo de campo en la población y universo plasmado.

4.6 Fases de la investigación

Figura 39.

Fases de la investigación



Diagnostico

Se observan que existen muy pocas investigaciones que involucren el mejoramiento del sistema de seguridad informática y perimetral en Instituciones Educativas. El Instituto Cristo Rey, reconoce la información como un activo de alta importancia que apoya los procesos críticos de la parte administrativa y financiera de la misma, por lo cual ha manifestado la necesidad de implementar controles perimetrales con el fin de minimizar los riesgos de perdida de información y a su vez garantizar confidencialidad, integridad y disponibilidad de los activos y la información que procesa, almacena o crea para cumplir su objetivo misional.

Por otro lado con los controles que se sugerirán en el desarrollo de este proyecto, se pretende minimizar el riesgo de pérdida de información y asegurarla con dispositivos, configuraciones de defensa perimetral, además de inspeccionar el uso y accesos hacia internet. Al proporcionar dichos controles se tratará de garantizar que las aplicaciones cuenten siempre con los recursos de red que necesitan y que se mitigue el impacto ante posibles ataques y pérdida de información.

Planeación

Después de obtener un diagnóstico sobre la situación, se procede a diseñar el planteamiento del problema, con su debida formulación; enumerando los principales objetivos que se pretendían encausar y con los cuales enmarca este estudio, además de plantear la debida justificación que argumenta la importancia de la realización de este proyecto. También se ejecutó una metodología a través de la cual se pudo obtener información en este proyecto consignada, bien sea de primera, segunda o tercera fuente; dentro de esta metodología se hizo la planeación de las siguientes actividades, que también se pueden apreciar en el cronograma:

1. Solicitar el permiso del Instituto Cristo Rey, por medio del consentimiento informado
2. Listado de activos de la información de las diferentes áreas de la institución educativa, en donde se presente análisis de los riesgos de los activos identificados
3. El análisis de los activos de la información resumidos en la matriz de riesgo establecida demostrando los riesgos que se presentan detalladamente en cada uno.
4. Plan de mejora para la seguridad perimetral de la institución educativa, el cual incluye todos los elementos sugeridos para mitigar los riesgos que se presentaron en el ítem anterior incluyendo un mapa de red propuesto a futuro donde se incluirían dichas mejoras.

5. Asistir a las bibliotecas públicas para recolectar la información tales como: Biblioteca Nacional, Biblioteca Pública el Tintal Manuel Zapata Olivella y el alquiler de material físico por medio de la página de Biblored.
6. Creación del formato de encuesta por medio de la página encuestas.com.
7. Envío del link a la muestra obtenida
8. Clasificación de la información y eliminación de la información inútil
9. Análisis y presentación de resultados
10. Redacción del proyecto final

Ejecución

En esta fase, se colocó en práctica toda y cada una de las actividades planeadas con antelación, siendo consecuente y constantes en la búsqueda de la información, se halla la fase de ejecución o puesta en marcha, como el motor del estudio ya que fue a través de ella que se desencadeno toda la argumentación del problema investigado. Durante el desarrollo se presentaron distintas dificultades, por tanto en muchas ocasiones los horarios de acceso o atención Imposibilitaron algunos de estos lugares, como también las restricciones por el COVID-19. Finalmente se puede destacar que hay material delicado idóneo para esta investigación; la cual no fue autorizada debidamente. Por ende se logró desarrollar el trabajo de campo a través de algunos informes, analizar y estudiar el objeto de estudio planteado.

Presentación de los resultados

Después de haberse recopilado el material pertinente para esta investigación y una vez estuviera clasificado, se procede a presentar los resultados obtenidos, en donde se observó la necesidad de realizar cuadros, diagramas e imágenes y, en los que se indican el número de informes

a través de entrevistas y la tabulación de la recolección de información obtenida por medio de los instrumentos planteados. Finalmente es importante destacar que se presentan los hallazgos de la investigación, de manera consistente y verídica con el fin de desarrollar los objetivos expuestos.

Análisis de resultados

Con base en el marco referencial y en los resultados que en él se presentan, se produce el análisis del objeto de estudio, que da pie a la formulación de conclusiones del proyecto, después de haber realizado un exhaustivo trabajo de investigación.

Presentación de resultados en el trabajo final

Consiste en la presentación del informe final escrito al auditorio con su debida sustentación.

4.7 Población y Universo

La actual investigación cuenta con universo conformado por los estudiantes, directivos y administrativos en las cuales han tenido riesgos cibernéticos y por ende de seguridad informática. El Instituto Cristo Rey cuenta en la actualidad con 600 estudiantes y en la parte administrativa el personal es de 86 individuos. Es importante destacar que mediante el universo de esta investigación se logró tener la muestra y por ende ejecutar el trabajo de campo en las instalaciones.

4.8 Muestreo

Es importante destacar que el muestreo se desarrolló a través de la fórmula maestral; el cual consiste calcular la muestra exacta para aplicar el instrumento de recolección de información encuesta.

1. **Tamaño de la población Año (2021):** 686
2. **Porcentaje de confiabilidad :** 95%

3. **Formula de muestreo :** = Z2 * (p) * (1-p) / c2
4. **Porcentaje error** = 5%
5. **c = Margen de error** (.04 = ±4)
6. **Resultado Muestreo :** 247 Unidades

Como se puede observar a través de la fórmula de muestreo, arrojó como resultado 247 unidades, a las cuales se les aplicó el instrumento de recolección de información encuesta; a través de la plataforma encuestas.com. Por otro lado el porcentaje de confiabilidad es del 95%, porcentaje de error 5% referente al tamaño de la población del año 2021 con un total de 686.

4.9 Variables

1. Controles de seguridad en la red para disminuir el riesgo y posibles sabotajes, robos de información y caídas del sistema.
2. Controles de acceso a contenidos y navegación en internet.
3. Controles de acceso a la red Wifi.
4. Implementar un nivel medio/alto de seguridad en los hosts.
5. Segmentar la red de la institución educativa para aumentar las opciones de seguridad.

4.10 Cronograma de actividades

Tabla 9.

Cronograma de actividades

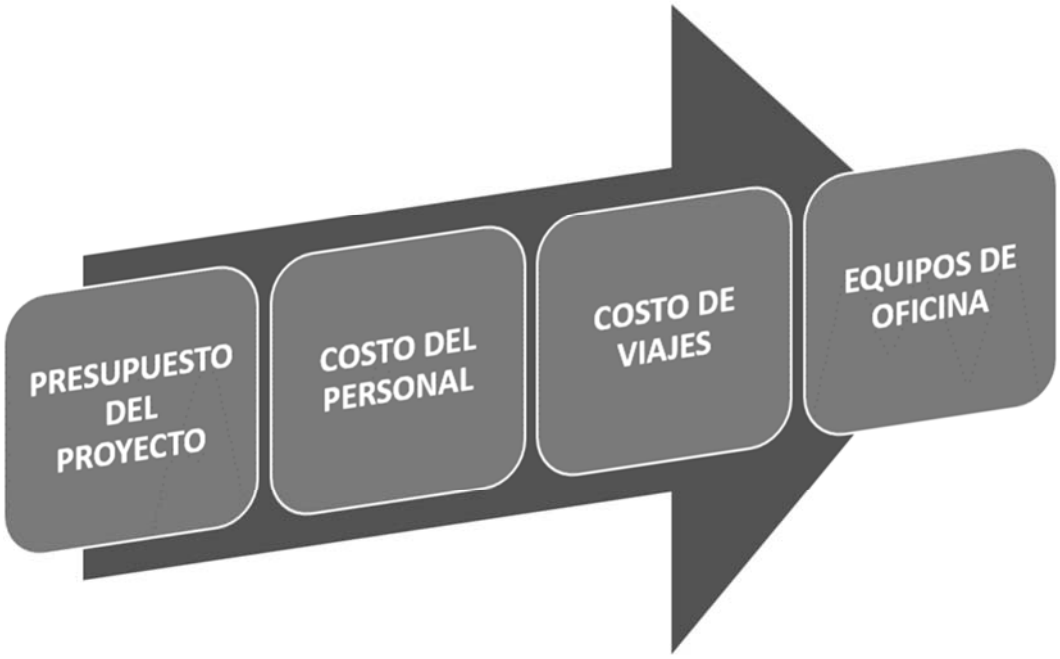
ACTIVIDADES	TIEMPO																											
	Enero /febrero				Marzo / abril				Mayo /junio				Julio / agosto				Septiembre /octubre				Noviembre / diciembre			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Solicitar el permiso del Instituto Cristo Rey, por medio del consentimiento informado																								
Listado de activos de la información de las diferentes áreas de la institución educativa, en donde se presente análisis de los riesgos de los activos identificados																								
El análisis de los activos de la información resumidos en la matriz de riesgo establecida demostrando los riesgos que se presentan detalladamente en cada uno.																								
Plan de mejora para la seguridad perimetral de la institución educativa, el cual incluye todos los elementos sugeridos para mitigar los riesgos que se presentaron en el ítem anterior incluyendo un mapa de red propuesto a futuro donde se incluirían																								

dichas mejoras.	
Creación del formato de encuesta	
Envío del link a la muestra obtenida	
Clasificación de la información y eliminación de la información inútil	
Análisis y presentación de resultados	
Redacción del proyecto final	

4.11 Aspectos administrativos

Figura 40.

Aspectos administrativos



4.11.1 Presupuesto del proyecto

Tabla 10.

Presupuesto del proyecto

Rubro	Costo en pesos	% Sobre el total del proyecto
Personal	$1.950.000	82,80%
Viajes	$984.000	6,37%
Material de trabajo y equipo de oficinas	$250.000	10,62%
Administrativos	$5.000	0,21%
Total	$8.184.000	100%

4.11.2 Costo del personal

Tabla 11.

Costo del personal

Dedicación	Funciones	Meses	Honorarios		Subtotales
			Monto	Total	
2 horas semanales	Investigar en las fuentes la información	22	57.500	1.258.400	1.258.400
1 hora semanal	Redacción de documento	22	31.436	691.600	691.600
Total					1.950.00
Porcentaje					82,80%

4.11.3 Costo de viajes

Tabla 12.

Costo de viajes

Viaje Nº	Destino	Nº Días	Nº Personas	Viáticos		Pasajes			Total por viaje
				Monto por día	Total	Aéreos		Terrestre	
						Costo por pasaje	Total		
1	Instituto Cristo Rey (2021).	2	1			246.000	492.000		70.000
2	Instituto Cristo Rey (2021).	2	1			246.000	492.000		80.000
Total									150.00
Porcentaje							$984.000		6,37%

4.11.4 Equipos de oficina

Tabla 13.

Descripción del material	Costo			Observaciones
	Unidad	Nº de unidades	Total	
Lápiz	600	1	600	Tomar apuntes
Esfero	800	1	800	Tomar apuntes
Hojas	50	20	1.000	Tomar apuntes
Fotocopias	100	260	26.000	Libros de investigación
Impresiones	250	380	95.000	Prestación de documentos de investigación
Internet	1.200	70	84.000	Internet investigación

Otros	42.600	Demás materiales
Total	250.000	
Porcentaje	10,62%	

Es importante destacar que dentro de los aspectos administrativos , se tuvo en cuenta el presupuesto del proyecto , costo personal , costo de viajes , equipos de oficina las cuales tuvieron gran importancia para la ejecución del actual proyecto ; teniendo en cuenta desde los mínimos gastos requeridos para la investigación , como también para la originalidad , confiabilidad y viabilidad del proyecto. No obstante estos aspectos administrativos tuvieron inicio desde el mes de Julio del presente año (2021).

5. Resultados

5.1Realizar una revisión bibliográfica sobre el objeto de estudio planteado.

Teniendo en cuenta el objeto de estudio planteado, se desarrolló la siguiente revisión bibliográfica sobre algunas Instituciones Educativas que han aplicado un mejoramiento en el sistema de seguridad informática y perimetral en Colombia. Por otro lado es importante destacar que esta revisión es necesaria para exponer la importancia de la presente investigación.

Dentro de los estudios e investigaciones que realizaron se encontró, la auditoría de seguridad informática para la institución educativa departamental Luis Carlos Galán en el municipio de Yacopi Cundinamarca. En la cual resalta el objetivo principal qué es el mejoramiento del sistema informático en la Institución Educativa teniendo en cuenta el diagnóstico inicial la cual es proteger las amenazas y vulnerabilidades que se presentan en la parte administrativa y estudiantil de dicha institución. Por otro lado la propuesta de mejoramiento continuo de la seguridad informática y de la información en las instituciones de educación superior, es una propuesta que resalta y contempla las universidades en Colombia teniendo en cuenta los reportes académicos y demás plataformas que manejan dichas instituciones, el principal objetivo de esta propuesta fue proteger la información en las bases de datos y por supuesto los usuarios y contraseñas de dichas plataformas. En cuanto al estudio en la gestión de seguridad de la información en la institución educativa León XIII del municipio de Soacha, consistió dar a conocer las problemáticas en la área administrativa ya que no existe una red LAN donde cada usuario tenga acceso a la información de otro usuario y por ende el objetivo principal es proteger esa confidencialidad de los certificados y demás documentos que en la institución educativa ejecuta.

Tabla 14.

Revisión bibliográfica

INSTITUCIONES	DETALLES
AUDITORIA DE SEGURIDAD INFORMÁTICA PARA LA INSTITUCIÓN EDUCATIVA DEPARTAMENTAL LUIS CARLOS GALÁN - MUNICIPIO DE YACOPÍ CUNDINAMARCA.	Los avances en el desarrollo de la tecnología, como también en materia de la sistematización de datos, han llevado a que las instituciones educativas implanten modelos de gestión de información en sus sedes; llevando así a que se realice una auditoria de seguridad informática para valorar la forma en que se venían archivando los documentos de las diferentes actividades que se realizan en la institución, relacionadas con el procesamiento y manejo de información de las calificaciones de los alumnos en la Institución Luis Carlos Galán, con el fin de implementar un sistema de seguridad informática que protejan las posibles amenazas y vulnerabilidades que se puedan presentar; beneficiando a todos los usuarios en la parte administrativa, alumnos, ex alumnos, docentes y comunidad en general.
PROPUESTA DE MEJORAMIENTO CONTINÚO DE LA SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR	La información es el activo más importante que posee una organización, dentro de una Institución de Educación Superior (IES) se encuentran diversas bases de datos que contienen información de todo el personal que se relaciona con ella de diversas maneras; reportes académicos de gran número de estudiantes, información personal de estudiantes y administrativos ,investigaciones, datos de proveedores o socios, diversos datos que son delicados como nombres de usuario y contraseñas con las que se pueden realizar modificaciones en códigos fuentes de programas , atacar otros equipos y redes , bloquear el sistema de información que puede conllevar a la pérdida total o parcial de la información.
GESTION DE SEGURIDAD DE LA INFORMACION EN LA INSTITUCIÓN EDUCATIVA LEÓN XIII DEL MUNICIPIO DE SOACHA.	La institución no cuenta con un esquema de backup definido para realizar el respaldo de la información al área administrativa, donde a diario se realizan actualizaciones a la información de los estudiantes como pueden ser constancias, certificados, calificaciones. En el área de las secretarias existe una rotación de personal muy continua, ya que la empresa contratista para suministrar el personal las rota por el resto de instituciones, esto ha permitido que las secretarias vengan con conocimientos de otras instituciones y así mismo se lleven los formatos o procedimientos de la institución, además por esta rotación, el compromiso de cada una por proteger la integridad de la información es muy poca permitiendo así que los datos sean borrados sin ningún reparo. Dentro de esta área existe una red LAN donde cada usuario tiene acceso a la información del otro usuario, lo que conlleva a producirse la perdida de confidencialidad al no tener restricciones de acceso; así mismo se generan certificados o constancias sin el respectivo respaldo de quién fue la persona que lo realizo produciéndose el no repudio.
LA GESTIÓN DE LA SEGURIDAD INTEGRAL EN LOS CENTROS EDUCATIVOS.	Los centros educativos deben ser espacios seguros tanto para el alumnado como para el personal docente y no docente. Cabe gestionar adecuadamente la seguridad para evitar que ocurran accidentes e incidentes, creado un entorno en el que se promuevan y garanticen la seguridad física emocional y social durante el horario escolar, implicando al alumnado y a las familias en la gestión de la seguridad y la promoción de la cultura preventiva. Por ese motivo se elaboró y ejecuto un plan de mejoramiento informático.

Nota: En la presente tabla se expone la revisión bibliográfica sobre el objeto de estudio planteado.

Tomado de Retamozo (2017), Mosquera (2013), Vicario (2015), UNAD (2019).

En cuanto a los tipos de amenazas comentados en los estudios e investigaciones sobre el objeto de estudio planteado se encontraron: Virus informático o código malicioso, uso no autorizado sistemas informáticos, robo de información, fraudes basados en el uso de computadores, suplantación de identidad, denegación de servicios, ataques de fuerza bruta, alteración de la información, divulgación de información, sabotaje y espionaje.

Es importante destacar qué uno de los antecedentes en la Educación Superior más relevantes de este año 2021, es el ataque informático que sufrió la Universidad el Bosque, la cual consiste en el sabotaje de alguno de los sistemas internos de la institución; cómo también el ciberataque a redes sociales como Twitter de la universidad. Por tanto la universidad desarrollo e implementó un plan de acción para solucionar el inconveniente con las redes sociales y también pidió que los alumnos tuvieran mucho cuidado con los correos usuario y contraseña, para mejorar la seguridad informática.

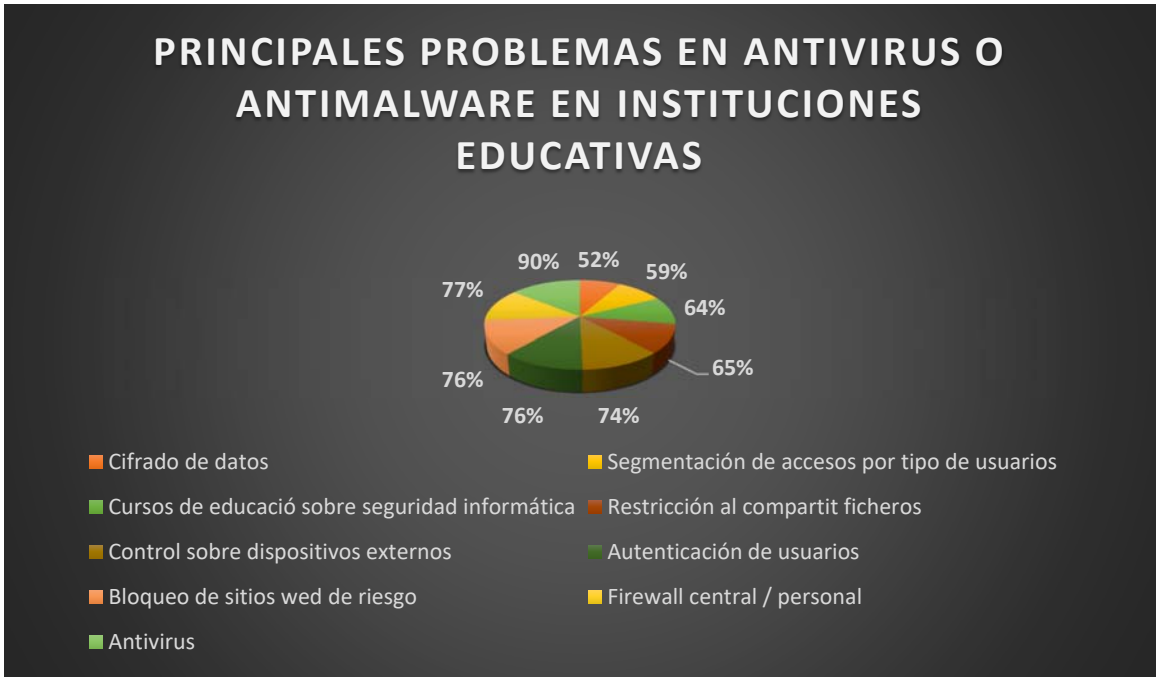
Teniendo en cuenta toda la información anterior, se destacan los informes de las instituciones a nivel Latinoamérica que han sido víctimas de ataques cibernéticos, arroja una cifra de 67% en la cual consiste en el estudio de colegios y universidades que han sido víctimas de ataque cibernético con el fin de realizar acciones de acoso o Bull ying dentro y fuera de las Instituciones Educativas.

Este informe dirigido por la FM Colombia (2021), revela que estos hechos han afectado significativamente a los estudiantes y docentes de las Instituciones Educativas es por ello que en la actualidad se realizan varias campañas para el mejoramiento de la seguridad informática.

5.1.1 Principales problemas de Seguridad en los colegios

Figura 41.

Principales problemas en antivirus o antimalware en Instituciones Educativas

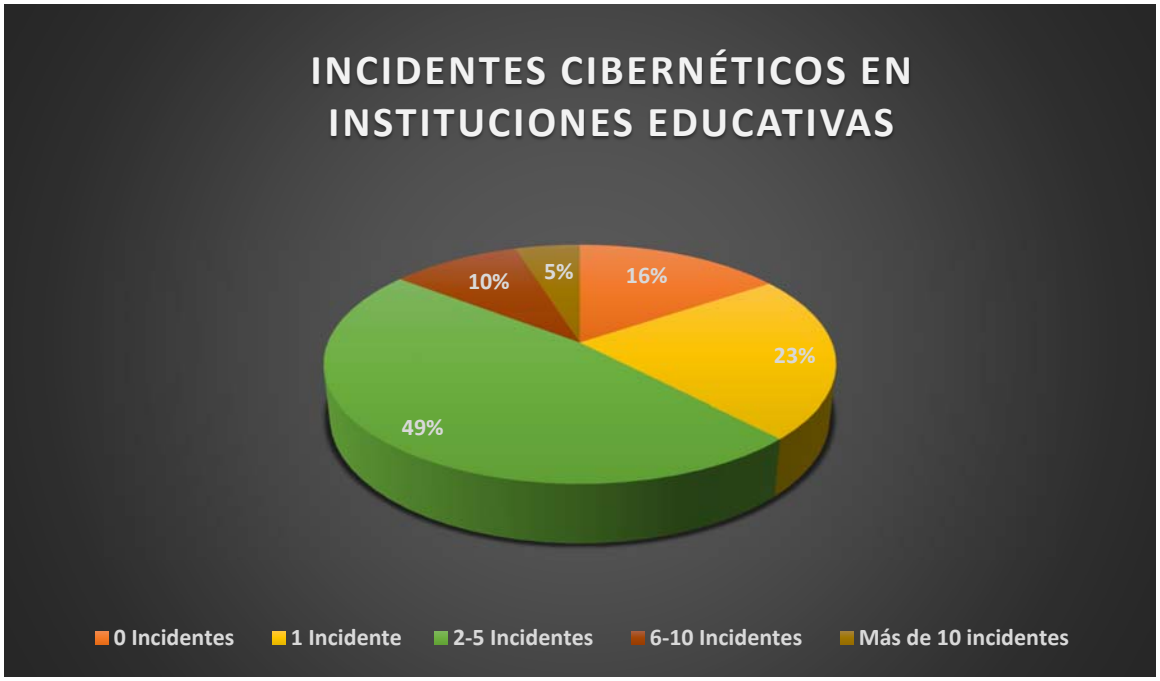


Nota: La figura expone los principales problemas en antivirus y antimalware en instituciones educativas. Tomado de Panda (2020).

Comentan Panda (2020) que el 63% de los colegios sufren de problemas de seguridad, Por otra parte el cifrado de datos es del 52%, la segmentación de accesos por tipo de usuarios del 59%, los cursos de educación sobre seguridad informática son del 64%, la restricción el compartir ficheros es del 65%, el control de dispositivos externos es del 74%, la autenticación de usuario desde el 76%, el bloqueo de sitios web de riesgo en 76%, Firewall central y personal 77% y el antivirus antimalware instalados del 90%.

Figura 42.

Incidentes cibernéticos en Instituciones Educativas

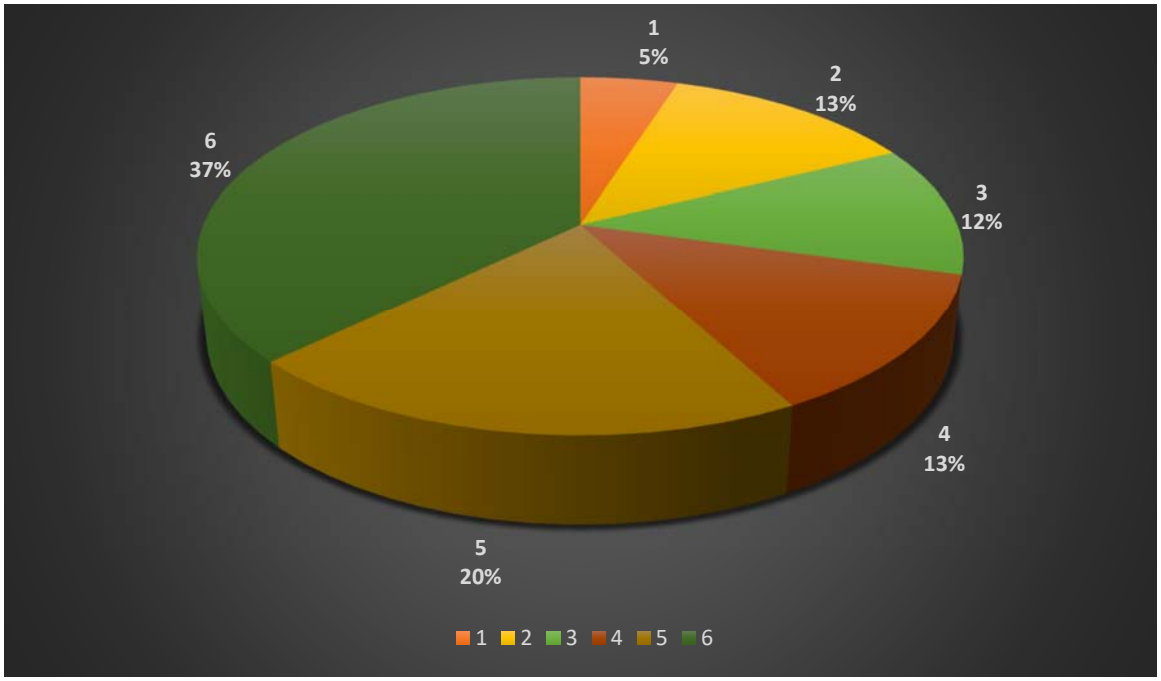


Nota: La figura exponen incidentes cibernéticos en Instituciones Educativas. Tomado de Panda (2020).

En cuanto a la distribución de amenazas a través de las redes sociales de acuerdo con los estudios de Panda (2020), el 64% de las situaciones educativas arrojan qué el 16% han tenido 0 incidentes, el 23% un incidente, el 49% 2 a 5 incidentes, el 10% 6-10 incidentes, y el 5% más de 10 incidentes.

Figura 43.

Desinfección de virus en Instituciones Educativas



Nota: La figura expone desinfección de virus en instituciones educativas. Tomado de Panda (2020).

La desinfección de virus en Instituciones Educativas tiene un promedio de nunca un 5%, una vez al mes o menos 13%, pocas veces al mes 12%, varias veces al mes 13%, en ocasiones 38%, no saben del tema 21%.

Figura 44.

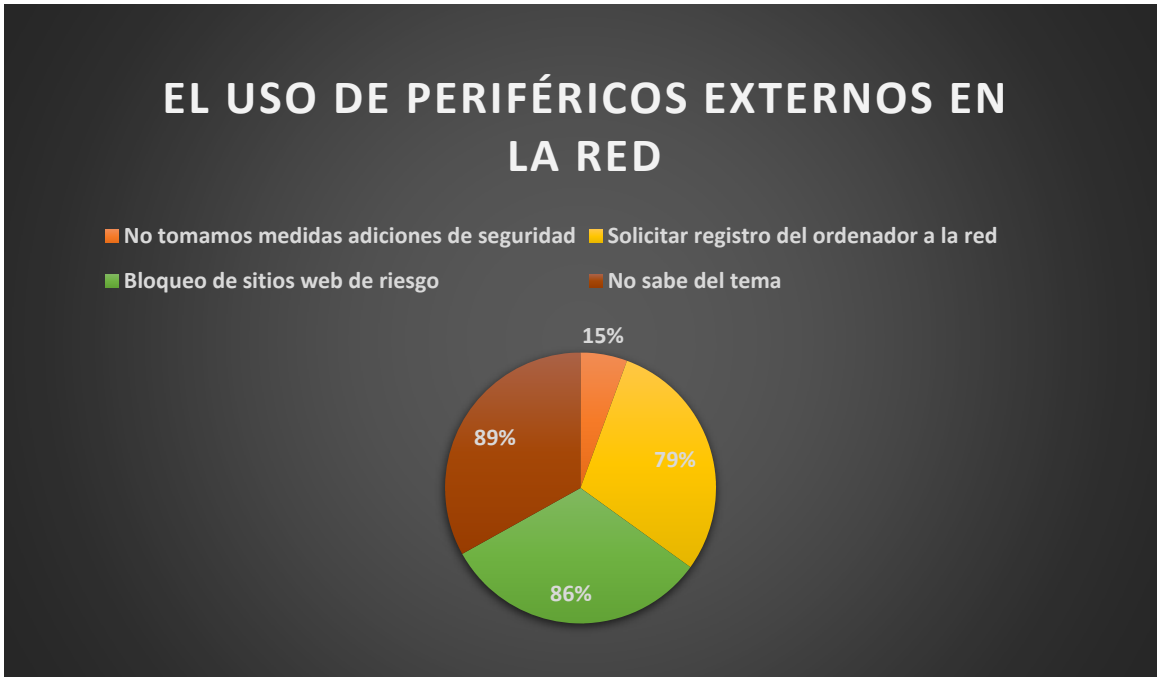
Uso de las redes sociales por parte de alumnos y docentes en las Instituciones Educativas.

Nota: La figura expone el uso de las redes sociales por parte de alumnos y docentes en las Instituciones Educativas. Tomado de Panda (2020).

El uso de las redes sociales por parte de alumnos y docentes en las Instituciones Educativas arroja un porcentaje en el acceso ilimitado 29%, sin acceso 32%, y acceso restringido 39%. Es importante destacar que las redes sociales actualmente son de mayor prevalencia tanto en los alumnos como en los docentes; ya que poseen bastante información y publican ya sean historias, fotografías, de las experiencias cotidianas. Por tanto la seguridad de toda esta información es riesgosa.

Figura 45.

El uso de periféricos externos en la red

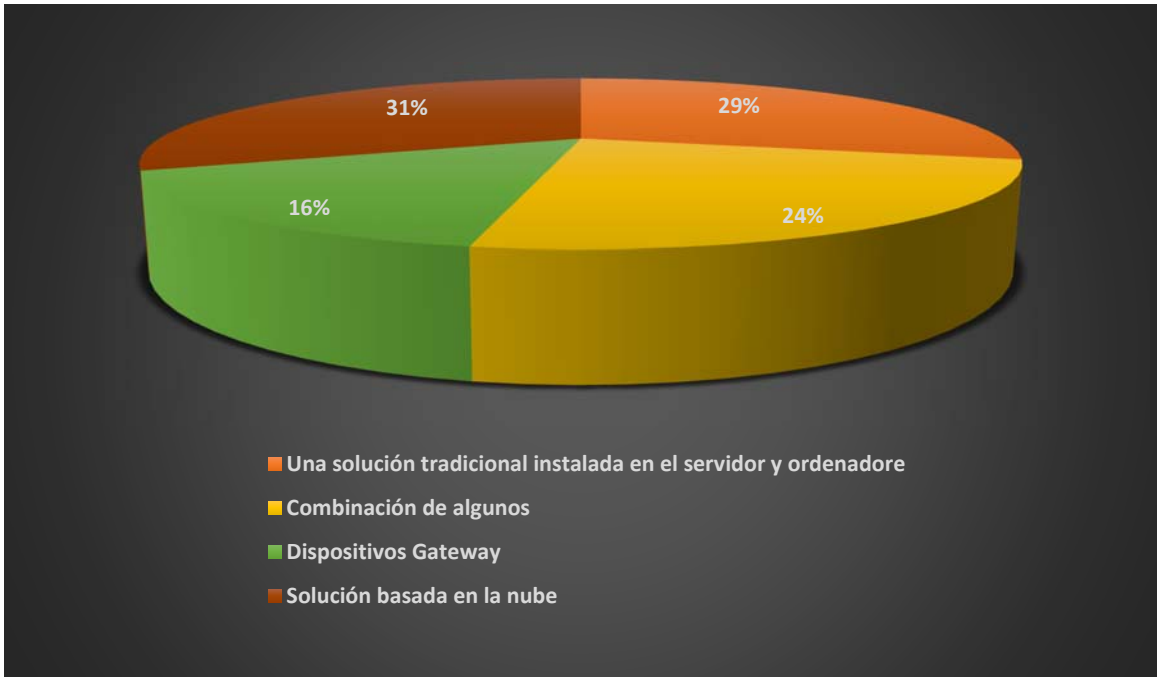


Nota: La figura expone el uso de periféricos externos en la red. Tomado de panda (2020).

El uso de periféricos externos en la red , comentan que no toman las medidas adicionales de la seguridad 15%, las solicitudes de registro del ordenador a la red desde el 79%, bloqueo de sitios web de riesgo 86%, no comenta nada del tema 89%. La mayoría de Instituciones Educativas no conocen los procedimientos o documentos que se deben tener en cuenta para la protección de datos de todo el personal de las instituciones, como también los estudiantes y terceros.

Figura 46.

Administración de IT de los colegios.



Nota. La figura expone la administración de IT de los colegios. Tomado de Panda (2020).

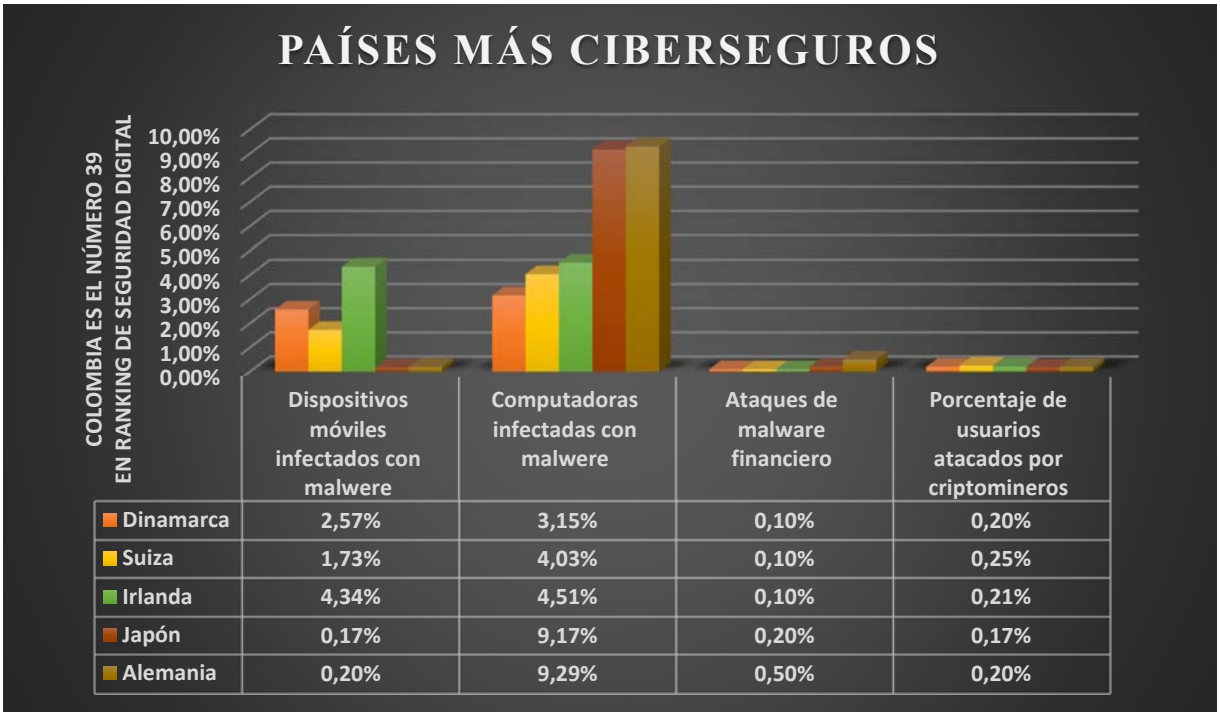
Finalmente cabe destacar la administración de IT de los colegios, la cual según el informe de panda 2020, la combinación de algunos es del 24%, dispositivos gateway 16%, una solución tradicional instalada en el servidor y ordenadores 29% y solución basada en la nube 31%.

5.1.2 Situación mundial ataques cibernéticos

A continuación se da a conocer los países más cibernéticos del mundo teniendo en cuenta los dispositivos móviles infectados con malware, computadoras infectadas con malware, ataques de malware financiero y porcentaje usuarios atacados por criptomineros. Esta información es importante para la investigación; ya que nos ayuda a conocer el ranking de Colombia y también observar la relación con otros países.

Figura 47.

Países más cibernéticos



	Dispositivos móviles infectados con malwere	Computadoras infectadas con malwere	Ataques de malware financiero	Porcentaje de usuarios atacados por criptomineros
Dinamarca	2,57%	3,15%	0,10%	0,20%
Suiza	1,73%	4,03%	0,10%	0,25%
Irlanda	4,34%	4,51%	0,10%	0,21%
Japón	0,17%	9,17%	0,20%	0,17%
Alemania	0,20%	9,29%	0,50%	0,20%

Nota: La figura expone los países más cibernéticos en el mundo. Tomado de información de FM Colombia (2021).

En la Figura 47 se expone los países más cibernéticos del mundo y su prevalencia en la seguridad informática, en la cual Colombia es el número 39 en ranking de seguridad digital. Por otro lado Dinamarca tiene un 2.57% en dispositivos móviles infectados con malware, Suiza 1,73 porciento, Irlanda 4,34 %, Japón 0, 17%, Alemania 0, 20%.

En cuanto a las computadoras infectadas con malware Dinamarca posee un 3, 15%, Suiza 4,0 3%, Irlanda 4,51 porciento, Japón 9,17%, Alemania 9,29%. Los ataques de malware financiero Dinamarca 0,10%, Suiza 0,10% Irlanda 0,10% Japón 0,20% Alemania 0,50%. Finalmente el porcentaje de usuarios atacados por criptomineros Dinamarca 0,20%, Suiza 0,25% Irlanda 0,21% Japón 0,17% Alemania 0,20%.

Teniendo en cuenta los antecedentes en el objeto de estudio planteado tanto de instituciones educativas como el nivel de gravedad en ataques cibernéticos en Colombia, según el informe de la Republica (2021) se observó que los datos relevantes son de los sectores más afectados por los ataques cibernéticos son las bancas y la industria financiera, cómo también las inversiones en ciberseguridad en Colombia crecieron un 12% desde el año 2017, los bancos recibieron hasta 10 intentos de ciberataques , y las empresas colombianas invierte en un 20% o menos de su presupuesto en tecnología de seguridad. Estos ataques reportados son de Defacement 64%, phising 23,5%, compromiso de aplicación 7,1 %, información crítica expuesta 2,9 %, Malwere 2,3 %, vulnerabilidad DNS 0,3 %.

5.2 Realizar levantamiento de información por medio de observación del estado actual de la infraestructura tecnológica de la Institución con base en planos, fotografías, encuestas y mapas de red. Con esto Identificar vulnerabilidades y riesgos de seguridad perimetral que exponen los activos de información.

5.2.1Observación del entorno

Se expone como antecedente la actual plataforma tecnológica de la institución, se identifica que no existe controles aceptables de seguridad implementados en la Institución Educativa Cristo Rey permitiendo el acceso no autorizado a la información, dispositivos de red, cableado y computadores de forma fácil, incrementando considerablemente conexiones no autorizadas, comprometiendo la disponibilidad, integridad y la confidencialidad de la información que se manipula dentro de la institución. Entre los hallazgos relevantes encontrados a nivel de seguridad perimetral y física, se observa que no hay un dispositivo (Firewall) que ofrezca un nivel de seguridad perimetral aceptable en la red, a su vez, que controle y monitoree el tráfico entrante y saliente (packet filter) , además, hay acceso y navegación libre hacia internet en el mismo

(único) segmento de red que poseen las diferentes áreas de empleados y estudiantes, esto incrementa de manera sustancial el riesgo de conexiones entrantes-saliente a sitios y servidores no seguros concediendo facilidad a posibles atacantes, propagación de código malicioso, rasomware y demás riesgos que se encuentran circulando dentro de la web.

Por otro lado a nivel de seguridad de usuario, se encuentra que no hay un sistema de administración centralizado de usuarios y contraseñas (Directorio activo) que permita gestionar fácilmente roles y perfiles de acceso, políticas, gestión de contraseñas y roles de usuario con mínimos privilegios (Least Privilege). Se identificaron falencias mayores, con base en planos, fotografías, encuestas y mapas de red, hechas por los integrantes de este proyecto, donde se observó lo siguiente:

Tabla 15.

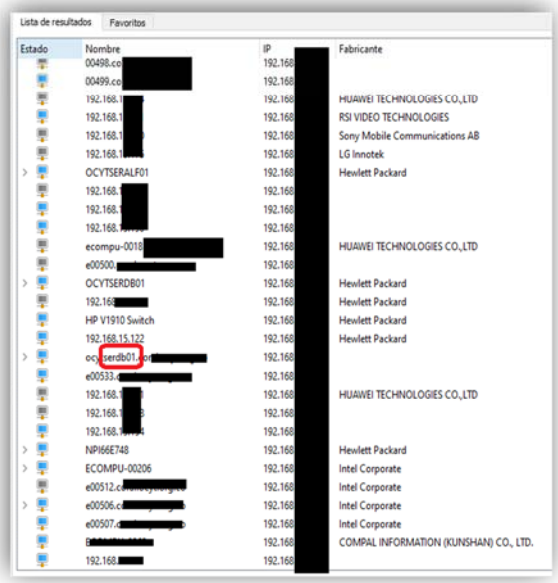
Identificación de vulnerabilidades/falencias

IDENTIFICACIÓN DE VULNERABILIDADES/FALENCIAS	EVIDENCIA
▪ Distribución de la red de forma inadecuada con elementos no certificados. ▪ Cableado no certificado	
▪ Exposición de activos de red sin ningún control de acceso físico, aumentando el riesgo de posibles conexiones no autorizadas. ▪ No hay un perímetro que restrinja de manera física el exterior y el Datacenter.	

- No hay un dispositivo tipo Firewall que controle el tráfico de la red tanto entrante y saliente, a su vez, que brinde seguridad perimetral.
- No hay segmentación de red, la navegación hacia internet es libre sobre en el mismo (único) segmento de red que poseen las diferentes áreas de empleados y estudiantes.
- No hay protección de la navegación de los usuarios.

- Equipos de red de hogar
- Autenticación débil en dispositivos de red (Access Point AP)

- No hay segmentación en la red, los equipos, servidores pueden ser vistos desde cualquier dispositivo conectado a la red con un simple barrido de ping, permitiendo que algún visitante que se conecte pueda visibilizarlo.
- No hay un control en el sistema que rechace las conexiones a servicios comprometidos.
- Áreas en la institución actualmente:
- Sala de Profesores



- Administrativo
- Sala informática 1
- Sala informática 2
- Aulas de clase (Un punto de red)
- Biblioteca
- Patio
- Visitantes

- Seguridad en el host, no hay directivas de grupo que puedan restringir o autorizar privilegios de acceso.
- La gestión de usuarios no es administrada de forma centralizada en ningún tipo de directorio activo o Ldap.
- Al no existir políticas de escritorio limpio, no hay una política que bloquee la pantalla para evitar accesos no autorizados.

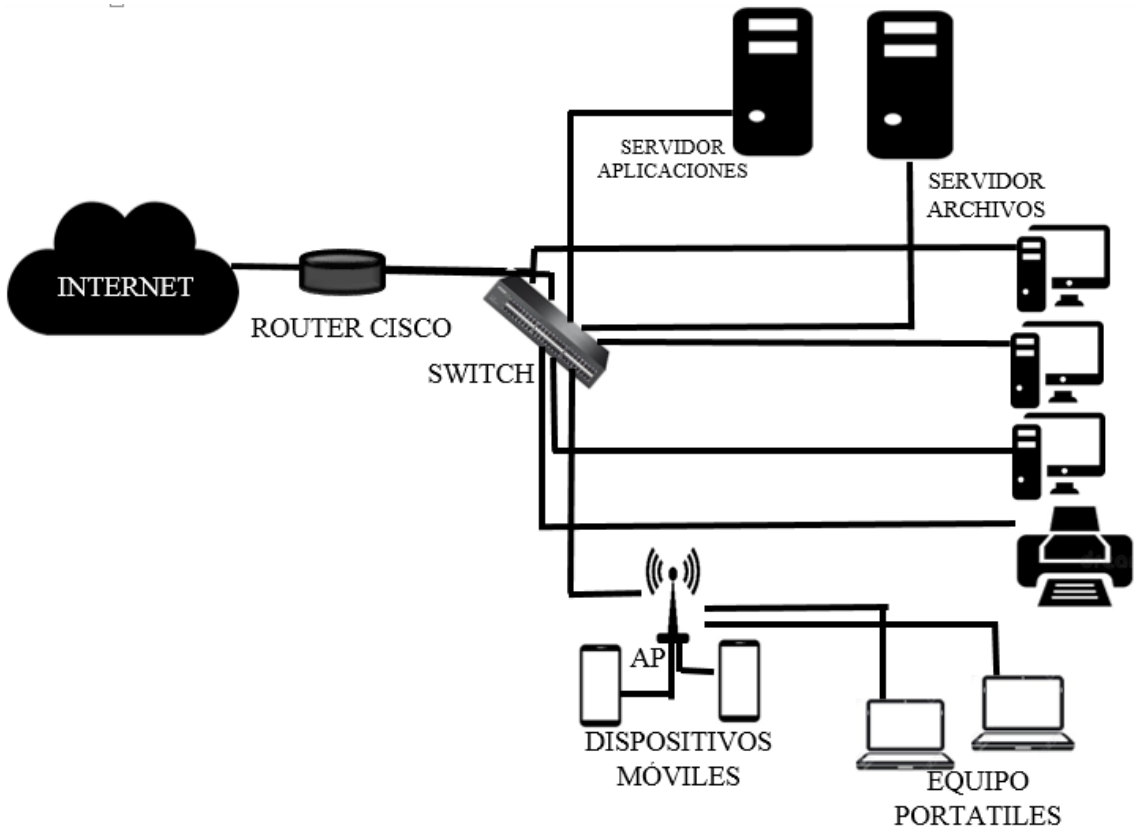
- Servidores con recursos desaprovechados.
- Puertos USB y Unidad de CD/DVD habilitados permitiendo que cualquier persona pueda insertar memorias, discos sin ningún tipo de control.
- No hay evidencia de ningún tipo de hardening aplicado anteriormente.

5.2.2 Mapa de red actual

La infraestructura tecnológica de red actual de la red no fue concebida con un enfoque de seguridad, en la institución existe una red LAN, en forma/topología de estrella, es decir, todas las estaciones (Servidores, switches o estaciones de trabajo) están conectadas a un solo concentrador o Router.

Figura 48.

Mapa de red en la actualidad



Nota: La figura expone el Mapa de red actual del Instituto Cristo Rey. Tomado del trabajo de campo ejecutado en el Instituto Cristo Rey (2021).

5.2.3 Conceptualización fase de Observación

A través del levantamiento de la información se observó que la infraestructura tecnológica de la red actual no fue concebida con un enfoque de seguridad, cómo tampoco no hay un dispositivo central tipo firewall qué controla el tráfico de paquetes (packet filter), de la red tanto entrante y saliente, a su vez que se pare la red de la empresa y brinde seguridad perimetral. Asimismo no se utilizan Vlans para la correcta segmentación de redes, permitiendo que terceros o visitantes que se conecten a la red puedan ver la red corporativa, hay deficiencia en cuanto a la seguridad en los host, prescindiendo de políticas de usuarios, contraseñas, gestión del losgs, roles de usuario como mínimo privilegios, (lets privilege) etc.

Por consiguiente la autenticación es débil en los dispositivos de red (Access Point AP), exponiendo la red ataques o conexiones no autorizadas. El segmento de red para la Institución Educativa se administra con un servicio DHCP para Ethernet como para la red inalámbrica. Finalmente no existe un mapa de topología de red actualizado.

5.2.4 Aplicación de encuestas usuarios del Instituto Cristo Rey

Durante la segunda parte del trabajo (levantamiento de información en la Institución Educativa), se hizo necesario realizar una breve encuesta a los usuarios con el objetivo de conocer en primer lugar, la percepción sobre seguridad y segundo, indagar más a fondo sobre eventos o incidentes que hayan comprometido la seguridad informática o causando indisponibilidad del sistema interrumpiendo así sus funciones laborales diarias, comprometiendo de alguna manera la operación normal del negocio.

La encuesta se envió por correo electrónico a los empleados de la Institución, hubo respuesta por parte de 20 personas. Aquí se presentan los principales resultados de la aplicación realizada en OCT-2021 para efectos de toma de decisiones sobre mejoras o ajustes a realizar en la plataforma tecnológica.

Tabla 16.

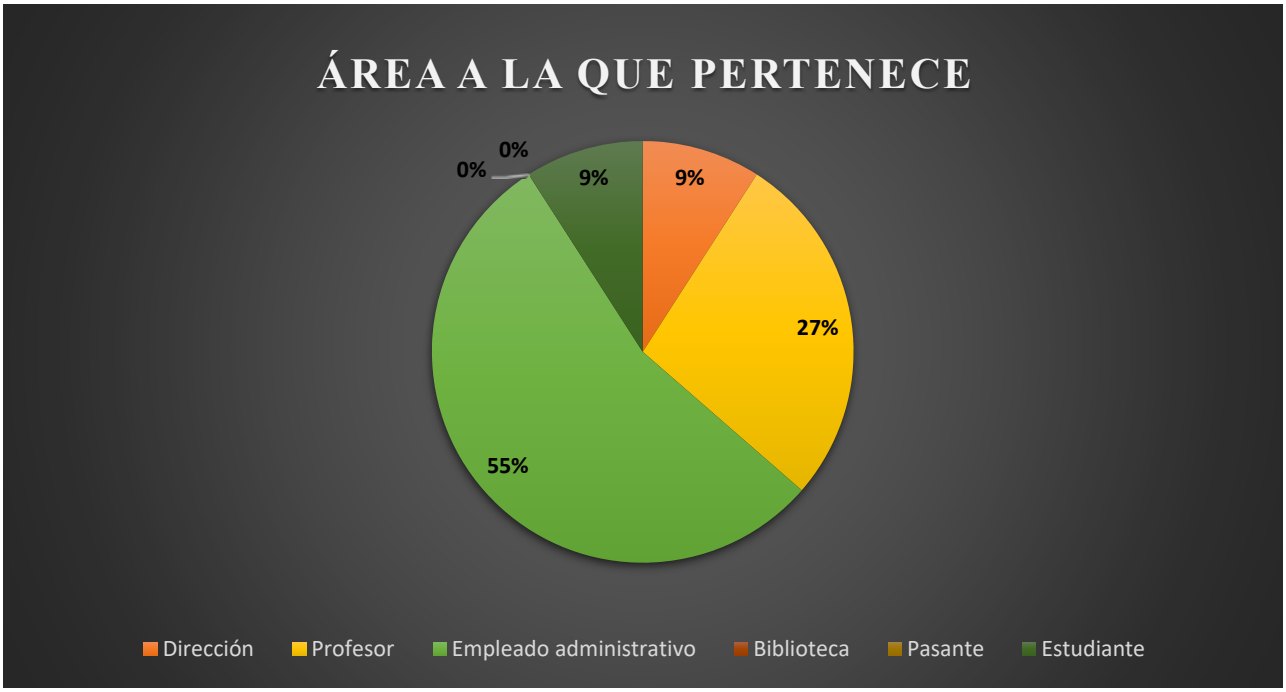
Ficha técnica Encuesta

	FICHA TÉCNICA ENCUESTA
Solicitada por:	Juan Fernando Corredor Niño
Realizada por:	Juan Fernando Corredor Niño
Nombre de la encuesta:	Recolección de Información Institución Educativa.
Universo:	Empleados de la Institución.
Unidad de muestreo:	Empleados que hacen uso de los activos de información de la Institución.
Fecha creación:	Octubre 15 del 2021
Área de cobertura:	Institucional.
Técnica de recolección de datos:	Formulario enviado por correo electrónico.
Objetivo de la encuesta:	Conocer la percepción sobre seguridad de los usuarios e indagar más a fondo sobre eventos o incidentes que hayan comprometido la seguridad informática o causando indisponibilidad del sistema.
Número de preguntas formuladas:	Dieciséis (17)
Tipo de preguntas aplicadas	Cerradas (16) y abiertas (2)

5.2.5 Resultados Encuesta

Figura 49.

Pregunta 1



Las personas que participaron en la encuesta pertenecen al área de docencia un 27%, dirección 9%, empleados administrativos 55%, estudiantes un 9%. No obstante el 55% que pertenece a los empleados administrativos tuvo mayor prevalencia en participación; ya qué son los que más información privada y delicada manejan en el Instituto Cristo Rey.

Figura 50.

Pregunta 2

En cuanto utilizar para el desarrollo de sus actividades laborales las siguientes tecnologías de la información y de la comunicación, los participantes respondieron un 45% computadores, el 10% telefonía móviles para uso empresarial, el 9% servidores, 27% impresoras y el 9% otras tecnologías.

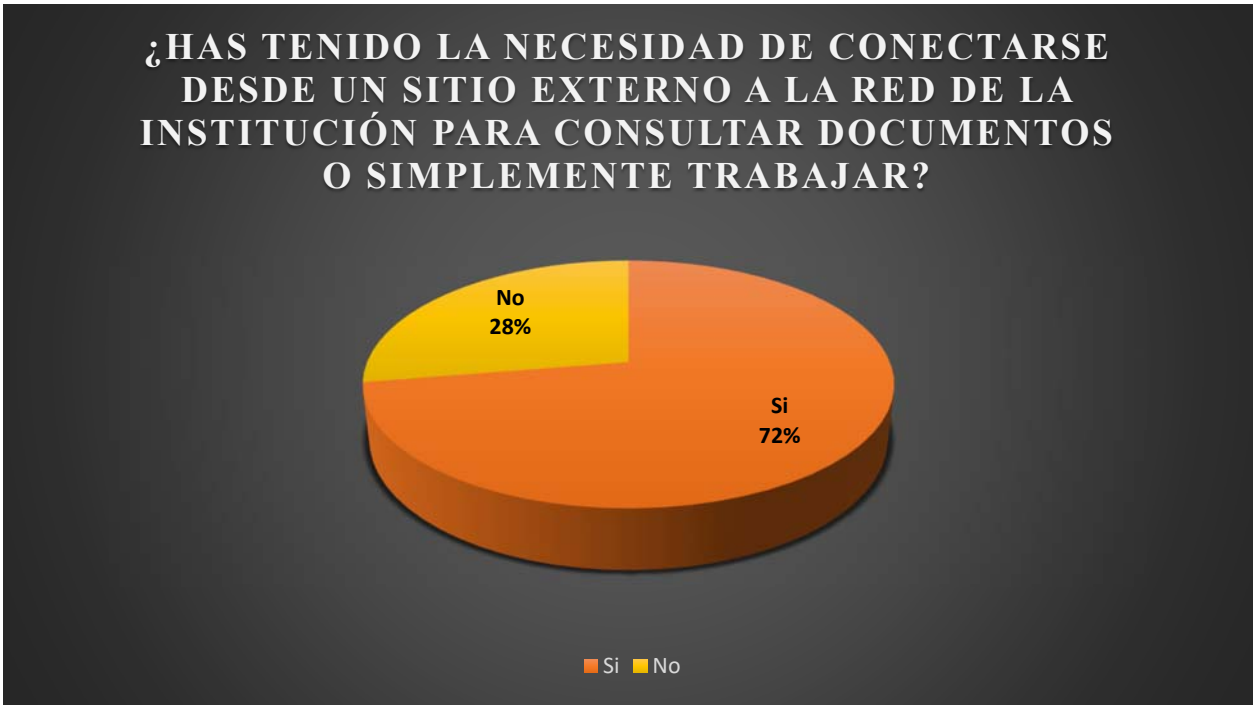
Figura 51.

Pregunta 3

El tipo de aplicaciones informáticas que utilizan hace referencia a ofimática 44%, software contable 14%, gestión de pedidos ,inventarios y logística 19%, gestión con entidades financieras 6%, programas didácticos 6% y software escolar 6%.

Figura 52.

Pregunta 4



En cuanto a la conectividad desde un sitio externo a la red la institución para consultar documentos simplemente para trabajar el 72% respondió si ha tenido necesidad, y el 28% no ha tenido necesidad.

Figura 53.

Pregunta 5

En la pregunta usted cuenta en la institución con conexión de internet El 100% contestó que sí cuentan con una conexión.

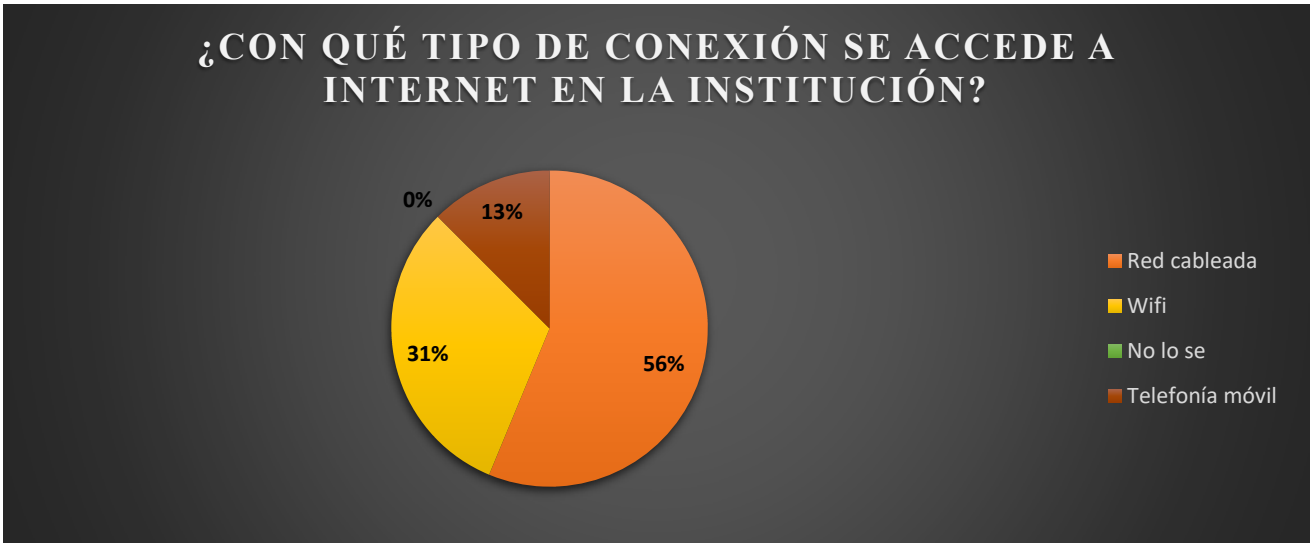
Figura 54.

Pregunta 6

El acceso internet es indispensable para el correcto desarrollo de sus actividades laborales el 100% contestó que sí es muy indispensable.

Figura 55.

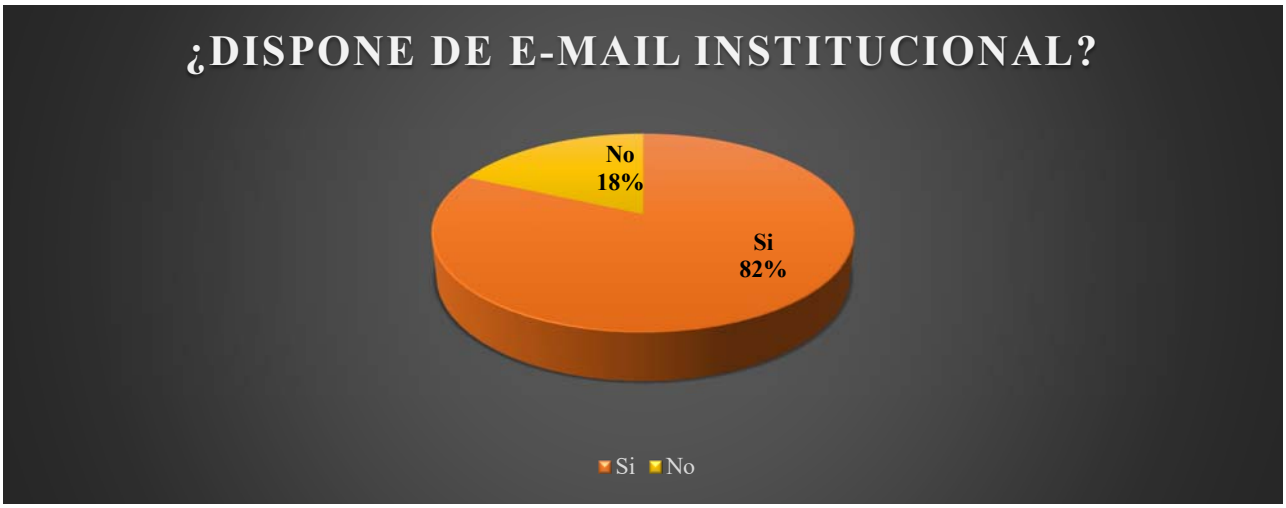
Pregunta 7



En referencia con qué tipo de conexión se accede internet en la Institución Educativa el 56% confirma qué es red cableada, el 31% wi-fi, no lo sabe 0%, y el 13% telefonía móvil.

Figura 56.

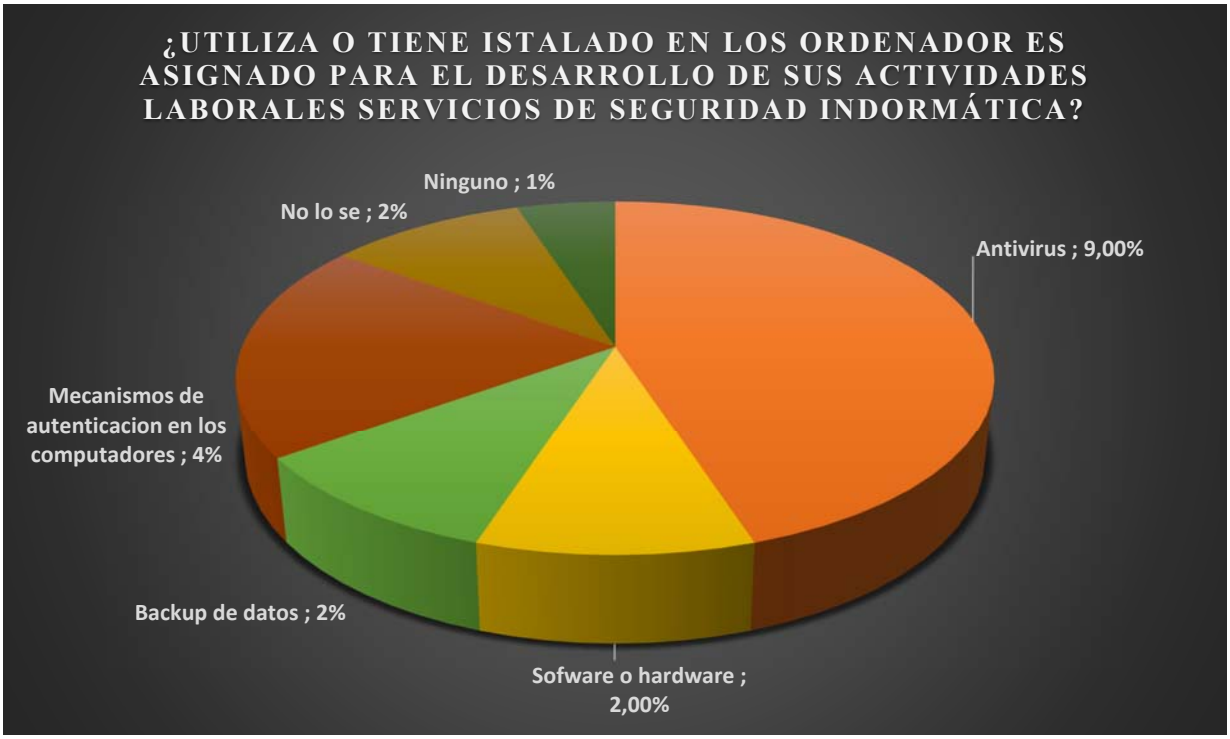
Pregunta 8



En cuanto a la pregunta dispone de email institucional el 82% respondió sí y no el 18%.

Figura 57.

Pregunta 9



En la utilización que tiene ordenadores asignado para el desarrollo laborales servicios de seguridad informática los participantes contestaron antivirus 9%, software o hardware 2%, Backup de datos 2%, mecanismo de autenticación en los computadores 4%, no lo sabe 2%, y ninguno 1%.

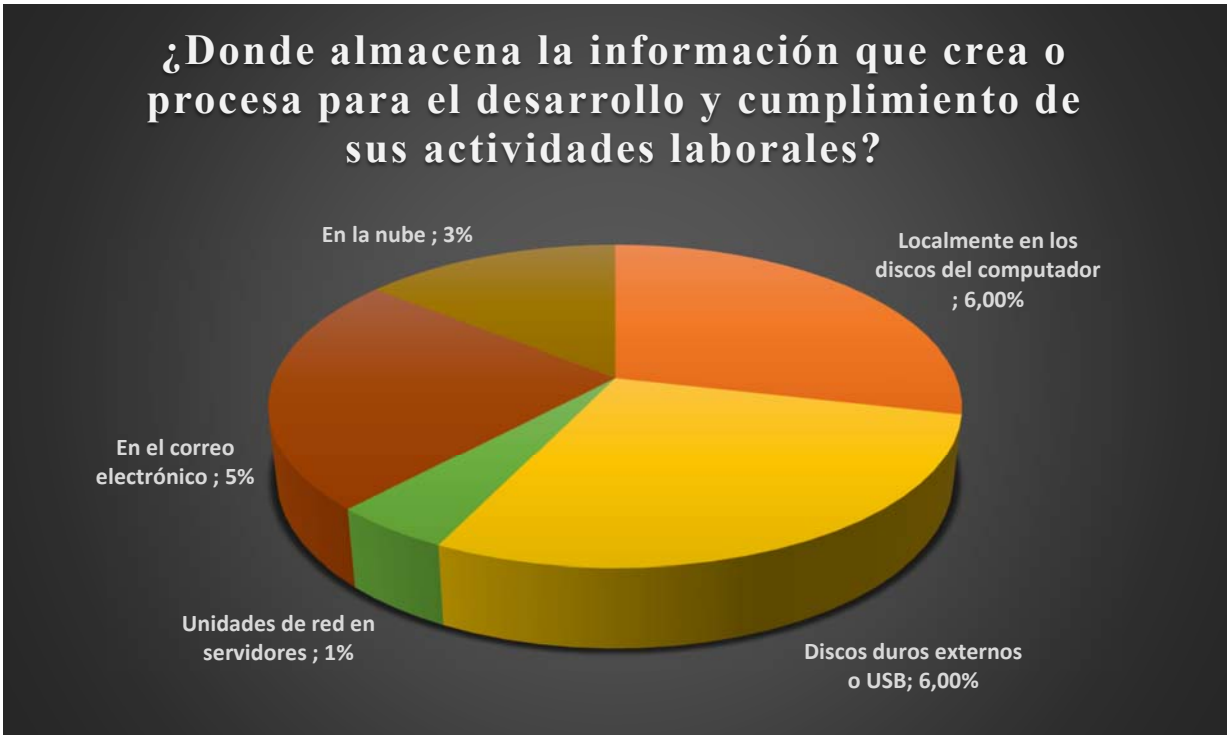
Figura 58.

Pregunta 10

En los problemas de seguridad relacionados con los sistemas de información en los últimos 12 meses, hace referencia a no ha tenido problemas de seguridad 7%, el robo perdida información física 2%, accesos a sospecha de acceso autorizado 2%, ataque virus informático 2%.

Figura 59.

Pregunta 11



Dónde almacena la información que crea proceso para el desarrollo y cumplimiento de sus actividades laborales los participantes respondieron localmente en los discos del computador 6%, discos duros externos USB 6%, unidades de red en servidores 1%, en el correo electrónico 5%, en la nube 3%.

Figura 60.

Pregunta 12

En referencia así se genera periódicamente backups en sus actividades laborales el 45% respondió si, y él no 55%.

Figura 61.

Pregunta 13

En cuanto a la generación periódicamente en los mantenimientos preventivos en los equipos el 73% responde si, el 27% respondió no hace mantenimiento a los equipos en dónde almacena la información laboral.

Figura 62.

Pregunta 14

Durante el año 2021 la institución proporcionó formación capacitación sobre las TIC en seguridad y manejo adecuado de los activos de la red, los participantes respondieron no 82%, Y si 18%.

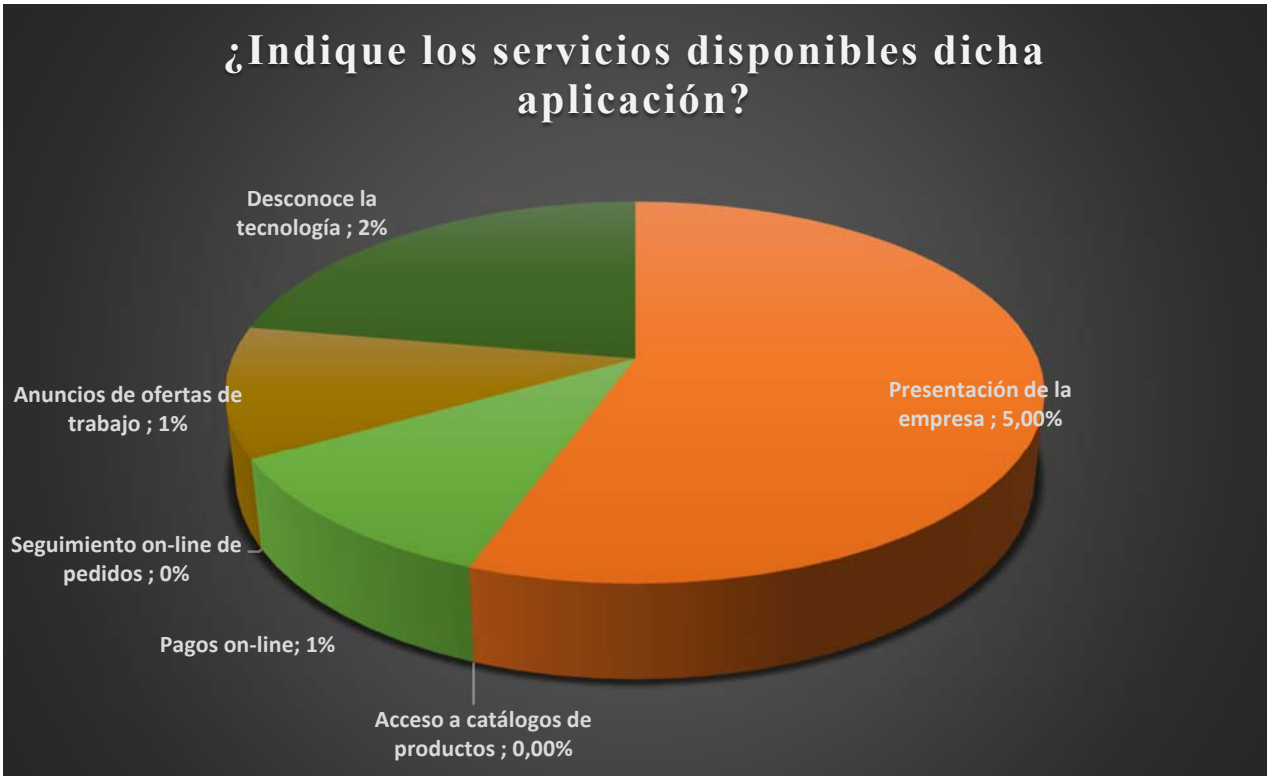
Figura 63.

Pregunta 15

Por otro lado la institución dispone de un sitio web aplicación o página web donde se efectúen pagos online de documentos perdidos etc, el 64% respondió Si, y el 36% No.

Figura 64.

Pregunta 16



En cuanto a los servicios disponibles de dicha aplicación en la presentación de la empresa 5%, acceso a catálogo de productos 0%, pagos online 1%, seguimiento online de pedido 0%, anuncio de oferta de trabajo 1% y desconoce la tecnología 2%.

5.2.6 Análisis de resultados encuesta

El 72% de los usuarios encuestados debe conectarse remotamente a la red LAN por motivos laborales, lo que hace que se tenga que instalar software externo para conexiones remotas sin ningún tipo de control avalado por la institución, pudiendo comprometer de alguna manera la información. El 100% de los encuestados manifiesta que el uso de internet es indispensable para realizar sus labores cotidianas, pero, en la institución no hay un control del tráfico saliente y entrante de internet. Por otro lado se accede a internet por medio de Wifi,

Red alámbrica. El 18% de los encuestados sospecha de accesos no autorizados a la información durante los últimos 12 meses. Si se han presentados infecciones por algún tipo de malware. Más del 50% de los encuestados manifiesta que no se realizan copias de seguridad BackUP de la información. Más del 50% almacena la información de manera local en los equipos, discos duros externos y USB, no hay un sistema centralizado de almacenamiento que permita generar copias de seguridad.

5.3 Analizar la seguridad perimetral actual para generar un plan que permita salvaguardar los activos de información mitigando el riesgo de daño, pérdida o robo.

EL objetivo de esta sección es realizar un análisis de la situación actual en cuanto seguridad perimetral en la Institución para conocer más a fondo las vulnerabilidades y amenazas a las que se ve expuesta la red en la Institución y de esta manera crear una propuesta y estrategia de mejora para contrarrestarlas, aumentando los niveles de disponibilidad, integridad y confidencialidad.

5.3.1 Análisis de vulnerabilidades

Con la información recolectada en el levantamiento de activos y su clasificación determinamos las falencias más pertinentes a mejorar. Empezando por el cableado estructural de la institución, el cual tiene muchos años de uso, los cuales son evidentes por el desgaste visible, las peladuras y uno que otro RJ45 roto.

En cuanto a nivel de funcionalidad este sistema de cableado cuenta con los requerimientos mínimos, pero no gracias a la ubicación y la forma en la que se distribuye por la institución: la mayor parte de dicho cableado no se encuentra asegurado a una canaleta o a una superficie, sino que se exhibe y se encuentra flotando sin ninguna restricción, expuesto a desconectarse por cualquier movimiento leve que se les realice. Los Router no se encuentran en mejores condiciones,

se identificó que no hay un dispositivo tipo Firewall que controle el tráfico de la red tanto entrante y saliente, a su vez, que brinde seguridad perimetral, seguridad que tampoco se ve fortalecida por una segmentación de red, la navegación hacia internet es libre sobre en el mismo (único) segmento de red que poseen las diferentes áreas de empleados y estudiantes consecuentemente no hay protección de navegación de los usuarios.

Del análisis de las zonas de seguridad donde encontramos lo rack, observamos en primera instancia que los switches se encuentran desactualizados en firmware, y aún más preocupante hay switches habilitados que no se utilizan, ofreciendo una puerta abierta para la vulnerabilidad de la red. La institución si cuenta sin embargo con puntos de acceso inalámbricos, los cuales cuentan con un sistema de autenticación WEP y otros WAP, estos protocolos no son los más recomendables para garantizar conexiones no autorizadas a la red. Adicionalmente no existe un control para la entrega de la contraseña para el uso de este. De las zonas de acceso de todos los usuarios de la institución, determinamos que no se les ha dado el cuidado e importancia necesaria a los equipos de cómputo, no cuentan con seguridad en el host ya que no hay directivas de grupo que puedan restringir o autorizar privilegios de acceso. La gestión de usuarios no es administrada de forma centralizada en ningún tipo de directorio activo o LDAP. Tampoco cuentan con políticas de escritorio limpio, por lo que no hay una política que bloquee la pantalla para evitar accesos no autorizados. Los equipos no cuentan con una política de actualizaciones periódicas por lo que la gran mayoría se encuentran con actualizaciones pendientes en todo momento, dejándolos vulnerables a posibles ataques.

Tabla 17.

Análisis de vulnerabilidades sin utilizar ningún tipo de herramienta

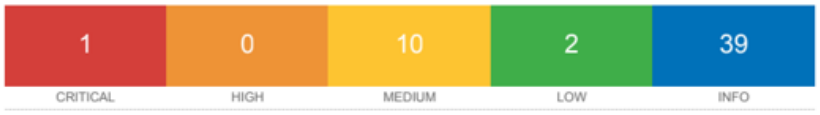
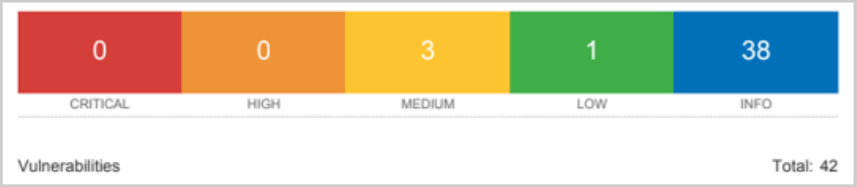
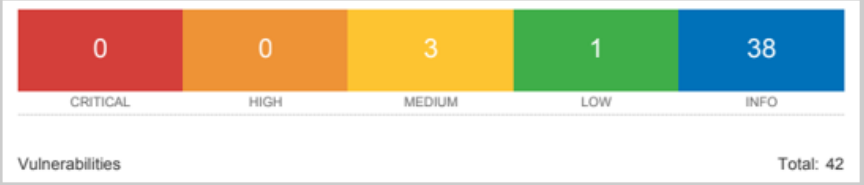
COMPONENTE	ANÁLISIS DE VULNERABILIDADES SIN UTILIZAR NINGÚN TIPO DE HERRAMIENTA
SERVIDOR 1	1. Habilita varios puertos por defecto a los cuales hay que entrar a validar la necesidad de mantenerlos abiertos. 2. Windows habilita el protocolo IPv6 por defecto. 3. Vulnerabilidades nativas de Windows por falta de parches. 4. Usuario Administrador Local por defecto habilitado.
SERVIDOR 2	1. Vulnerabilidades nativas de Windows por falta de parches. 2. Windows habilita el protocolo IPv6 por defecto. 3. Usuario Administrador Local por defecto habilitado.
EQUIPO CLIENTE	1. Vulnerabilidades nativas de Windows por falta de parches. 2. Windows habilita el protocolo IPv6 por defecto.
ROUTER	1. Vulnerabilidades nativas por falta de actualización en Firmware.
SWITCH	1. Vulnerabilidades nativas por falta de actualización en Firmware. 2. Puertos sin uso habilitados por defecto.
REDES INALÁMBRICAS	1. Protocolos de cifrado WEP en algunos Acces point. 2. No hay controles de acceso, a muchas personas se les permite la conexión incrementando el riesgo de un posible ataque interno.

5.3.2 Análisis de vulnerabilidades en servidores

Durante el estudio de vulnerabilidades en los servidores se realizó un análisis de vulnerabilidades utilizando herramientas de software para automatizar el proceso, se encontró lo siguiente:

Tabla 18.

Análisis de vulnerabilidades en servidores

SERVIDOR	REMEDIACIONES PARA VULNERABILIDADES CRÍTICAS Y MEDIAS
  	▪ Microsoft has released a set of patches for Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, and 2012 R2. ▪ Purchase or generate a proper certificate for this service.
 	▪ Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to replace or modify the default error page ▪ Contact the vendor of the DNS software for a fix.

5.3.3 Matriz de riesgo

Tabla 19.

Matriz de riesgo

Componentes	Riegos	Riesgo	Impacto	Riesgo*Impacto	Controles	Nueva clasificacion	% de riesgo reducido aplicando controles
Cableado Estructurado	a.) Cables Desgastados b.) RJ45 Rotos c.) Cables sueltos	3	4	12	a.) Renovacion del sistema de cableado	6	50
Switches	a.) Firmware desactualizado b.) Puertos sin uso se encuentran habilitados.	3	3	9	a.) Actualizacion del firmware b.) Deshabilitar puertos que se encuentren sin uso	6	33,33333333
Router ISP	a.) Firmware desactualizado b.) No existe Firewall c.) Sin filtrador de contenidos	3	4	12	a.) Actualizacion del firmware b.) Implementacion de firewall c.) Implementacion de filtrador de contenidos	6	50
Acess Point	a.) Auntenticacion Debil (WEP) b.) Equipos para hogar	4	3	12	a.) Cambiar el tipo de seguridad a WPA2	9	25
Equipos de computo	a.) No existe gestion de usuarios ni directorio activo b.) Sistemas operativos muy antiguos sin soporte. c.) Vulnerabilidades nativas de Windows por falta de parches	3	3	9	a.) Implementacion del directorio activo b.) Actualizar los sistemas operativos a windows 10 c.) Aplicar una politica de actualizaciones periodicas	4	55,55555556

Clasificacion	
Baja	1-3
Media	4-7
Alta	8-11
Critica	12-16

5.4 Presentar al Instituto Cristo Rey una solución, mediante controles y técnicas de defensa cibernética, resguarden y mitiguen los riesgos de pérdida o robo de activos críticos de información de la institución, con esto cubrir los aspectos mínimos de seguridad perimetral.

A continuación ciudad a conocer la propuesta que consiste en dar solución a las problemáticas expuestas en el actual documento el Instituto Cristo Rey en cuanto a seguridad de la información. Es importante destacar que dentro de la propuesta se da a conocer la segmentación de redes, la cual consiste en el aumento de las opciones de seguridad, amplificación de la administración, principios de seguridad para la segmentación de red. Por otro lado se expone firewall perimetral , la selección de UTM, conexiones externas seguras, sistemas de control de acceso, actualizaciones de software en clientes de forma automática, contraseñas seguras, servidor de autenticación, la selección de software para administración de Radius, el mapa de red actualizado.

5.4.1 Segmentación de redes

Una de las cuestiones a la que las empresas no suelen prestar especial atención es a la red de comunicaciones interna. Segmentar y dimensionar tu red LAN de comunicaciones puede ayudar a resolver muchos de los problemas que se producen a nivel de comunicaciones en las empresas. Para ello es imprescindible identificar que departamentos requieren un mayor ancho de banda para trabajar y medir el flujo de datos de la red interna.

1. **Aumenta las opciones de seguridad**

La mayoría de los dispositivos de seguridad de red funcionan mediante la evaluación de tráfico entre redes. Al poner los recursos sensibles en la misma subred que cualquier otro usuario, se hace más difícil implementar medidas de seguridad. La separación de las funciones vitales en subredes permite implementar medidas de seguridad como firewalls. Éstos pueden ser

configurados para asegurar que sólo los nodos y otras subredes autorizadas tengan acceso a estos servidores, así como otras redes.

2. **Simplifica la administración**

Normalmente, una organización tiene diferentes departamentos que requieren acceso a diferentes tipos de recursos. Si los departamentos de contabilidad y limpieza se encuentran en la misma subred, por ejemplo, entonces las restricciones de acceso tienen que ser controladas en base de nodo-a-nodo. Pero cuando los dos departamentos se colocan en subredes separadas, entonces las opciones de seguridad se pueden aplicar sobre la base de esas subredes.

3. **Principios de seguridad para la segmentación de red**

Así pues, estos son los principios de seguridad mínimos para enmarcar la segmentación:

Figura 65.
Principios de seguridad para la segmentación de red

Teniendo en cuenta la información dada se tiene que, para la segmentación por áreas de la institución educativa, asignaremos un segmento de red Clase B privado para la red LAN. Para la red de la DMZ se utilizará un segmento de IP Clase C privado. Para la red LAN tenemos un segmento de red 172.19.0.0/22 el cual comprende:

Tabla 20.

Segmento de red

Address	**172.19.0.0**
Netmask	**255.255.252.0 = 22**
Network	**172.19.0.0/22**
HostMin	**172.19.0.1**
HostMax	**172.19.3.254**
Broadcast	**172.19.3.255**
Hosts/Net	**1022**

Dada las diferentes áreas de la institución tenemos:

- **Sala de profesores -> 172.19.0.128/26**

Tabla 21.

Sala de profesores -> 172.19.0.128/26

Address	**172.19.0.128**
Netmask	**255.255.255.192 = 26**
Network	**172.19.0.128/26**
HostMin	**172.19.0.129**
HostMax	**172.19.0.190**
Broadcast	**172.19.0.191**
Hosts/Net	**62**

- Administrativo -> 172.19.0.192/26

Tabla 22.

Administrativo -> 172.19.0.192/26

Address	**172.19.0.192**
Netmask	**255.255.255.192 = 26**
Network	**172.19.0.192/26**
HostMin	**172.19.0.193**

HostMax	**172.19.0.254**
Broadcast	**172.19.0.255**
Hosts/Net	**62**

- Sala de Informática 1 -> 172.19.2.0/27

Tabla 23.

Sala de Informática 1 -> 172.19.2.0/27

Address	**172.19.2.0**
Netmask	**255.255.255.224 = 27**
Network	**172.19.2.0/27**
HostMin	**172.19.2.1**
HostMax	**172.19.2.30**
Broadcast	**172.19.2.31**
Hosts/Net	**30**

- Sala de Informática 2 -> 172.19.2.32/27

Tabla 24.

Sala de Informática 2 -> 172.19.2.32/27

Address	**172.19.2.32**
Netmask	**255.255.255.224 = 27**
Network	**172.19.2.32/27**
HostMin	**172.19.2.33**
HostMax	**172.19.2.62**
Broadcast	**172.19.2.63**
Hosts/Net	**30**

- Aulas de Clase -> 172.19.2.64/27

Tabla 25.

Aulas de Clase -> 172.19.2.64/27

Address	**172.19.2.64**
Netmask	**255.255.255.224 = 27**
Network	**172.19.2.64/27**
HostMin	**172.19.2.65**

- Biblioteca -> 172.19.2.96/27

Tabla 26.

Biblioteca -> 172.19.2.96/27

Address	**172.19.2.96**
Netmask	**255.255.255.224 = 27**
Network	**172.19.2.96/27**
HostMin	**172.19.2.97**
HostMax	**172.19.2.126**
Broadcast	**172.19.2.127**
Hosts/Net	**30**

- Patio -> 172.19.0.0/25

Tabla 27.

Patio -> 172.19.0.0/25

Address	**172.19.0.0**
Netmask	**255.255.255.128 = 25**
Network	**172.19.0.0/25**
HostMin	**172.19.0.1**

HostMax	**172.19.0.126**
Broadcast	**172.19.0.127**
Hosts/Net	**126**

- Visitantes -> 172.19.1.0/24

Tabla 28.

Visitantes -> 172.19.1.0/24

Address	**172.19.1.0**
Netmask	**255.255.255.0 = 24**
Network	**172.19.1.0/24**
HostMin	**172.19.1.1**
HostMax	**172.19.1.254**
Broadcast	**172.19.1.255**
Hosts/Net	**254**

- Estudiantes

Tabla 29.

Estudiantes

Address	**172.19.3.0**
Netmask	**255.255.255.0 = 24**
Network	**172.19.3.0/24**
HostMin	**172.19.3.1**
HostMax	**172.19.3.254**
Broadcast	**172.19.3.255**
Hosts/Net	**254**

Como se observa se deja un estimado de 128 host disponibles para un posible crecimiento ya sea de personal o de infraestructura. Para la red DMZ se tomó el segmento 192.168.0.0/27 Clase C en donde se tomó:

- Red Servidores -> 192.168.0.0/28

Tabla 30.

Red Servidores -> 192.168.0.0/28

Address	**192.168.0.0**
Netmask	**255.255.255.240 = 28**
Network	**192.168.0.0/28**
HostMin	**192.168.0.1**
HostMax	**192.168.0.14**
Broadcast	**192.168.0.15**
Hosts/Net	**14**

Como se evidencia se dejan libre 15 host, por un posible crecimiento de infraestructura.

5.4.2 Firewall perimetral

Según información recolectada, es necesario que el Instituto Cristo Rey ofrezca un servicio de internet seguro a los usuarios de la institución para el correcto desarrollo de sus actividades laborales. Como observamos anteriormente en los apartados del presento documento , hay ausencia de un dispositivo tipo Firewall UTM que monitoree y controle las conexiones y que a su vez conceda seguridad entre la red interna LAN, la red WAN y una posible zona DMZ; Se puede observar una falla y riesgo de seguridad con la que cuenta la institución, ya que bastarían

algunos ataques simples aprovechando las vulnerabilidades vistas en la sección anterior para poder denegar servicios, o en el peor de los escenarios un ataque con rasomware que pueda encriptar información crítica impactando la normal operación y perjudicando gravemente del negocio.

5.4.2.1 Selección de UTM

Para elegir el software Firewall UTM que se sugiere implementar en la institución, se listaron los servicios necesarios y se confrontaron 3 marcas conocidas de firewall tipo software Open Source, de la siguiente manera:

Tabla 31.

Firewall UTM

Firewall UTM	Función de un firewall de inspección de paquetes	Función de VPN (para hacer túneles o redes privadas)	Antispam (para evitar los correos no deseados o spam)	Antiphishing (evitar el robo de información)	Filtrado de contenidos (para el bloqueo de sitios no permitidos mediante categorías)	Antivirus de perímetro (evitar la infección de virus informáticos en computadoras clientes y servidores)	Detección/Prevención de Intrusos (IDS/IPS)
PfSense	Si	S	Si	S	S	S	**Si**
Endian	Si	S	Si	S	S	S	**Si**
IPcop	**Si**	**S**	**No**	**S**		**S**	**Si**

Luego del primer filtro, se descarta una marca y se prosigue con el siguiente análisis:

Tabla 32.

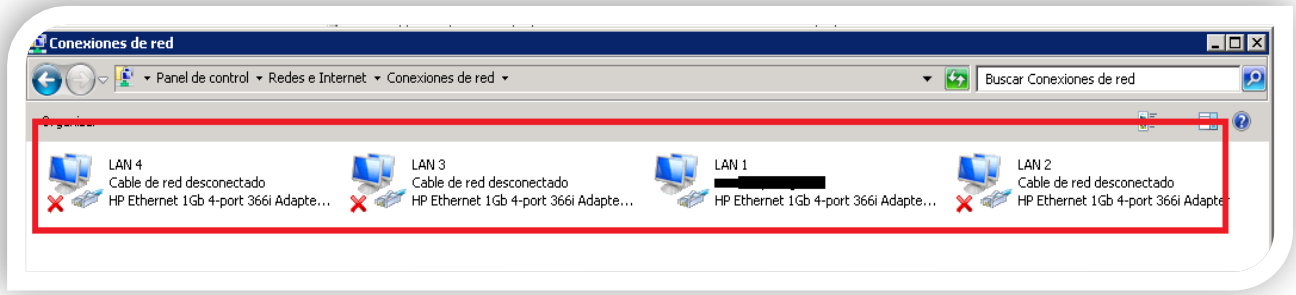
Ventajas y desventajas firewalls software

Firewall	Ventajas	Desventajas
PfSense	1. Interfaz intuitiva 2. Configuración sencilla una vez que te has familiarizado con el interfaz, en un par de horas con el producto 3. Paquetes instalados del repositorio bajo demanda.	1. Poca documentación. 2. Algunos módulos son de pago.
Endian	1. Bastante intuitivo para la 2. configuración 3. No es muy pesado. 4. Logs bastante claros 5. Interface cómoda a través de navegador. 6. Las funciones de routing.	Poca documentación.

Luego del análisis anterior y aprovechando uno de los dos servidores que tiene actualmente la institución, se sugiere implementar un firewall de software tipo UTM con licencia OpenSource llamado Endian Firewall v 3.3.0 de manera virtualizada, los servidores de la institución cuentan con 4 tarjetas de red con capacidad de 1Gb que pueden ser aprovechadas por entornos de virtualización como Hyper-V (3 tarjetas para el firewall, 1 tarjeta para el servidor), por el momento dichas tarjetas de red no se están utilizando.

Figura 66.

Tarjetas de red servidores



4.4.2.2 Endian 3.3.0 Firewall

Figura 67.

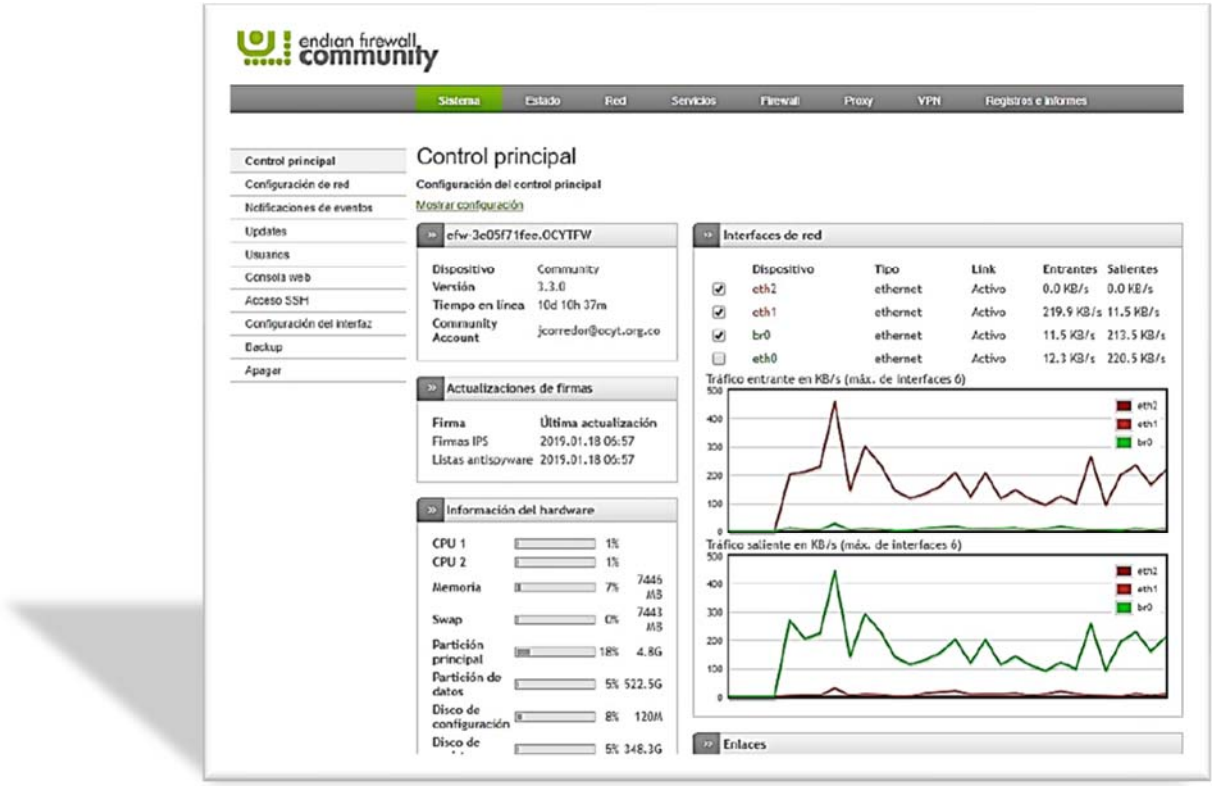
Logo Endian Firewall

Nota: La figura expone el Logo Endian Firewall. Tomado de Endian (2021).

Es un Firewall de software UTM para la gestión unificada amenazas de es una distribución GNU/Linux libre (Open Source) especializada en ruteo. Endian está basado en Red Hat Enterprise Linux, por lo cual Endian Firewall es 100% de código abierto. Esta distribución de Linux incluye una amplia variedad de funciones, como firewall de inspección con estado, filtrado de paquetes, antivirus HTTP / FTP, filtro de contenido, antivirus POP3 / SMTP, antiphishing y herramientas de contra el spam, SSL / TLS VPN, IDS y otras características de que brindan un nivel alto de seguridad.

Figura 68.

Interface principal Endian Firewall

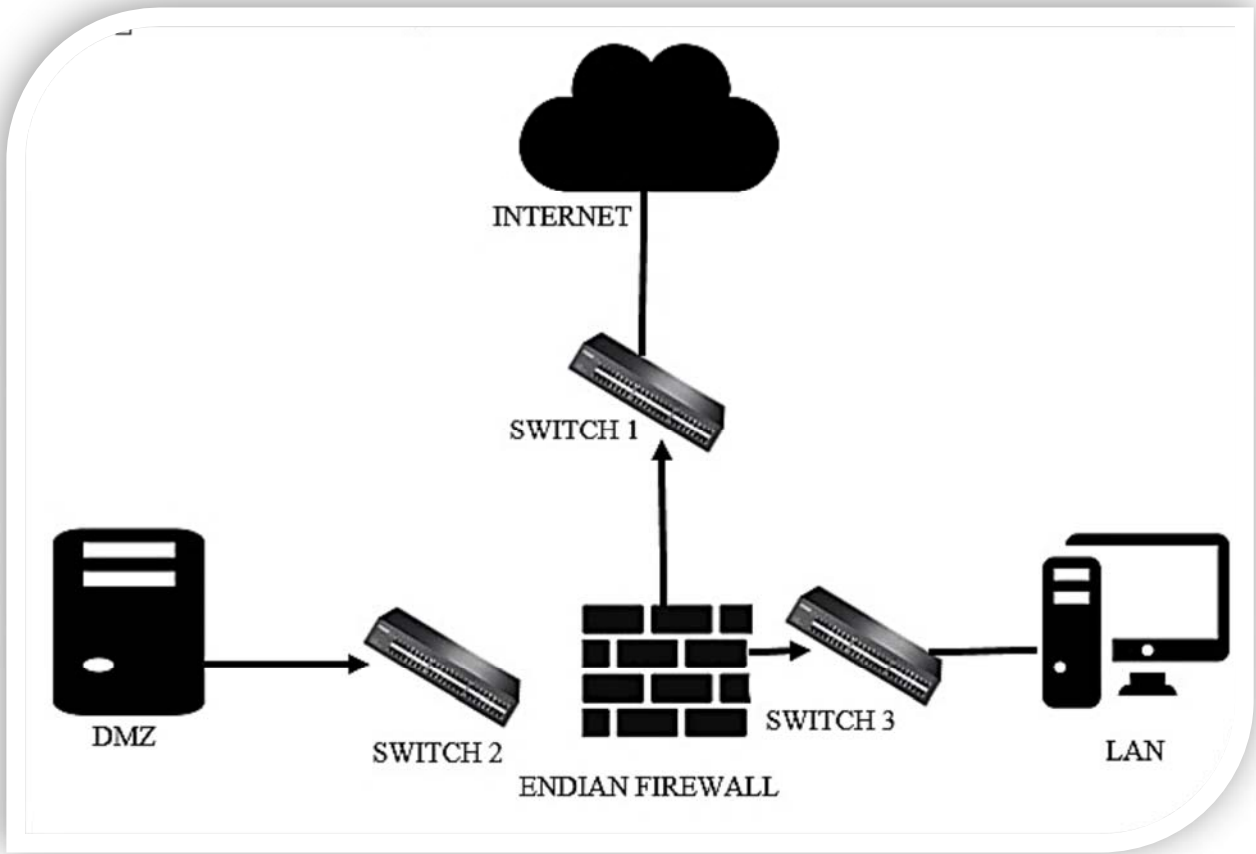


Nota: La figura expone el Interface principal Endian Firewall. Tomado de Endian (2021).

El firewall que se sugiere instalar puede ser implementado como una máquina virtual utilizando el servicio de virtualización Hyper-V que ofrece Windows Server en versiones standard o datacenter 2012 o superiores, la topología de red del firewall una vez implementada quedaría de la siguiente manera:

Figura 69.

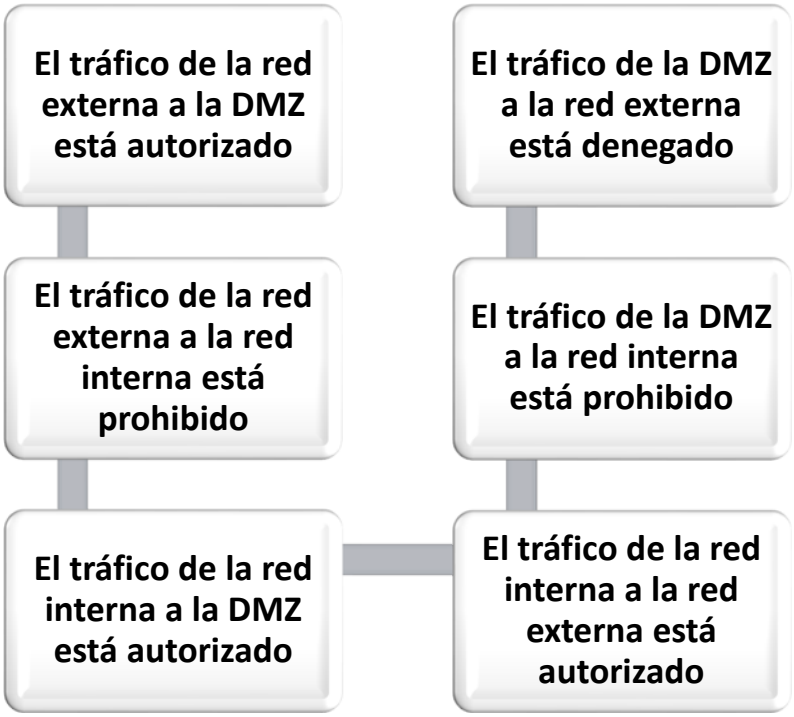
Topología de red firewall



Se configurará el firewall bajo una política restrictiva, es decir que se denegará todo el tráfico excepto el que está explícitamente permitido según el previo análisis. El cortafuego obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten. Políticas de Seguridad entre zonas.

Figura 70.

Trafico de Seguridad entre zonas



Si el firewall es implementado en la institución, se reducirá el riesgo de que ataques comprometan la seguridad, este dispositivo brindará un nivel alto de seguridad en cuanto a:

1. **Seguridad en la recepción de Correos**

Endian Firewall permite asegurar cualquier cliente de correo como Outlook o Thunder-bird este tipo de software sestará protegido y los correos serán filtrados por Endian Firewall antivirus y antispam.

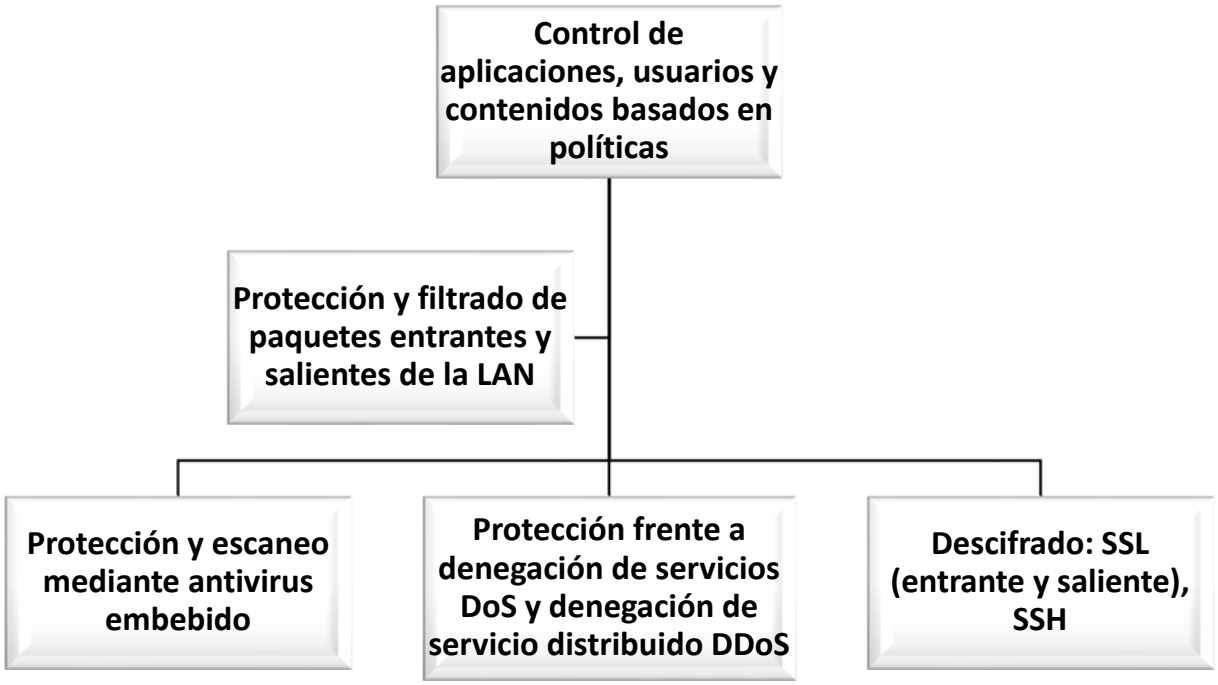
2. **Seguridad en acceso a la Web**

Se habilitará un filtro de contenido en el Endian Firewall que ofrece navegación web de forma segura, resguardando los equipos contra malware y contenidos no deseados. Permitirá al administrador de la red monitorizar accesos.

Otros aspectos para mejorar con el montaje del Firewall perimetral:

Figura 71.

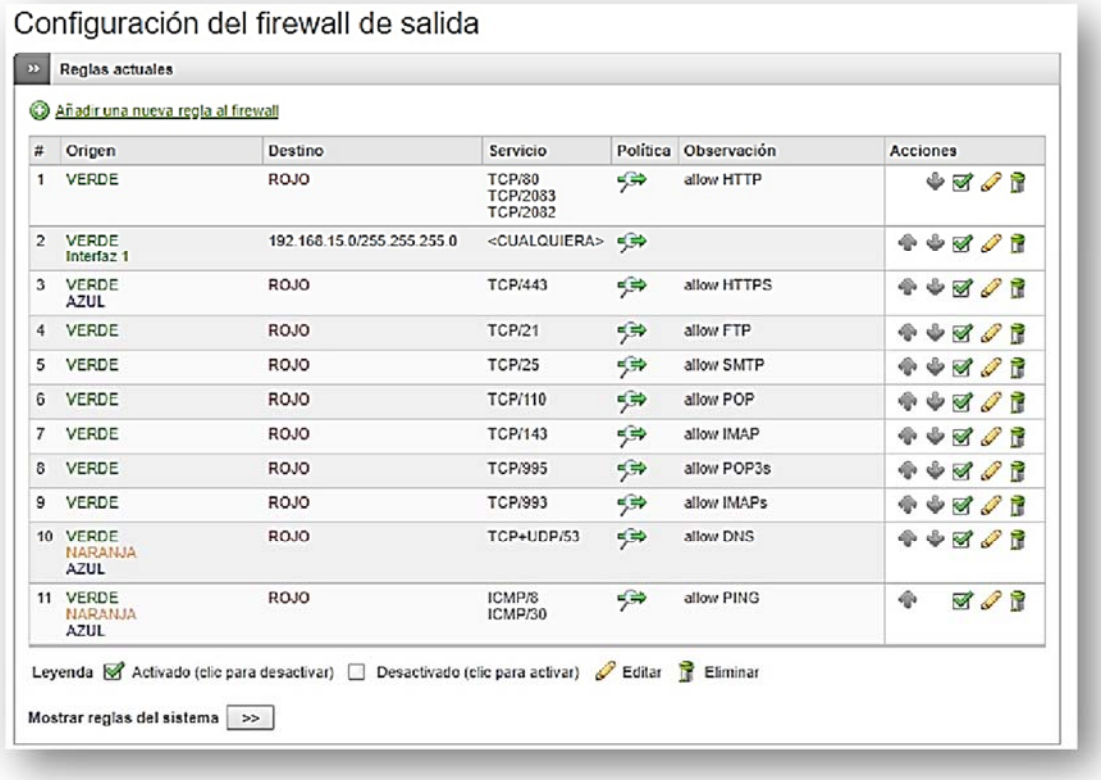
Aspectos para mejorar con el montaje del Firewall perimetral



Tráfico de salida, ya que se establecerá una política de configuración restrictiva en el firewall, y por seguridad de las conexiones que se realicen desde el interior hacia la red de internet, estas conexiones estarán reguladas por el servicio de cortafuegos, donde se habilitara únicamente los puertos y servicios necesarios:

Figura 72.

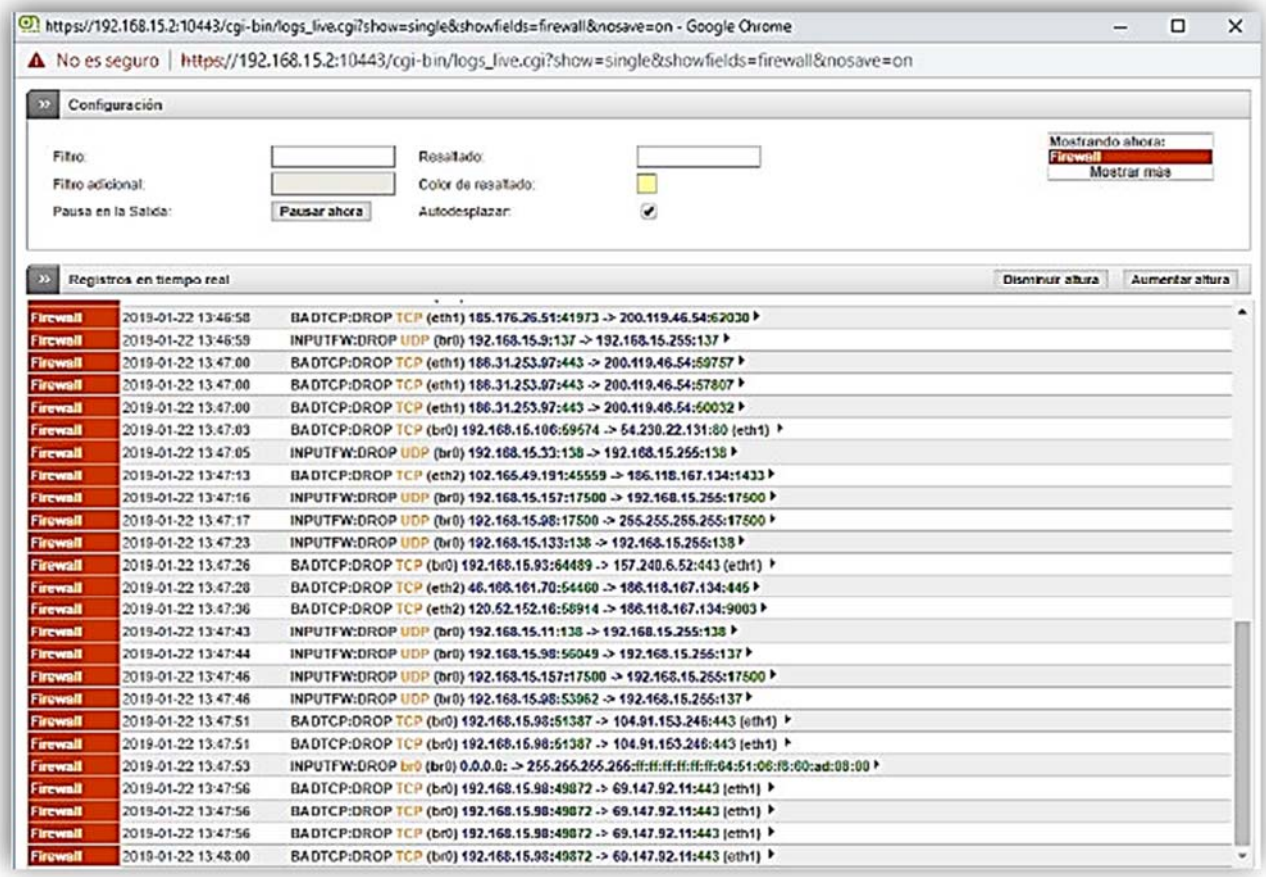
Políticas de salida en el firewall Endian



Prevención de Intrusos IPS, uno de los servicios que ofrece el firewall es un sistema de IPS (Sistema de prevención de intrusos), este despliega un control de accesos en la red protegiendo la LAN de ataques e ilegalidades. El Firewall UTM analiza la información del ataque y genera una serie de reglas en el firewall deteniéndolo en tiempo real.

Figura 73.

Logs IPS Endian Firewall



Servicio de conexiones seguras utilizando VPN, durante la recolección de información el 72% de los usuarios manifestó la necesidad de conectarse desde un sitio externo (Ej.: Hogar) a la red de la institución para consultar o realizar sus actividades laborales, para ello utilizan algún tipo de software libre que ofrece conexiones remotas, pero no se garantiza un cifrado alto o control de las conexiones desde el exterior.

Figura 74.

Pregunta 17.

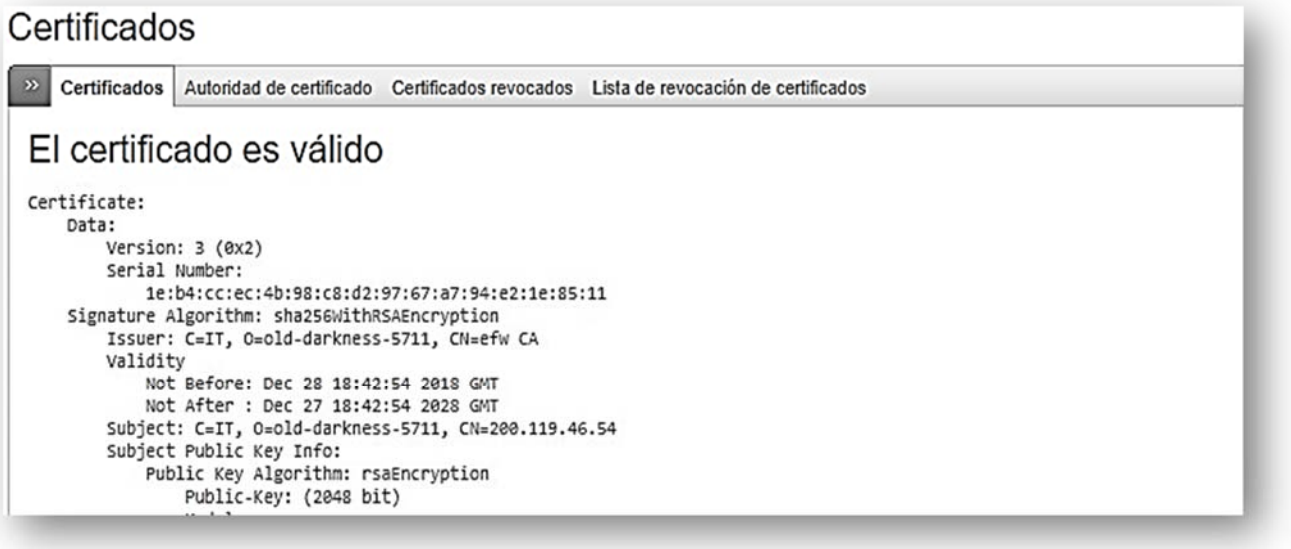
En cuanto a la necesidad de conectarse desde un sitio externo a la red de la institución para consultar documentos o simplemente trabajar los participantes respondieron si el 72, 70% y no el 27, 30%.

4.4.2.3 Conexiones externas seguras

Se sugiere habilitar el servicio de conexión remota vía VPN, estará habilitado para que el usuario autorizado por la entidad tenga acceso a recursos de red desde una red diferente a la LAN. El túnel que une los dos extremos de la conexión usa sistemas de encriptación, certificado CA y autenticación para asegurar la confidencialidad e integridad de los datos que se transmiten, utilizando un certificado digital con Signature Algorithm: sha256-RSA Encryption y un tamaño de la llave publica de Public-Key: (2048 bit).

Figura 75.

Ejemplo certificado digital emitido por Endian Firewall

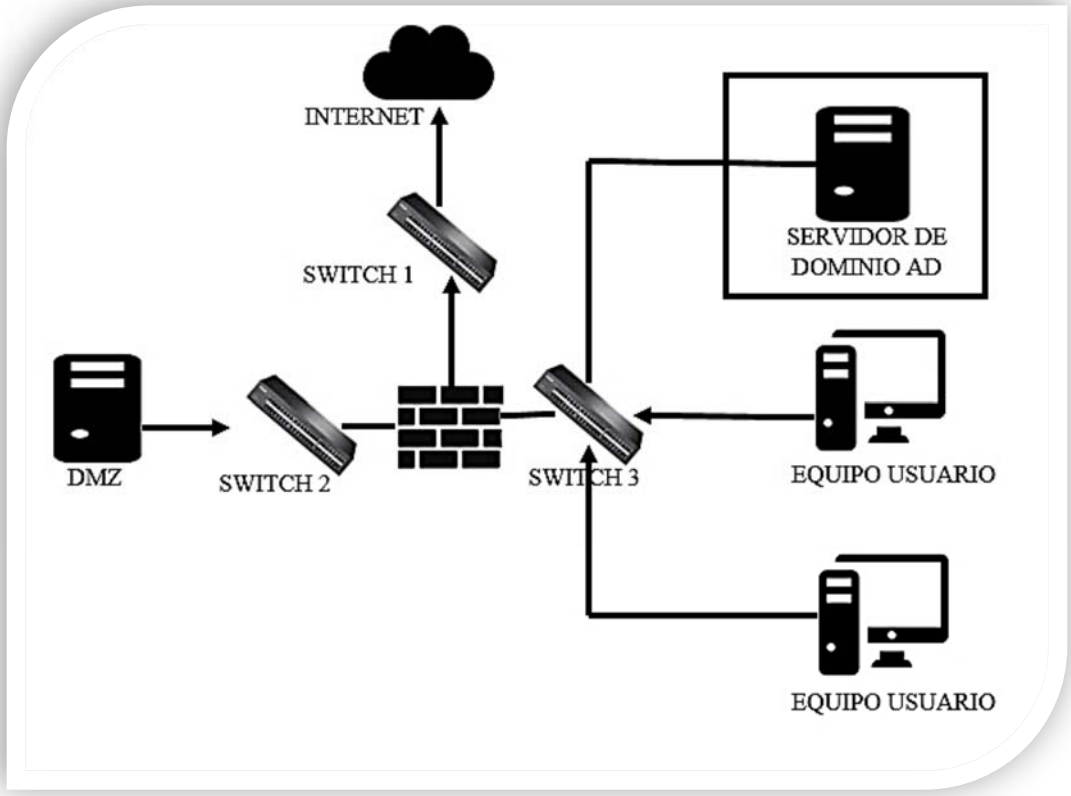


4.4.2.4 Sistemas de control de acceso

Según información recolectada, no hay un sistema seguro de acceso que refuerce la seguridad en los hosts, por lo que se sugiere implementar un sistema tipo AAA (Authentication, Authorization and Accounting), por esta razón se instiga a realizar la implementación de un servidor con servicio de directorio activo (LDAP) que permita asegurar el acceso a la información y equipos por roles y perfiles, permitiendo delimitar el modo de acceso ya de sea de lectura o escritura, garantizando a su vez que, la información contenida en equipos o unidades de red, pueda ser accesada únicamente por las personas que de antemano tengan autorización. Aprovechando uno de los dos servidores que tiene actualmente la institución, se implementará un controlador de dominio AD, donde se gestionarán los usuarios activos e inactivos, es decir los usuarios en el AD que salen de la institución serán suspendidos quedando inoperable el usuario.

Figura 76.

Topología de red, ubicación servidor de dominio



Actualizaciones de software en clientes de forma automática:

Se creará una política que instale automáticamente las actualizaciones de seguridad enviadas por Microsoft.

Mínimos privilegios (least rivilege):

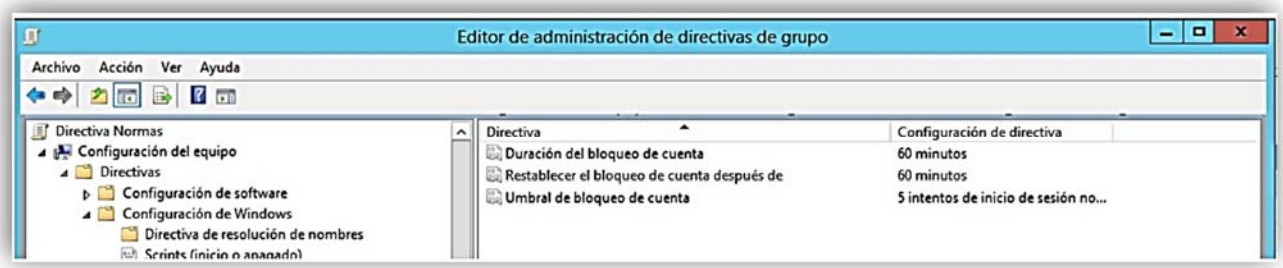
Mediante una política GPO se prohibirá la instalación de cualquier tipo de software sin la autorización del administrador de la red, lo cual puede ser aprovechado en algún ataque de malware.

Contraseñas seguras:

Como control de seguridad en las estaciones de trabajo y usuarios administradores, se sugiere configurar una GPO que obligue a los usuarios a cambiar su contraseña cada 60 días, esta debe cumplir requisitos de complejidad (Mayúsculas, minúsculas, caracteres especiales), con una longitud mínima de 7 caracteres y al acumular 3 intentos fallidos de inicio de sesión el usuario quedará bloqueado.

Figura 77.

Configuración de GPO

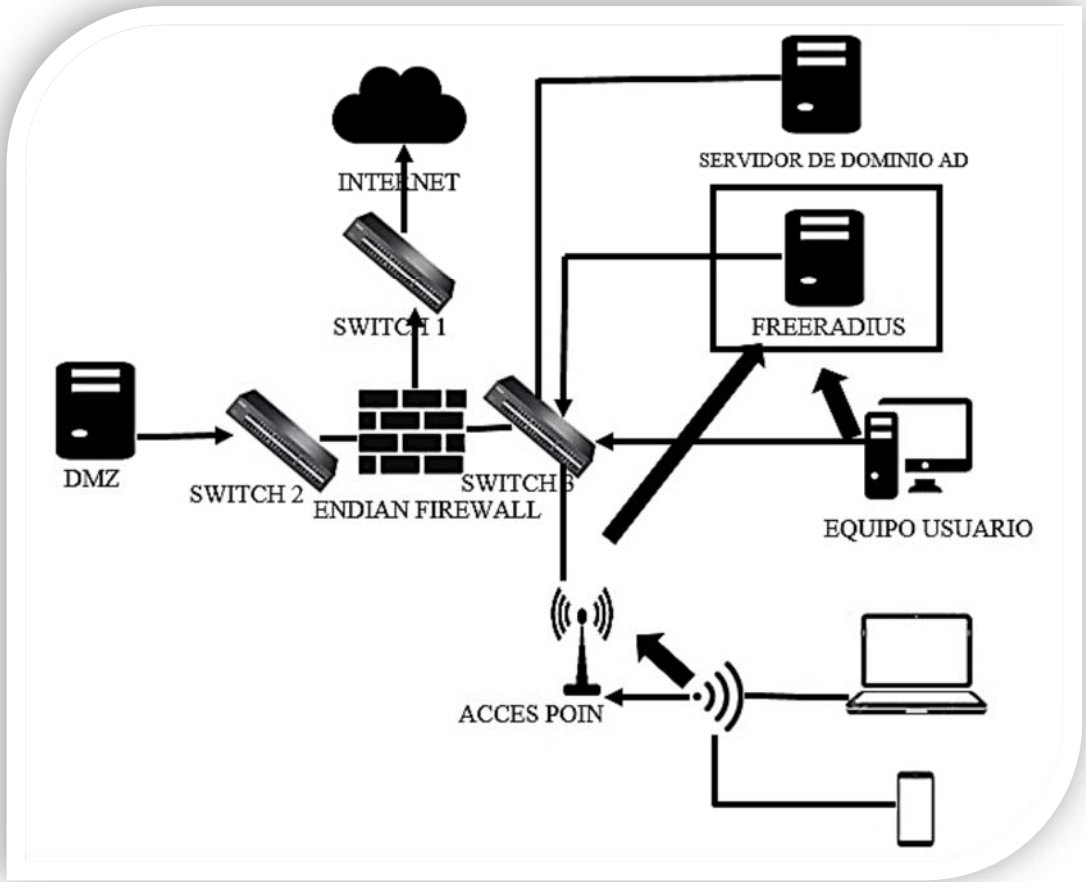


4.4.2.5 Servidor de autenticación

Durante la etapa de levantamiento de información se pudo observar que no existe un mayor control de acceso y conexión por medio de las redes alámbricas e inalámbricas incrementando el riesgo de un posible ataque interno. Por lo anterior, se sugiere la instalación de un servidor RADIUS (Remote Authentication Dial- In User Server), este es un protocolo utilizado para la autenticación y autorización y de esta forma acceder a las redes, el usuario solicitante envía información por medio del equipo cliente al servidor RADIUS (usuario y contraseña). El servidor valido la información utilizando protocolos de autenticación como EAP, PAP o CHAP. Si es el usuario es admitido, el servidor autorizará el acceso a la red del dispositivo.

Figura 78.

Topología de red, ubicación servidor RADIUS

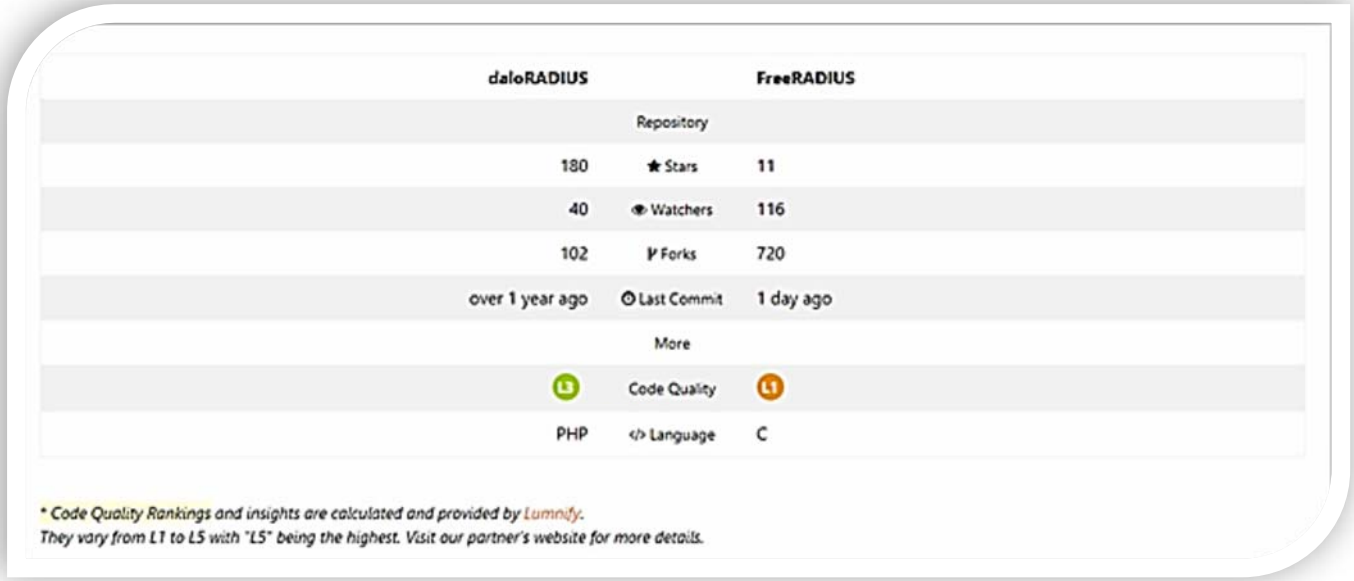


4.4.2.6 Selección software para administración de Radius

Para ofrecer mayor seguridad y control en cuanto al acceso a la red por medio WiFI y realizar la gestión de administración del RADIUS en los puntos de acceso se hace sugiere la implementación de un software especial centralizado. El mercado ofrece varias marcas OpenSource, para ello se realiza un comparativo de calificaciones por usuarios, estabilidad en el tiempo y calidad de código.

Figura 79.

Comparativo daloRADIUS vs Free RADIUS



daloRADIUS		FreeRADIUS
	Repository	
180	★ Stars	11
40	Watchers	116
102	Forks	720
over 1 year ago	Last Commit	1 day ago
	More	
L5	Code Quality	L1
PHP	</> Language	C

* Code Quality Rankings and insights are calculated and provided by Lumnify.
They vary from L1 to L5 with "L5" being the highest. Visit our partner's website for more details.

Del anterior filtro se sugiere implementar el software Daloradius, este es un software OpenSource que permite la administración avanzada Radius, se accede por medio de una interfaz Web permite configurar de una manera fácil el servidor Radius.

Figura 80.

Interfaz Web DaloRadius

Con la configuración e instalación del controlador de dominio y el servidor Radius, se busca controlar el número de equipos conectados en la red para brindar mayor seguridad y reducir el riesgo de ataques internos o externos, evitando:

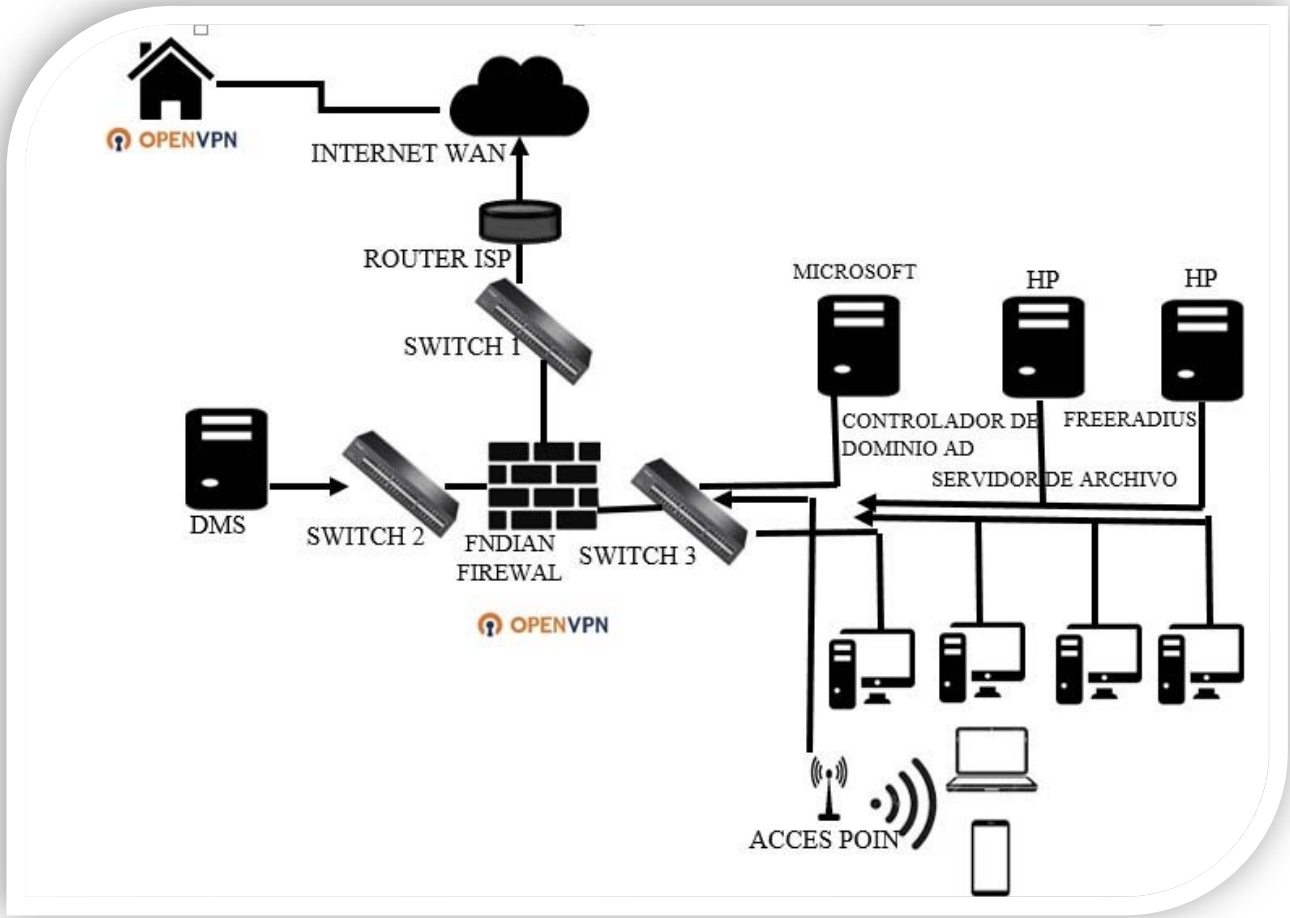
1. Ataques de DoS
2. Limitar el número de conexiones y proveer un mejor servicio QoS
3. Controlar el tiempo máximo de conexión de usuarios invitados
4. Posibilidad de emplear restricciones de acceso a un usuario/grupo/perfil en particular.

4.4.2.7 Mapa de red actualizado

Si las recomendaciones anteriores son implementadas en la institución, el siguiente sería el mapa de red a futuro, lo cual es una representación gráfica de los dispositivos de red y sus interrelaciones, esta herramienta proporcionará a los administradores de tecnología una mejor comprensión de la red.

Figura 81.

Mapa de red post implementación



Conclusiones

Los adelantos en ciencia y tecnología del uso intensivo de las TIC y la dependencia de las organizaciones en los sistemas de información como estrategia para establecer ventajas competitivas más duraderas y difíciles de imitar , así como el apoyo para la toma de decisiones obliga de tender y administrar los riesgos asociados con la implementación de nuevas tecnologías mantener los procesos principales de las organizaciones de las actividades operativas , enfatiza en la importancia implementar sistema de administración de seguridad de la información que proporcionan esquemas esenciales para soportar procesos críticos de las Instituciones Educativas.

Los sistemas de administración de seguridad de la información están conformados por elementos cómo: estándares, políticas, procedimientos, análisis de riesgos y auditoría de sistemas. La implementación de ISMS (Information Security Management) es una decisión estratégica de la organización; y por lo tanto, debe ser apoyada desde los altos mandos hasta el personal de mandos medios; el diseño, desarrollo e implementación del ISMS debe cumplir con los objetivos organizacionales y cumplir con las expectativas de las áreas involucradas.

Por otro lado, la definición del perímetro de seguridad debe ser establecida como un control interno de la organización. Las políticas de seguridad deben estar alineadas a los objetivos organizacionales, ser flexibles y adecuados para cada una de las áreas donde se van a aplicar. La creación del ISMS considera el diseño, la implementación, el monitoreo y el mantenimiento de los sistemas de seguridad y la estrategia en la elaboración de políticas, procedimientos, planes y grupos de trabajo. La ejecución de un análisis de riesgos consiste en la identificación de los activos, amenazas y vulnerabilidades. Es una metodología que busca maximizar los recursos escasos de la organización a través de una valoración de los riesgos y la tolerancia de ya sea una empresa o Institución Educativa a estos.

En la investigación ejecutada se pudo apreciar que las implementaciones sugeridas y en base a la tabla de riesgos acerca de la infraestructura de la institución, podemos observar que en la escala que manejamos de 1-16 siendo este último un estado crítico el cual debe ser tratado con suma urgencia, en base a las clasificaciones que se les dieron a dichos activos podemos observar que se deben tratar con prioridad los elementos de infraestructura, gracias a los controles y aplicaciones que se toman en cuenta en la propuesta de mejora de seguridad perimetral dichos riesgos se ven claramente reducidos pasando de muchos controles rojos a prácticamente ninguno.

Por otro lado es importante destacar que los switches presentan una clasificación alta de riesgo, aplicando los controles de la propuesta este pasa a un amarillo, reduciendo el porcentaje de riesgo en un 33%, el router muestra una clasificación critica de riesgo, aplicando los controles de la propuesta este pasa a un amarillo, reduciendo el porcentaje de riesgo en un 50%, los Access point tienen una clasificación critica de riesgo, aplicando los controles de la propuesta este pasa a un amarillo, reduciendo el porcentaje de riesgo en un 25%, los equipos de cómputo presentan una clasificación alta de riesgo, aplicando los controles de la propuesta este pasa a un amarillo, reduciendo el porcentaje de riesgo en un 55%, en un conglomerado total de todos los elementos de infraestructura podemos concluir que los riesgos totales de estos se reducirían en un 57,4% gracias a las mejoras propuestas.

Con base a la matriz de riesgo establecida y adicionalmente contando con los resultados que esta arroja, los controles que se sugieren para la institución ayudarían a mitigar los riesgos presentes por lo que es necesario tener un plan a futuro para una posible próxima mejora de la seguridad y seguir con un plan de mejora establecido. En el diseño que se realizó esto está contemplado debido a que se segmento de tal manera para dejar campo suficiente para futuros crecimientos de la institución y aún más importante, implementaciones que puedan ayudar a seguir

mitigando riesgos. Lo más importante para resaltar en el esquema que se propone es la zona de DMZ la cual quedaría disponible en dado caso que se quiera hacer uso de ella. Esta mejora no fue sugerida en la propuesta inicial, pero se estableció una segmentación específicamente para ella y esta se encuentra en el diseño el diseño presentado con el fin de demostrar que a pesar de no estar presente sus beneficios en los indicadores de mitigación de riesgos en la matriz, dichos riesgos se reducen considerablemente. Esto da entender que siempre hay maneras para seguir mejorando y mitigando todos los riesgos posibles.

Finalmente cabe concluir que se puede comprobar que es posible realizar mejoras e implementaciones de seguridad perimetral a cualquier tipo de infraestructura, las cuales aminoran los riesgos de la institución adaptándose al presupuesto con el que se cuenta. En cuanto a la falta de concientización y asesoría por parte de los usuarios que utilizan las infraestructuras tecnológicas, en este caso la alta dirección, hacen que los riesgos de perdida de información e incidentes graves de seguridad aumenten. Asimismo el levantamiento de información toma un papel importante a la hora de realizar el análisis y de sugerir las mejoras ya que saber el estado actual y con lo que cuenta la institución nos da un panorama más claro de que se debe implementar, mejorar y mitigar urgentemente sin salirse del plan y presupuesto establecido al inicio del proyecto.

Glosario de términos

Para los efectos del presente documento es importante tener claridad sobre los siguientes conceptos.

Activo: todo lo que tiene valor para la organización.

BackUP: Copia de seguridad de uno o muchos archivos con el fin de poder restaurar en caso de pérdida.

Confidencialidad: Propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.

Control de acceso: Consiste en la verificación de si una entidad (una persona, vehículo, ordenador, etc.) solicitando acceso a un recurso tiene los derechos necesarios para hacerlo.

Datos: Son la unidad mínima de información (en cualquier formato y/o extensión). Deliberadamente su marcha, averiando sus equipos, herramientas, programas y/o operaciones.

Disponibilidad: Propiedad de permanecer accesible y disponible para su uso cuando se requiera.

Filtro de contenido: se refiere a un programa diseñado para controlar qué contenido se permite mostrar, especialmente para restringir el acceso a ciertos materiales de la Web.

Firewall: Dispositivo principal que bloquea todo el tráfico entre la Internet y la red, y subredes locales.

IDS: Detectan posibles ataques en un sistema, pudiendo activar alarmas o ejercer respuesta coordinada

Información: La información constituye uno de los activos más importantes de la organización, esencial para la continuidad de la operación.

Infraestructura: La infraestructura tecnológica agrupa y organiza el conjunto de elementos tecnológicos que integran un proyecto, soportan las operaciones de una organización o sustentan una operación.

Integridad: Característica de salvaguardar la exactitud y completitud de los activos.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Segmentación: Segmentar una red consiste en dividirla en subredes para poder aumentar el número de ordenadores conectados a ella y así aumentar el rendimiento.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Seguridad Informática: es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras.

Sistema Seguro: Un sistema es seguro si en todo momento se comporta como lo desea su propietario.

Spam: Correo electrónico no deseado.

Suplantación informática: Utilización de una clave por una persona no autorizada y que accede al sistema suplantando una identidad.

Topología: se define como el mapa físico o lógico de una red para intercambiar datos. **Usuario:** en el presente documento se emplea para referirse a directivos, funcionarios, contratistas, terceros y otros colaboradores del OCyT.

Virus: Código diseñado para introducirse en un programa, modificar o destruir datos.

VPN (Virtual Private Network): es una tecnología de red que permite una extensión segura de la red privada de área local (LAN) sobre una red pública o no controlada como Internet. **Vulnerabilidad:** Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Debilidad presente en un sistema operativo, software o sistema.

WPA2: WI-FI Protected Access 2 o en castellano Acceso WI-FI protegido 2, es un sistema para proteger las redes inalámbricas WI-FI, creado para corregir las vulnerabilidades en WPA.

+

Anexo 1

Anexo 1. Consentimiento informado

CARTA DE CONSENTIMIENTO INFORMADO TRABAJO DE CAMPO

Señores

INSTITUTO CRISTO REY

Ciudad

Yo **JUAN FERNANDO CORREDOR NINO** estudiante de Especialización en Seguridad de la Información de la **FUNDACION UNIVERSITARIA LOS LIBERTADORES,** me dirijo a usted con el fin de solicitar **AUTORIZACION;** para desarrollar el trabajo de campo del proyecto de grado denominado **PROPUESTA DE MEJORAMIENTO DEL SISTEMA DE SEGURIDAD INFORMATICA Y PERIMETRAL PARA EL INSTITUTO CRISTO REY, UBICADO EN LA CIUDAD DE FONSECA, LA GUAJIRA**, La cual en la actualidad está en proceso de ejecución.

Agradezco de ante mano la atención prestada a esta

Cordialmente

JUAN FERNANDO CORREDOR NINO

Anexo 2. Permiso trabajo de campo Instituto Cristo Rey

INSTITUTO CRISTO REY
Nit. 800.013.817-9
Fonseca – La Guajira

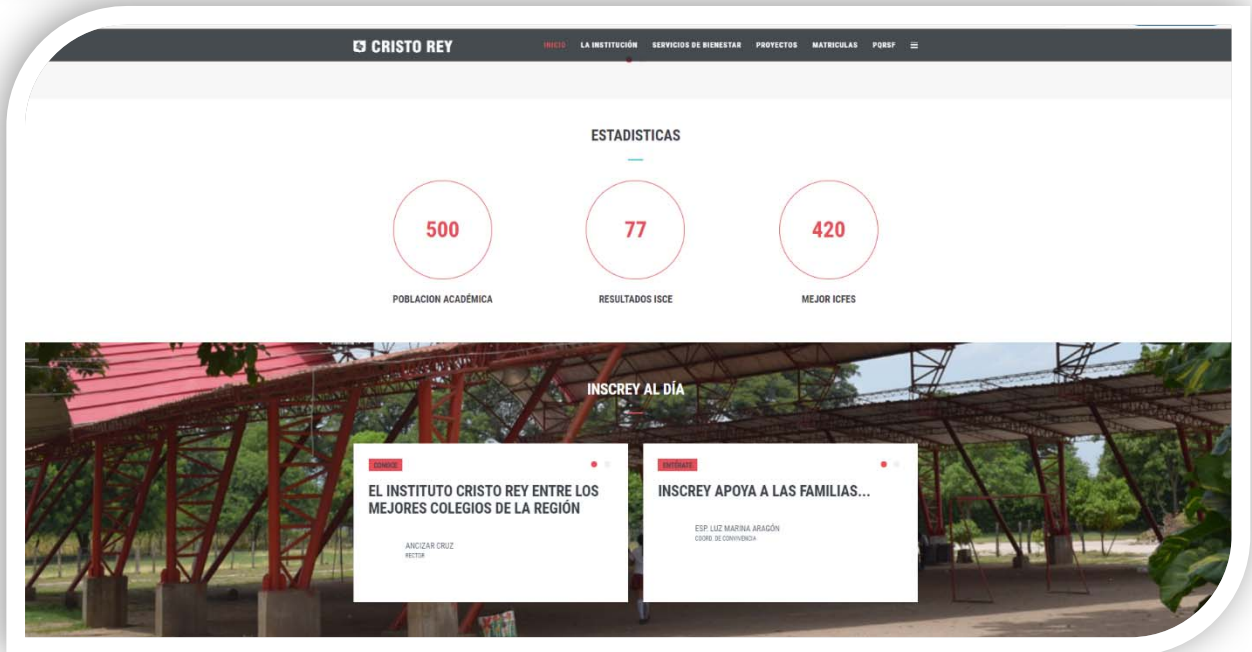
Aprobado por resolución 457 de Mayo 17 de 2012, para todos los grados de Preescolar, Básica y Media, Registro Educativo No. 032 22-V-96 de la Secretaria de Educación Departamental. DANE: 344279001037

Fonseca, La Guajira 5 de septiembre de 2021

Señor
JUAN FERNANDO CORREDOR
Fundación Universitaria Los Libertadores

En medio de la presente el INSTITUTO CRISTO REY se compromete con el estudiante JUAN FERNANDO CORREDOR, a permitir el acceso a la información necesaria para realizar una propuesta de mejoramiento el sistema de seguridad informática y perimetral actual de la Institución.

Esta carta de compromiso se expide a los 5 días del mes de septiembre del año 2021 en la ciudad de Fonseca, La Guajira.

LUZ MARINA ARAGÓN FUENTES
Representante Legal INSCREY

Anexo 3. Página web Instituto Cristo Rey