**DECANATO DE INGENIERÍAS E INFORMÁTICA**
**ESCUELA DE INFORMÁTICA**

# "Análisis y diseño de un sistema de seguridad utilizando la tecnología biométrica (Start Tech) para la empresa Gestiones de aduanas D&M, en la ciudad de Santo Domingo, durante el periodo enero-abril 2019"

Trabajo de grado para optar por el título de:
**Ingeniero de Sistemas de Computación**


## Sustentantes:

| | |
|---|---|
| Carlos Ballast | 2014-1886 |
| Jeffrey Martínez | 2015-0378 |
| Wilson Hazin | 2014-1996 |


**"Los conceptos expuestos en esta investigación son de la exclusiva responsabilidad de sus autores".**


## Asesor:
Ing. Freddy Jiménez


**Santo Domingo, Rep. Dom.**

# “Análisis y diseño de un sistema de seguridad utilizando la tecnología biométrica (Start Tech) para la empresa Gestiones de aduanas D&M, en la ciudad de Santo Domingo, durante el periodo enero-abril 2019”

# ÍNDICE

# ÍNDICE GENERAL

**AGRADECIMIENTOS** ..... I

**DEDICATORIAS** ..... III

**RESUMEN EJECUTIVO** ..... V

**INTRODUCCIÓN** ..... VII

**ASPECTOS METODOLÓGICOS** ..... IX

**CAPÍTULO 1. ANTECEDENTES DE GESTIONES DE ADUANAS D & M** ..... 001

1.1 INTRODUCCIÓN ..... 002

1.2 HISTORIA DE GESTIONES DE ADUANAS D & M ..... 003

1.3 MISIÓN, VISIÓN, VALORES ..... 003

1.4 FILOSOFÍA ..... 004

1.5 ACTIVIDAD ECONÓMICA ..... 004

1.6 COMPETENCIAS DE GESTIONES DE ADUANAS D & M ..... 005

1.7 LOS PRINCIPIOS BÁSICOS DE LA GESTIONES DE ADUANAS D&M . 005

1.8 ORGANIGRAMA ..... 006

1.9 CONCLUSIÓN ..... 007

**CAPÍTULO 2. CONCEPTOS DE REDES Y SEGURIDAD** ..... 008

2.1. INTRODUCCIÓN ..... 009

2.2. CONCEPTOS DE REDES DE DATOS ..... 010

2.3. VENTAJAS DE LAS REDES DE DATOS ..... 010

2.4. TIPOS DE REDES DE DATOS ..... 011

2.4.1 Redes LAN ..... 012

2.4.2 Redes WAN ..... 013

2.4.3 Redes MAN ..... 014

2.4.4 Redes WLAN ..... 015

2.4.5 Redes SAN ..... 016
2.5. CARACTERÍSTICAS DE REDES DE DATOS ..... 017
2.6. SEGURIDAD INFORMÁTICA ..... 018
2.7. VENTAJAS DE LA SEGURIDAD INFORMÁTICA ..... 019
2.8. TIPOS DE SEGURIDAD INFORMÁTICA ..... 020
2.8.1 Seguridad Lógica ..... 021
2.8.2 Seguridad Física ..... 021
2.9. CARACTERÍSTICAS DE SEGURIDAD ..... 022
2.10. FIREWALL ..... 022
2.11. TIPOS DE FIREWALL ..... 024
2.12. CARACTERÍSTICAS DEL FIREWALL ..... 025
2.13. PROXY ..... 027
2.14. IMPORTANCIA DEL PROXY ..... 027
2.15. CONCEPTO DE VIRUS INFORMÁTICOS ..... 028
2.16. TIPOS DE VIRUS INFORMÁTICOS ..... 028
2.16.1 Por Su Capacidad De Propagación ..... 028
2.16.1.1 Virus ..... 028
2.16.1.2 Gusanos ..... 029
2.16.1.3 Troyanos ..... 029
2.16.2 Por Las Acciones Que Realizan En El Equipo Infectado ..... 030
2.16.2.1 Adware ..... 030
2.16.2.2 Bloqueador ..... 030
2.16.2.3 Bomba lógica ..... 031
2.16.2.4 Broma (Joker) ..... 031
2.16.2.5 Bulo (Hoax) ..... 032

2.16.2.6 Capturador De Pulsaciones (Keylogger) ..... 032
2.16.2.7 Clicker ..... 033
2.16.2.8 Criptovirus (Ransomware) ..... 033
2.16.2.9 Descargador (Dowloader) ..... 034
2.16.2.10 Espía (Spyware) ..... 034
2.16.2.11 Exploit ..... 035
2.16.2.12 Herramienta De Fraude ..... 035
2.16.2.13 Instalador (Dropper) ..... 036
2.16.2.14 Ladrón De Contraseñas (Pwstaler) ..... 036
2.16.2.15 Marcador (Dialer) ..... 037
2.16.2.16 Puerta Trasera (Backdoor) ..... 037
2.16.2.17 Rootkit ..... 038
2.16.2.18 Secuestrador De Navegador (Browser Hijacker) ..... 038
2.17. CARACTERÍSTICAS DE LOS VIRUS ..... 039
2.18. MÉTODOS DE TRANSMISIÓN DE LOS VIRUS ..... 039
2.19. MÉTODOS DE PROTECCIÓN CONTRA LOS VIRUS ..... 039
2.20. POLÍTICAS DE SEGURIDAD ..... 040
2.21. POLÍTICAS DEL SISTEMA ..... 040
2.22. TOPOLOGÍAS DE REDES ..... 041
2.23. TIPOS DE TOPOLOGÍAS ..... 042
2.23.1 Topología de Bus ..... 042
2.23.2 Topología Punto a Punto ..... 042
2.23.3 Topología en árbol ..... 043
2.23.4 Topología en Anillo ..... 043
2.23.5 Topología en Estrella ..... 044

2.23.6 Topología en Malla ..... 044
2.23.7 Topología Mixta ..... 045
2.24. IMPORTANCIA DE LA TOPOLOGÍA DE RED ..... 045
2.25. CONCLUSIÓN ..... 046
**CAPÍTULO 3. TECNOLOGÍAS BIOMÉTRICAS** ..... 047
3.1. INTRODUCCIÓN ..... 048
3.2. CONCEPTOS DE TECNOLOGÍA BIOMÉTRICA ..... 049
3.3. SEGURIDAD BIOMÉTRICAS ..... 049
3.4. TIPOS DE TECNOLOGÍA BIOMÉTRICA ..... 050
3.4.1 Reconocimiento Oculares ..... 050
3.4.2 Reconocimiento Facial ..... 052
3.4.3 Reconocimiento Dactilar ..... 053
3.4.4 Reconocimiento por Voz ..... 053
3.5 VENTAJAS DE LAS TECNOLOGÍAS BIOMÉTRICA ..... 054
3.6. IMPORTANCIA DE LAS TECNOLOGÍA BIOMÉTRICA ..... 054
3.7. CARACTERISTICAS DE LA TECNOLOGIA BIOMETRICA ..... 055
3.8. TECNOLOGIA BIOMETRICA HUELLA DACTILAR ..... 055
3.8.1. Características ..... 055
3.8.1.1. Puntos Singulares ..... 057
3.8.2. Ventajas ..... 057
3.8.3. Técnicas de Reconocimiento ..... 057
3.8.4. Modelo de Identificación ..... 058
3.9. CONCLUSIÓN ..... 059

**CAPÍTULO 4. PROPUESTA DE DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA BIOMÉTRICO PARA LA EMPRESA GESTIONES DE ADUANAS D & M** ..... 060

4.1. INTRODUCCIÓN ..... 061

4.2. SITUACIÓN TECNOLÓGICA DE GESTIONES DE ADUANAS D & M . 062

4.3. DIAGRAMA DE RED ACTUAL ..... 067

4.4. ANÁLISIS FODA ..... 070

4.5. PROPUESTA DE DESARROLLO E IMPLEMENTACIÓN DE UN DATA CENTER ..... 071

4.5.1. Equipos Propuestos ..... 071

4.5.2. Fundamento de la Propuesta ..... 075

4.5.3. Objetivos de la Propuesta ..... 075

4.5.4. Ubicación del Data Center ..... 076

4.6. PROPUESTA DE IMPLEMENTACIÓN DE LA NUEVA RED ..... 077

4.6.1. Componentes Necesarios ..... 077

4.6.2. Diseño de la Nueva Red ..... 079

4.6.3. Fundamentos de la Propuesta ..... 080

4.6.4. Objetivos de la Propuesta ..... 080

4.7. PROPUESTA DE IMPLEMENTACIÓN DE LA TECNOLOGÍA DE HUELLA DACTILAR ..... 081

4.7.1. Equipos Necesarios ..... 081

4.7.2 Fundamentos de la Propuesta ..... 082

4.7.3 Objetivos de la Propuesta ..... 082

4.8. ESTUDIO DE FACTIBILIDAD ..... 083

4.9. TÉCNICA OPERATIVA ..... 083

4.10. INVERSIÓN DEL PROYECTO ..... 084

4.11. CÁLCULO DE RETORNO DE INVERSIÓN ..... 086

4.12. CRONOGRAMA DEL PROYECTO ..... 086

4.13. CONCLUSIÓN ..... 088

**CONCLUSIÓN** ..... 089

**RECOMENDACIÓN** ..... 091

**BIBLIOGRAFÍA** ..... 093

**GLOSARIO** ..... 098

**ANEXOS** ..... 101

# ÍNDICE DE TABLAS

## CAPÍTULO 4. PROPUESTA DE DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA BIOMÉTRICO PARA LA EMPRESA GESTIONES DE ADUANAS D & M

TABLA 4. 1. Características del Servidor ..... 071

TABLA 4. 2. Características del Router EdgeRouter 4 ..... 072

TABLA 4. 3. Características del Switch D-Link ..... 073

TABLA 4. 4. Características del Access Point ..... 073

TABLA 4. 5. Especificaciones de ZKTECO ..... 081

TABLA 4. 6. Inversión en Equipos Informáticos ..... 084

TABLA 4. 7. Inversión del Cableado Estructurado ..... 084

TABLA 4. 8. Inversión en Sistemas de Seguridad ..... 085

TABLA 4. 9. Inversión en Herramientas ..... 085

TABLA 4.10. Inversión Total ..... 085

# ÍNDICE DE IMÁGENES

FIGURA 0.1. Seguridad en la Red ..... X

FIGURA 1. 1. logo de la empresa Gestiones de Aduanas D&B ..... 003

FIGURA 1. 2. Organigrama de la empresa Gestiones de Adunas D&M ..... 006

FIGURA 2. 1. Redes y Seguridad ..... 009

FIGURA 2. 2. Redes LAN ..... 012

FIGURA 2. 3. Redes WAN ..... 013

FIGURA 2. 4. Redes MAN ..... 014

FIGURA 2. 5. Redes WLAN ..... 015

FIGURA 2. 6. Redes SAN ..... 016

FIGURA 2. 7. Seguridad Informática ..... 018

FIGURA 2. 8. Seguridad Lógica ..... 021

FIGURA 2. 9. Seguridad Física ..... 021

FIGURA 2. 10. Firewall ..... 022

FIGURA 2. 11. Firewall Hardware ..... 024

FIGURA 2. 12. Firewall Software ..... 025

FIGURA 2. 13. Características del Firewall 1 ..... 025

FIGURA 2. 14. Características del Firewall 2 ..... 026

FIGURA 2. 15. Características del Firewall 3 ..... 026

FIGURA 2. 16. Proxy ..... 027

FIGURA 2. 17. Tipos de Virus ..... 028

FIGURA 2. 18. Virus ..... 028

FIGURA 2. 19. Gusanos ..... 029

FIGURA 2. 20. Troyanos ..... 029

FIGURA 2. 21. Adware ..... 030

FIGURA 2. 22. Bloqueador ..... 030
FIGURA 2. 23. Bomba Lógica ..... 031
FIGURA 2. 24. Joker ..... 031
FIGURA 2. 25. Hoax ..... 032
FIGURA 2. 26. Keylogger ..... 032
FIGURA 2. 27. Clicker ..... 033
FIGURA 2. 28. Ransomware ..... 033
FIGURA 2. 29. Downloader ..... 034
FIGURA 2. 30. Spyware ..... 034
FIGURA 2. 31. Exploit ..... 035
FIGURA 2. 32. Herramienta de fraude ..... 035
FIGURA 2. 33. Dropper ..... 036
FIGURA 2. 34. PWstaler ..... 036
FIGURA 2. 35. Dialer ..... 037
FIGURA 2.36. Backdoor ..... 037
FIGURA 2. 37. Rootkit ..... 038
FIGURA 2. 38. Browser Hijacker ..... 038
FIGURA 2. 39. Topologías de Red ..... 041
FIGURA 2. 40. Topología Bus/Lineal ..... 042
FIGURA 2. 41. Topología Punto a Punto ..... 042
FIGURA 2. 42. Topología de Árbol ..... 043
FIGURA 2. 43. Topología de anillo ..... 043
FIGURA 2. 44. Topología de Estrella ..... 044
FIGURA 2. 45. Topología de malla ..... 044
FIGURA 2. 46. Topología Mixtas ..... 045

FIGURA 3. 1. Conceptos Tecnología Biométrica ..... 049
FIGURA 3. 2. Reconocimiento Ocular ..... 050
FIGURA 3. 3. Reconocimiento de Iris ..... 050
FIGURA 3. 4. Reconocimiento de Retina ..... 051
FIGURA 3. 5. Reconocimiento Facial ..... 052
FIGURA 3. 6. Reconocimiento Dactilar ..... 053
FIGURA 3. 7. Reconocimiento por voz ..... 053
FIGURA 3. 8. ventajas de la tecnología biométrica ..... 054
FIGURA 3. 9. Características de las Huellas Dactilares ..... 055
FIGURA 3. 10. Puntos Característicos de la Huella Dactilar ..... 056
FIGURA 3. 11. Puntos Singulares de la Huella Dactilar ..... 057
FIGURA 4. 1. Situación actual de la empresa Gestiones de Aduanas D&M 1 ..... 062
FIGURA 4. 2. Situación actual de la empresa Gestiones de Aduanas D&M 2 ..... 063
FIGURA 4. 3. Situación actual de la empresa Gestiones de Aduanas D&M 3 ..... 063
FIGURA 4. 4. Situación actual de la empresa Gestiones de Aduanas D&M 4 ..... 064
FIGURA 4. 5. Situación actual de la empresa Gestiones de Aduanas D&M 5 ..... 064
FIGURA 4. 6. Situación actual de la empresa Gestiones de Aduanas D&M 6 ..... 065
FIGURA 4. 7. Situación actual de la empresa Gestiones de Aduanas D&M 7 ..... 065
FIGURA 4. 8. Situación actual de la empresa Gestiones de Aduanas D&M 8 ..... 066
FIGURA 4.9. Situación actual de la empresa Gestiones de Aduanas D&M 9 ..... 066
FIGURA 4. 10. Diagrama de Red Actual de la empresa Gestiones de Aduanas D&M .... 067
FIGURA 4.11. DELL Poweredge T30 Tower ..... 071
FIGURA 4.12. Router Ubiquiti edgerouter 4 ..... 072
FIGURA 4. 13. Switch ..... 072
FIGURA 4.14. Access Point ..... 073

FIGURA 4.15. Teléfono IP ..... 074
FIGURA 4.16. Ubicación del Data Center ..... 076
FIGURA 4.17. Gabinete ..... 077
FIGURA 4.18. Patch Panel ..... 078
FIGURA 4.19. FacePlate ..... 078
FIGURA 4.20. Diagrama de la Nueva Red de Gestiones de Adunas D & M ..... 079
FIGURA 4.21. ZKTECO ZK-K214 ..... 081
FIGURA 4.22. Cronograma del Proyecto ..... 086
FIGURA 4.23. Cronograma del Proyecto Etapa 1 ..... 087
FIGURA 4.24. Cronograma del Proyecto Etapa 2 ..... 087
FIGURA 4.25. Cronograma del Proyecto Etapa 3..... 087

# AGRADECIMIENTO

# Agradecimiento

Antes de todo primero quiero agradecer a Dios por abastecernos de sabiduría para el desarrollo de este trabajo. Como también dar gracias a Dios por permitirme disfrutar a mí familia. Por darme la fuerza para superar cada obstáculo que aparecieron en el camino, por permitirme conocer a lo largo de este camino a tantas personas que nos suman en nuestras vidas.

Gracias a mis padres y hermanos: Wilson Hazin, Fátima Matos, Miguel Hazin Matos y Magaly Hazin Matos.

También quiero agradecer a nuestro asesor, el profesor Freddy Jiménez por la ayuda y orientación que nos brindó a lo largo del desarrollo de este trabajo de grado.

**Wilson Hazin**

Agradezco a Dios por dotarme de la perseverancia, sabiduría y determinación para trazar y llevar a cabo mis metas, a mis padres por su presencia, apoyo y ardua dedicación a mi total desarrollo como un individuo de bien, a mis amigos por darme su apoyo en los momentos más difíciles de la carrera.

Agradezco a nuestro asesor Freddy Jiménez por guiarnos en las buenas prácticas y quehaceres y en el desarrollo de este trabajo de Grado.

Agradezco a Julio Profe cuyo canal de YouTube me permitió avanzar en las matemáticas más complicadas.

Agradezco a mi coro de las mesas azules ya que gracias a ellos la estancia en APEC que ellos saben que fueron pasadías ha sido de lo más divertido.

Agradezco a Jose Garcia Apolinar un excelente profesor y maestro que nos enseñe más que números y calculo.

A nuestro Decano Emin Rivera que nos enseñó no solo para aprobar la materia también para la vida.

**Jeffrey Martínez**

Agradezco a dios ante todos por dame los conocimientos para el desarrollo de este trabajo, a mis compañeros por la cooperación que me ofrecieron. También agradezco a la Compañía Gestiones de Adunas D & M por permitirme hacer este trabajo que va dedicado para ellos, a mis padres que siempre están con amigos en los momentos difíciles y los felices.

Agradezco a todos los profesores que me dieron los conocimientos en el transcurso de mis estudios universitarios y al profesor Freddy Jiménez por guiarme a mí y mis compañeros en este trabajo de grado.

**Carlos Ballast**

# DEDICATORIAS

# Dedicatorias

Dedico este trabajo principalmente a dios por darme sabiduría y fuerza.

A mis padres Carlos Ballast y Carmen Maritza que estuvieron para mí en todo momento dándome su apoyo incondicional para alcanzar esta meta.

A mis hermanos Alexis Ballast y Eduardo Ballast que estuvieron apoyándome y dándome consejos para elaborar este trabajo.

A Jeffrey Martinez y Wilson Hazin que fueron mis compañeros en la universidad y luego se convirtieron en mis amigos, además de que fueron los que me ayudaron en este trabajo de grado.

**Carlos Ballast**

Dedico este trabajo a mis Padres Teófilo Martínez Gonzales, a mi madre Neida Elizabeth Pérez de la Paz, a todos mis amigos que a lo largo de estos años de estudios me han brindado apoyo para continuar y perseverar en mis estudios.

A Dios por brindarme la fuerza y conocimiento para asimilar las enseñanzas de mis maestros y para avanzar en cada uno de los cuatrimestres de esta carrera.

A mis compañeros de Wilson Hazin y Carlos Ballast que aceptaron ser mis compañeros de tesis y me acompañaron a lo largo de esta travesía universitaria.

**Jeffrey Martínez**

Este trabajo va dedicado a mis padres Wilson Hazin y Famita Matos. Como también a mis hermanos Miguel y Magaly Hazin Matos por brindarme su apoyo y tiempo a lo largo de mi carrera universitaria.

También quiero dedicar este trabajo a mis compañeros Carlos Ballast y Jeffrey Martínez por brindarme su amistad durante todo este tiempo.

**Wilson Hazin**

# RESUMEN EJECUTIVO

## Resumen Ejecutivo

En el presente trabajo de investigación, se plantea la problemática que presenta actualmente la carencia de un sistema de seguridad eficiente y efectivo en la empresa Gestiones de Aduanas D & M, esta problemática supone para la empresa un sinnúmero de vulnerabilidades dentro de esta institución, dichas vulnerabilidades se pueden ver como futuras brechas para diversos tipos de ataques dentro de la empresa, lo que a futuro se puede reflejar como pérdidas invaluables dentro de esta.

Esta empresa no cuenta con ninguna infraestructura propia, por lo cual dificulta la integración de cualquier tipo de sistema de seguridad o cualquier medio para salvaguardar los datos más importantes de esta, por ende, dentro de los objetivos de dicho trabajo diseñaremos un sistema capaz de albergar dicha infraestructura.

La contribución en este trabajo de investigación trata sobre analizar un diseño de sistema de seguridad utilizando las diversas tecnologías biométricas para así asegurar que la empresa funcione de manera eficaz y eficiente, lo que conlleva rediseñar a través de métodos de investigación rigurosos, así como la observación, análisis, encuestas, investigación y consultas con expertos.

Con el fin de optimizar y mejorar los recursos a emplear y con el fin de llegar a resolver la problemática que pasa esta empresa buscamos y analizamos diversas informaciones provenientes de trabajos de grado tanto de años anteriores como extranjeras con el fin de recopilar información y poder optar por las mejores opciones para la condición y situación de la empresa tanto a nivel tecnológica como a nivel social y económica. Con la información recopilada se creará una propuesta óptima para las necesidades de la organización, capaz de satisfacer cada requisito demandado y ser capaz de sostenerse por un periodo de tiempo amplio sujeto a crecimiento.

En este trabajo también se verá agregado varios documentos externos como son las encuestas realizadas a los usuarios o mejor dicho empleados de la institución, con el fin de recopilar información de la situación actual de la institución y para así conocer la opinión actual de los empleados sobre los servicios, de esta manera tomando estos datos y hablando con los expertos encargados de la infraestructura y las redes de la empresa desarrollamos la propuesta explicada en este documento.

# INTRODUCCIÓN

# Introducción

A través de los años la implementación de mecanismos de seguridad se han vuelto un factor imprescindible, y más cuando se trata de proteger la integridad tanto física como de los datos de una organización o empresa. Por esto es importante una buena elección del mecanismo que de seguridad se va a implementar, ya que si no se contempla las soluciones correctas la organización estará expuesta a que personas mal intencionadas traten de extraer información valiosa o equipos valiosos para la organización.

Debido a que cada humano tiene rasgos únicos con lo cual combinado con la tecnología de hoy en día nos permite tener controles de seguridad más confiables, uno de ellos es la seguridad utilizando huellas dactilares.

Cuando hablamos de estas huellas no estamos refiriendo la biometría en sí, y esta son aquellos rasgos físicos (huellas dactilar, facial, iris, etc.) con lo cual un humano que diferencian de otro.

La situación tecnológica actual de la empresa que cuenta con un total de 3 computadoras, de estas 2 son computadoras de escritorio y una laptop, todas conectadas a la misma red, así mismo como seguridad mínima poseen cámaras de vigilancia en diversos puntos de la institución, dado que, aunque su posición tecnológica no es mala no poseen un sistema centralizado de trabajo a nivel informático con lo cual están expuestos a desastres naturales con el cual se haga una pérdida total de los archivos.

Debido a lo anterior, la empresa Gestiones de aduanas D&M carece de un mecanismo de seguridad que les garantice que la continua monitorización de su personal o de personas ajenas a dicha empresa. Por esto, en este proyecto veremos como la utilización de mecanismos de seguridad mediante el uso de rasgos biométricos podemos brindar un grado mayor de seguridad a la empresa de forma que no esté expuesta a situaciones que puedan perjudicar el tiempo de producción, a su vez introduciremos un data center para mejorar la calidad de red y de eficiencia dentro de la institución donde los programas y servicios de uso común podrán ser centralizados y donde se podrá introducir los respaldos de manera periódicas para la protección de datos en caso de algún incidente o daño permanente en los equipos de trabajo, estas mejoras permitirán un aumento en la eficiencia y en la gestión de procesos dentro de la institución y a su vez centralizara los procesos haciendo toda la labor más eficiente.

# ASPECTO METODOLÓGICO

## I. Planteamiento Del Problema

Se delimitará a la República Dominicana, Santo Domingo, en la empresa Gestiones de aduanas D&M ubicada en el Edificio 1, Manzana 12, Local 105, Km. 10 10/2, Plaza José Contreras, Carret, Sánchez, Santo Domingo, R.D en el periodo enero-abril 2019.

En todas las empresas de servicios públicas o privadas ocurre mucho tráfico de personas ya estas siendo empleados o visitantes; los visitantes se trasladan por toda la institución aunque existe una seguridad interna contratada, pero esta no brinda confiabilidad de que las áreas más críticas de la institución como los data center y cuartos de servidores no sean violados por algún descuido del personal o visitante, por lo que la mejor opción es reforzar esta seguridad con elementos electrónicos y software para tener un sistema más robusto, la utilización de dispositivos de verificación biométrica, cámaras de vigilancia y confirmación por pin o credenciales ante cada entrada de las zonas críticas.

A raíz de estos males sin los medios defensivos correctos, las consecuencias pueden ser bastantes altas como podría ser la pérdida de información valorada en miles de dólares, daños en la infraestructura de la empresa o robo de información vital, también una fuerte vulnerabilidad al hackeo.

Esta situación se debe a la falta de controles de acceso en la institución, los cuales permiten evitar la entrada a personas ajenas. También nos permite tener un control sobres la personas que han intentado acceder sin autorización y poder reaccionar de la mejor manera de evitar que dicho intruso haga más daño.

*Figura 0. 1. Seguridad en la Red*
**Fuente: https://www.tecnoseguro.com/**

Dado lo citado con anterioridad se hace necesario el diseño de un sistema de seguridad asistido por verificación biométrica en toda la institución, cubriendo y creando la barrera que permitirá que solo el personal apto o cualificado pueda acceder a las zonas que se le sea permitida, especificado por el departamento de TI en conjunto con recursos humanos.

Instalaciones de cámaras de vigilancias en zonas estratégicas para crear un ambiente de seguridad tanto para los equipos como para toda persona que entre en la empresa y a su vez trabajar en el diseño de las redes para proteger el sistema de ataques virtuales con fuertes y robustos firewall y seguridad protegiendo así los datos de la empresa, de esta manera la organización obtendrá un grado de seguridad elevado no sólo para su información sino también para el personal y visitantes dentro de ella.

## II. Justificación

Desde tiempos inmemorables se ha dado la diversas situaciones donde individuos no deseados o personas no autorizadas accedan a lugares u áreas no accesible , en consecuencia se han presentados diversos inconvenientes o problemas, para eso trabajaremos con el diseño de un sistema de seguridad o autentificación biométrica donde solo las personas autorizadas tendrán acceso a las áreas permitidas y donde las áreas más sensibles estarán más segura, esto tendrá como pie a que se deberá trabajar o diseñar una red lo suficientemente robusta para albergar o sustentar el sistema, para este fin es necesario diseñar una infraestructura con los dispositivos capaces de llevar a cabo este cometido .

Se partirá con la tecnología biométrica por el hecho de que nos ofrece una gran variedad de métodos de autenticación biométrica, a su vez permite combinar los medios de autenticación existentes como lo es la combinación entre autentificación biométrica y pin o mediante una tarjeta de acceso, esta solución permite también el máximo nivel de seguridad ya que el material o elemento biométrico a usar es único e irrepetible en cada persona o ser vivo en el planeta, esto nos permite un 100% de efectividad a la hora del control de acceso.

Este trabajo arroja como resultado el diseño o modelado de un sistema con diversas áreas específicas, como es una red LAN con las configuraciones necesarias para albergar el sistema y capacidad suficiente para un buen rendimiento de este, un diseño de seguridad óptimo con sistemas biométricos, cámaras de seguridad y medios de acceso a través de contraseñas, este diseño será de gran provecho ya que permitirá mejorar exponencialmente la seguridad y el rendimiento de la red de la institución.

# III. Objetivos

## Objetivos General

Diseñar un sistema de seguridad utilizando la tecnología biométrica (Start Tech) para la empresa Gestiones de Aduanas D&M durante el periodo enero-abril 2019 en la ciudad de santo domingo.

## Objetivos Específicos

- Definir las redes LAN para el correcto funcionamiento de múltiples sistemas.
- Determinar qué tipo de sistema biométricos se utilizarán.
- Señalar las áreas sensibles y críticas donde se empleará más el sistema de seguridad.
- Diagnosticar qué tipo de autenticación se utilizará en la empresa
- Analizar y señalar los tipos de depósitos que se utilizaran en la infraestructura de la empresa.

## V. Fuentes y técnicas para recolección de información

La técnica que utilizaremos la investigación descriptiva, explicativa lo cual estaremos comunicando con nuestro cliente para que este nos facilite información sobre los parámetros necesarios para iniciar el análisis y diseño del sistema en cuestión.

Como métodos secundarios de recolección de información nos auxiliamos de revistas, libros, tesis, documentos y proyectos anteriores que estén validados y sean de temas relacionados al nuestro para así obtener la información necesaria para este trabajo.

# CAPÍTULO 1
# ANTECEDENTES DE GESTIONES DE ADUANAS D & M

## 1.1 Introducción

En la empresa Gestiones de Aduanas D&B se tiene como principal actividad la desaduanización de las mercancías de nuestros clientes, donde nos encargamos de todo el proceso que lleva para lograr retirar la mercancía de los puertos de adunas, nuestra característica principal es que la eficacia atada a la seguridad que esta debe tener.

Unos de los servicios más buscados en nuestra empresa es la asesoría, por la misma hemos captado un número de clientes considerables dándole la calidad que se merecen al momento de brindarle nuestros servicios. Dentro de las garantías que ofrecemos están la confianza, responsabilidad y transparencia con la que trabajamos cada expediente que depositan en las oficinas de Gestiones Aduanales D&B.

El equipo de trabajo está preparado para dirigidos a cada persona que desee importar y exportar sus productos con la responsabilidad que estos requieren, teniendo como base la complejidad que tiene cada servicio de aduanas que nosotros ofrecemos y tratamos de que esto sea de fácil manejo para nuestros clientes. Como compañía adquirimos el compromiso que tiene cada persona que pertenece a nuestro equipo de trabajo, de dar lo mejor al momento de estar realizando los manejos correspondientes para entregar un trabajo terminado.

## 1.2 Historia de Gestiones de Aduanas D & M

*Figura 1. 1 Logo de la empresa Gestiones de Aduanas D&B*

En Gestiones de Aduanas D&B nos encargamos de realizar todas las diligencias aduaneras para nuestros clientes, con la finalidad de que estos reciban a tiempo su producto de importación, los acompañamos desde su pedido hasta que su mercancía llega al puerto de aduanas correspondiente, le garantizamos un servicio íntegro, rápido y que no altera su presupuesto.

Gestiones de Aduanas D&B inicio desde el año 2015 y hasta la fecha hemos brindado un servicio de calidad a nuestros principales clientes, destacándose en nosotros la responsabilidad y la seriedad en la entrega de los compromisos asumidos.

La organización también realiza envíos de mercancía al exterior, garantizando el tiempo y su seguridad en la entrega.

Esta compañía fue fundada por "Lic. Juan Miguel Domínguez", su gerente actualmente.

## 1.3 Misión, Visión, Valores

**Misión:**

Gestión de Aduanas D&B tiene como misión principal el buen servicio para garantizar sus clientes, pero en su labor se principalmente es brindar el mejor servicio para la desaduanización.

Asegurar que cada empresa pueda contar con su mercancía en el tiempo prudente y pueda disponer de esta en su cartelera de producto para su comercialización, que esta cuente con la seguridad de tiempo al momento que realice su pedido contando con nosotros para sus trámites finales.

**Visión:**

Convertirnos en la agencia aduanal número uno en el territorio nacional, ofreciendo el mejor servicio personalizado en gestiones aduaneras y lograr que nuestros y futuros clientes tengan de manera rápida y eficaz su mercancía en el menor tiempo posible de una manera confiable y eficaz.

**Valores:**

Dentro de nuestros valores podemos mencionar:

- **Responsabilidad**, porque se está comprometido con cada cliente de nuestra compañía.
- **Transparencia**, porque todos nuestros servicios son verificables en cualquier momento.
- **Calidad**, por la garantía que tienen con nuestros servicios.
- **Lealtad**, porque somos fiel a nuestro desempeño.
- **Seriedad**, la demostramos a entregarla en cada trabajo.
- **Conocimiento**, porque tenemos vasta experiencia en el área.
- **Integridad**, al momento de planear nuestro esquema de trabajo.
- **Respeto**, a cada compañía que elige nuestros servicios.
- **Trabajo en Equipo**, porque todos juntos hacemos un buen trabajo.
- **Experiencia**, con cada embarcación que trabajamos y obtenemos el mejor resultado.
- **Compromiso**, porque siempre estamos comprometidos con nuestro deber en particular.

## 1.4 Filosofía

En Gestiones de Aduanas D&M creemos en ofrecer el mejor servicio de calidad y soluciones de logísticas a nuestros clientes mediante una nueva innovación continua en nuestros servicios y contamos con una mejora de nuestros profesionales. Lo hacemos mediante armonía y el respeto a nuestros clientes y personal. Nos esforzamos en perfeccionar todo lo que nos proponemos. Nuestra filosofía es la calidad en cada servicio.

## 1.5 Actividad Económica

Gestión de Aduanas D&M nos caracterizamos por realizar cualquier tipo de asesoría aduanal para la importación y exportación de su mercancía, le orientamos para la realización de los trámites necesarios para colocar el producto en aduanas.

La empresa se dedica a presentan la mercancía del importador a las aduanas del país, con la finalidad de viabilizar el proceso para que nuestros clientes puedan pagar su impuesto correspondiente a sus mercancías.

Realizamos el proceso de verificación física en aduana cuando llega la mercancía al puerto primario de verificación, como esto es requerido por el departamento de la Dirección general de aduanas.

Nos encargamos de facilitar el transporte correcto para movilizar la mercancía lo más segura posible a su destino, creando una logística para asegurar el proceso de despacho de dicha mercancía.

Revisamos cada clasificación por producto en sus partidas o en sus códigos arancelario correspondiente para así evitar que esta pueda ser penalizado por una mala clasificación arancelaria y no sea viable y oportuno su despacho de las instalaciones aduanales.

En nuestra compañía cada cliente es tratado como parte importante de nuestra empresa como un ente único, especial y prioritario, dándole un seguimiento personalizado a su necesidad e integrando el carácter de urgencia que merece cada proceso de su servicio.
Nos hemos catalogado como un equipo capacitado en este tipo de gestión con la más vasta experiencia en gestiones aduanales.

## 1.6 Competencia de Gestiones de Aduanas D&M

Estamos dirigidos a cada persona que desee importar y exportar sus productos con la responsabilidad que estos requieren, siempre tomamos en cuenta la necesidad que tiene cada servicio de aduanas que nosotros ofrecemos. El compromiso que tiene cada persona que pertenece a nuestro equipo de trabajo, estos se comprometen en cada servicio brindado a cada uno de los clientes. Los trabajos que realizamos son exportaciones, importaciones y regímenes aduaneros. Toda persona que desee monitorear de cerca su mercancía, con la confiabilidad de su propia empresa, nosotros como empresa le brindamos esa seguridad y transparencia en todo su proceso de desembarque.

## 1.7 Los principios básicos de Gestiones de Aduanas D&M son:

Proveer un servicio de calidad que cumpla con las necesidades de nuestros clientes y que estas cumplan con todas las fases contratadas, minimizando los servicios que no sean de conformidad al cliente.

Cumplir con todas las disposiciones y reglamentaciones ligadas a los servicios que ofrecemos a nuestros clientes, incluyendo con estos los requisitos aplicables a los sistemas de gestión que nosotros implementados en nuestra gestión aduanera.

Pretendemos obtener una mejora en la prestación de nuestros servicios y en el manejo del desempeño de nuestro sistema para mejorar la Calidad, Seguridad, Salud y mejor Ambiente de negocios.

Tratamos de Motivar y ofrecer desarrollo profesional a nuestro personal.

Proveer lugares de trabajos limpios, sanos y seguros, estableciendo controles apropiados para la prevención de los riesgos de seguridad y salud de nuestros empleados, visitantes, contratistas y clientes.

Asegurar la integridad de la empresa y de las mercancías en términos físicos, así como en el manejo de documentos e información.

Establecer controles apropiados para la prevención de la contaminación ambiental y a la vez mantener nuestro compromiso con la mejora continua de nuestro desempeño ambiental.

Sensibilizar e informar al personal y a nuestros relacionados sobre sus responsabilidades en materia de seguridad y salud, así como sobre la importancia del cuidado del medioambiente.

Garantizar al personal sus derechos humanos y laborales.

Mantener una relación y un compromiso de trabajar con los empleados, con la comunidad y con la sociedad, con la finalidad de contribuir en su proceso de desarrollo.

Garantizamos el éxito de nuestra política mediante el compromiso del equipo humano de la organización con el cumplimiento de nuestros objetivos, así como con las revisiones periódicas de cumplimiento y mejora continua.

## 1.8 Organigrama

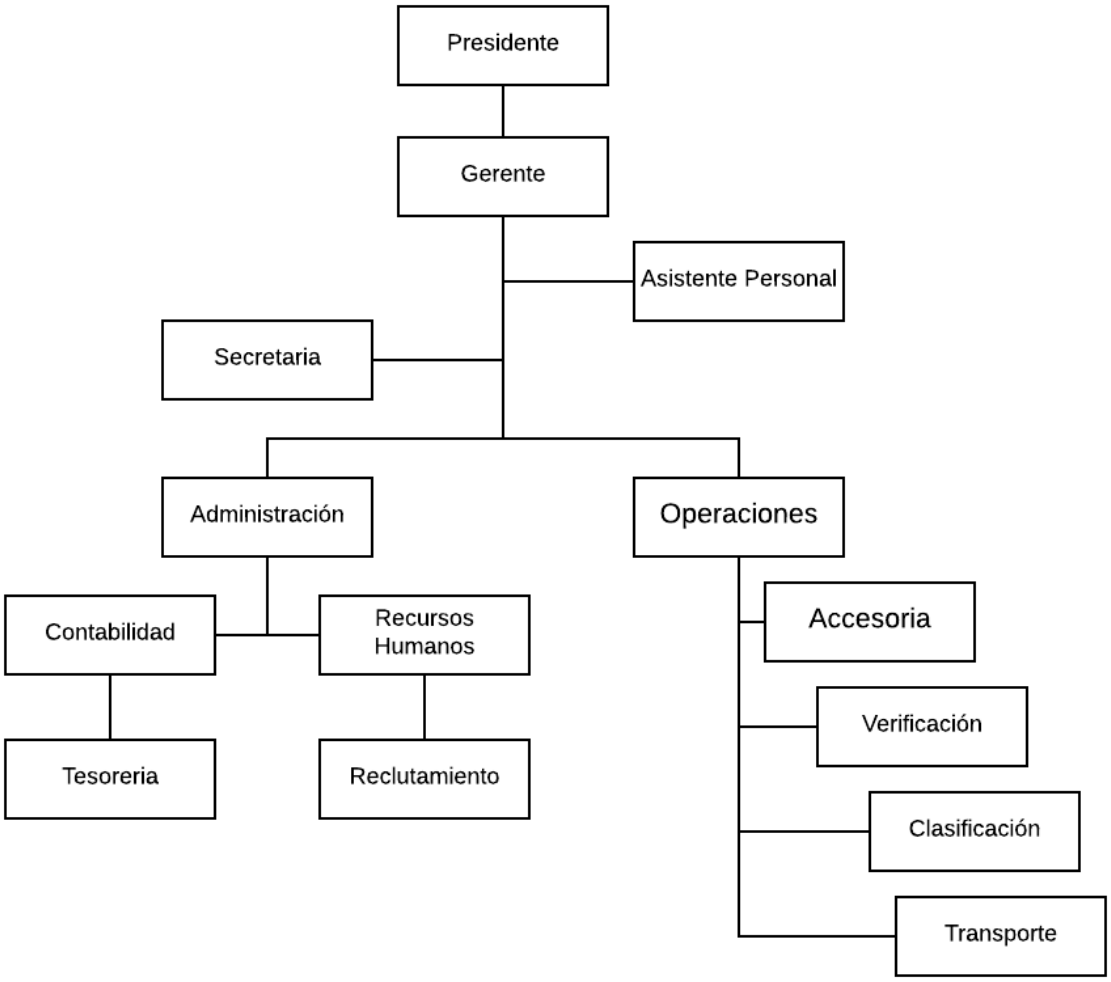



*Figura 1. 2 Organigrama de la empresa Gestiones de Adunas D&M*

## 1.9 Conclusión

En Gestiones de Aduanas D&B es un equipo de trabajo que está comprometido con cada una de sus clientes, dándole como fuente inicial la transparencia a nuestros clientes, para cada día estar más especializados en nuestra área de trabajo.

Nuestra meta más importante es la de convertirnos en la agencia aduanal número uno en el territorio nacional, ofreciendo el mejor servicio personalizado en gestiones aduaneras y lograr que nuestros y futuros clientes tengan de manera rápida y eficaz su mercancía en el menor tiempo posible de una manera confiable y eficaz.

Tratar de ofrecer el mejor conjunto de servicios posible para que cada caso, se puede completar totalmente con nosotros, ya sea desde el monitoreo de cada mercancía hasta el transporte hacia nuestros clientes como destino final. Nos satisface que cada proceso pueda realizarse cada vez más rápido para así garantizarles una entrega más efectiva.

# CAPÍTULO 2
# CONCEPTO DE REDES Y SEGURIDAD

## 2.1 Introducción

En este capítulo se hablará de los conceptos básicos de redes y de seguridad informática, elementos que son indispensables para el correcto seguimiento de este trabajo. En este segundo capítulo desarrollaremos a fondo lo que son las redes, sus tipos, la seguridad informática y sus tipos y las diferentes vertientes que van acorde a estos temas y su debida importancia.

Como también veremos las ventajas y desventajas que tiene la utilización de una red, y también la implementación de mecanismo de seguridad.

Por ejemplo, entre los tipos de redes estaremos desarrollando las redes LAN, WAN, MAN, WLAN, etc. También se estará desarrollando el tema de los firewalls, como sus características, ventajas, tipos, entre otros. Como también las diferentes topologías de redes que existen e importancia de las mismas a la hora de decantarse por una.

Dentro del aspecto de seguridad estaremos desarrollando lo que es un proxy, así como también su importancia. También estaremos viendo el tema de los virus, de cómo podemos protegernos de los mismo, también los diferentes tipos de virus que se conocen actualmente. Por otro lado, estaremos hablando sobre las políticas de seguridad y políticas de sistema. Y por igual se estará desarrollando los tipos de seguridad, tanto la física como la lógica.

*Figura 2. 1. Redes y Seguridad.*
**Fuente: https://www.sageotech.com/single-post/2016/10/17/The-Importance-of-Having-a-Firewall**

## 2.2 Conceptos de Redes de datos

(Castaño Ribes, 2013, Pag 9) "Una red de área local (LAN) es un sistema informático que permite la conexión entre ordenadores que se encuentran físicamente próximos entre sí, normalmente en una misma habitación." Con este concepto podemos decir que Una Red es un conjunto de equipos conectados por medios físicos (cables, señales, etc.) con la finalidad de intercambiar información, delimitado por un área geográfica.

(Abad, 2013, Pag 8) "Una red de área local (LAN, Local Área Network) es un conjunto de elementos físicos y lógicos que proporcionan interconexión entre dispositivos en un área privada y restringida de la red de área local tiene."

Basándonos en el concepto de Ribes podemos decir que una red es la conexión e interconexión de varios equipos, ya sean computadoras o cualquier equipo electrónico que son capaces de acceder a una red, para que esto pueda intercambian información entre sí.

## 2.3 Ventajas de las Redes de datos

"Los principales beneficios de las redes de área local son los siguientes: – Recursos compartidos: conseguir que un único recurso pueda ser utilizado por multitud de dispositivos es la principal ventaja de las redes de ordenadores. Por ejemplo, podemos hacer que 20 ordenadores impriman con una sola impresora y, así, logramos obtener beneficios económicos, ya que el ahorro es considerable, y también funcionales, ya que hay que preocuparse de la configuración y el mantenimiento de una única impresora. – Ficheros y datos compartidos: esto posibilita el trabajo en grupo, ya que muchos usuarios pueden trabajar sobre el mismo fichero, disponer de la información en todo momento o comunicarse instantáneamente con distintos elementos de la red. – Administración centralizada: la existencia de una red simplifica las tareas de administración, ya que permite que muchas de las operaciones se realicen de forma centralizada en el servidor de la red o que se puedan resolver remotamente problemas de configuración." (Castaño Ribes, 2013, Pag 10)

Entre las ventajas que tenemos de una red, es que nos permite aprovechar de una mejor forma los recursos informáticos de la empresa. Como también es una ventaja a la hora de compartir información de manera eficiente y eficaz. También con una red bien diseñadas se mejorar la administración de los equipos, por ende, habrá una reducción de presupuesto tanto de hardware como software.

## 2.4 Tipos de Redes de datos

Las redes se dividen se pueden clasificar según su alcance. Primero tenemos una red LAN, por sus siglas en inglés “Local area Network”. Este tipo de red se puede definir como un grupo de dispositivos conectados entre sí en un área geográfica delimitada, usualmente entre 200 metros a 1 kilómetro de distancia.

Luego tenemos una red WAN (Wide Area Network), este tipo son redes que brindan acceso a área geométricamente extensas, generalmente esta infraestructura es utilizada por los ISP (Proveedor de servicios). También cabe destacar que el internet es una red WAN, ya que permite el acceso a los distintos usuarios sin importar su ubicación geográfica.

También están las redes MAN (Metropolitan Area Network), esta brinda acceso a áreas geográficas mayor que una LAN y menor que un WAN. Usualmente este tipo de redes están a cargo de una organización de gran tamaño.

Por otro lado, tenemos las redes WLAN (Wireless Local Area Network). Este tipo tiene el mismo concepto que las LAN, pero con la diferencia que las LAN utilizan medios físicos para la comunicación entre los dispositivos y las WLAN utilizan medios inalámbricos para el intercambio de información.

Por último, de los tipos de redes más importantes, tenemos las redes SAN (Storage Area Network). Las SAN son un tipo de red en la cual cuentan con una infraestructura orientada a la inclusión de servidores de archivos, como también brindan opciones de almacenamiento, recuperación y replicación de datos.

### 2.4.1 Redes LAN

"Red de área local (LAN): una infraestructura de la red que proporciona acceso a usuarios o terminales en un área geográfica pequeña, generalmente una empresa, hogar y pequeña red empresarial que es propiedad de una persona o departamento de TI, quienes también la administran." (Cisco Networking Academy)

Con esta red que lo buscamos es interconectar cada ordenador o dispositivo electrónico en una misma red.

Gracias a las redes LAN se pueden compartir documento de un ordenador a otro, imprimir en una sola impresora, compartir recursos entre otras cosas.

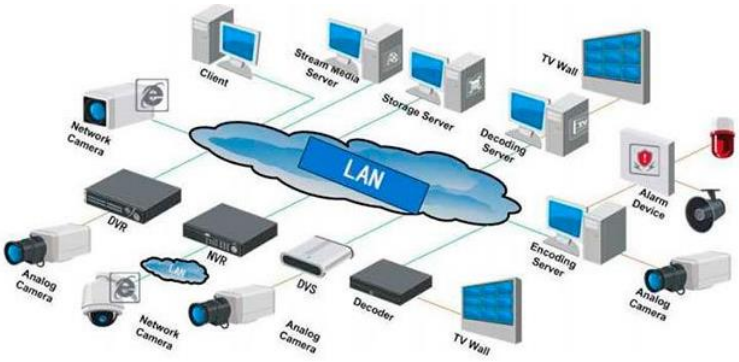



*Figura 2. 2. Redes LAN.*
**Fuente: https://netcloudengineering.com/funcionamiento-redes-lan/**

Si no se posee un servidor físico, la PC principal que trabaja como HOST puede sobrecargarse y este trae como consecuencia la desconexión continua de la red, esto provoca que los ordenadores no tengan acceso a la red o al compartimiento de archivos. Entre las Ventajas de las redes LAN tenemos:

- Compartir archivos y programas.
- Compartir recursos físicos.
- Mejora organizacional de la red.

Entre las desventajas de la red LAN tenemos:

- Mayor riesgo de infección de virus.
- Los dispositivos conectados a la red deben estar cerca geográficamente.

### 2.4.2 Redes WAN

"Red de área amplia (WAN): una infraestructura de la red que proporciona acceso a otras redes en un área geográfica extensa, que suele ser propiedad de un proveedor de servicios, quien también la administran**."** (Cisco Networking Academy)

las redes WAN es la red que conocemos hoy en día como "Internet", ya que este tipo no está limitado geográficamente, lo cual nos permite enviar y recibir archivos de cualquier parte del mundo.

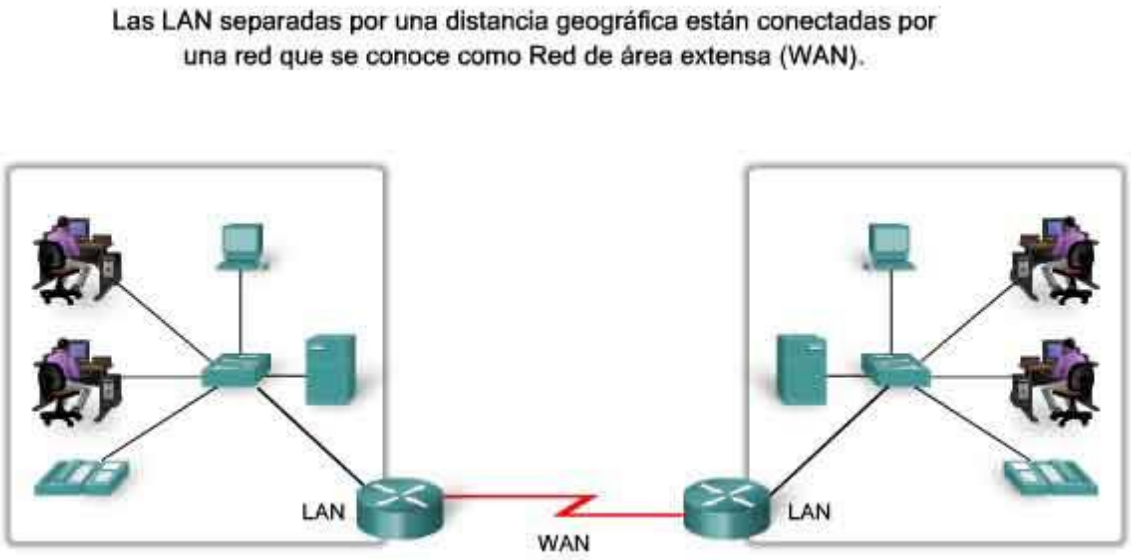



*Figura 2. 3. Redes WAN.*
**Fuente: http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro27/136_tipos_de_redes_lan_man_wan.html**

Una ventaja de este tipo de red es que los pc no necesitan estar tan cerca geográficamente para compartir archivos o recursos.

Una desventaja de estas redes es que los equipo que se utilizan para la comunicación están expuestos ataques maliciosos (Virus) lo cual nos obliga a utilizar software y aparatos (hardware) de seguridad.

### 2.4.3 Redes MAN

"Red de área metropolitana (MAN): son infraestructuras de red que abarcan un área física mayor que la de una LAN, pero menor que la de una WAN (por ejemplo, una ciudad). Por lo general, la operación de MAN está a cargo de una única entidad, como una organización de gran tamaño." (Cisco Networking Academy)

Las redes MAN se puede decir que puede abarcar un campus, como también puede ser de ciudad en ciudad. Una de las desventajas de este tipo de red, es que se requiere una gran inversión en cableado, ya que por lo general las MAN están interconectadas por fibra que es una tecnología bastante costosa.

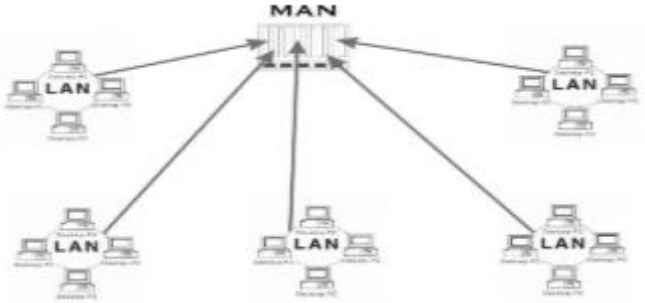



*Figura 2. 4. Redes MAN.*
**Fuente: http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro27/136_tipos_de_redes_lan_man_wan.html**

Las ventajas de las redes MAN:

- Son más seguras que las redes WAN.
- Son redes que no requieren un ancho de banda fijo.
- Son menos costosas que una red WAN

Entre las desventajas están:

- Esta red no puede exceder los 50km de diámetro.
- Por limitaciones legales se podría imposibilitar la creación de una red MAN privada y por ende se tendría que dar uso a una red MAN pública.

### 2.4.4 Redes WLAN

"LAN inalámbrica (WLAN): son similares a las LAN, solo que interconectan de forma inalámbrica a los usuarios y los extremos en un área geográfica pequeña." (Cisco Networking Academy)

*Figura 2. 5. Redes WLAN.*
**Fuente: https://www.accoladewireless.com/what-is-wlan/**

Ya como su nombre lo dice, estas redes son muy similares a las redes LAN, pero estas son capaces de conectar dispositivos a través de la conexión inalámbrica utilizando tecnología, así como Wi-Fi.

Esto significa que lleva toda ventaja y desventaja de una red LAN, pero entre las ventajas que conlleva es:

- Nos ofrece mayor flexibilidad y escalabilidad.
- Reducción de costos y tiempo de instalación.

Entre las desventajas están:

Las transmisiones de datos, estas redes no transmiten a la velocidad que lo hacen las redes cableadas.

Las redes inalámbricas carecen de seguridad a diferencia de una red cableada.

### 2.4.5 Redes SAN

"Red de área de almacenamiento (SAN): son infraestructuras de red diseñadas para admitir servidores de archivos y proporcionar almacenamiento, recuperación y replicación de datos." (Cisco Networking Academy)

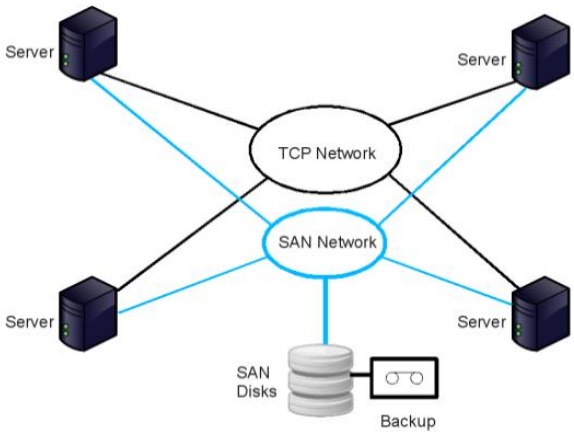



*Figura 2. 6. Redes SAN.*
**Fuente: https://redescableadas.wordpress.com/2013/02/25/redes-s-a-n-storage-area-network-parte-2/**

Ventajas:

1. Poseen una alta velocidad de transmisión pues es necesario por la alta tasa de transferencia de datos que son utilizados en los servidores.
2. La transmisión de datos de la red SAN trabaja independiente al ancho de banda de la red de cada usuario.
3. Minimizan la latencia.

Desventajas:

Las redes SAN son altamente costosas a diferencia de las otras.

## 2.5 Características de Redes

"Las principales características que definen a cada una de las redes locales son las siguientes:

– El tipo de cableado que usa para realizar las conexiones (UTP, STP…) o si no usa ninguno (inalámbrica).

– La velocidad de transmisión de los medios de la red (entre 1 Mbps y 1 Gbps). – En las redes cableadas, la longitud de los cables, que pueden medir, como máximo, 100 m. Esta medida puede aumentar utilizando repetidores, que son dispositivos intermedios de red. – El hardware que conecta los nodos a la red: tipo de tarjetas y estándares que los definen.

– La tecnología de comunicación que usa la red: por difusión o por paso de testigo (actualmente solo como modelo teórico).

– La gran variedad de equipos que pueden conectarse a una red: ordenadores, móviles, tabletas digitales, etc." (Castaño Ribes, 2013, Pág. 10)

Como menciona el señor Castaño en su libro "Redes Locales", cada red informática se caracteriza por el tipo de cableado que se utiliza, ya sea utilizar cable UTP, fibra óptica, etc. o identificar si va a hacer una WLAN la cual no utiliza cableado, sino que utiliza el espectro de ondas para la transmisión de información. Otra característica de una red que debe tener una red es la de determinar la velocidad en la que se transmite la información dentro de la red, también esta característica está ligada a la anterior ya que dependiendo del tipo de cableado que utiliza la red, la velocidad estará determinada por dicho cable.

Elementos indispensables para tener en cuenta a la hora de hacer una red son los tipos de cableado. Por ejemplo, existen varios tipos de cable UTP, como son los Cat 5, 5e y 6, esto son los más utilizado hoy en día, pero la diferencia entre el 5 y 5e es la transferencia de datos, la capacidad que soportan, y la Cat 6 es que este también de soportar grandes transferencias de datos, este posee mayor resistencia que los demás.

También se ha de tomar en cuenta el número de dispositivos que ha de albergar ya que se utilizará diferente cableado para la conexión de dispositivos o conexión entre un cuarto de datos a otro, un cuarto de servidor o de un edificio a otro en caso de que la institución crezca.

## 2.6 Seguridad Informática

*Figura 2. 7. Seguridad Informática.*
**Fuente: https://netcloudengineering.com/seguridad-datos-empresa/**

"La seguridad informática, en general, está teniendo una importancia cada vez mayor. Los usuarios, particulares y trabajadores de las empresas, deben ser conscientes de que el funcionamiento correcto de sus sistemas depende en gran medida, de protegerlos como el mayor de sus tesoros." Costas, Santos, Jesús. Seguridad informática, RA-MA Editorial, 2014. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/bibliounapecsp/detail.action?docID=3228430.

(Gema Escrivá Gascó, 2013, Pag 8) "Un activo se define como aquel recurso del sistema (informático o no) necesario para que la organización alcance los objetivos propuestos; es decir, todo aquello que tenga valor y que deba ser protegido frente a un eventual percance, ya sea intencionado o no." Por esto es importante la utilización de mecanismo de seguridad física para proteger la integridad de los activos informáticos de la empresa."

(Gema Escrivá Gascó, 2013, Pag 8) "En el campo de la seguridad informática se considera como vulnerabilidad a cualquier debilidad de un activo que pueda repercutir de alguna forma sobre el correcto funcionamiento del sistema informático." Mediante la implementación de un mecanismo de seguridad, como los biométricos, se pueden eliminar las vulnerabilidades de la empresa."

(Gema Escrivá Gascó, 2013, Pag 9) "Una amenaza es cualquier entidad o circunstancia que atente contra el buen funcionamiento de un sistema informático."

(Gema Escrivá Gascó, 2013, Pag 10) "Un ataque es una acción que trata de aprovechar una vulnerabilidad de un sistema informático para provocar un impacto sobre él e incluso tomar el control del mismo."

(Gema Escrivá Gascó, 2013, Pag 12) "El riesgo es una medida de la probabilidad de que se materialice una amenaza."

Evitar un ataque malicioso es lo que buscamos al implementar una seguridad, cuando hablamos de esto nos estamos refiriendo a la protección de activos informáticos o a la información guardada en una base de datos para evitar pérdidas de información buscamos evitar que estas amenazas no atenten con el buen funcionamiento como dice Gema Escrivá.

## 2.7 Ventajas de Seguridad

Con una red informática conjunta con medidas de seguridad se puede asegurar la integridad tanto de los datos como los activos de la empresa, lo cual se traduce en una reducción de costos en hardware y el invaluable valor que tiene la información de la empresa. También con medidas de seguridad implementadas a la red podemos evitar robo de información, como también podemos brindar el mayor tiempo posible de disponibilidad del sistema al usuario.

"Reducir el riesgo
Convierta su red en un sistema seguro con soluciones diseñadas para interoperar y brindar protección multicapa.

Obtener visibilidad total
Usar datos en tiempo real para proteger el acceso seguro, proporcionar inteligencia y detectar actividades sospechosas incluso en tráfico cifrado.

Reducir la complejidad
Elija entre las opciones integradas, dedicadas y administradas en la nube para una seguridad integral completa.

Proteger contra amenazas
Aplique políticas y adopte medidas para proteger la red de su organización de amenazas conocidas y desconocidas." (Cisco Networking Academy)

A partir de esta información las ventajas de la seguridad informática recae en reducir la probabilidad de que alguna amenaza penetre nuestros sistemas esto se logra haciendo un análisis de las posibles vulnerabilidades que pueden afectar nuestros sistemas, estudiando las posibles soluciones eficaces que solucionen dicha vulnerabilidad y tomando acción median hardware y software para así formar una barrera lo suficientemente sólida como para evitar o lograr que la amenaza ingrese.

Como principal ventaja de efectuar este método tenemos el poder salvaguarda todos nuestros datos más importantes y personales dentro de nuestros sistemas informáticos o computadores de cualquier persona que atente contra ellos o contra el bienestar de una persona, un personal o una entidad.

## 2.8 Tipos de Seguridad

En toda información electrónica que es envía por distintas vías, ya sea redes sociales, correos, mensajes, etc. estos tienden ser enviados con programas que protejan sus informaciones ya sean encriptado, por eso la seguridad informática ha desarrollado distintos tipos de seguridad los cuales son:

Seguridad Física: Abarca toda medida que proteja o asegure la integridad física de los diversos dispositivos o equipos que estén en un data center o en toda la organización, estos comúnmente son llamados seguridad de hardware y seguridad de red:

- Seguridad de Red: Este protégete las redes de datos, es decir asegura que a nivel de red los datos de entrada y salida a nuestros servidores y computadores sean totalmente seguros, aislando la red del personal de la red más importante.
- Seguridad de hardware: Es una forma de seguridad donde se protege los medios tangibles de nuestros sistemas informatizado donde se utilizan todos los medios posibles para que ese sistema funcione al máximo de su capacidad en un ambiente empresarial

.

Seguridad Lógica: Abarca toda protección a los datos no tangible o información no tangible que maneja los diversos sistemas, esta información pueden ser archivos de suma importancia para la empresa, contraseñas, registros etc. que se alojen en cualquier parte de un data center, este es también llamado Seguridad de Software:

- Seguridad de software: este tipo de seguridad es el que protege la integridad de nuestro sistema operativo así que como todo diversos programas contra ataques maliciosos para que estos sigan operando con normalidad, un ejemplo de estos son los antivirus.

### 2.8.1 Seguridad Lógica

(Gema Escrivá Gascó, 2013, Pag 45) "La seguridad lógica es el conjunto de medidas destinadas a la protección de los datos y aplicaciones informáticas, así como a garantizar el acceso a la información únicamente por las personas autorizadas."

*Figura 2. 8. Seguridad Lógica.*
**Fuente: https://www.lavanguardia.com/tecnologia/20180928/452060224473/virustotal-enterprise-google-seguridad-chronicle.html**

Cómo define Gema Gascó, la seguridad lógica se refiere a aquellas medidas de seguridad que permite la protección de los datos y como también permite el acceso de un personal autorizado. Estas medidas pueden ser el uso de un PIN que se utilice para desbloquear un móvil, como también el PIN que se utiliza para sacar dinero del cajero automático, y/o contraseñas para tener acceso a un correo.

### 2.8.2 Seguridad Física

(Gema Escrivá Gascó, 2013, Pag 25) "El conjunto de medidas de prevención y detección destinadas a evitar los daños físicos a los sistemas informáticos y proteger los datos almacenados en ellos."

*Figura 2. 9. Seguridad Física.*
**Fuente: https://www.obs-edu.com/int/blog-investigacion/sistemas/seguridad-fisica-informatica-que-se-enfrenta**

La seguridad física la podemos definir como un conjunto de medidas o mecanismo implementadas para asegurar, prevenir y detectar la integridad física de los activos informáticos. Por ejemplo, la utilización sistemas de seguridad biométricas para prevenir el acceso de personas ajenas a una institución, las cuales puedan causar daños a dichos activos, ya sea de manera deliberada y por accidente. Pero también no solo se puede proteger al activo de personal humano, sino también se puede utilizar mecanismos para la protección frente a incendios.

## 2.9 Características de Seguridad

Se dice que, aunque se utilicen cualquier medio para tener una buena seguridad, nunca se lograra conseguir un 100%, pero se debe de siempre buscar la mejor manera de proteger los equipo y la información de los usuarios, para obtener este resultado se debe cumplir los principios básicos de la seguridad informática:

1. Integridad
2. Confidencialidad
3. Disponibilidad
4. Otras características deseables en un sistema seguro

## 2.10 Firewall

*Figura 2. 10. Firewall.*
**Fuente: https://cwatch.comodo.com/free-firewall-protection.php**

(Urbina, 2016, Pag 204) "La función de un firewall es proteger de ataques externos a computadoras personales o redes de computadoras, ya sea que esos ataques sean maliciosos, debido a que se haya introducido un software malicioso en la red, o simplemente porque haya un exceso de tráfico en la red." De este modo podemos definir un Firewall como un dispositivo con el cual su función principal es la de proteger nuestros dispositivos del tráfico que entra desde la red, entre otras cosas.

(Roa, 2013, Pag 183) “El firewall es un software especializado que se interpone entre las aplicaciones y el software de red para hacer un filtrado de paquetes.” Como el señor Buendía definió un firewall como un software, lo cual refleja que los firewalls pueden ser tanto por software como también existen firewalls físicos.

(Santos, 2014, Pag 152) “El concepto de firewall o cortafuegos apareció en el ámbito de las redes de datos para describir los diferentes mecanismos de seguridad destinados a bloquear la transferencia de datos que no cumplan unos criterios de seguridad determinados. Está considerado en la actualidad como un mecanismo de seguridad necesario, pero no suficiente para proteger las redes y los equipos conectados a las mismas.”

(Cisco Networking Academy) “Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red -entrante y saliente- y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.”

(Ansejo, 2006, Pág. 25) “Un Firewall es un dispositivo que filtra el tráfico entre redes, como mínimo dos. El firewall puede ser un dispositivo físico o software sobre un sistema operativo. En general debemos verlo como una caja con dos o más interfaces de red en la que se establecen unas reglas de filtrado con las que se decide si una conexión determinada puede establecerse o no. Incluso puede ir más allá y realizar modificaciones sobre las comunicaciones, como el NAT. Esa sería la definición genérica, hoy en día un firewall es un hardware específico con un sistema operativo o una IOS que filtra el tráfico TCP/UDP/ICMP/../IP y decide si un paquete pasa, se modifica, se convierte o se descarta. Para que un firewall entre redes funcione como tal debe tener al menos dos tarjetas de red.”

(Gómez, 2014, Pag 144) “Un cortafuegos (firewall) es un dispositivo que realiza un filtrado de paquetes de datos a partir de unas reglas definidas por el administrador de la red, teniendo en cuenta las direcciones IP fuente o destino (es decir, de qué ordenador provienen y a qué ordenador van dirigidos los paquetes de datos) y el servicio de red al que se corresponden.”

Tomando en cuenta todas las definiciones según los diversos autores que están citados en este campo podemos definir el Firewall o cortafuego como definición al español como un dispositivo electrónico conectado vía cable a una red que filtra o selecciona los elementos de entrada a una red cualquiera o a un computador, evitando así la entrada de elementos no deseados como virus o programa maligno.

## 2.11 Tipos de firewall

"**Nivel de aplicación de pasarela:** Si se utilizan aplicaciones específicas, este tipo de firewall puede proporcionar mecanismos de seguridad. Por ejemplo, para Telnet (Telecommunication Network), que es un protocolo de red que permite utilizar la funcionalidad de administración remota, con la cual es posible realizar cierto tipo de acciones desde un equipo local y que éstas se ejecuten en un equipo remoto, como checar todas las computadoras de una red desde una sola máquina, con el fin de identificar si hay problemas de intrusión o de cualquier otro tipo, el único requisito es que la computadora a la que se acceda debe tener un programa especial y reciba instrucciones que gestionan las conexiones.

**Circuito a nivel pasarela:** Cuando se utiliza una conexión TCP (Transfer Control Protocol) o de UDP (User Datagram Protocol) es posible aplicar algunos mecanismos de seguridad, lo que permite establecer una sesión entre una zona de mayor seguridad hacia una zona de menor seguridad, pues una vez que se ha iniciado la sesión, los paquetes fluyen entre las computadoras conectadas sin control. Un firewall protege a una sola computadora o a toda una red interna contra intrusos provenientes de otras redes, ya que filtra paquetes de datos que son enviados por Internet. Un sistema firewall es un software que también puede contar con el apoyo de un hardware de red dedicada." Baca, Urbina, Gabriel. Introducción a la seguridad informática, Grupo Editorial Patria, 2016. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/bibliounapecsp/detail.action?docID=4849850.

En otros términos, cuando hablamos de los tipos de firewall a nivel de aplicación de pasarela nos referimos a los firewalls a nivel de software y cuando hablamos de los firewalls Circuito a nivel pasarela nos referimos a los firewalls de hardware.

Establecido eso podemos decir que los firewalls se subdividen en hardware y software:

**Firewall Hardware:** Son dispositivos electrónicos que filtran o regulan el paso de elementos de la internet a nuestro sistema computacional o a nuestra red de datos, podríamos decir que es el medio por el cual se evita o se elimina todos aquellos elementos maliciosos que pueden contaminar nuestra red o sistema a nivel físico, como los ya conocidos firewall de cisco o fortine.

*Figura 2. 11. Firewall Hardware.*
**Fuente: https://www.cisco.com/c/en/us/support/security/firepower-2120-security-appliance/model.html (Cisco)**

**Firewall Software**: Son los sistemas que instalamos en nuestras computadoras o dispositivos que regularmente utilizamos para navegar en la web y que nos protegen de esos elementos maliciosos que se alojan en la internet, archivos que descargamos entre otros.

*Figura 2. 12. Firewall Software.*
**Fuente: https://lam.norton.com/**

Estos firewalls de software pueden subdividirse en firewall de red y de aplicación

**Los firewalls de software de red:** son una subdivisión donde a nivel de configuración se puede redirigir o configurar los puertos de un router para evitar el tráfico de datos de un punto a otro.

**Los firewalls de software de aplicación:** son el tipo de firewall que se monta en un servidor proxy con el fin de limitar o controlar el tráfico de red a nivel de software este suele nombrarse firewall proxy.

## 2.12 Características del firewall

"Al emplear un cortafuegos todo el tráfico entrante o saliente a través de la conexión corporativa debe pasar por una única máquina, por lo que el administrador puede permitir o denegar el acceso a Internet y a los servicios de la empresa de manera selectiva. Se consigue, de este modo, que todo el tráfico de la organización pueda ser filtrado por esta máquina, obligando a los usuarios, tanto internos como externos, a cumplir las restricciones que se hayan impuesto.

De este modo, el cortafuegos permite establecer dos zonas de trabajo independientes: la zona fiable o de confianza, correspondiente a los equipos de la red interna de la organización, en contraposición con la zona no fiable, en la que se ubicaran todos los demás equipos externos.

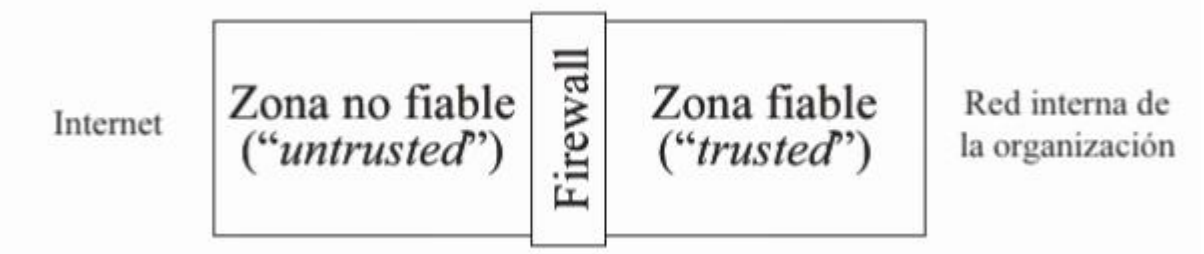



*Figura 2. 13. Características del Firewall 1.*

El cortafuegos también puede ser configurado para facilitar la conexión de usuarios remotos a través de túneles seguros, utilizando protocolos de redes privadas virtuales (VPN).

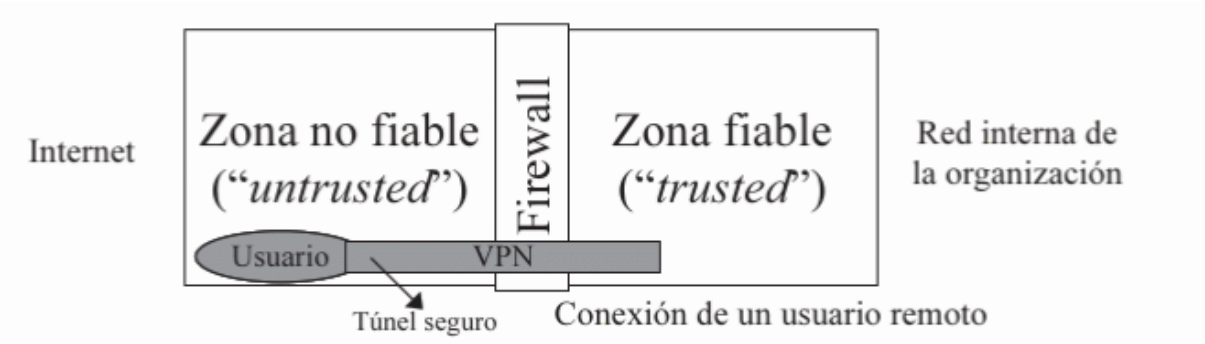



*Figura 2. 14. Características del Firewall 2.*

Conexión de un usuario remoto a través de un túnel VPN

Una configuración típica de un cortafuegos que permite aislar físicamente la red interna del exterior es la que se puede establecer mediante un equipo conocido como "host bastión", que cuenta con dos tarjetas de red, conectadas a dos redes diferentes, por lo que también recibe el nombre de "dual-homed bastion host". Su papel es crítico para garantizar la seguridad de la red (de ahí el nombre de "bastión"), ya que permite establecer reglas de filtrado desde el nivel de red hasta el nivel de aplicación."

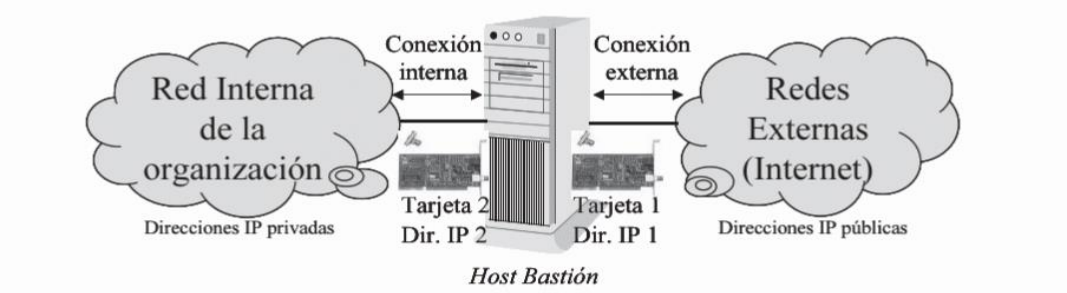



*Figura 2. 15. Características del Firewall 3.*

Instalación típica de un cortafuegos mediante un Host Bastion

Gómez, Vieites, Álvaro. Auditoría de seguridad informática, RA-MA Editorial, 2014. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/bibliounapecsp/detail.action?docID=3229127.
Created from bibliounapecsp on 2018-12-19 06:45:47.

La principal característica de un firewall (en español cortafuego) es la de a partir de políticas puestas por los administradores delegar el paso o el bloqueo de una solicitud de un usuario interno o externo a la red de una empresa, institución o red domenstica, por lo cual el firewall aisla los sistemas a su cuidado de elementos no autorizados, una de las facilidades del firewall es que a partir de este se pueden configurar las vpn que son canales seguros de conexión a algún elemento de la red interna al cual se desea acceder desde el exterior, solo personas con la contraseña y el usuario permitido tiene el acceso para utilizar estas funciones

## 2.13 Proxy

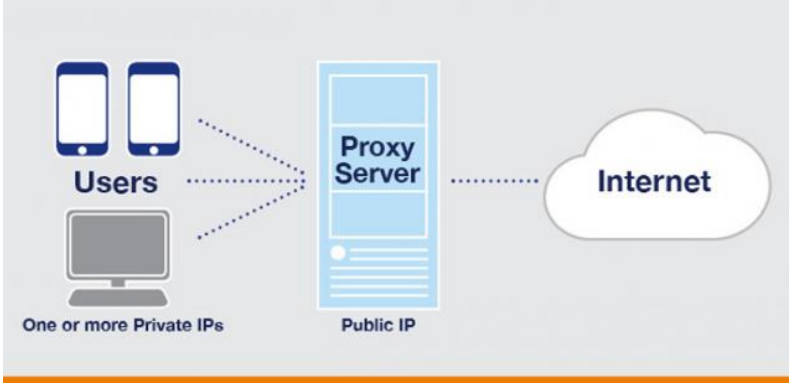



*Figura 2. 16. Proxy.*
**Fuente: https://www.vpnranks.com/proxy-vs-vpn/**

"La palabra "proxy" significa ´abogar´ y esto es, como se analiza en esta sección, lo que hace un servidor proxy o Gateway de aplicación". Como dice Díaz, G Proxy es un filtro un mediador que aboga y permite el paso o niega el paso a elementos extraños o incluso conocidas." Díaz, G., Mur, F., & Sancristóbal, E. (2004). Seguridad en las comunicaciones y en la información. Retrieved from https://ebookcentral.proquest.com pag 193.

"Un proxy, o servidor proxy, en una red informática, es un servidor —programa o dispositivo—, que hace de intermediario en las peticiones de recursos que realiza un cliente (A) a otro servidor (C). Por ejemplo, si una hipotética máquina A solicita un recurso a C, lo hará mediante una petición a B, que a su vez trasladará la petición a C; de esta forma C no sabrá que la petición procedió originalmente de A." Greg Ferro, Fast Introduction to SOCKS Proxy

Así como dice Ferro, Un proxy hace de su vez de mediador, por lo que podríamos decir que aparte de ser un filtro como concluimos con la definición de Diaz este software también nos permite intermediar entre varios dispositivos conectados a una misma red, otorgándoles un control sobre el tráfico que circula en la misma y nos da la facilidad para seleccionar la más conveniente para otorgar acceso o simplemente denegarlo a las páginas o servicios que no nos sean convenientes.

## 2.14 Importancia del Proxy

El proxy juega un papel muy importante en todo Sistema informatizado que esté en una red bien estructurada ya que todo paquete que entre o salga de estos dispositivos primero tendrá que pasar por el filtro que es el proxy y este último determinará si ese paquete obtendrá el paso para seguir su camino o será bloqueado dado la forma en la que el proxy sea estructurado, el proxy como tal es una herramienta muy conocida para evitar que software o elementos extraños infecten o se vean alojados en nuestros dispositivos , también es una herramienta perfecta para controlar el acceso a páginas no deseadas o simplemente crear un ambiente único en algún área laboral restringiendo en si la cantidad de permisos que posea un usuario a ciertas páginas de internet, gracias a este software las redes de información dentro de las empresas son más seguras, más estables e incluso las maquinas que estén conectadas a estas disfrutan de dichos beneficios.

## 2.15 Concepto de Virus Informáticos

Los virus informáticos son software dañino que estropean el funcionamiento de los aparatos electrónicos como Ordenadores, Celulares, tabletas, entre otros, se podría decir que es un archivo que se introduce sin el permiso del usuario con la finalidad de indagar y despojar información privada.

## 2.16 Tipos de Virus

*Figura 2. 17. Tipos de Virus.*
**Fuente: tecnología-informatica.com**

Los virus informáticos están clasificados por dos tipos los cuales son:

### 2.16.1 Por su capacidad de propagación:

#### 2.16.1.1 Virus

*Figura 2. 18. Virus.*
**Fuente: https://www.lavozdelsandinismo.com/ciencia-tecnica/2015-06-19/se-creo-un-virus-informatico-cada-cuatro-segundos-durante-2014/**

Este tipo de virus es el que se aloja en los ficheros dentro de un ordenador o equipo, estos ficheros suelen ser archivos ejecutables que al ser iniciados causan un sin número de síntomas tal cual como los virus reales que entorpecen o dificultan el funcionamiento del ordenador o de los dispositivos electrónicos.

### 2.16.1.2 Gusanos

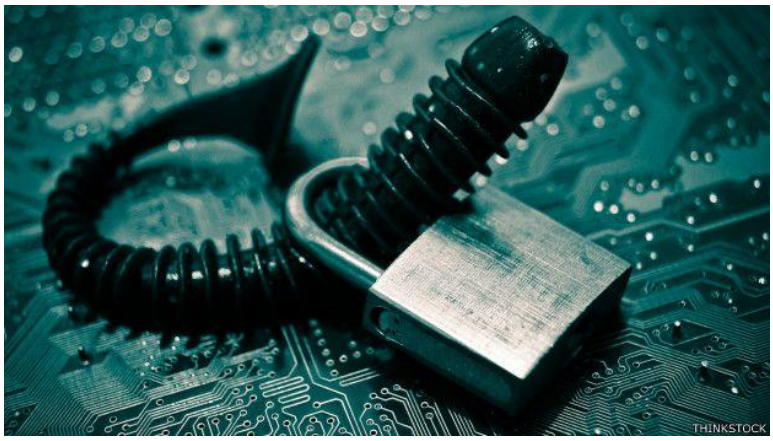



*Figura 2. 19. Gusanos.*
**Fuente: https://www.bbc.com/mundo/noticias/2015/08/150805_tecnologia_gusano_desmitifica_seguridad_mac_lv**

Los gusanos son un tipo de virus que son iniciados generalmente por la ingeniería social y se propagan para crear un gran número de copias de sí mismos para así infectar otros equipos con el fin de molestar al usuario que es infectado por este virus.

Este tipo de virus se propaga de las siguientes maneras:

- Correo electrónico
- Compartimiento de archivos de una red.
- Aprovechar una vulnerabilidad.
- Mensajería instantánea.
- Mensajes de chat

### 2.16.1.3 Troyanos

*Figura 2. 20. Troyanos.*
**Fuente: https://www.muyseguridad.net/2012/10/05/troyano-infografia-panda/**

Este tipo de virus se adquiere a través de otros programas alterados maliciosamente o a través de ingeniería social, visitando páginas con contenido malicioso son conocimiento previo y dentro de un programa que finge ser inofensivo.

## 2. 16. 2 Por las acciones que realizan en el equipo infectado

### 2.16.2.1 Adware

*Figura 2. 21. Adware.*
**Fuente: https://www.tecnologiadetuatu.elcorteingles.es/actualidad/11-aplicaciones-gratuitas-para-acabar-con-los-virus-adware-y-spyware-del-pc/**

Es un tipo de virus que utiliza la publicidad como medio de pesca para recopilar información de los usuarios, estos normalmente son instalados en programas donde se frecuenta la publicidad.

### 2.16.2.2 Bloqueador

*Figura 2. 22. Bloqueador.*
**Fuente: https://www.pcrisk.es/guias-de-desinfeccion/7720-cryptofortress-ransomware**

Es como su nombre lo dice, este virus bloquea el acceso a los programas y direcciones de internet donde se pueda analizar o verificar la existencia de un virus y también impide la ejecución de programas específicos así complicando la forma de verificar la existencia de este.

### 2.16.2.3 Bomba lógica

*Figura 2. 23. Bomba Lógica.*
**Fuente: http://peligroseninternett.blogspot.com/2013/06/bombas-logicas-o-de-tiempo.html**

Este tipo de virus se aloja en el sistema y solo se ejecuta cuando se cumple los requerimientos o un tiempo específico y este puede ser un programa o ser parte del código de un programa.

### 2.16.2.4 Broma (Joker)

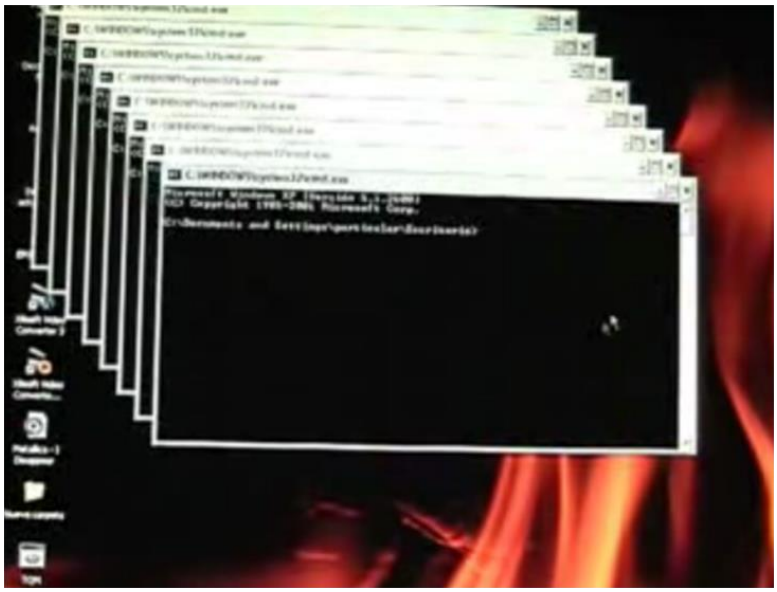


*Figura 2. 24. Joker.*
**Fuente: http://infolosmejoresjuegos.blogspot.com/2012/11/virus-de-broma-para-pc-xdxd.html**

Este tipo de virus no es malicioso, es decir no daña al equipo, solamente le hace creer al usuario que va a iniciar una secuencia o actividad negativa dentro del dispositivo.

### 2.16.2.5 Bulo (Hoax)

*Figura 2. 25. Hoax.*
**Fuente: http://virusequipo.blogspot.com/2016/01/virus-informaticos.html**

Este virus engaña al usuario haciéndole creer mediante un mensaje electrónico que es enviando por alguien de confianza y en el cuerpo de este mensaje declaró una situación falsa o no realista alarmando al individuo para realizar un proceso dañino para el equipo.

### 2.16.2.6 Capturador de pulsaciones (Keylogger)

*Figura 2. 26. Keylogger.*
**Fuente: https://blog.360totalsecurity.com/en/keylogger-protection-useful-tips-to-protect-against-personal-info-theft/**

Este virus al infectar un equipo monitoriza las pulsaciones del teclado, guardándolas para ser enviadas al creador de esta, con el fin de capturar cuentas bancarias, cuentas de juegos en línea, conversaciones o mensajes escritos en la máquina.

### 2.16.2.7 Clicker

*Figura 2. 27. Clicker.*
**Fuente: http://virus.com.ar/2017/07/12/the-magala-trojan-clicker-a-hidden-advertising-threat/**

Este redirecciona de un enlace oficial de una página a una falsa, totalmente idéntica con el fin de adquirir la información personal de la víctima.

### 2.16.2.8 Criptovirus (Ransomware)

*Figura 2. 28. Ransomware.*
**Fuente: https://www.pbs.org/newshour/science/everything-need-know-wannacrypt-ransomware-attack**

Este virus cifra la información local del usuario, así como imágenes, documentos, multimedia, etc.… y envía un mensaje de rescate (Ransom) con el fin de recuperar o descifrar la información capturada.

### 2.16.2.9 Descargador (downloader)

*Figura 2. 29. Downloader.*
**Fuente: https://community.norton.com/en/forums/downloader-virus-0**

Este virus se obtiene descargando un archivo infectado y accede al internet descargando otros programas maliciosos con el fin de estropear el ordenador.

### 2.16.2.10 Espia (Spyware)

*Figura 2. 30. Spyware.*
**Fuente: http://www.css.edu/administration/information-technologies/security/adware-and-spyware.html**

Recopila información de diversas acciones del usuario y la envía a un servidor remoto donde el autor de dichos virus recibe dicha información, esta información suele ser, páginas web visitadas, tiempo de uso del ordenador, contraseñas.

Los espías que roban información de autentificación suelen llamarse “Troyanos Bancarios”

### 2.16.2.11 Exploit

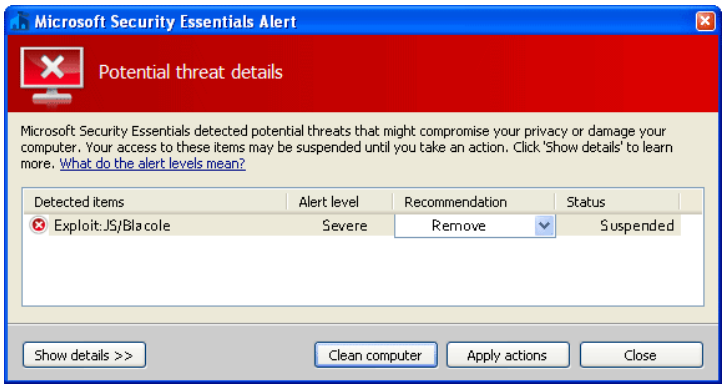



*Figura 2. 31. Exploit.*
**Fuente: https://malwaretips.com/blogs/js-exploit-blacole-virus/**

Es un virus que emplea las aberturas desprotegidas por el usuario para tomar acceso dentro del sistema.

### 2.16.2.12 Herramienta de fraude

*Figura 2. 32. Herramienta de fraude.*
**Fuente: https://www.le-vpn.com/es/los-fraudes-mas-comunes-de-internet/**

Es un virus que simula la conducta defectuosa de un programa instalado en el sistema, con el fin de incitar al usuario que compre otro software para resolver dicho error.

### 2.16.2.13 Instalador (Dropper)

*Figura 2. 33. Dropper.*
**Fuente: http://www.solucionavirus.com/2013/11/eliminar-win32dropper-gen-drp.html**

Es un virus que ejecuta e instala otros programas maliciosos en el sistema.

### 2.16.2.14 Ladrón de contraseñas (PWStaler)

*Figura 2. 34. PWstaler*
**Fuente: https://es.123rf.com/photo_45658647_ladrón-hacker-robar-datos-confidenciales-como-contraseñas-desde-un-ordenador-personal-útil-para-campañas-anti-phi.html**

Es un virus que accede a la meta data de ficheros con el fin de obtener contraseñas y nombres de usuarios.

### 2.16.2.15 Marcador (Dialer)

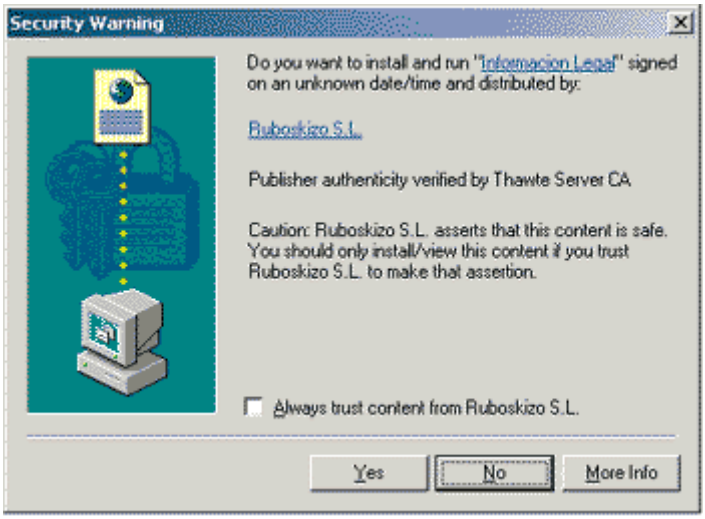



*Figura 2. 35. Dialer.*
**Fuente: https://www.pandasecurity.com/es/security-info/**

Este virus hoy en día está en desuso ya que utilizaba la conexión a internet a través del modem para utilizar la NTA (Números de tarificación adicional), lo que causaba un incremento en la tarifa telefónica.

### 2.16.2.16 Puerta trasera (Backdoor)

*Figura 2.36. Backdoor.*
**Fuente: http://www.virusremovalguidelines.com/tag/what-is-backdoor-plaintee**

Este tipo de virus como su nombre bien dice (Puerta trasera) aprovecha una vulnerabilidad como, por ejemplo: el firewall no este activo, para burlar la seguridad y tomar control del sistema.

### 2.16.2.17 Rootkit

*Figura 2. 37. Rootkit.*
**Fuente: http://techsalsa.com/steps-to-remove-win32rootkit-genrtk-virus/**

Este virus roba el control de la cuenta administradora en caso de que el SO sea Windows y en Linux/Unix el "ROOT" para darle autorización a un tercero o ejecutar programas maliciosos dentro del ordenador.

### 2.16.2.18 Secuestrador de Navegador (Browser hijacker)

*Figura 2. 38. Browser Hijacker.*
**Fuente: http://reparacionordenador.es/reparacion-de-secuestro-del-navegador/**

Este es el clásico virus que cambia la página predeterminada del navegador y también puede agregar barras de herramientas o insertar enlaces en la carpeta de favoritos.

Esto normalmente se hace para agrandar el número de visitas a la página.

## 2.17 Características de los Virus

Debido que los virus mientras más pequeño es, más fácil es la propagación del mismo. Por esto, existen unas características que todo virus debe tener para que no sea detectado.

Primero tenemos la de reorientación, esta característica consiste que el virus tiene la capacidad de reacomoda la lectura de un disco con la finalidad de no ser detectado. Luego tenemos la característica de que el virus debe ser encriptado para que así no deje huellas a simple viste a la hora de infectar un equipo informático.

También está la característica de polimorfismo, en otras palabras, el virus debe estar cambiando segmentos de su código para parecer distinto, lo cual hace difícil la detección de este.

## 2.18 Métodos de Transmisión de los Virus

Entre los métodos de transmisión de virus tenemos, entre los más conocidos como la descarga de un archivo que a primera vista parece inofensivo, pero en realidad la persona está descargando un programa con el cual el hacker estará infectando su PC.

Otra manera en el cual un computador se puede infectar de un virus es mediante el correo, infectado con este, en el momento en el que un correo de procedencia desconocida y sea abierto, nuestros pc pueden ser infectada de spyware o cualquier otro malware.

Carencia de protección de un antivirus, mientras navegamos por la web uno nunca sabe en qué página hay un virus o en qué momento se infecte de uno, por ende, el no poseer un antivirus actualizado y habilitado es una de las maneras en la que nuestro sistema se infecte.

## 2.19 Métodos de Protección contra los Virus

Para la protección contra virus, tenemos el software antivirus el cual se encarga de analizar el ordenador (PC) en búsqueda de software malicioso, y como también se encarga de bloquear y/o eliminar dicho software malicioso.

“Un antivirus es un programa informático específicamente diseñado para detectar, bloquear y eliminar códigos maliciosos.”

Costas, Santos, Jesús. Seguridad informática, RA-MA Editorial, 2014. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/bibliounapecsp/detail.action?docID=3228430.

También tenemos los firewalls. Estos nos ayudan tener un mayor control de qué información entra y sale de nuestra red.

## 2.20 Políticas de seguridad

“Las políticas de seguridad son un conjunto de reglas, normas y protocolos de actuación que se encargan de velar por la seguridad informática de la empresa. Se trata de una especie de plan realizado para combatir todos los riesgos a los que está expuesta la empresa en el mundo digital. De esta forma mantendremos nuestra organización alejada de cualquier ataque externo peligroso.”

Para ayudar a la pyme a poner en marcha los procesos internos con los que mejorar su ciberseguridad presentamos una serie de documentos que hemos denominado como «políticas de seguridad».

Estas políticas tratan los aspectos y elementos esenciales donde debemos aplicar seguridad y que deben estar bajo control. Cada política contiene una lista de chequeo de las acciones que debe tomar el empresario, su equipo técnico y sus empleados.” (emprendepyme.net/politicas-de-seguridad)

Bajo este concepto podemos concluir que las políticas de seguridad son un conjunto de pasos que establece un experto para evitar o reducir el porcentaje de que una posible amenaza en este caso un virus o un hacker invada el sistema de una empresa.

Como ya habíamos visto en la definición anterior las políticas de seguridad son una serie de normas en este caso escritas que se usan para reducir o erradicar la posibilidad de que una amenaza invada un sistema informático, basándose en la preparación de los empleados e impartido por un equipo cualificado.

## 2.21 Políticas de Sistema

Las políticas de sistemas son una serie de normativas, pautas y reglas que el tecnólogo o un usuario deben seguir para el correcto funcionamiento o correcto manejo de sus herramientas, Estas políticas se pueden manejar en software como en un manual de buenas prácticas para una institución o una empresa.

Estás políticas a nivel de software son dadas por un ingeniero a cargo de la red o de los diferentes softwares que se usan en la institución y a su vez a cargo de todos los equipos informáticos dentro de la institución o empresa, con el fin de evitar fugas de seguridad o de información, protegiendo así la integridad de la organización.

Dado esto último las políticas de buenas prácticas salen a relucir ya que, estas normativas acompañadas de las políticas aplicadas a los diversos sistemas o plataformas computacionales fortalece la integridad de los datos e información de este último.

## 2.22 Topologías de Redes

"Se conoce con el nombre de topologías a las formas de conectar los diferentes equipos entre sí en una LAN." Hillar, G. C. (2004). Redes: diseño, actualización y reparación. Retrieved from https://ebookcentral.proquest.com

"La topología de red se refiere al detalle de la distribución geométrica de las distintas conexiones entre dispositivos., esta se puede representar de forma física o lógica." (Campo, 2017, Pág. 16)

Las topologías son las diferentes formas de interconectar varios dispositivos o equipos mediante el cableado en una red LAN.

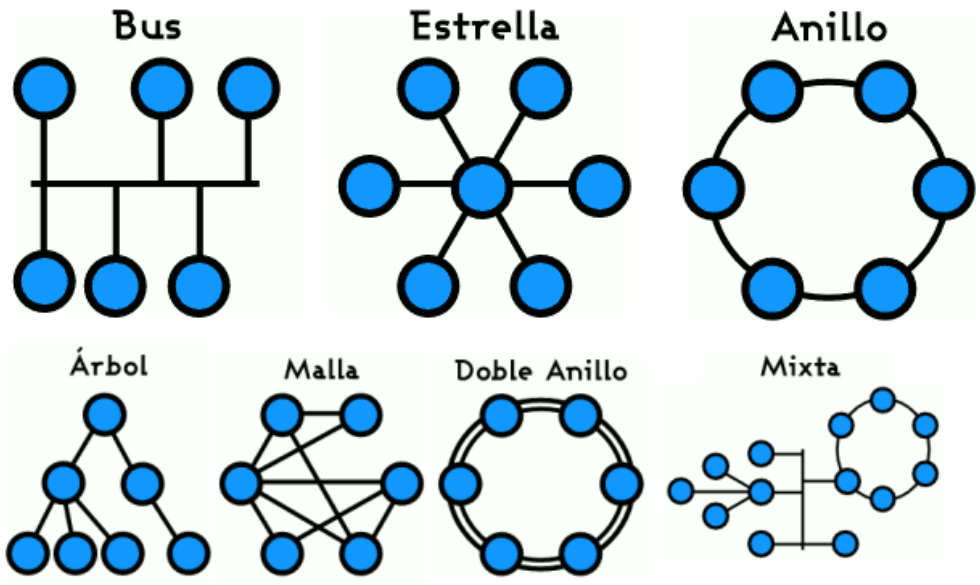



*Figura 2. 39. Topologías de Red.*
**Fuente: https://searchdatacenter.techtarget.com/es/definicion/Topologia-de-red**

## 2.23 Tipos de Topologías:

### 2.23.1. La topología de bus/lineal:

Es la topología que también es conocida como lineal, utiliza un medio compartido de difusión (broadcast) multipunto, al cual se encuentran conectados todos los nodos.

Su mayor ventaja es que es fácil y económica de construir y no requiere de otros dispositivos de red específicos como concentradores o conmutadores. Sin embargo, a la hora de agregar o quitar nodos lleva mucho más trabajo que otras configuraciones.

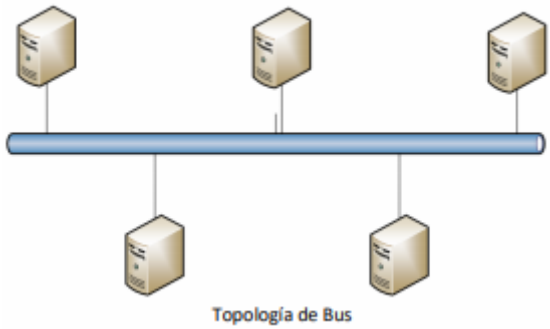



*Figura 2. 40. Topología Bus/Lineal.*
**Fuente: (Campo, 2017, Pág. 17)**

### 2.23.2 Topología punto a punto

Son aquellas arquitecturas de red en la que los dispositivos están conectados únicamente para comunicarse de un dispositivo A a un dispositivo B, es decir dos nodos para el tráfico de datos.

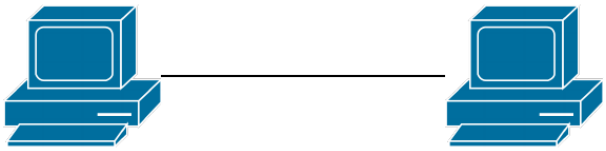


*Figura 2. 41. Topología Punto a Punto.*

### 2.23.3 La topología de árbol

Es muy similar a la de bus, pero utiliza un medio compartido que comienza en la raíz y extiende en varias líneas de difusión no lineales (broadcast) multipunto, a las cuales se encuentran conectados todos los nodos.

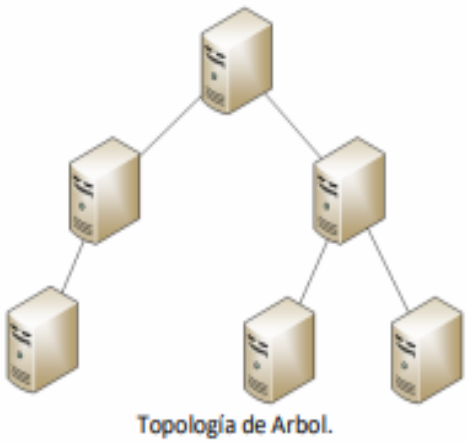



*Figura 2. 42. Topología de Árbol.*
**Fuente: (Campo, 2017, Pág. 17)**

### 2.23.4 La topología de anillo

Utiliza un medio compartido de difusión (broadcast) multipunto formando un bucle cerrado, al cual se encuentran conectados todos los nodos. También se puede describir como un conjunto de enlaces punto a punto entre los nodos, que terminan cerrando un lazo. Generalmente, los nodos utilizan repetidores encargados de recibir la información y transmitirla por el medio y de esta manera, la misma puede circular por todo el anillo.

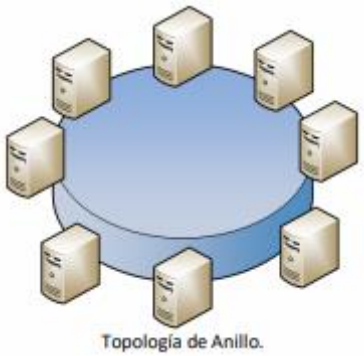



*Figura 2. 43. Topología de anillo.*
**Fuente: (Campo, 2017, Pág. 17)**

### 2.23.5 La topología estrella

Utiliza enlaces punto a punto (generalmente dos, uno para enviar datos y el otro para recibir) entre cada nodo y un nodo central. Este último puede ser un concentrador, conmutador o repetidor y más adelante analizaremos en detalle las diferencias entre cada uno de ellos.

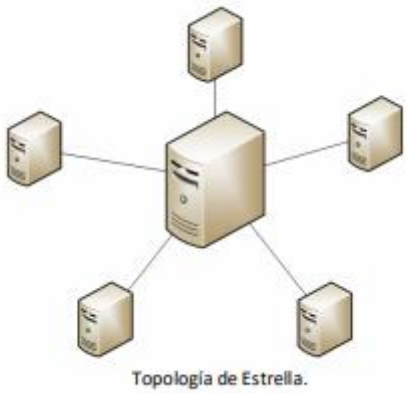



*Figura 2. 44. Topología de Estrella.*
**Fuente: (Campo, 2017, Pág. 17)**

### 2.23.6 La topología de Malla

En esta topología cada nodo de la red está conectados a cada uno, lo cual permite que la información que se envía a través de los nodos atraviesa distintas rutas para que llegara a su destino. Este tipo de topología es más utilizada en aquellas redes en la cuales no se pueden permitir interrupción a la hora de comunicarse, ya que por lo dicho esta topología se caracteriza por brindar bastante redundancia para el proceso de comunicación entre los nodos.

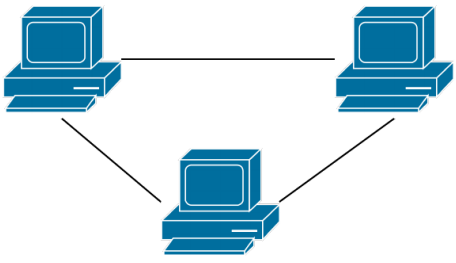


*Figura 2. 45. Topología de malla.*

### 2.23.7 Las topologías mixtas

También llamadas topologías híbridas: son aquellas en las cuales se unen dos o más tipos de topologías para crear una arquitectura más robusta y redundante en la red, aprovechando las ventajas y disminuyendo las desventajas de una topología y la otra.

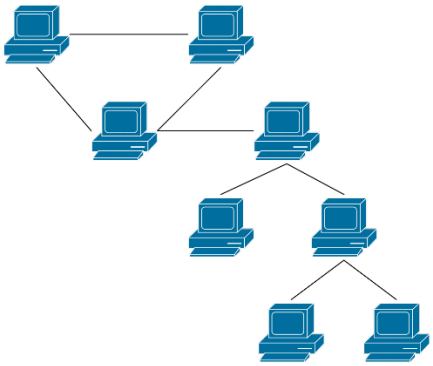


*Figura 2. 46. Topología Mixtas.*

Esta imagen representa una topología malla combinada con una de árbol.

## 2.24 Importancia de las topologías de redes

Estas diversas formas de conexión de dispositivos nos presentan diversas formas de diseño de redes de acuerdo con las necesidades del usuario y la disponibilidad de presupuesto existente ya que mientras más robusta una red más eficiente y fuerte es.

la topología mediante su correcta aplicación e implementación pude brindar al negocio alta disponibilidad de recursos y por ende esto impacta positivamente al nivel de productividad de la empresa.

Mediante la topología se puede obtener un mayor aprovechamiento de los recursos tecnológico de la empresa mejorando así el desempeño de la red en cuestión.

## 2.25 Conclusión

En conclusión, podemos afirmar que hoy en día la implementación de una red informática es imprescindible, ya que ayuda a las organizaciones a facilitar su trabajo en una forma más eficiente y eficaz ya que el flujo de datos seria consistente y en alta velocidad reduciría los intervalos de interrupción de tiempo laborar, permitiría la extensión de equipos de trabajo, seguridad o extender la red aún más permitiendo escalabilidad y posibilidades de crecimiento a mediado o largo plazo.

Y también la importancia que tiene la seguridad en las redes, ya que sin mecanismo de seguridad nuestra red estaría al expuesta a las diferentes fuentes de amenazas tantos físicas como digitales y que amenazan en contra del buen funcionamiento, seguridad o integridad de la organización, para esto dentro de la red que se diseñara se especificara elementos que permitan el correcto funcionamiento de la institución.

Es de suma importancia conocer la gama de virus existentes en el vasto internet y es de suma importancia poder combatirlos por el bien de la enorme cantidad de datos que se alberga en los servidores con este fin en este capítulo hablamos de los virus, su forma de combatirlos y evitarlos.

# CAPÍTULO 3
# TECNOLOGÍAS BIOMÉTRICAS

## 3.1 Introducción

**E**n este capítulo pasaremos a hablar de las diversas tecnologías biométricas existentes y un breve desarrollo de cada elemento que compone el tema, conceptos necesarios para el continuo desarrollo del trabajo.

En ese breve desarrollo hablaremos de los conceptos necesarios para entender y conocer sobre la tecnología biométrica, pasaremos a como la tecnología biométrica trabaja de la mano con la seguridad de diversas áreas, como influye está en la seguridad. También sobre los diferentes tipos de tecnología biométrica, ya que conocer la gran variedad de estas tecnologías nos dará la oportunidad de comparar, conocer, saber ventajas y desventajas entre ellas y así poder elegir la mejor opción no solo para esta empresa si no para cualquier otro tipo de establecimiento, hogar e incluso organización en el cual se planea o en un futuro se elija introducir dicha tecnología.

Hablaremos también de las ventajas que conlleva poseer un sistema biométrico sobre los sistemas de verificación convencionales, en la cual tocaremos puntos claves de suma importancia, su importancia como avance tecnológico en especial en la orientación de seguridad y sobre todo hablaremos sobre la tecnología biométrica de huella dactilar.

En ese apartado hablaremos de varios puntos que componente dicha tecnología, su funcionamiento como tal y sus diversas características, ventajas y desventajas y su importancia y por último hablaremos de la tecnología biométrica en República Dominicana.

Tocaremos como tal este apartado individual ya que es una de las principales tecnologías de mayor fiabilidad en el mercado y es una de tecnologías más interesantes ya que más adelante describiremos a fondo esta tecnología, el que la vuelve tan fiable y dicho de cierta manera amigable al usuario final que es el principal interesado en esta tecnología.

## 3.2 Conceptos de Tecnología Biométrica

*Figura 3. 1. Conceptos Tecnología Biométrica.*
**Fuente: https://www.ticbeat.com/seguridad/identificacion-biometrica-que-es-como-funciona-y-cuales-son-sus-riesgos/**

(Luis Chuqui, 2014, Pág. 1) "El término biometría proviene de las palabras: BIOS (vida) y metrón (medida). "La biometría es la ciencia que estudia las características únicas que posee una persona" tales como: rostro facial, mano, huella, dactilar, voz, silueta e iris, mediante el uso de métodos estadísticos y algoritmos para conseguir la detección del individuo. Dichos métodos "presentan un pequeño margen de error en la realización de la identificación de la persona."

Las tecnologías biométricas son dispositivos electrónicos que a partir de un elemento único e irrepetible que le pertenece a cada individuo, es decir cada ser humano que puede iniciar un proceso o simplemente identificar a dicho individuo, cabe destacar que dichos dispositivos son incorporados en diferentes equipos con el fin de crear una barrera de seguridad o elementos de identificación con el cual efectuar comandos, instrucciones o simplemente una acción programada.

## 3.3 Seguridad Biométricas

La seguridad biométrica podemos definir como el uso de tecnologías de seguridad y autenticación mediante el uso de rasgos biométricos de la persona, por ejemplo, el uso de huellas dactilares, escaneo de iris, escáner facial, etc.

Las tecnologías de seguridad biométrica tienen un rol muy importante como controles de acceso, ya que son muy comunes su uso en la empresa, organización, y hasta se ha extendido al uso del hogar. Ya que nos permite tener un mayor control, confiabilidad y comodidad que tener, por ejemplo, utilizar llaves para tener acceso.

Todo esto es posible porque la persona se determina por los rasgos, los cuales se pueden clasifican en dos tipos.

El primero es el Fisiológicos: en este tenemos la retina, iris, reconocimiento facial, geometría de la mano y huella dactilar.

De segundo el Comportamiento: en este se encuentra la Firma, voz, dinámica de teclado.

Estos dos rasgos son diversas maneras de cómo usar la tecnología biométrica, pero unos son mejores que otros, pero otros son más económicos, más adelante hablaremos de los tipos de biométrica que existen y cuáles son sus ventajas entre otras cosas.

## 3.4 Tipos de Tecnología Biométrica

### 3.4.1 Reconocimiento Oculares

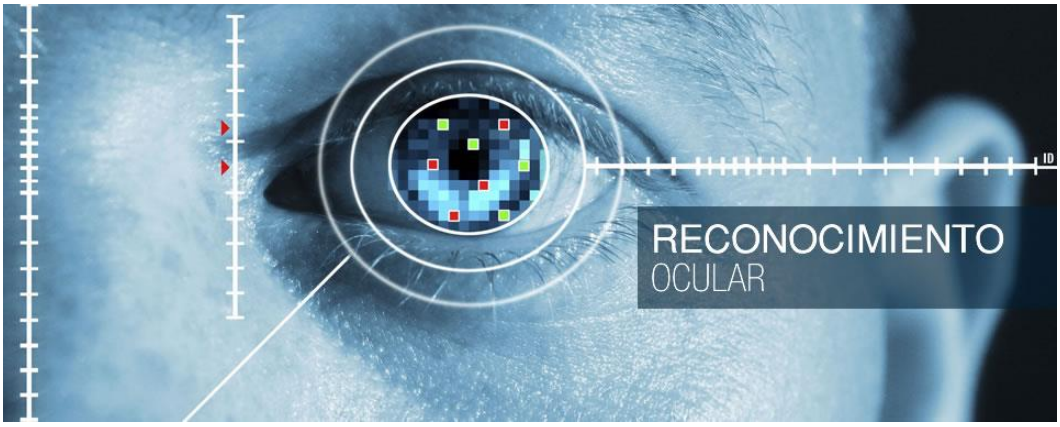



*Figura 3. 2. Reconocimiento Ocular.*
**Fuente: https://thecuttingedgenews.com/index.php?article=85497**

Este tipo es uno de los más seguro y confiable ya que la semejanza de una persona con otra es cercana a cero. Cuando decimos que son segura es debido a que tienen:

- Integridad Alta
- Perdura toda la vida

Esta técnica se subdivide en: reconocimiento de iris y reconocimiento de retina ambas tienen muchas similitudes, pero a su vez poseen muchas diferencias.

**Reconocimiento de iris**: este método toma una imagen del iris del individuo en cuestión escanea cada patrón de dicho iris y lo compara con el guardado en la base de datos, ya que cada persona poseemos un patrón de iris distinto esto hace esta técnica confiable.

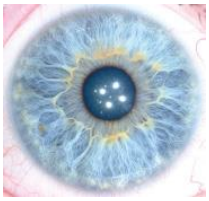


*Figura 3. 3. Reconocimiento de Iris.*
**Fuente: http://www.m2sys.com/blog/biometric-hardware/iris-recognition-vs-retina-scanning-what-are-the-differences/**

**Reconocimiento de retina**: este método escanea las pequeñas venas que poseemos en la retina y analiza el patrón de estas para luego comprarlo en una base de datos con el fin de validar si dicho patrón existe o es el que intenta ingresar o validarse en el sistema.

*Figura 3. 4. Reconocimiento de Retina.*
**Fuente: http://www.m2sys.com/blog/biometric-hardware/iris-recognition-vs-retina-scanning-what-are-the-differences/**

Desventajas

Este tipo de reconocimiento no es muy agradable a la hora de utilizarse porque el usuario tiene que hacer una lectura de láser, no importa si para el escaneo de retina.

También de que, si el usuario sufre de la vista, ya sea miopía o astigmatismo, u otro tipo de enfermedad ocular, esto puede afectar a la hora de hacer el escanea, debido a que los ojos van a ir haciendo permutaciones.

Similitudes:

a. Ambos métodos poseen bajas aceptaciones y falsos positivos, esto quiere decir que son técnicas muy rechazadas por el público en general y su taza de error es cercana a cero.
b. Ambas técnicas son muy confiables ya que el material biométrico a verificar jamás será encontrado con exactitud en dos personas, porque cada material biométrico es único en cada individuo.
c. Alta velocidad de verificación de datos biométricos.

Diferencia entre Iris y retina:

La principal diferencia entre estas técnicas recae en la forma en que se escanea o verifica la una con la otra ya que el escaneo del iris se realiza con una cámara cualquiera de alta resolución, porque el iris es perfectamente fisible sin profundizar tanto en el ojo humano, a diferencia del escaneo de retina donde se da uso de un láser de baja frecuencia que penetra para conseguir que los pequeños vasos sanguíneos se iluminen haciendo visible para el equipo, luego un vez el patrón visible es guardado en la base de datos como un código legible para el equipo.

### 3.4.2 Reconocimiento Facial

*Figura 3. 5. Reconocimiento Facial.*
**Fuente: https://www.unocero.com/noticias/la-policia-esta-usando-la-tecnologia-de-reconocimiento-facial-de-amazon/**

Esta tecnología biométrica consiste en realizar un escaneo de los rasgos físicos del rostro humano, para luego crear un perfil del usuario. Este tipo de tecnología no es muy usado, debido a que el rosto humano tiende a tener cambio al pasar los años.

Este tipo de sistema de seguridad no es muy beneficioso al menos de que se combine con otros tipos, por ejemplo, si utilizamos sistema de vigilancia, estos 2 sistemas unido pueden crear una seguridad impecable, debido a que, si se está buscando a una persona en específico, mediante los rasgos pueden obtener resultados.

Unas de las ventajas que tiene este tipo es que es más preventivo que los demás, debido a que el usuario no tiene que tener contacto con el aparato para hacer el proceso de escaneo, por esa razón rendimiento que otorga para evitar la contaminación es altamente alto.

Cabe destacar que, si el software que implementa no está bien desarrollado, este tipo de biometría no será la mejor adecuada de usar, ya sea en una empresa u otro tipo de lugar donde se requiera dicha tecnología.

### 3.4.3 Reconocimiento Dactilar

*Figura 3. 6. Reconocimiento Dactilar.*
**Fuente: https://cerrajeria-cerrajero.com/blog/identificacion-y-acceso-con-huella-digital**

La tecnología de reconocimiento dactilar se puede definir como un dispositivo capaz de escanear, almacenar e identificar el patrón dactilar de una persona.

También esta tecnología es de las más utilizadas, debido a que cada individuo posee un rasgo propio y único.

Este tipo de tecnología está incluido en los smartphones de las gamas alta, y gamas medias de la actualidad, pero ya lleva más de 12 años implementándose.

### 3.4.4 Reconocimiento por Voz

*Figura 3. 7. Reconocimiento por voz*
**Fuente: https://www.tn8.tv/tecnologia/455376-siri-ahora-podra-reconocer-voz-diferentes-usuarios/**

El reconocimiento por voz es una tecnología que mediante software capta el tono, la velocidad y ritmo de la voz de la persona, para luego crear un perfil el cual se utilizado para conceder acceso a un área determinada.

Primero, mediante un micrófono se capta la voz, para luego la señal análoga que capta el micrófono enviarla a la computadora. Por último, mediante un software de reconocimiento de voz convierte la dicha señal análoga a digital, y como también ser procesada para poder descifrar las palabras.

Pero esta tecnología tiene la desventaja que a la hora de captar la voz se debe estar en un ambiente poco ruidoso, sino el software podría tener problemas para procesar la voz e identificar las palabras. Otra desventaja, es que debido a que un país habla un idioma, cada ciudad tiene un acento diferente a las otras ciudades. Y esto puede ser un problema para el software a la hora de identificar las palabras.

## 3.5 Ventajas de las Tecnologías Biométricas

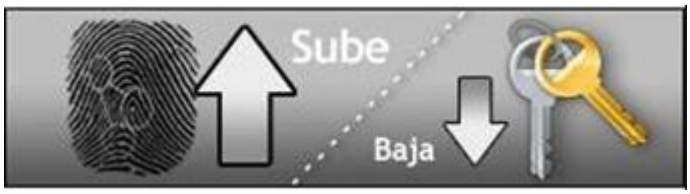



*Figura 3. 8 ventajas de la tecnologia biometrica*
**Fuente: http://caracol.com.co/radio/2012/01/04/tecnologia/1325691060_600612.html**

Como se puede visualizar en la imagen, la tecnología biometría nos da mayor seguridad que el método tradicional, debido a que no es fácil de eludir esta tecnología.

Una de las grandes ventajas que tenemos al implementar estos dispositivos es que el usuario final no tiene que introducir sus credenciales a la hora de entrar a algún lugar o equipo, basta con utilizar su dedo, retina, voz o simplemente su rostro, con estos dispositivos para validar su acceso a cualquier otro lado, sea un área específica, su computadora, celular, entrada a su trabajo o incluso validar sus datos en algún centro comercial.

Otra ventaja es que, para acceder a un lugar, de la forma tradicional como ya se menciona, se debe de utilizar una tarjeta de acceso o llave, pero a la hora de implementar esta tecnología, nada de estos accesorios pude ser robados porque no tenemos que andar con ellos de la mano, por eso la probabilidad al robo es extremadamente bajo, no como en caso tradicional.

## 3.6 Importancia de las Tecnología Biométrica

Las tecnologías biométricas tienen un rol muy importante a la hora de implementar un control de acceso, ya sea para permitir el acceso a un área determina y/o hasta para poner un grado más de seguridad a nuestro hogar. Estos tipos de tecnología, debido a que utilizan rasgos únicos de una persona, lo cual hace que sean tecnología de seguridad bastante robusta y eficaz. Ya que envés de que un empleado tenga que usar una tarjeta o un pin de seguridad para tener acceso a la organización existe la posibilidad que dicho empleado se le extravié la tarjeta o se la roben ya un tercero podría tener acceso debido a la organización. Con las tecnologías biométricas con tan solo escanear la huella dactilar del personal autorizo lo último dicho se puede eliminar.

## 3.7 Características de las Tecnología Biométrica

Entre las características generales que debe poseer un sistema biométrico debe estar:

Desempeño: con esto nos referimos a la rapidez, exactitud y robustez que alcanza al hacer su cometido también este incluye los recursos invertidos, los factores operaciones y ambientales.

Aceptabilidad: indica la capacidad que tiene las personas de aceptar estos dispositivos en su vida diaria ya que ningún dispositivo biométrico debe suponer un peligro o problema para los usuarios.

Fiabilidad: refleja que tan difícil es para los intrusos burlar estos sistemas, el sistema biométrico.

## 3.8 Tecnología Biométrica Huella Dactilar

Esta tecnología permite tomar los patrones que están en los dedos de las manos para crear un perfil en la base de datos dentro del dispositivo o en la base de datos de la empresa para así validar la entrada de las personas o simplemente validar el acceso de una persona.

### 3.8.1 Características

Esta tecnología se basa en tomar los patrones geométricos de la cresta que son reconocibles a simple vista. Usualmente se determina el dueño de dicho patrón mediante el conocimiento de sus puntos singulares, que son guardados y digitalizados en una computadora y una vez el dueño vuelve a colocar su dedo en el escáner la computadora busca en su base de datos y compara cada patrón guardado hasta encontrar el patrón al que pertenece dicha huella digital.

Es necesario explicar dos conceptos que están relacionados a esta técnica:

**Área Patrón**: Esta área es la principal y es la que alberga la cresta y todas aquellas características que el sensor y la computadora guardan en la base de datos.

**Líneas Tipo**: Están definidas como dos crestas que inician paralelamente y divergen sobre el área del patrón.

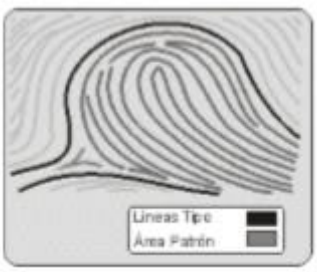



*Figura 3. 9. Características de las Huellas Dactilares.*
**Fuente: (Hidalgo, 2010, Pág. 28)**

Como se puede visualizar en la imagen, la línea negra es la que representa las líneas tipos, y la parte gris muestra las Aérea Patrón.

Puntos característicos

Cada dispositivo que se encarga de examinar las huellas dactilares debe de saber identificar los diferentes tipos de características que posee, a continuación, se le mostrara una imagen de cada una de estas características.

*Figura 3. 10. Puntos Característicos de la Huella Dactilar.*
**Fuente: http://ellegadoenlascenadeldelito.blogspot.com/2014/05/puntos-caracteristicos-de-las-huellas.html**

- Fragmento: Es una diminuta proporción de papilas que conforman las crestas lineales.
- Empalme: Es la unión en paralelo de dos crestas unidas por un fragmento formando un ángulo
- Ojal: Es la formación de un círculo entre las crestas mediante la unión de una convergencia y una bifurcación.
- Desviación: Son dos crestas que jamás se cruzan entre sí.
- Transversal: Es cuando una cresta pasa por el medio de otra cresta dactilar.
- Abrupta: Es una cresta en la cual su recorrido se interrumpe.
- Bifurcación: Tomamos una cresta y la colocamos en la dirección de las manecillas del reloj, pero según esa cresta avanza en su vía llega un momento en que se divide y la otra parte que se obtiene toma la dirección opuesta.
- Interrupción: Es una cresta con recorrido discontinuo.
- Punto: Son pequeños fragmentos de la huella dactilar en forma de un punto.

#### 3.8.1.1 Puntos Singulares

Dentro de los puntos singulares de una huella dactilar tenemos dos, Punto Core y Punto Delta.

El **Punto Core** se encuentra en el Área Patrón, donde las crestas tienen una curvatura mayor.

El **Punto Delta** es en el cual existe una discrepancia en las líneas Tipo internas que envuelven el Área Patrón. Delta se refiere a una formación tipo triangulo.

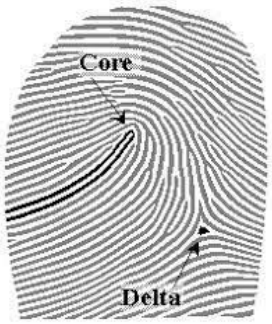



*Figura 3. 11. Puntos Singulares de la Huella Dactilar.*
**Fuente: https://biometrics-on.com/identificacion-biometrica-a-traves-de-huella-dactilar/**

### 3.8.2 Ventajas

- Es una técnica de fácil uso.
- Es fiable pues usa elementos biométricos irrepetibles.
- Es compacto por lo que puede estar en múltiples lugares.
- Bajo costo de mantenimiento.
- No requiere de elementos adicionales para accionar puertas o diversos dispositivos.

### 3.8.3 Técnicas de Reconocimientos

Para poder hacer un reconocimiento de huellas dactilares debemos de seguir 2 técnicas, las cuales son:

1. Basada en Detalles: este tipo fabrica un plano por encima de la huella, con el fin de poder buscar de forma segura al sujeto. La desventaja de esta es que, si la huella que se va a examinar no es de buena calidad, será muy difícil de situar.

2. Basada en Correlación: este tipo se creó con el fin de mejorar las fallas de la técnica anterior (Basa en detalles) pero este también presenta fallas, esta es que necesita la ubicación de una marca del registro, este se ve afectado por el traslado por la figura.

### 3.8.4 Modelo de identificación

Para cualquier proceso de identificación existe un modelo, H.AK., el cual significa "How, Are, Know" por sus siglas en ingles. Y se refiere al proceso de validar a un usuario mediante:

- Algo que sabe, por ejemplo: una contraseña, pin, etc.
- Algo que es o posee, como un usuario o una tarjeta.
- Y por último algo que es, una característica única de la persona. Como, por ejemplo, las huellas dactilares, reconocimiento fácil, de iris, etc.

Mediante este modelo es posible fusionar los distintos indicadores anteriormente mencionados para tener un proceso de autenticación más robusto, y tener varios niveles de seguridad a la hora de identificar a una persona.

## 3.9 Conclusión

En conclusión, las tecnologías biométricas son aquellas que nos permiten obtener acceso a alguna función o acceso a algún lugar físico gracias a la verificación que esta hace con algún elemento físico de nuestro cuerpo sea nuestras caras, iris, huellas digitales, manos, retina y voz, gracias a esos elementos irrepetibles en nuestros cuerpos somos capaces de tener una identificación única e irrepetible con el cual estos equipos electrónicos son capaces de identificarnos y así dotarnos de el acceso necesario para nuestras funciones.

Existen distintos tipos de tecnologías biométricas como son:

- Reconocimiento facial
- Reconocimiento de ocular que se subdividen en: iris y retina.
- Reconocimiento por voz
- Reconocimiento de palma o mano

Cada tipo de reconocimiento utiliza una parte única del ser humano y cada una de esas partes llevan características que solo cada individuo posee y eso hace que estos sistemas sean confiables.

# CAPÍTULO 4
# PROPUESTA DE DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA BIOMÉTRICO PARA LA EMPRESA GESTIONES DE ADUANAS D & M

## 4.1 Introducción

En este capítulo hablaremos de la situación actual de la empresa Gestiones de Aduanas D & M que nos permitirá observar el nivel de la tecnología empleada dentro de los diversos niveles de la empresa sea como redes, computación, servidores entre otros, permitiéndonos así tener una visión general de la empresa y a partir de esta generar diversas ideas a partir de los conocimientos adquiridos y planteados anteriormente para mejorar en un 100% los sistemas de la empresa, gracias a la recopilación de información de la situación actual podremos visualizar cuál de las diversas topologías utiliza actualmente la empresa y así decidir un cambio óptimo para la empresa.

Emplearemos un análisis FODA para conocer las fortalezas y debilidades de la empresa con esos resultados presentar un estado más detallado de esta aparte de la información ya marcada anteriormente, posterior a esto plantearemos nuestra propuesta de implementación y desarrollo para nuestro data center donde detallaremos los dispositivos, diferentes equipos, precios y razones por los cuales son elegidos para esta labor a continuación de esto detallaremos las bondades del uso de nuestro sistema de data center, las bonificaciones de desarrollo y de productividad que acarrearía esta implementación. Los fundamentos por los cuales hacemos esta propuesta y nuestros objetivos a mediano y largo plazo con esta implementación, dentro de esto hablaremos de la ubicación de esta enorme estructura que es un elemento de suma importancia ya que a partir de esta estructura se ramificarán las diversas conexiones y cableados que existirán en la empresa.

El diseño de la nueva red mejorada a partir del diagrama de red actual ya anteriormente mencionado de la institución con este nevo diagrama tendremos la estructura ara el diseño de la nueva red que se establecería en la institución, con la cual se busca mejorar el flujo de datos, dado y creado este diseño e implementación de esta nueva red se darán a conocer los objetivos y fundamentos de esta misma dando a relucir los beneficios y mejoras que traerían consigo esta nueva red.

El estudio de factibilidad para conocer qué tan viable y efectivo es todo lo mencionado anteriormente, la técnica operativa con esto trazaremos las pautas y pasos para llevar a cabo este trabajo planteado, la inversión de la operación con esto mostraremos los gastos que conlleva todo el proyecto planteado a lo largo de este capítulo y posteriormente a eso el retorno de esta inversión que será la velocidad con la cual estos cambios futuros dejaran benéficos a nivel de valor agregado y por último el cronograma del proyecto que nos mostrara paso a paso como se desarrollara el proyecto.

## 4.2 Situación Tecnológica De Gestiones de Aduanas D & M

En la empresa De Gestiones de Aduanas D & M en el área de tecnología tan solo cuenta con un switch, el cual conecta a las computadoras a un router hacia su ISP. Lo cual representa la carencia de un red LAN bien estructurada, que a su vez la empresa está perdiéndose de los beneficios que brinda una red LAN bien estructurada, tales como mayor seguridad, mayor eficiencia a la hora de compartir información o como mencionan Rafael Jesús Castaño Ribes y Jesús López Fernández en su libro "Redes Locales" las redes LAN pueden brindar una Administración centralizada, ya que la existencia de una red simplifica las tareas de administración, ya que permite que muchas de las operaciones se realicen de forma centralizada en el servidor de la red o que se puedan resolver remotamente problemas de configuración. Y como también "Ficheros y datos compartidos: esto posibilita el trabajo en grupo, ya que muchos usuarios pueden trabajar sobre el mismo fichero, disponer de la información en todo momento o comunicarse instantáneamente con distintos elementos de la red."

La empresa carece de base tecnológica sustentable o suficiente para albergar un posible aumento o crecimiento tecnológico porque lo que es recomendable diseñar y preparar una nueva red capaz de sobrellevar estos avances y por supuesto acorde a las necesidades de dicha empresa.

Dentro de la empresa se alberga 3 máquinas, 2 desktop y 1 laptop como se apreciará en las siguientes imágenes:

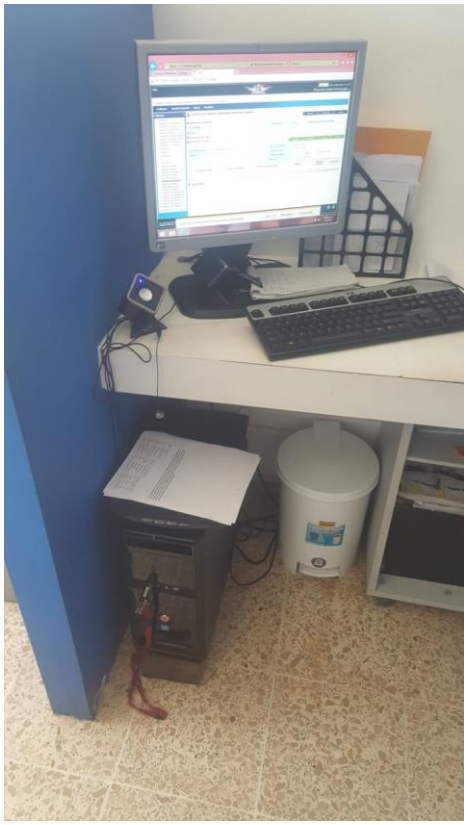


*Figura 4. 1. Situación actual de la empresa Gestiones de Aduanas D&M 1.*
**Fuente: Gestiones de Aduanas D&M**

*Figura 4. 2. Situación actual de la empresa Gestiones de Aduanas D&M 2.*
**Fuente: Gestiones de Aduanas D&M**

Esta es una computadora ensamblada sin marca especifica que posee las siguientes características, ya que son clon una de la otra comparte especificaciones similares.

*Figura 4. 3. Situación actual de la empresa Gestiones de Aduanas D&M 3.*
**Fuente: Gestiones de Aduanas D&M**

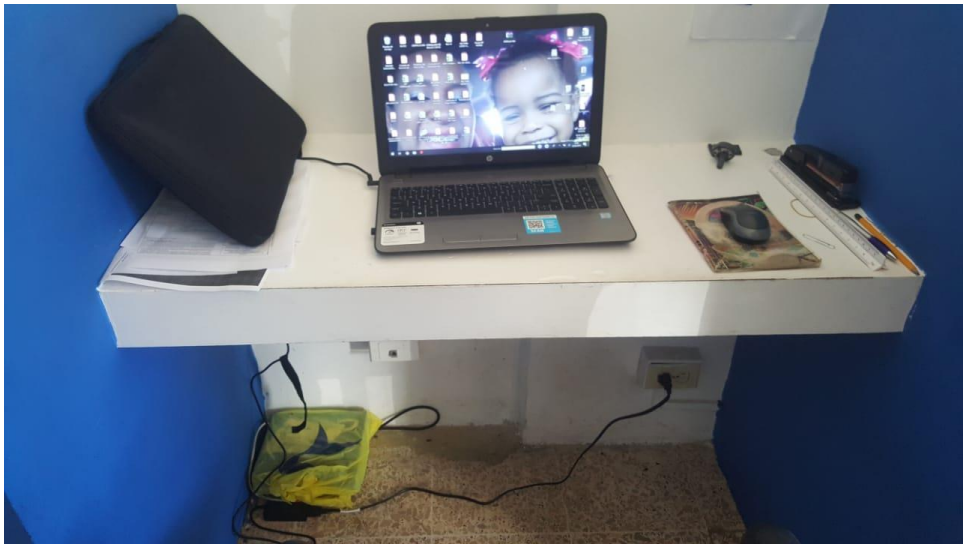


*Figura 4. 4. Situación actual de la empresa Gestiones de Aduanas D&M 4.*
**Fuente: Gestiones de Aduanas D&M**

Las características de esta computadora son:

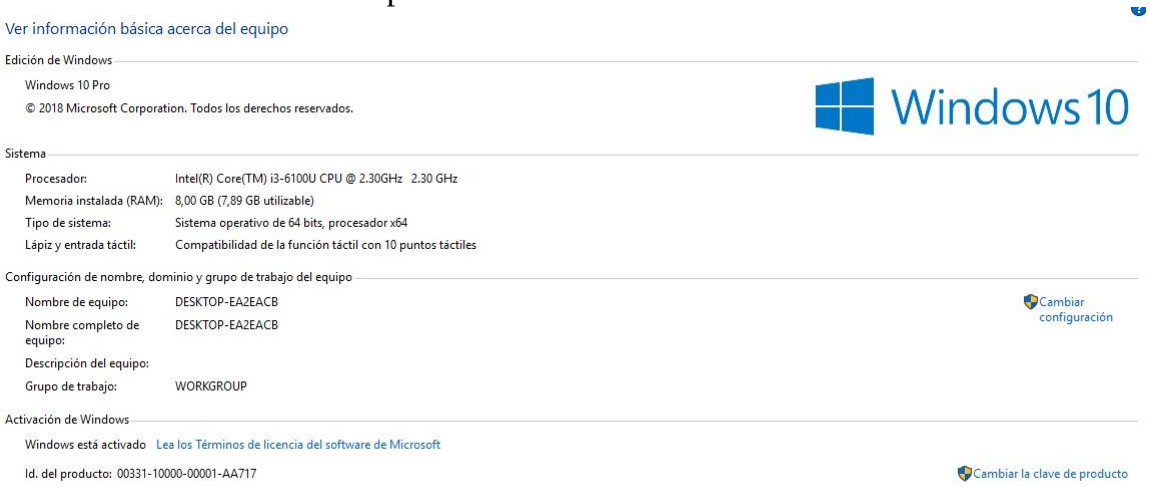



*Figura 4. 5. Situación actual de la empresa Gestiones de Aduanas D&M 5.*
**Fuente: Gestiones de Aduanas D&M**

Aparte de las diferentes maquinas también la empresa cuenta con 2 impresoras

*Figura 4. 6. Situación actual de la empresa Gestiones de Aduanas D&M 6.*
**Fuente: Gestiones de Aduanas D&M**

Estas están conectadas a la red de la empresa e imprimen desde cada computadora de manera independiente, esta impresora es del uso de los empleados.

El modelo de esta impresora es E-Studio203L

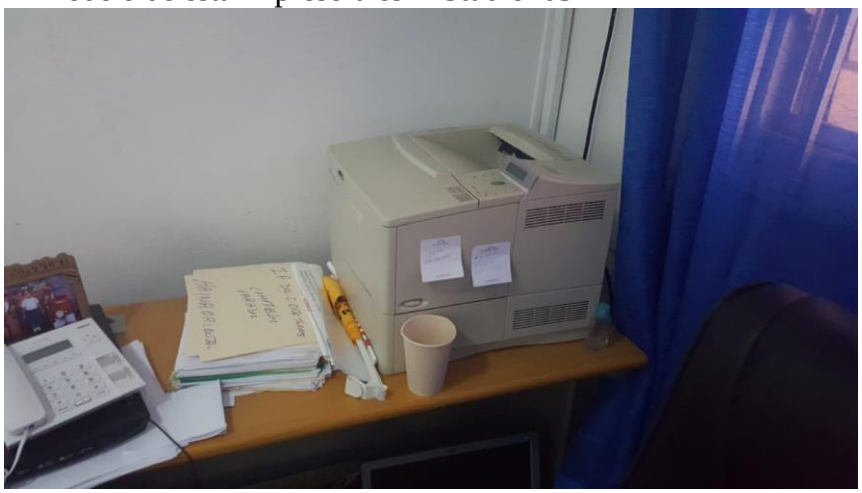


*Figura 4. 7. Situación actual de la empresa Gestiones de Aduanas D&M 7.*
**Fuente: Gestiones de Aduanas D&M**

Esta impresora es de uso exclusivo del jefe de la empresa. También conectada por red, el modelo de esta impresora es HP laserJet4000N.

Pese a que sus equipos son capaces de entregar el mayor desempeño y comodidad para el trabajo la empresa no cuenta con una estructuración del cableado adecuado y equipos para las redes capaces de soportar el crecimiento y aumento de demanda dentro de la red.

*Figura 4.8. Situación actual de la empresa Gestiones de Aduanas D&M 8.*
**Fuente: Gestiones de Aduanas D&M**

Los cables de red par trenzado que usan para estructurar su red son categoría 5, de muy mala calidad, propenso a rupturas y sin ser certificados.

En la siguiente imagen se presenta la seguridad de vigilancia que poseen

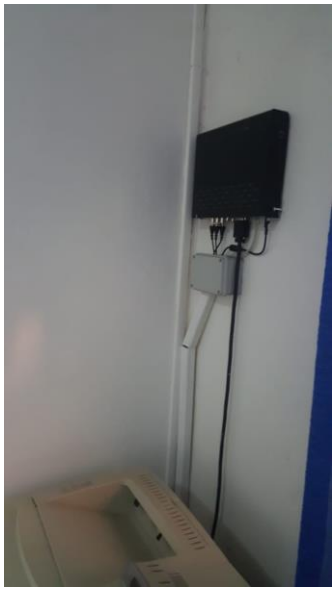


*Figura 4.9. Situación actual de la empresa Gestiones de Aduanas D&M 9.*
**Fuente: Gestiones de Aduanas D&M**

En el cual emplean un DVR enlazado en la red y con el cual a través de un monitor observan el flujo de personal, es un DVR análogo con resolución HD con almacenamiento interno, a través de una aplicación son capaces de visualizar la situación de la empresa desde cualquier lugar.

## 4.3 Diagrama de red actual

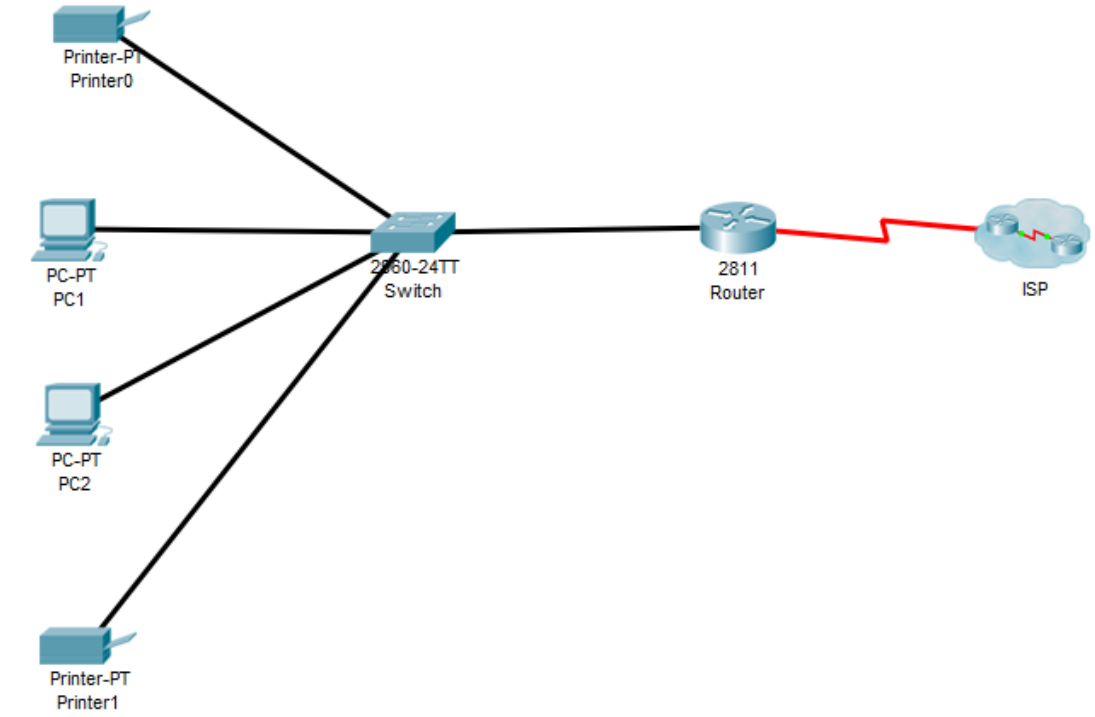
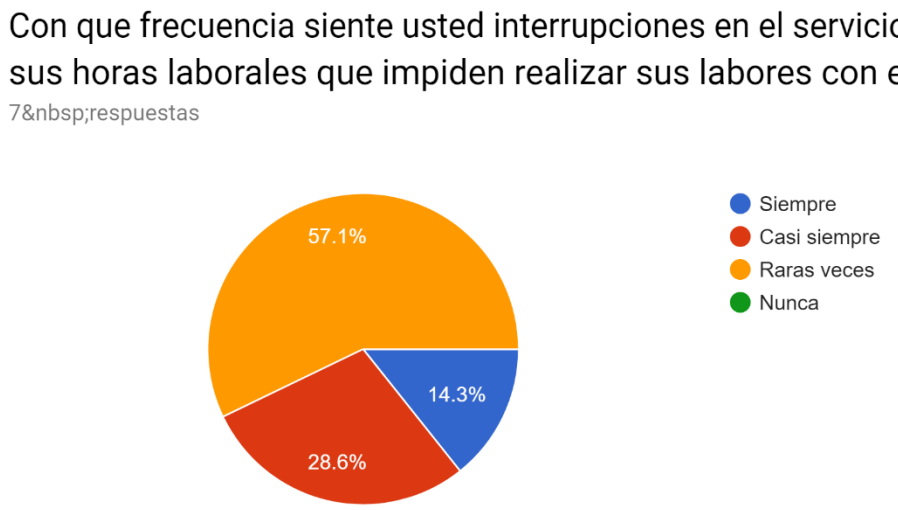
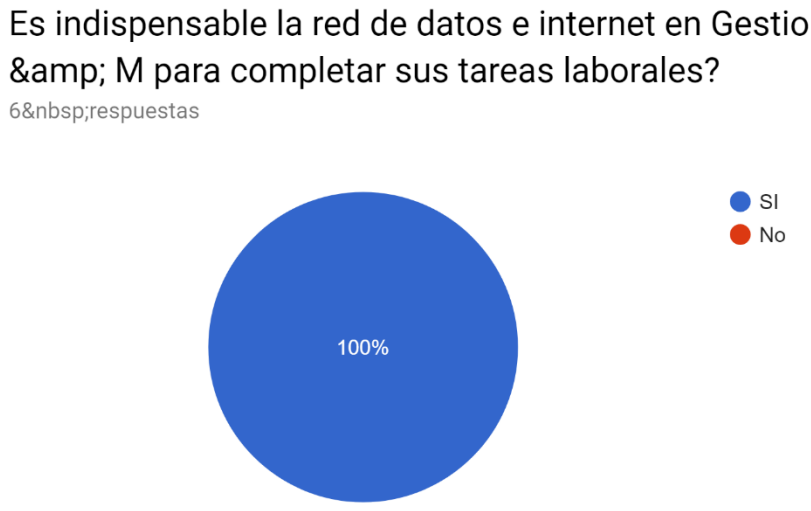



*Figura 4. 10. Diagrama de Red Actual de la empresa Gestiones de Aduanas D&M.*
**Fuente: Gestiones de Aduanas D&M**

En el siguiente diagrama se puede ver el diagrama de red actual en la empresa Gestiones de Aduanas D & M en la imagen podemos apreciar un diseño simple de red donde un proveedor de internet alimenta la edificación completa a través de un router estándar de dicho proveedor conectado a un switch de distribución, esta es una configuración básica adecuada para un hogar donde no se requiere ningún tipo de seguridad , pero en una empresa en crecimiento es poco eficiente ya que carece de elementos de seguridad, configuración para albergar múltiples dispositivos y para la capacidad de aplicar un servidor donde se puedan gestionar roles dentro de esta.

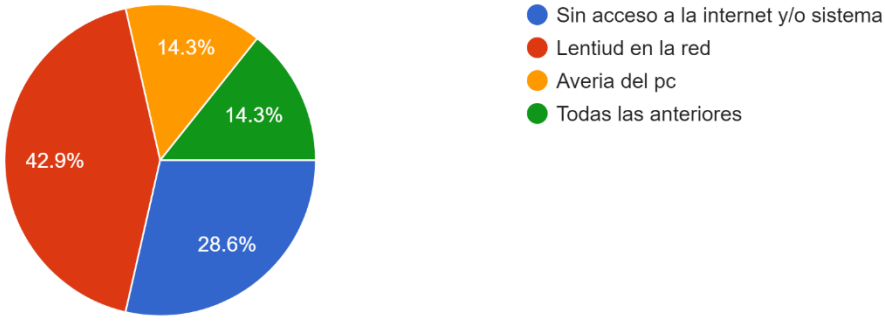
En el proceso de investigación de la situacion actúal organizamos una serie de preguntas para los empleados de la empresa, la totalidad de estos es de 7 empleados a los cuales como muestra tomamos la totalidad ya que todos estos trabajan usando la infraestructura tecnológica de la institución, a continuación le presentaremos varias de las preguntas de mayor importancia y las cuales tomamos como base para el desarrollo de los posteriores itemes de este trabajo, a su vz aparte de las preguntas le presentaremos un diagrama porcentual de las respuestas.



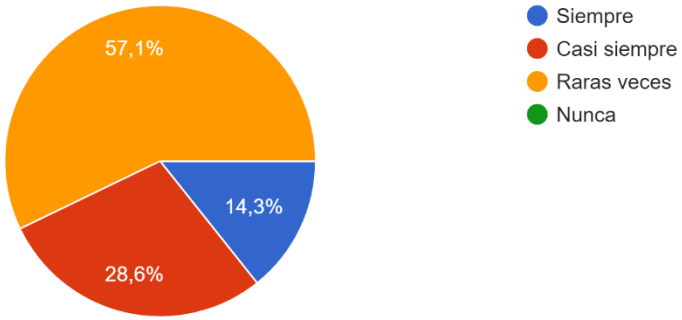
Que tipo de inconvenientes suele presentarse?

7 respuestas




Con que frecuencia siente usted interrupciones en el servicio de red durante sus horas laborales que impiden realizar sus labores con exito?

7 respuestas



## 4.4 Análisis FODA

El análisis FODA es una técnica que analiza el estado actual de una empresa para obtener una evaluación detallada de esta, con el fin de a partir de esos resultados tomar decisiones acordes a los objetivos y metas que se hayan propuestos.

Para elaborar el análisis FODA se debe analizar 4 variables que son: las fortalezas, debilidades, oportunidades y amenazas, de estas 4 variables 2 son internas como son las fortalezas y debilidades donde se hace un estudio interno de la organización en búsqueda de elementos de fortalezas y carencias de la organización y luego se prosigue con las 2 variables externas que son oportunidades y amenazas que l analizar estas variables buscamos conocer la viabilidad de que la organización pueda iniciarse en un nuevo mercado o ámbito y de conocer que elementos externos pueden obstaculizar su crecimiento o desarrollo.

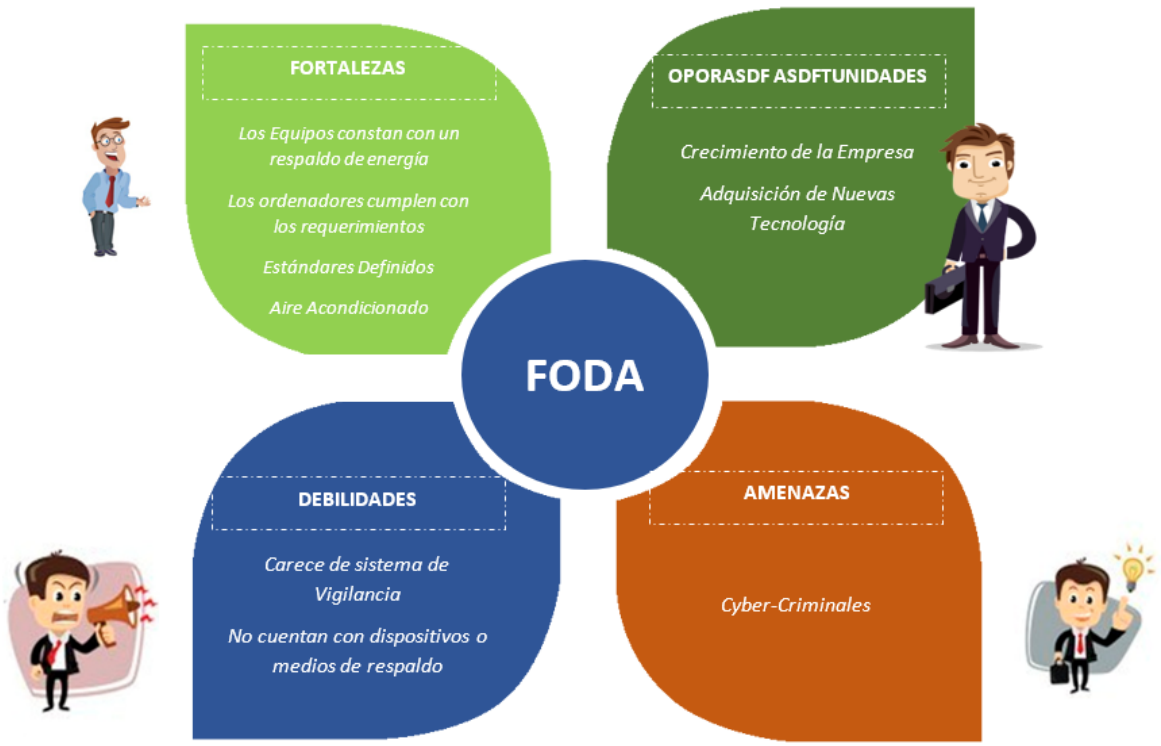
**Fortalezas:** Son las aptitudes o especialidades que tienen una empresa u organización.

**Oportunidades**: Son las situaciones u ocasiones que hacen posible que se realice algo de la empresa.

**Debilidades**: Son aquellos recursos o procesos que no posee una empresa, lo cual necesita para desarrollarse y alcanzar todo su potencial.

**Amenazas:** Posible peligro que en un futuro podría explotar una vulnerabilidad.

Tomando en cuenta cuales son los cuatros variables del análisis FODA podemos decir que la empresa Gestiones de Adunas D&M se observan los análisis ante la Propuesta de Diseño e Implementación de un Sistema Biométrico.



## 4.5 Propuesta de desarrollo e implementación de un Data center

En este apartado detallaremos de los diferentes elementos que proponemos para la formación de un data center para la compañía Gestión de Aduanas D & M, con la cual pretendemos mejorar los servicios y procesos llevados a cabo en esta compañía de servicios en las Aduanas, estos diferentes equipos fueron seleccionados dado el tamaño de la empresa, el capital que maneja y los requisitos y servicios que se trabajan día a día dentro de la institución.

### 4.5.1 Equipos Propuestos

- **Servidor DELL POWEREDGE T30 TOWER**

*Figura 4.11. DELL Poweredge T30 Tower.*
**Fuente: https://www.dell.com/do/empresas/p/poweredge-t30/pd**

| Características | |
|---|---|
| **Procesador (CPU)** | Intel ® Xeon® E3-1225 v5 |
| **Sistema Operativo** | Microsoft® Windows Server® 2012 |
| **Memoria** | 8 GB de RAM DDR4 a 2133 mt/s |
| **Dimensions** | 6.89 x 14.17 x 17.12 in |
| **Puertos** | 10x USB, 1x Micrófono, auriculares, PS2, DisplayPort, HDMI, RJ45, Puerto Serial, Entrada y Salida de Audio |
| **Chasis** | Mini torre |
| **Disponibilidad** | Memoria de código de corrección de errores 9ECC) |
| **Alimentación** | 290W |
| **Chisepset** | Intel C236 |
| **Red** | Intel I219-LM Gigabit Ethernet LAN 10/100/1000 |
| **Almacenamiento** | 1 TB |
| **Garantía** | 1 año |

*Tabla 4. 1. Características del Servidor*

- **Router Ubiquiti edgerouter 4**

*Figura 4.12. Router Ubiquiti edgerouter 4.*
**Fuente: https://www.ui.com/edgemax/edgerouter-4/**

El EdgeRouter ™ 4 ofrece un valor de precio / rendimiento de próxima generación: hasta 3.4 millones de paquetes por segundo de procesamiento con una tasa de línea de hasta 4 Gbps.

| Características |
|---|
| 4 puertos RJ45 gigabit |
| 1 GB de RAM |
| 1 puerto SFP |
| 1 puerto para consola |
| 1 puerto USB 3.0 |
| 4 núcleos a 1ghz |

*Tabla 4. 2. Características del Router EdgeRouter 4.*

- **Switch D-Link DGS-1100 Series Gigabit Managed**

*Figura 4. 13. Switch.*
**Fuente: http://us.dlink.com/products/business-solutions/dgs-1100-24p/**

| Características |
|---|
| 24 puertos |
| POE o Power Over Ethernet de los puertos 1 al 12. |
| Potencia del POE desde 64 Watt a 370 watt. |
| Vienen con gabinete de metal listo para montar en un escritorio o rack. |
| Cuenta con una interfaz GUI web. |
| Cuenta con las características de los Switches de capa 2 (Vlan, Qos, IGMP Snooping, etc). |
| Cuenta con Static Mac, Storm Control, etc. |

*Tabla 4. 3. Características del Switch D-Link.*

- **Access Point Ubiquiti Networks Unifi 802.11ac ((UAP-AC-PRO-US)**

*Figura 4.14. Access Point.*
**Fuente: https://www.ui.com/unifi/unifi-ap-ac-pro/**

| Características | |
|---|---|
| **LAN Inalámbrica Estándar** | IEEE 802.11ac |
| **Banda de Frecuencia** | 2.40 GHz, 5 GHz |
| **Numero de Antenas** | 3 |
| **Numero de Antenas Internas** | 3 |
| **Velocidad de Transmisión Inalámbrica** | 1.27 Gbit/s |
| **Tecnología MIMO** | si |
| **Tecnología Ethernet** | Gigabit Ethernet |
| **Cantidad de puertos de red (RJ-45)** | 2 |
| **PoE PD Port** | Si |

*Tabla 4. 4. Características del Access Point.*

- **Teléfono IP Cisco de 4 Líneas y Pantalla LCD (SPA504G)**

Los teléfonos IP de cisco permiten conectarse en la misma de red de la empresa permitiendo que cada empleado de cada departamento tenga una línea personal, también de que ayuda a tener llamadas en espera, hacer marcaciones rápidas entre muchas otras cosas, esto teléfonos IP pueden energizarse por el mismo cable de red que es lo que conocemos como PoE.

*Figura 4.15. Teléfono IP.*
**Fuente: https://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/small-business-spa500-series-ip-phones/data_sheet_c78-548564.html (Cisco)**

Características

- Capacidad de transferir las llamadas.
- Puede hacer conferencia hasta 3 llamadas.
- Llamadas = selectiva y/o agrupadas.
- Capacidad de puesta en espera.
- Bloqueo de llamadas.
- Llamadas automáticas a servicios de asistencia.
- Bloque a llamadas desconocidas.
- Registros de las llamadas.
- Contiene integrada servicios Web para la administración y configuración.
- Dimensiones 214 X 44 X 212 mm.

### 4.5.2 Fundamento de la propuesta

La empresa Gestiones de Aduanas D & M es una empresa que actualmente maneja sus servicios de red e informática con equipos básicos y hogareño haciendo que su red e información se vea expuesta a cualquier tipo de ataque externo y a su vez su información descentralizada se vea perdida en cualquiera momento, también ya que en la empresa no existe una topología definida y tampoco equipos capaces de soportar y manejar software o dispositivos de seguridad nuestro equipo realizo una investigación profunda y validada por diversos libros de renombre, trabajos de tesis ya aprobados y diversas fuentes de alta tecnología como lo es la gran compañía Cisco para poder crear esta propuesta que estamos presentando en este trabajo.

Tomando todo el conocimiento adquirido de las investigaciones optamos por iniciar con el diseño y propuesta de un datacenter exequible para esta institución, tomando en cuenta sus necesidades elegimos un servidor mini torre con suficiente poder de procesamiento para las diversas transferencias de archivos dentro de la red y para posibles y diversas gestiones de usuarios, políticas y permisos. Varios switch de 24 puertos para la distribución de la red desde el servidor hasta cada punto de red de cada computador.

Utilizaremos también teléfonos VO/IP estos teléfonos permiten tener una comunicación entre departamentos y una buena calidad de llamada y permiten la visualización de quien llamada sea dentro o fuera de la empresa, permite trabajar bajo la red de la empresa y también funciona como puente entre el punto de red y el computador para así tener una conexión entre estos dispositivos y optimizar los puntos de red, estos teléfonos permiten tener una pequeña o gran red telefónica dentro de una empresa sin la necesidad de una central telefónica de algún operador telefónico ya que esta central puede crearse a nivel virtual sobre una red bien formada y esta central queda totalmente automatizada.

### 4.5.3 Objetivos de la propuesta

Los objetivos a lograr con esta propuesta es buscar una infraestructura que permita solucionar la problemática en la empresa Gestiones de Aduanas D & M con respecto a la falta de seguridad y una red bien estructurada, con este objetivo en mente buscamos optimizar la eficiencia de toda la organización y a su vez los sub objetivos para llegar a esa meta son:

Brindar capacidades de crecimiento, robustez.

- Aprovechar los recursos viables actuales de la empresa al máximo
- Introducir en la empresa los centros de datos.
- Facilitar la administración de los sistemas y servicios.
- Brindar a la empresa un sistema de seguridad robusto.
- Ofrecer crecimiento futuro sin cambios en la red provista.

### 4.5.4 Ubicación del Data center

*Figura 4.16. Ubicación del Data Center.*
**Fuente: Gestiones de Aduanas D & M**

En esta habitación de aproximadamente 2 metros de largo y 3 metros de ancho con pre instalación de tubería y de aire acondicionado, instalaremos lo propuesto en el apartado 4.5 y 4.6, esta habitación fue elegida por sus pre instalaciones capaces de mantener los equipos en una temperatura amigable y que no reduzca su tiempo de vida o capacidad de operación, a partir de este punto céntrico se distribuirán los cableados a través de las diversas tuberías hasta los diferentes puntos donde están las pc y las impresoras y a su vez los teléfonos y dvr para globalizar los servicios dentro del servidor.

## 4.6 Propuesta de implementación de la nueva red

En el tema anterior, el 4.5 hablamos de la propuesta para un data center, dado que la organización carece de una red óptima para manejar todos los servicios dictado en ese tema, en este apartado diseñaremos bajo las topologías ya mencionadas antes y bajo los conocimientos adquiridos trabajaremos en el desarrollo de una red para la empresa Gestiones de Aduanas D & M.

### 4.6.1 Componentes Necesarios

- **Gabinete NITROTEL 9U 600X650 GLASS DOOR**
  Los gabinetes son rack con una cubierta que protege su interior.

*Figura 4.17. Gabinete.*
**Fuente: http://www.cablecomm.com.do/tienda/index.php/eshop/gabinetes/gabinete-97/nit-gab-9u-600x650-glass-door**

Características
Puerta de vidrio templado, con un giro de 180 grados rotativo Key Lock.

- También cuenta con paneles traseros y laterales desmontables para una rápida instalación de los equipos.
- Cableado de Knock-Outs en la parte superior e inferior.
- El cableado puede ser instalado directamente y más simplemente en la pared con tornillos 6U-21U. con una capacidad de carga estática de 60kg.
- Gabinete fácil de instalar ajustable de 19”, sin paneles en la parte de atrás esto ayuda a una ventilación más eficaz y como también ayuda a una instalación de los quipos más sencilla.

- **Patch Panel LANPRO CAT6 24P**

  Esto son utilizado para poder tener un orden de los cables, es decir podemos identificar rápidamente un punto de red en el gabinete, Ejemplo: existen diferentes tipos de patch panel según su tamaño, pero el más común es el de 24 entradas, cada entrada es un Jack y están enumeradas o normalmente vienen sin enumerar para que el usuario las enumere como guste.

*Figura 4.18. Patch Panel.*
***Fuente: http://www.cablecomm.com.do/tienda/index.php/eshop/componentes/patch-panel-87/lan-patch-panel-cat6-24p***

- **FacePlate de 2 salidas**

  Esto son utilizado para colocar los Jack

*Figura 4.19. FacePlate.*
**Funerte: http://www.cablecomm.com.do/tienda/index.php/eshop/componentes/face-plate-83/or-tc-fp-keystone-2hole-sg-pc**

### 4.6.2 Diseño de la nueva red

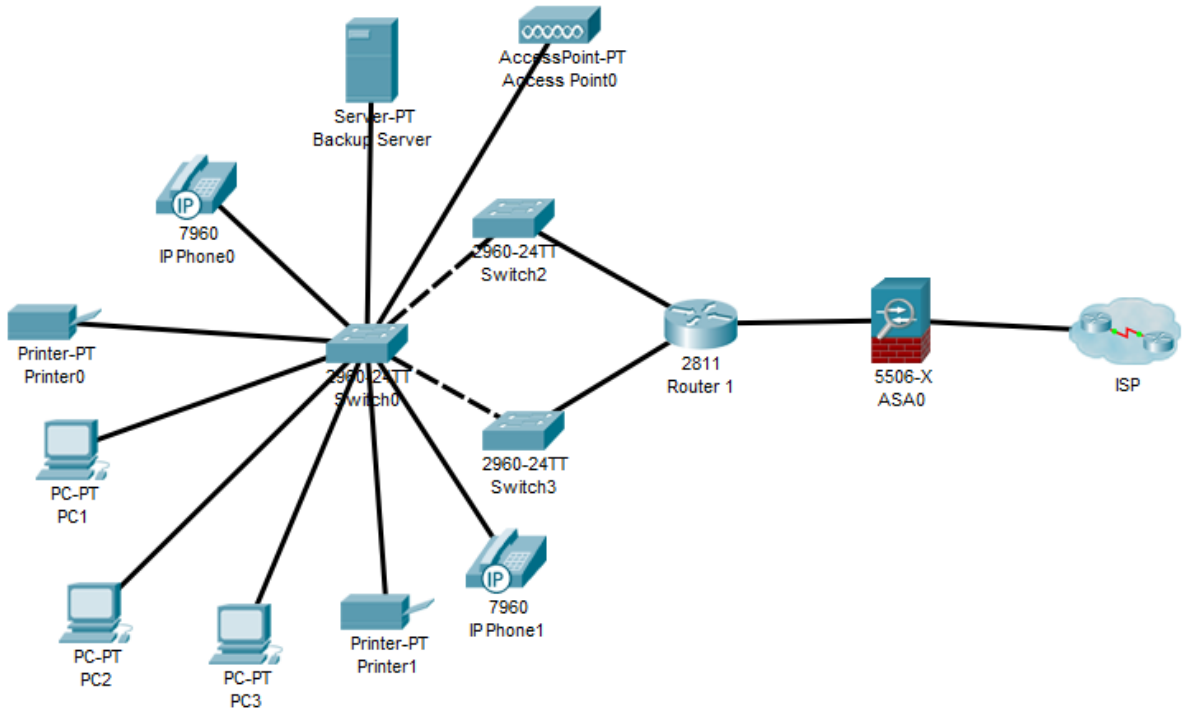



*Figura 4.20. Diagrama de la Nueva Red de Gestiones de Adunas D & M.*

### 4.6.3 Fundamentos de la propuesta

La empresa Gestiones de Aduanas D & M es una empresa que actualmente maneja sus servicios de red e informática con equipos básicos y hogareño haciendo que su red e información se vea expuesta a cualquier tipo de ataque externo y a su vez su información descentralizada se vea perdida en cualquiera momento, también ya que en la empresa no existe una topología definida y tampoco equipos capaces de soportar y manejar software o dispositivos de seguridad nuestro equipo realizo una investigación profunda y validada por diversos libros de renombre, trabajos de tesis ya aprobados y diversas fuentes de alta tecnología como lo es la gran compañía Cisco para poder crear esta propuesta que estamos presentando en este trabajo.

Tomando todo el conocimiento adquirido de las investigaciones optamos por iniciar con el diseño y propuesta de una nueva red con la cual estará acorde a las necesidades de la institución, una red adecuada para el datacenter mencionado y propuesto con anterioridad y una red preparada para un futuro crecimiento en la empresa.

### 4.6.4 Objetivos de la propuesta.

Los objetivos a lograr con esta propuesta es buscar una infraestructura que permita solucionar la problemática en la empresa Gestiones de Aduanas D & M con respecto a la falta de seguridad y una red bien estructurada, con este objetivo en mente buscamos optimizar la eficiencia de toda la organización y a su vez los sub objetivos para llegar a esa meta son:

Brindar capacidades de crecimiento, robustez.

- Aprovechar los recursos viables actuales de la empresa al máximo.
- Introducir en la empresa equipos de vanguardia entorno a las redes.
- Facilitar el flujo de datos y la seguridad de la red.
- Brindar a la empresa un sistema de seguridad robusto.
- Ofrecer crecimiento futuro sin cambios en la red provista.

## 4.7 Propuesta de implementación de la tecnología de huella dactilar

Dado lo hablado en los temas 4.5 y 4.6 que son las bases de esta propuesta ya que gracias a eso nos permite instalar equipos de tecnología biométrica específicamente las de huella dactilar en los diferentes puntoso áreas críticas donde se desea mayor restricción de acceso, con esto en mente buscamos la mejor opción en el mercado ajustándonos en los deseos de la empresa para formar esta propuesta.

### 4.7.1 Equipos necesarios

- **Control de Acceso Biométrico ZKTECO ZK-K214**

*Figura 4.21. ZKTECO ZK-K214.*
**Fuente: https://www.zktecolatinoamerica.com/documentos/tiempo-y-asistencia/standalone/K20/K20.pdf**

ZKTECO ZK-K214 es un dispositivo e innovador terminal biométrico que trabaja sobre una plataforma de red con el protocolo TCP/IP o de manera independiente brindando asistencia los empleados de una organización para el reconocimiento de huellas digitales para el acceso a algún lugar, el K14 es una unidad confiable, precisa y de alta velocidad de verificación,

| Especificaciones | |
|---|---|
| Pantalla | TFT de 2.8 Pulgadas |
| Capacidad de Huellas | 500 |
| Capacidad de Tarjetas | 500 |
| Comunicación | TCP/IP, USB-host |
| Alimentación | 5v DC 2A |
| Temperatura de Operación | 0°c a 45°c |
| Humedad de Operación | 20% - 80% |
| Dimensiones | 185 x 140 x 30 mm |

*Tabla 4. 5. Especificaciones de ZKTECO.*

### 4.7.2 Fundamentos de la propuesta

La empresa Gestiones de Aduanas D & M es una empresa que actualmente maneja sus servicios de red e informática con equipos básicos y hogareño haciendo que su red e información se vea expuesta a cualquier tipo de ataque externo y a su vez su información descentralizada se vea perdida en cualquiera momento, también ya que en la empresa no existe una topología definida y tampoco equipos capaces de soportar y manejar software o dispositivos de seguridad nuestro equipo realizo una investigación profunda y validada por diversos libros de renombre, trabajos de tesis ya aprobados y diversas fuentes de alta tecnología como lo es la gran compañía Cisco para poder crear esta propuesta que estamos presentando en este trabajo.

Tomando todo el conocimiento adquirido de las investigaciones optamos por iniciar con el diseño y propuesta de implementación de un sistema biométrico que permitirá otorgar mayor robustez en la seguridad de data center y las diversas zonas donde se requiera mayor seguridad o restricción de acceso.

### 4.7.3 Objetivos de la propuesta

Los objetivos a lograr con esta propuesta es buscar una infraestructura que permita solucionar la problemática en la empresa Gestiones de Aduanas D & M con respecto a la falta de seguridad y una red bien estructurada, con este objetivo en mente buscamos optimizar la eficiencia de toda la organización y a su vez los sub objetivos para llegar a esa meta son:

Brindar capacidades de crecimiento, robustez.

- Aprovechar los recursos viables actuales de la empresa al máximo.
- Introducir en la empresa equipos de las tecnologías biométricas.
- Aumentar la seguridad en las zonas críticas.
- Brindar a la empresa un sistema de seguridad robusto.
- Ofrecer crecimiento futuro sin cambios en la red provista.

## 4.8 Estudio de Factibilidad

En este apartado hablaremos de la viabilidad de las propuestas, tocando diversas partes por separadas que son el aspecto financiero, económico y social.

**Ámbito financiero**: La empresa cuenta con los recursos económicos necesarios para llevar a cabo los cambios propuestos en los temas anteriores, ya que cada elemento presentado en los temas anteriores fue consultado y analizado con las personas autorizadas dentro de esta, basándonos en sus necesidades y capital establecido hemos seleccionado y desarrollado las características de cada producto mostrado en las anteriores propuestas.

**Ámbito Económico:** Las diferentes soluciones previamente presentadas, analizadas y expuestas a las personas autorizadas dentro de esta organización y luego de plantear y exponer los diferentes puntos de vistas, ejemplos sobre las diferentes soluciones hasta el planteamiento que se optara por poner en marcha.

**Ámbito Social:** Las diferentes tecnologías sumaran a la hora de producción y facilitara el uso de diversas plataformas, servicios y funciones dentro de la red de la empresa, logrando así la comodidad de los empleados y aumentando la eficiencia de la institución.

## 4.9 Técnica Operativa

Como técnica operativa, el usuario administrador solo será dado al encargado de TI, los usuarios tendrán permisos específicos sobre sus ordenadores y solo el administrador tendrá acceso al servidor y los diversos permisos para la asignación de políticas, el acceso a los diversos discos de almacenamiento serán distribuidos por departamento permitiendo asi que los datos no se mesclen y el backup será un proceso rutinario semanal, supervisado por el encargado de TI y realizado fuera de las horas de producción.

Se le asignará un pin a cada empleado en caso de que surge un error con las huellas digitales y cada registro será guardado sin ser borrado en el servidor.

## 4.10 Inversión del Proyecto

| Equipos Informáticos | | | | |
|---|---|---|---|---|
| **Nombre** | **Descripción** | **Unidad** | **Precio (RD)** | **Importe (RD)** |
| DELL POWEREDGE T30 TOWER | XEON E3-1225 V5 3.30GHZ | 1 | 41,265.00 | 41,265.00 |
| Cisco IP Phone SPA504G | VoIP | 3 | 9,150.00 | 27,450.00 |
| Switch D-Link DGS-1100 | 24-Port Gigabit PoE Switch | 3 | 13,000.00 | 39,000.00 |
| Ubiquiti Networks Unifi 802.11ac | Frecuencia de 2.40 GHz, 5 GHz | 1 | 6,350.00 | 6,350.00 |
| Router Ubiquiti edgerouter 4 | 4 puertos RJ45 gigabit | 1 | 8,000.00 | 8,000.00 |
| ZKTECO ZK-K214 | Pantalla TFT LCD a Color de 2.8 Pulgadas | 1 | 10,000.00 | 10,000.00 |
| **Total** | | | | **132,065.00** |

*Tabla 4.6. Inversión en Equipos Informáticos*

| Cableado Estructurado | | | | |
|---|---|---|---|---|
| **Nombre** | **Descripción** | **Unidad** | **Precio (RD)** | **Importe (RD)** |
| Patch Cord | Patch Cord Cat. 6 FTP 7ft | 20 | 192.5.00 | 3,850.00 |
| Jack | | 20 | | |
| FacePlate | FacePlate de 2 salidas | 5 | 50.00 | 250.00 |
| Patch Panel | Landro CAT6 24P | 1 | 3,700.00 | 3,700.00 |
| Rack de Tipo Gabinete | De pare de 9U | 1 | 15,500.00 | 15,500.00 |
| Rj45 | Rj45 Cat.6 | 30 | 30 | 900.00 |
| | | | | |
| **Total** | | | | **24,000.00** |

*Tabla 4. 6. Inversión del Cableado Estructurado*

| Sistemas de Seguridad | | | | |
|---|---|---|---|---|
| **Nombre** | **Descripción** | **Unidad** | **Precio (RD)** | **Importe (RD)** |
| Control de Acceso ZKTECO ZK-K214 | Sistema Biométrico con capacidad de tener Pin y tarjeta de Aproximación | 1 | 10,000.00 | 10,000.00 |
| Extintor Manual | CO2 20 libras | 1 | 6,500.00 | 6,500.00 |
| **Total** | | | | **16,500.00** |

*Tabla 4. 7. Inversión en Sistemas de Seguridad*

| Herramientas | | | | |
|---|---|---|---|---|
| **Nombre** | Descripción | Unidad | Precio (RD) | Importe (RD) |
| **Herramientas de Red** | Kit para poder trabajar en el Data center | 2 | 2,350.00 | 4,700.00 |
| **Plan de Contingencia** | Botiquín de Primeros Auxilios | 1 | 1,200.00 | 1,200.00 |
| **Total** | | | | 5,900.00 |

*Tabla 4. 8. Inversión en Herramientas*.

| Gasto Totales | |
|---|---|
| Descripción | **Importe (RD$)** |
| Equipos Informáticos | 132,065.00 |
| Cableado Estructurado | 24,000.00 |
| Sistemas de Seguridad | 16,500.00 |
| Herramientas | 5,900.00 |
| **Total** | **178,465,00** |

*Tabla 4. 9. Inversión Total*

## 4.11 Cálculo de retorno de inversión.

El cálculo de retorno de inversión (ROI) es una práctica con la cual a partir de una formula simple se busca obtener un porcentaje de manera anual del retorno del capital invertido, de esta manera se verifica lo hablado en el estudio de factibilidad

La fórmula para realizar este proceso es:

ROI = (Beneficio-Inversion/Inversion)*100

El beneficio total que recibe la empresa es de 280,000.00 y ya calculado el costo de la inversión que es 178,465.00 partimos a hacer el cálculo de retorno.

RIO= ((280,000.00-178,465.00)/178,465.00)*100

Rio =56.89% de retorno anual

Lo que quiere decir que tras hecha la inversión calculada anteriormente esta traería un retorno de un 56.89% de los gastos realizados al año.

## 4.12 Cronograma del Proyecto.

GANTT project

| Nombre | Fecha de inicio | Fecha de fin |
|---|---|---|
| Implementacion de la Propuesta | 03/05/19 | 12/07/19 |
| Sistema Electrico | 03/05/19 | 20/05/19 |
| Cableado Estructurado | 21/05/19 | 30/05/19 |
| UPS | 31/05/19 | 06/06/19 |
| Sistema de Control de Acceso | 07/06/19 | 13/06/19 |
| Gabinete (Rack) | 14/06/19 | 20/06/19 |
| Patch Panel | 21/06/19 | 25/06/19 |
| Switch y Router de Comunicacón | 26/06/19 | 03/07/19 |
| Servidor y Teléfonos IP | 04/07/19 | 11/07/19 |
| Finalización | 12/07/19 | 12/07/19 |

*Figura 4.22. Cronograma del Proyecto.*

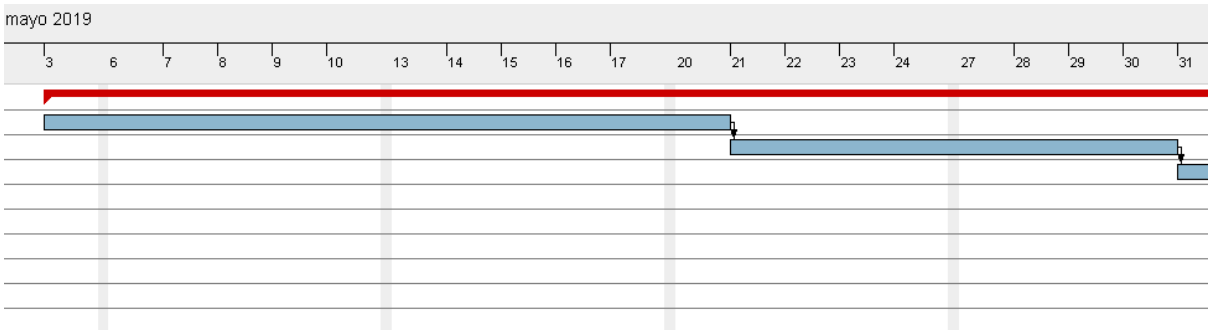



*Figura 4.23. Cronograma del Proyecto Etapa 1.*

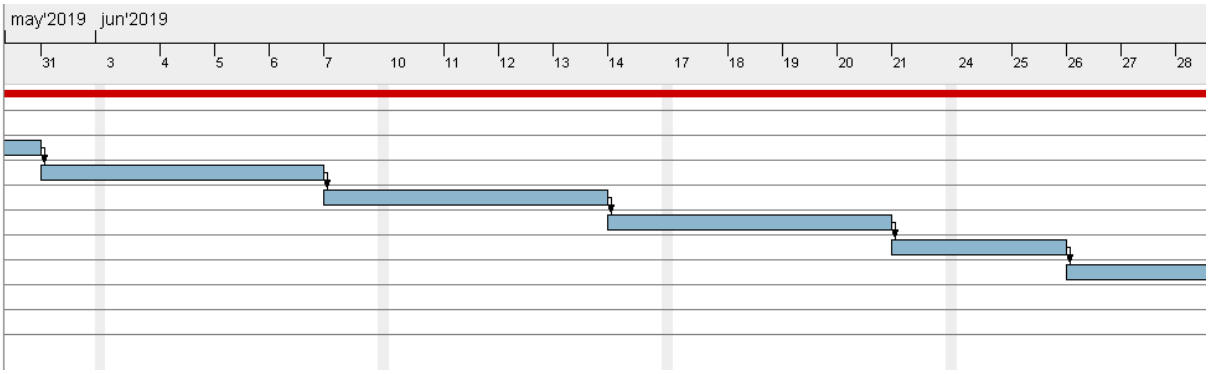



*Figura 4.24. Cronograma del Proyecto Etapa 2.*

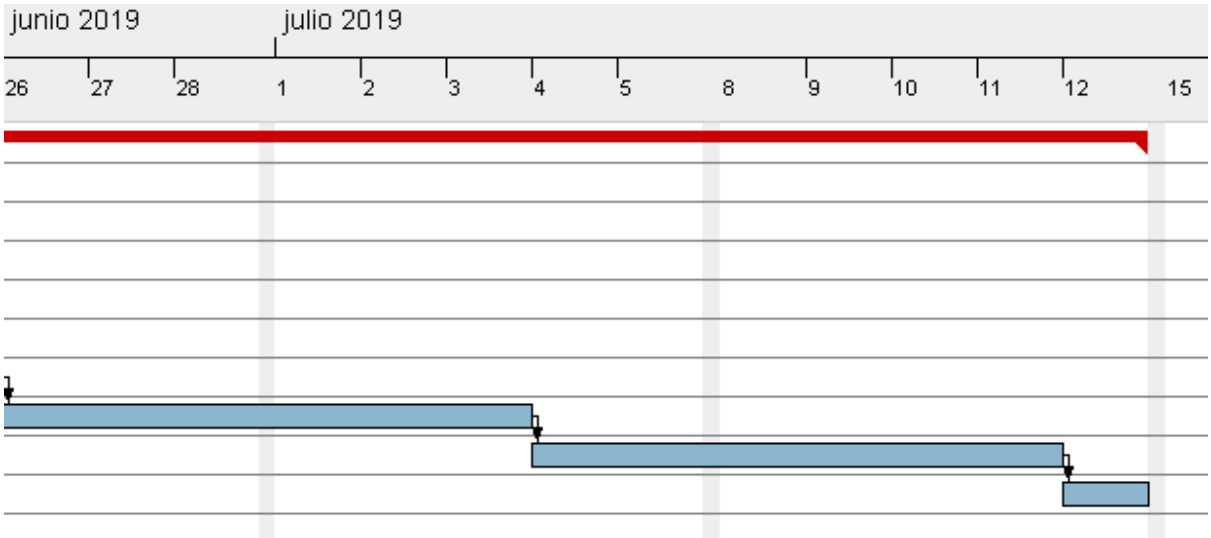



*Figura 4.25. Cronograma del Proyecto Etapa 3.*

## 4.13 Conclusión

En este capítulo hemos hablado de la situación actual tecnológica de la empresa donde presentamos los recursos tecnológicos actuales que posee la empresa a partir de este análisis plantearemos los elementos a mejorar para aumentar la efectividad tecnológica de la empresa, a partir de la situación actual presentamos el diagrama actual de la empresa donde se muestra los elementos de red que posee la empresa en ese momento.

En el análisis FODA establecemos las fortalezas, debilidades, oportunidades y amenazas que posee la empresa, en las propuestas de implementación que son la de un data center, una nueva red de datos y la tecnología de huella dactilar presentaremos los elementos, componentes o equipos que vamos a usar para llevar a cabo eso, los fundamentos y el diseño de la nueva red, los fundamentos, razones por la cual hacemos la propuesta y los objetivos o metas que se alcanzaran al momento en que se ponga en marcha dicha propuesta.

Estudio de factibilidad con el cual se observará las diversas razones por la cual se pondrá en marcha las diferentes propuestas y acciones dentro del proyecto, las diferentes técnicas operativas que prevendrán diversos accidentes dentro de la institución, la inversión de cada equipo , componente o elemento mencionado dentro de las propuestas, el cálculo de retorno de las diversas inversiones en cuestión al valor agregado, tiempo , producción y ganancias y el cronograma del proyecto con el cual se podrá observar en que tiempo y fecha se llevara a cabo cada fase de las propuestas.

# CONCLUSIÓN

## Conclusión

Los bienes y recursos de Tecnología (TI) son elementos esenciales en las empresas, estas permiten que las tareas diarias dentro de la institución se realicen con mayor eficacia, es debido a esto que se enfatiza en el dicño e implementación de centros de datos con la mayor eficiencia tanto en costos como en eficacia lo cual impulsara y eventualmente ayudara en el cumplimiento de las metas de la empresa.

En el transcurso de la realización de este trabajo de grado realizamos diversas observaciones y análisis en la situación actual de la empresa con la cual medimos la condición y calidad de la infraestructura existente y el manejo de estos recursos ya instalados para así iniciar un plan aplicando nuestros conocimientos adquiridos en la institución APEC y mejorar lo ya evaluado.

Actualmente la empresa de gestiones de aduanas D & M no cuenta con infraestructura tecnológica capaz de albergar los diferentes elementos de seguridad capaces de resguardar los datos que se trabajan día a día, los diferentes recursos tecnológicos y carece de dar escalabilidad para satisfacer las futuras demandas dentro de esta institución y los servicios actuales dentro de la institución se ven mermadas por la situación detrimento en la que están los componentes tecnológicos de la empresa.

Estas mejoras en la situación tecnológica se dividirán en diferentes partes, una de estas es la red ya que se trabajará en un sistema de seguridad es necesario trabajar en un diseño de red capaz y suficiente de manejar el flujo de datos y luego el diseño e implementación de data center con esto se centrarían los servicios y sistemas de operación.

Al igual que en otras instituciones Gestiones de Aduanas D & M los centros de datos tendrá una importancia relevante a causa de que esta aumentaría cada uno de los procesos y servicios que se manejan dentro de dicha empresa, esta propuesta no solo se limita a suplir los requerimientos especificados para las tareas del día, sino que también genera un incremento en el valor agregado con los costos operacionales que indica de que la inversión es factible y sumamente considerada.

Se debe de tomar él cuenta que en el momento en el que se implemente esta propuesta se verán resultados al instante, uno de estos es el beneficio de la gestión de los bienes de TI y de obtención de datos en tiempo real ya que gracias a esto se puede analizar dichos datos y gestionar los tiempos de cada proceso , corregir las interferencias y generar escalabilidad lo que permitirá que Gestiones de aduanas D & M introducir nuevos servicios, mejoras en la tecnología usada y mayor estaciones de trabajo.

Entre otras mejoras a notar será una mayor eficiencia en la transferencia de datos y la facilidad de hace respaldo en el momento más oportuno, gracias a la nueva estructura de red mejor gestionada y estandarizada la red disminuirá sus interrupciones.

En conclusión, del grupo con este trabajo esperamos ofrecerle a la institución una opción de mejora factible y viable a sus necesidades, también esperamos que no solo sea de provecho a la institución que trabajamos sino a toda persona con deseo de aprender y de conocer de las diversas tecnologías que se alverga en la informática.

# RECOMENDACIÓN

## Recomendaciones

- Se recomienda la reestructuración de las cámaras de seguridad abarcando el centro de datos.

- Se recomienda guiarse de los estándares de seguridad y de implementación de centro de datos.

- Se recomienda seguir los estándares de ISO 20000 e ITIl.

- Se recomienda realizar un diagrama actualizado de la nueva red.

- Se recomienda contratar técnicos certificados para el mantenimiento del nuevo centro de datos.

- Se recomienda contratar a un Ing. en sistema para la administración general de los servicios de TI.

- Se recomienda establecer un plan contra desastres en caso de la entrada de un elevado voltaje al data center o de inundación entre otros.

- Se recomienda uso de cable par trenzado cat. 6 y de su correcta documentación.

- Se recomienda crear un plan para el mantenimiento y la creación de respaldo del data center y equipos en general.

- Se recomienda la utilización de equipos de respaldo de energía eléctrica para los equipos informáticos.

- Se recomienda utilizar las subredes 192.168.1.0/28 y 192.168.1.16/28 para configuración de los servidores, impresoras y equipos informáticos, por motivos de crecimiento. Se determino que no se requiere desperdiciar un rango de 100 direcciones IP libres para asignación.

# BIBLIOGRAFIA

## Bibliografía


Álvarez, M. G., & Pérez, G. P. P. (2004). Seguridad informática para empresas y particulares. Retrieved from https://ebookcentral.proquest.com/

Arnedo, M. J. (2013). Redes de comunicaciones. Retrieved from https://ebookcentral.proquest.com/

Abad, D. A. (2013). *Redes locales*. Retrieved from https://ebookcentral.proquest.com

Anandamurugan, S., & Nandhini, P. S. (2016). Wireless Networks. Hauppauge, New York: Nova Science Publishers, Inc. Retrieved from http://search.ebscohost.com.ezproxy.unapec.edu.do/login.aspx?direct=true&db=e000xww&AN=1385389&lang=es&site=ehost-live

Baca, U. G. (2016). Introducción a la seguridad informática. Retrieved from https://ebookcentral.proquest.com/

Borrelli, M. (2013). Malware and Computer Security Incidents : Handling Guides. New York: Nova Science Publishers, Inc. Retrieved from http://search.ebscohost.com.ezproxy.unapec.edu.do/login.aspx?direct=true&db=e000xww&AN=650538&lang=es&site=ehost-live

Castaño, R. R. J., & López, F. J. (2013). Redes locales. Retrieved from https://ebookcentral.proquest.com

Costas, S. J. (2014). Seguridad informática. Retrieved from https://ebookcentral.proquest.com

Costas, S. J. (2014). Seguridad y alta disponibilidad. Retrieved from https://ebookcentral.proquest.com/

Díaz, G., Mur, F., & Sancristóbal, E. (2004). Seguridad en las comunicaciones y en la información. Retrieved from https://ebookcentral.proquest.com

Escrivá, G. G., Romero, S. R. M., & Ramada, D. J. (2013). Seguridad informática. Retrieved from https://ebookcentral.proquest.com

Ficarra, F. (2006). Antivirus y seguridad informática : El nuevo. Retrieved from https://ebookcentral.proquest.com/

Giménez, A. J. F. (2014). Seguridad en equipos informáticos (mf0486_3). Retrieved from https://ebookcentral.proquest.com

Gómez, V. Á. (2014). Seguridad en equipos informáticos. Retrieved from https://ebookcentral.proquest.com

Gómez, V. Á. (2014). Auditoría de seguridad informática. Retrieved from https://ebookcentral.proquest.com

Hillar, G. C. (2004). Redes: diseño, actualización y reparación. Retrieved from https://ebookcentral.proquest.com

Harrington, J. L. (2005). Network Security : A Practical Approach. Amsterdam: Morgan Kaufmann. Retrieved from http://search.ebscohost.com.ezproxy.unapec.edu.do/login.aspx?direct=true&db=e000xww&AN=166255&lang=es&site=ehost-live

López, M. Y. (2009). Los virus informáticos: una amenaza para la sociedad. Retrieved from https://ebookcentral.proquest.com

Ling Ngo, D. C., Jin Teoh, A. B., & Hu, J. (2015). Biometric Security. Newcastle upon Tyne, England: Cambridge Scholars Publishing. Retrieved from http://search.ebscohost.com.ezproxy.unapec.edu.do/login.aspx?direct=true&db=e000xww&AN=960122&lang=es&site=ehost-live

McKenna, R., & Contos, B. T. (2007). Physical and Logical Security Convergence: Powered By Enterprise Security Management. Burlington, MA: Syngress. Retrieved from http://search.ebscohost.com.ezproxy.unapec.edu.do/login.aspx?direct=true&db=e000xww&AN=230832&lang=es&site=ehost-live

Pfaller, C., Nipkow, T., & Grumberg, O. (2008). Formal Logical Methods for System Security and Correctness. Amsterdam, Netherlands: IOS Press. Retrieved from http://search.ebscohost.com.ezproxy.unapec.edu.do/login.aspx?direct=true&db=e000xww&AN=244454&lang=es&site=ehost-live

Roa, B. J. F. (2013). Seguridad informática. Retrieved from https://ebookcentral.proquest.com/

Santos, G. M. (2014). *Diseño de redes telemáticas*. Retrieved from https://ebookcentral.proquest.com

Vacca, J. R. (2014). Network and System Security. Amsterdam: Syngress. Retrieved from http://search.ebscohost.com.ezproxy.unapec.edu.do/login.aspx?direct=true&db=e000xww&AN=596635&lang=es&site=ehost-live

Vacca, J. R. (2013). Computer and Information Security Handbook (Vol. 2nd ed). Amsterdam: Morgan Kaufmann. Retrieved from http://search.ebscohost.com.ezproxy.unapec.edu.do/login.aspx?direct=true&db=e000xww&AN=485997&lang=es&site=ehost-live

Vacca, J. R. (2014). Cyber Security and IT Infrastructure Protection. Waltham, MA: Syngress. Retrieved from http://search.ebscohost.com.ezproxy.unapec.edu.do/login.aspx?direct=true&db=e000xww&AN=635568&lang=es&site=ehost-live

Vacca, J. R. (2007). *Biometric Technologies and Verification Systems*. Amsterdam: Butterworth-Heinemann. Retrieved from http://search.ebscohost.com.ezproxy.unapec.edu.do/login.aspx?direct=true&db=e000xww&AN=320816&lang=es&site=ehost-live

Ansejo, E. A. (2006). *Cybertesis*. Obtenido de http://cybertesis.uach.cl/tesis/uach/2006/bmfcia816o/doc/bmfcia816o.pdf

Campo, A. A. (2017). *poligran*. Obtenido de http://repository.poligran.edu.co/bitstream/handle/10823/934/Aguilar%20campo%20FINAL.PDF?sequence=1&isAllowed=y

Escobar, R. F. (2016). Obtenido de http://repository.udistrital.edu.co/bitstream/11349/3430/1/VargasGarciaCristianGerman2016.pdf

Gamez, D. A. (2012). *unilibre*. Obtenido de https://repository.unilibre.edu.co/bitstream/handle/10901/6372/GamezPrietoDanielAlberto%202012.pdf?sequence=1&isAllowed=y

Gutierrez, J. E. (2007). *lasalle*. Obtenido de http://repository.lasalle.edu.co/bitstream/handle/10185/2158/T91.07%20G985e.pdf?sequence=1

Isabel, J. R. (2013). *Orff.uc3m*. Obtenido de https://orff.uc3m.es/bitstream/handle/10016/19246/TFG_GONZALEZ_ISABEL_JOSE_%20RAMON.pdf

Jacomes, V. A. (2010). *espoch*. Obtenido de http://dspace.espoch.edu.ec/bitstream/123456789/376/1/38T00185.pdf

Montaña, D. (2017). *Unilibre*. Obtenido de https://repository.unilibre.edu.co/bitstream/handle/10901/10557/Proyecto%20de%20grado%20Daniel%20Felipe%20Monta%C3%B1a%20Duque.pdf?sequence=1&isAllowed=y

Parra, P. (2014). *usta*. Obtenido de https://repository.usta.edu.co/bitstream/handle/11634/742/Propuesta%20de%20mejoramiento%20del%20desempeno%20de%20la%20red%20de%20Telecomunicacione.pdf?sequence=1&isAllowed=y

Pinilla, D. (2013). *unilibre*. Obtenido de https://repository.unilibre.edu.co/bitstream/handle/10901/8878/Proyecto%20Final%20CISCO%202013.pdf?sequence=1

# GLOSARIO

## Glosario

**Cable Par Trenzado:** en telecomunicaciones, el cable de par trenzado o cable UTP es un tipo de cable que tiene dos conductores eléctricos aislados y entrelazados para anular las interferencias de fuentes externas y diafonía de los cables adyacentes, estos cables constan de 4 pares que en total son 8 hilos de cable de cobre por el cual viaja data o de manera nativa un flujo de cargas eléctricas.

**Cableado Estructurado:** es la forma en la cual un cableado de un edificio o una serie de edificios es llamado, esta permite interconectar equipos activos en diferentes áreas permitiendo la integración de los diferentes servicios que dependen del tendido de cables como datos, telefonía, control, entre otros, estas deben cumplir una serie de normas y estándares antes de ser llamado cableado estructurado.

**Centro de Datos:** es el área o espacio donde se aloja, se mantiene y se gestiona todos los servicios y equipos de TI que utiliza la empresa para facilitar toda la gestión de ella misma, se puede considerar el núcleo de operaciones de todas las TIC que puede contener una empresa.

**Escalabilidad:** es el termino usado para referirse a la capacidad que tiene un centro de datos, equipos o red de reaccionar a los diferentes cambios o mejor dicho aumento de trabajo u usuarios dentro de esta sin perder calidad y eficiencia dentro de esta.

**Estándares:** son normas o reglas que se usan y por la cual se rigen las empresas o centros de servicio para medir o valorar la calidad de servicio que se brinda.

**Ethernet:** Es el estándar que usan todas las computadoras para la conexión a internet en áreas locales, esta permite la escucha de portadora y la detección de colisiones (CSMA/CD).

**Fibra Óptica:** Tipo de cable que usa como materiales filamentos de polímero de cristal que permite en su interior el viaje de haces de luz a alta velocidad, este tipo de cable permite una mayor velocidad de transmisión de datos y mayor distancia de transmisión sin perdidas en ello.

**Información:** es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

**Infraestructura:** conjunto de medios técnicos, servicios e instalaciones necesarios para el desarrollo de una actividad o para que un lugar pueda ser utilizado.

**Interferencia:** señal que altera la recepción de otra.

**IP:** significa Internet Protocol y este protocolo asigna dentro de una red un número de identidad a los diversos dispositivos que ingresan a ella, con este número los diferentes dispositivos dentro de la red son identificables y a la hora de ser enviado un paquete a alguno de estos equipos no se pierde.

**Path Panel:** un panel de conexiones (path panel), también denominado bahía de rutas, es el elemento encargado de recibir todos los cables del cableado estructurado.

**PoE:** es una tecnología que incorpora alimentación eléctrica a una infraestructura LAN estándar. Permite que la alimentación eléctrica se suministre a los dispositivos de red conectados a esta tecnología sobre los mismos cableados de red.

**Rack:** es un soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones. Las medidas para la anchura están normalizadas para que sean compatibles con equipamiento de distintos fabricantes. También son llamados bastidores, cabinas, gabinetes o armarios.

**Red de computadoras:** Es un conjunto de dispositivos sean móviles, computadores, equipos de comunicación y demás interconectados entre si vía inalámbrica o alámbrica por el cual comunican y comparten datos.

**Router:** es un dispositivo de red que permite el enrutamiento de paquetes en una red o diferentes redes.

**Servidor:** Computadora con capacidades superiores a la media con datos, programas u archivos conectada a la red o varias redes, destinada a brindar servicio a las demás computadoras o equipos que soliciten.

**Sistema Informático:** Es un conjunto de equipos, software y hardware interconectado para el procesamiento, almacenamiento y gestión de datos.

**Spyware:** Es un software malicioso que recopila y envía información de algún usuario a otro sin previo aviso o consentimiento.

**Switch:** es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI.

**VoIP:** voz sobre protocolo de internet, es un conjunto de recursos que hacen posible que la señal de voz viaje a través de Internet empleando el protocolo IP.

# ANEXOS

## Anexo 1: Encuesta, preguntas

1-Sexo:

a. M
b. F

2-Edad:

a. 18-25
b. 26-35
c. 36-45
d. Mas de 45

3- ¿Cuántas horas al día usa la computadora en el trabajo?

a. 1h
b. 3h
c. 4h
d. 6h
e. Mas de 6h

4- ¿Con cuanta frecuencia utiliza usted la red de datos o la internet en sus horas laborales?

a. Mucho
b. Poco
c. Casi nunca
d. Nunca

5- ¿Es indispensable la red de datos e internet en Gestiones de Aduanas D & M para completar sus tareas laborales?

a. Si
b. No

6- ¿Con que frecuencia siente usted interrupciones en el servicio de red durante sus horas laborales que impiden realizar sus labores con éxito?

a. Siempre
b. Casi siempre
c. Raras veces
d. Nunca

7- ¿Qué tipo de inconvenientes suele presentarse?

a. Sin acceso a la internet y/o sistema
b. Lentitud en la red
c. Avería del pc
d. Todas las anteriores

8-En una escala del 1 al 5 donde 5 es malo y 1 es excelente, ¿Cómo considera usted que los servicios ofrecidos en la red como el acceso a internet y el acceso al sistema satisfacen sus necesidades conforme a la velocidad y disponibilidad?

1. Excelente
2. Bueno
3. Regular
4. Malo
5. Muy malo

9- ¿Cómo califica usted los servicios tecnológicos?

a. Eficientes
b. Regular
c. Deficiente

10- ¿Le gustaría que se implementara un centro de datos para que de esta manera pueda desempeñar sus funciones de una manera más eficaz?

a. Si
b. Tal vez
c. No

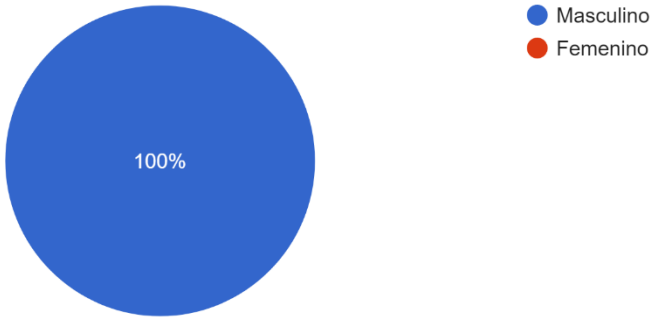
11- ¿Le gustaría que se integre dispositivos de acceso a áreas de solo personal autorizado?

a. Si
b. Tal vez
c. No

## Anexo 2: Representación Graficas de de la Encuesta

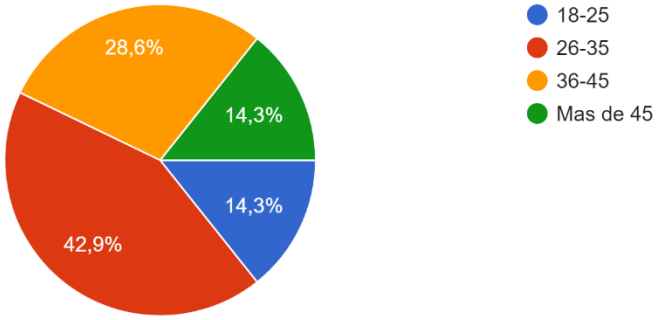
Sexo

7 respuestas



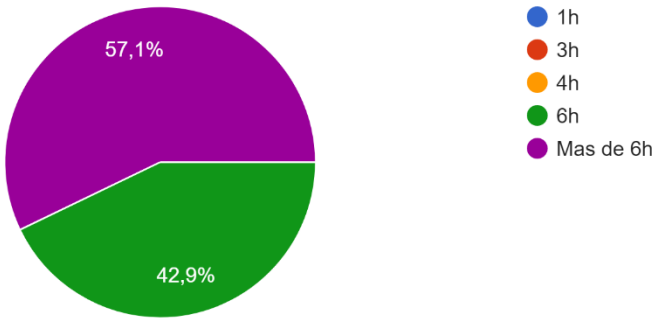

Edad

7 respuestas



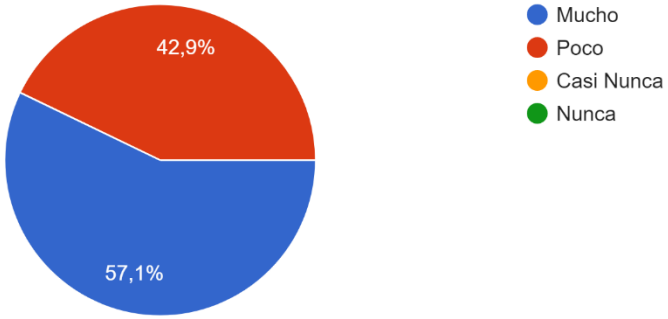

Cuantas horas al dia usa la computadora en el trabajo?

7 respuestas



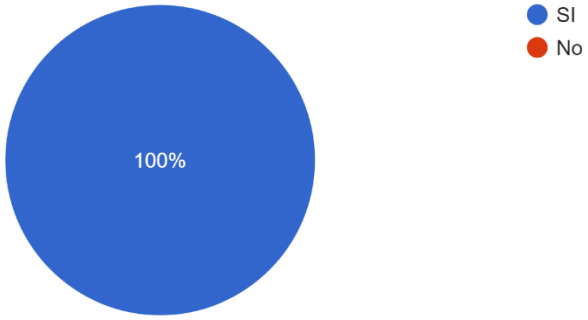
Con cuanta frecuencia utiliza usted la red de datos o la internet en sus horas laborales?

7 respuestas



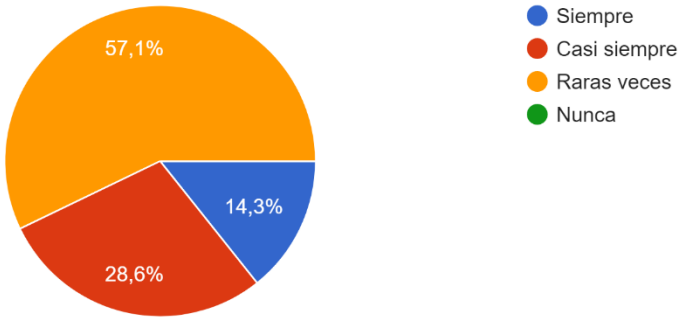

Es indispensable la red de datos e internet en Gestiones de Aduanas D & M para completar sus tareas laborales?

6 respuestas



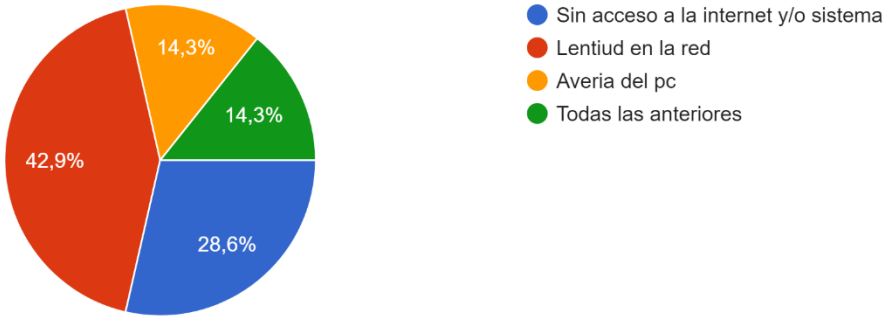

Con que frecuencia siente usted interrupciones en el servicio de red durante sus horas laborales que impiden realizar sus labores con exito?

7 respuestas



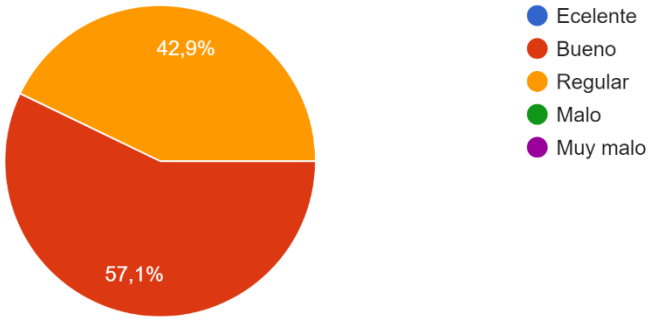
## Que tipo de inconvenientes suele presentarse?

7 respuestas



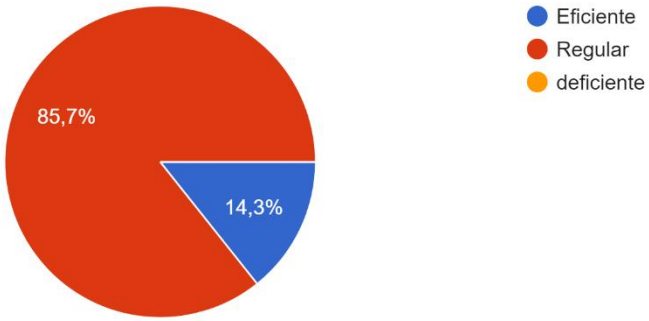

## En una escala del 1 al 5 donde el 5 es malo y e 1 es excelente, Como considera usted que los servicios ofrec...forme a la velocidad y disponibilidad?

7 respuestas



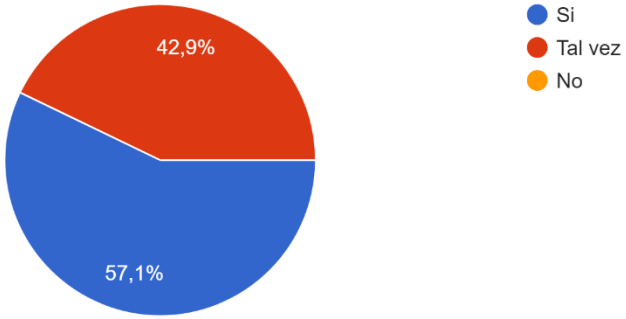

## Como califica usted los servicios tecnologicos?

7 respuestas



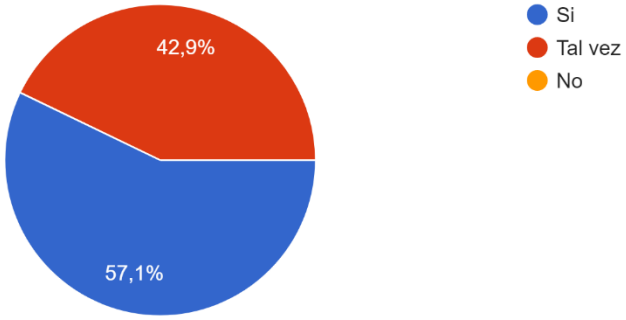
Le gustaria que se implementara un centro de datos para de esta manera pueda desempeñar sus funciones de una manera mas eficaz?

7 respuestas




Le gustaria que se integre dispositivos de acceso a areas de solo personal autorizado?

7 respuestas



## Anexo 3: Aprobación del Anteproyecto

UNAPEC
UNIVERSIDAD APEC

**DECANATO DE INGENIERIAS E INFORMATICA**

Anteproyecto de Tesis

**Asesor**

Ing. Freddy Jiménez

**Tema:**

Análisis y diseño de un sistema de seguridad utilizando la tecnología biométrica (Start Tech) para la empresa Gestiones de aduanas D&M, en la ciudad de Santo Domingo, durante el periodo enero-abril 2019

**Fecha**

26-10-2018

**Sustentantes:**

Carlos Ballast 2014-1886

Jeffrey Martínez 2015-0378

Wilson Hazin 2014-1996

**Santo Domingo, Rep. Dom.**

DEPARTAMENTO DE SOCIALES
PROYECTO DE TRABAJO DE GRADO
APROBADO
FIRMA
FECHA 8-11-18

## Anexo 4: Anteproyecto

**DECANATO DE INGENIERÍAS E INFORMÁTICA**

Anteproyecto de Tesis

**Asesor**

Ing. Freddy Jiménez

**Tema:**

Análisis y diseño de un sistema de seguridad utilizando la tecnología biométrica (Start Tech) para la empresa Gestiones de aduanas D&M, en la ciudad de Santo Domingo, durante el periodo enero-abril 2019

**Fecha**

26-10-2018

**Sustentantes:**

Carlos Ballast 2014-1886

Jeffrey Martínez 2015-0378

Wilson Hazin 2014-1996

**Santo Domingo, Rep. Dom.**

## Título del tema

“Análisis y diseño de un sistema de seguridad utilizando la tecnología biométrica (Start Tech) para la empresa Gestiones de aduanas D&M, en la ciudad de Santo Domingo, durante el periodo enero-abril 2019”

## Introducción

A través de los años la implementación de mecanismos de seguridad se han vuelto un factor imprescindible, y más cuando se trata de proteger la integridad tanto física como de los datos de una organización o empresa.  Por esto es importante una buena elección del mecanismo que de seguridad se va a implementar, ya que si no se contempla las soluciones correctas la organización estará expuesta a que personas mal intencionadas traten de extraer información valiosa o equipos valiosos para la organización.

Debido a que cada humano tiene rasgos únicos con lo cual combinado con la tecnología de hoy en día nos permite tener controles de seguridad más confiables, uno de ellos es la seguridad utilizando huellas dactilares.

Cuando hablamos de estas huellas no estamos refiriendo la biometría en sí, y esta son aquellos rasgos físicos (huellas dactilar, facial, iris, etc.) con lo cual un humano que diferencian de otro.

Debido a lo anterior, la empresa Gestiones de aduanas D&M carece de un mecanismo de seguridad que les garantice que la continua monitorización de su personal o de personas ajenas a dicha empresa. Por esto, en este proyecto veremos como la utilización de mecanismos de seguridad mediante el uso de rasgos biométricos podemos brindar un grado mayor de seguridad a la empresa de forma que no esté expuesta a situaciones que puedan perjudicar el tiempo de producción.

## Justificación

Desde tiempos inmemorables se ha dado la diversas situaciones donde individuos no deseados o personas no autorizadas accedan a lugares u áreas no accesible , en consecuencia se han presentados diversos inconvenientes o problemas, para eso trabajaremos con el diseño de un sistema de seguridad o autentificación biométrica donde solo las personas autorizadas tendrán acceso a las áreas permitidas y donde las áreas más sensibles estarán más segura, esto tendrá como pie a que se deberá trabajar o diseñar una red lo suficientemente robusta para albergar o sustentar el sistema, para este fin es necesario diseñar una infraestructura con los dispositivos capaces de llevar a cabo este cometido .

Se partirá con la tecnología biométrica por el hecho de que nos ofrece una gran variedad de métodos de autenticación biométrica, a su vez permite combinar los medios de autenticación existentes como lo es la combinación entre autentificación biométrica y pin o mediante una tarjeta de acceso, esta solución permite también el máximo nivel de seguridad ya que el material o elemento biométrico a usar es único e irrepetible en cada persona o ser vivo en el planeta, esto nos permite un 100% de efectividad a la hora del control de acceso.

Este trabajo arroja como resultado el diseño o modelado de un sistema con diversas áreas específicas, como es una red LAN con las configuraciones necesarias para albergar el sistema y capacidad suficiente para un buen rendimiento de este, un diseño de seguridad óptimo con sistemas biométricos, cámaras de seguridad y medios de acceso a través de contraseñas, este diseño será de gran provecho ya que permitirá mejorar exponencialmente la seguridad y el rendimiento de la red de la institución.

## Delimitación del tema y Planteamiento del Problema

Se delimitará a la República Dominicana, Santo Domingo, en la empresa Gestiones de aduanas D&M ubicada en el Edificio 1, Manzana 12, Local 105, Km. 10 10/2, Plaza José Contreras, Carret, Sánchez, Santo Domingo, R.D en el periodo enero-abril 2019.

En todas las empresas de servicios públicas o privadas ocurre mucho tráfico de personas ya estas siendo empleados o visitantes; los visitantes se trasladan por toda la institución aunque existe una seguridad interna contratada, pero esta no brinda confiabilidad de que las áreas más críticas de la institución como los data center y cuartos de servidores no sean violados por algún descuido del personal o visitante, por lo que la mejor opción es reforzar esta seguridad con elementos electrónicos y software para tener un sistema más robusto, la utilización de dispositivos de verificación biométrica, cámaras de vigilancia y confirmación por pin o credenciales ante cada entrada de las zonas críticas.

A raíz de estos males sin los medios defensivos correctos, las consecuencias pueden ser bastantes altas como podría ser la pérdida de información valorada en miles de dólares, daños en la infraestructura de la empresa o robo de información vital, también una fuerte vulnerabilidad al hackeo.

Esta situación se debe a la falta de controles de acceso en la institución, los cuales permiten evitar la entrada a personas ajenas. También nos permite tener un control sobres la personas que han intentado acceder sin autorización y poder reaccionar de la mejor manera de evitar que dicho intruso haga más daño.

**Fuente: https://www.tecnoseguro.com/faqs/control-de-acceso/que-es-la-biometria**

Dado lo citado con anterioridad se hace necesario el diseño de un sistema de seguridad asistido por verificación biométrica en toda la institución, cubriendo y creando la barrera que permitirá que solo el personal apto o cualificado pueda acceder a las zonas que se le sea permitida, especificado por el departamento de TI en conjunto con recursos humanos.

Instalaciones de cámaras de vigilancias en zonas estratégicas para crear un ambiente de seguridad tanto para los equipos como para toda persona que entre en la empresa y a su vez trabajar en el diseño de las redes para proteger el sistema de ataques virtuales con fuertes y robustos firewall y seguridad protegiendo así los datos de la empresa, de esta manera la organización obtendrá un grado de seguridad elevado no sólo para su información sino también para el personal y visitantes dentro de ella.

## Formulación del problema

¿Qué impacto causará el diseño y desarrollo sistema de seguridad utilizando la tecnología biométrica (Start Tech) para la empresa Gestiones de aduanas D&M, en la ciudad de Santo Domingo, durante el periodo enero-abril 2019 en la ciudad de santo domingo?

## Sistematización del problema

- ¿Cuáles topologías de red LAN se debería de usar para el correcto funcionamiento o eficiencia del sistema?
- ¿Cuáles tipos de sistemas biométricos se utilizarán?
- ¿Cuáles son las áreas sensibles y críticas donde se emplearán el sistema de seguridad?
- ¿Qué tipos de autenticación se utilizarán en la empresa?
- ¿Qué tipos de depósitos que se utilizaran en la infraestructura de la empresa?

# Objetivos

## Objetivos General

Diseñar un sistema de seguridad utilizando la tecnología biométrica (Start Tech) para la empresa Gestiones de Aduanas D&M durante el periodo enero-abril 2019 en la ciudad de santo domingo.

## Objetivos Específicos

- Definir las redes LAN para el correcto funcionamiento de múltiples sistemas.
- Determinar qué tipo de sistema biométricos se utilizarán.
- Señalar las áreas sensibles y críticas donde se empleará más el sistema de seguridad.
- Diagnosticar qué tipo de autenticación se utilizará en la empresa
- Analizar y señalar los tipos de depósitos que se utilizaran en la infraestructura de la empresa.

## Marco Teórico Referencial

(Escobar, 2016) en su investigación "Diseño e implementación de un prototipo para el control de acceso en la sede de ingeniería de la universidad Distrital Francisco José de Caldas Mediante el uso de Torniquetes controlados por carnet con tecnología NFC y lector biométrico de huella dactilar.", Últimamente se han notado grandes avances en los sistemas de acceso, los cuales se han implementado en prácticamente cada uno de los lugares que cuentan con visitas masivas. Dada la gran demanda de sistemas para el control de acceso, se han incorporado tecnologías mejoradas de comunicación e identificación de datos. En nuestro caso particular se desea incluir el NFC (Near Field Communication) como método de solución, que complementado con un sistema biométrico para identificación de huella crean un sistema confiable para la institución. En conclusión, Los módulos seleccionados para la lectura y escritura de las tarjetas cuentan con un Software que permite asignar a cada usuario el número único de identificación que posee a la tarjeta, con lo cual se logra reconocer al personal y aumentar la seguridad en aproximadamente un 80% a la hora del ingreso.

(Gonzales, 2013) En su investigación "Sistema de identificación biométrica basado en huella dactilar mediante binarización sobre plataformas android", La constante evolución de la tecnología no supone otra cosa que una creciente dependencia por parte de las personas de todo tipo de dispositivos electrónicos, llegando al punto actual en el que se confía a éstos datos vitales como claves de cuentas bancarias, números de identificación personal o contraseñas de acceso a documentos y archivos personales. Es por esto que surge la necesidad de mantener la privacidad del usuario a toda costa y en todo momento mediante técnicas de seguridad. La identificación biométrica por huella dactilar está totalmente presente en nuestra vida cotidiana y ha demostrado ser un método eficaz de protección de datos debido a la prácticamente nula similitud entre las huellas dactilares de todas las personas. En conclusión, Finalmente se puede decir que se ha realizado un proyecto interesante que proporciona una gran funcionalidad a la hora de identificar personas mediante huella dactilar. Actualmente, la implantación de esta aplicación en los dispositivos móviles tendría un uso limitado debido a la carencia del hardware necesario para tomar imágenes latentes de huellas, ya que FprintApp requiere imágenes de huellas digitalizadas para su correcto funcionamiento.

(Asenjo, 2006) En su investigación "Optimización e implementación de la red LAN del instituto de electricidad y electrónica UACH", Hoy en día se habla de Gigabit Ethernet como protocolo de acceso al medio. Sin embargo, no basta solo con aumentar el ancho de banda, también se debe tener en cuenta otros puntos para obtener una red realmente eficiente. En conclusión, Clasificar el diseño de una red en niveles jerárquicos, como la propuesta en este trabajo de tesis, permite seleccionar el hardware apropiado para cada nivel que se traduce en eficiencia y por consiguiente un aumento de rendimiento de la red, por lo tanto, disminuyen los costos y tiempo de implementación.

(Chuqui, 2014) En su investigación "Diseño e implementación de un sistema de control de asistencia de personal, mediante el uso de tecnología biométrica de huella dactilar", Describe las características necesarias, que posee un sistema biométrico para realizar la identificación de la persona como es: unicidad, universalidad, permanecía y cuantificación. Estas características poseen los sistemas biométricos de huella dactilar, iris, retina, geometría de la mano, reconocimiento facial, termo gramas faciales y análisis de ADN. Además, se describe el proceso de autenticación de cada uno de estos sistemas, y se realiza una comparación de estos procesos de autenticación y el hardware que necesita cada sistema. Finalmente, se describe el modelo de arquitectura distribuido de n capas, describiendo el funcionamiento, ventajas y desventajas de esta arquitectura. En conclusión, en comparación con las otras técnicas de reconocimiento biométrico, La técnica de autenticación por huella dactilar tiene mayor penetración en el mercado, debido a que ha sido desarrollada e investigada por largo tiempo, por su bajo costo y su confiabilidad para la identificación del individuo.

(Gamez, 2012) En su investigación "Metodología para el Análisis y Diseño de Redes Fundamentados en ITIL 4, para Empresas de Servicio" Una vez finalizado el diplomado de CISCO se encontró que las técnicas definidas para el diseño y análisis centran su interés en comunicar usuarios, acceder a información, aplicaciones y otros recursos, es por esta razón que se ve la necesidad de crear una metodología de redes basada en servicios para dar un enfoque diferente, que permita realizar el análisis y diseño de una red tomando consideraciones necesarias para el crecimiento continuo y a su vez implementar estrategias de servicio para el control, manejo y atención de incidentes que se presentan en la red. En colusión la evolución en la definición de procesos planteados en las prácticas de ITIL ha permitido dar un enfoque diferente para el análisis y diseño de red, permitiendo así una mejor comunicación entre el área de TI y el usuario final.

(Giraldo, 2017) En su investigación "Estado del arte de la seguridad en sistema biométrico", Los sistemas biométricos control de acceso e identificación que actualmente se encuentran más estables, los cuales serán tratados en el presente proyecto son: los sistemas de reconocimiento e identificación de: huella dactilar, facial, retina, iris y firma, los sistemas de geometría de dedos y mano y sistemas de (Montaña, 2017) autenticación por voz. A través del análisis de las técnicas como son: los sensores, el procesamiento de la información, la captura de datos, la transmisión de datos biométricos, el procesamiento de señal, los algoritmos de decisión y plantillas de almacenamiento de los sistemas biométricos, se realizará un análisis comparativo de especificaciones de aspectos de funcionalidad, Estabilidad, aceptabilidad, facilidad de uso y estándares actuales de control de acceso e identificación. En conclusión, El auge y la necesidad de mejorar la seguridad en los sistemas de control de acceso e identificación, ha generado que hoy en día los sistemas tradicionales sean sustituidos por sistemas automáticos de reconocimiento e identificación biométrica, los cuales permiten responder más eficazmente a un entorno tecnológico creciente.

(Montaña, 2017) En su investigación "Sistema de identificación mediante huella digital para el control de acceso de la universidad libre sede bosque popular simulado en un entorno web", En el mundo actualmente se utiliza la biometría para distintos fines, pero principalmente son de gran ayuda para la seguridad de establecimientos en los que diariamente se presentan altos flujos de entrada y salida de personas. Los sistemas biométricos se dividen en tres diferentes tipos para ser aplicados a un sistema de seguridad, el primero se denomina biometría estática la cual se compone por detectar características físicas de las personas, como los ojos (iris, retina), la cara y las manos (Geometría, huellas dactilares). En colusión un sistema de control de accesos resulta ser una gran herramienta ya que permite controlar el acceso, limitando la entrada a personas de lo ajeno. El uso de un aplicativo web genera grandes ventajas, como la flexibilidad de acceder desde cualquier parte del mundo para hacer control.

(Hidalgo, 2010) En su investigación "Implementación de un sistema de autenticación biométrica basada en huellas digitales" La palabra biometría se deriva de las palabras: bio (vida) y metría (medida). La ciencia biométrica se define como el análisis estadístico de observaciones biológicas. En colusión se ha logrado desarrollar un sistema de autenticación biométrica basado en huellas digitales con la ayuda de un scanner de papel, el software que sirvió para su procesamiento y con la ayuda de un sistema de bases de datos para su implementación.

(Aguilar y Ocampo, 2017) En su investigación "Propuesta de Mejoramiento del Diseño de Red LAN para el primer Comando Aeronáutico (RAC)", En la actualidad hay diferentes aspectos que una entidad, sin importar su naturaleza, debe tener en cuenta para el diseño y posterior puesta en marcha de su red de datos. Temas como la seguridad y el desempeño de la red son de gran importancia para que la información pueda transitar desde el origen a través de la red hasta su destino. Actualmente la información es considerada uno activo más al interior de cualquier organización, la importancia de los datos les da vida a las empresas. En conclusión, la red de datos del Primer Comando Aeronáutico presenta diversas falencias, que para la actualidad podrían hacer una diferencia importante al momento de llevar a buen término diversas operaciones o tareas administrativas propias de la organización, por ello fue de primordial importancia plantear diversas estrategias, que una vez implementadas, van a representar una mejora sustancial en aspectos como seguridad, disponibilidad, eficiencia y tolerancia a fallos.

(Pinilla, 2013) En su investigación "Diseño y propuesta de implementación de Cableado Estructurado para Diselectros LTDA", Con el pasar del tiempo la red WIFI con la que contaba el edificio, empezó a presentar inconvenientes en cuanto a estabilidad, seguridad y velocidad de los servicios; a esto se le suma el aumento de usuarios y la compra de nuevas herramientas para la gestión del negocio, que saturaban diariamente la capacidad de la red inalámbrica actual. En colusión La configuración del protocolo de enrutamiento OSPF hace más fácil la estabilidad de la red y simplifica su administración. El éxito de un proyecto de cableado estructurado en una organización depende de una adecuada planeación de los aspectos físicos que la red requiere, así como de los aspectos lógicos y de seguridad, debido a que permite llevar un seguimiento y control mediante los cronogramas del proyecto.

(Parra, 2014) En su investigación "Propuesta de mejoramiento del desempeño de la red de telecomunicaciones para la empresa Kamilion S.A." Las empresas de telecomunicaciones día tras día requiere de actualizaciones de tipo electrónico y estructural para sus diversas áreas (soporte técnico, administrativo, financiero, gestión humana, entre otras). Por esta razón la necesidad de tener tecnología crece conjuntamente con la habilidad para recolectar, procesar y distribuir información, en búsqueda de mejorar el desempeño de las áreas internas de la compañía. De ahí la importación de contar con las mejores herramientas de conectividad en las empresas de telecomunicaciones, lo cual implica que haya un acondicionamiento de dichas empresas desde sus redes eléctricas hasta sus redes de comunicaciones cumpliendo una serie de normas que garanticen el buen funcionamiento. En conclusión, el diseño de la topología de

red más adecuada para la empresa es la jerárquica, porque permite detectar algún tipo de fallo, el mantenimiento de la misma es más económico y fácil que la topología actual.

(Gutiérrez, 2017) En su investigación "Estudio de Facilidad para el Control de Acceso Biométrico, En una Empresa Empleando Lectores de Huella Digital" Los avances tecnológicos con los que se relaciona la gente hoy en día están sujetos a cambios constantes, por tal razón motivan a las diferentes entidades o personas a estar a la vanguardia. Es importante que una institución esté consciente de este avance, compare en qué nivel tecnológico está ubicada y esté dispuesta a realizar los cambios necesarios. La tecnología brinda herramientas para establecer distintos niveles de seguridad en industrias, contra fenómenos naturales, seguridad informática e identificación y acceso de personal. En Colusión a nivel técnico es viable realizar el proyecto, pues la arquitectura es de fácil desarrollo, lo único para mejorar el sistema es buscar un scanner especializado para poder obtener mayor tráfico en cuanto a usuarios y poder ofrecer el producto a otro tipo de empresas.

## Marco Teórico Conceptual

**Redes:** Una red de Computadores es una colección de dispositivos autónomos interconectados. La conexión entre ellas se puede establecer vía cable de cobre, fibra óptica, microondas o satelitales, de comunicación. Generalmente existen dos tipos de tecnología de transmisión: difusión (Broadcast), y punto a punto (point to point). Las redes por difusión tienen un canal simple de comunicación que es compartido por todas las máquinas en la red. Mensajes cortos, (llamados paquetes en este contexto) enviados por cualquier máquina son recibidos por todos las demás. (Paola Parra, 2014, pág. 33)

**Fuente: http://edaprospo.org/redes-para-el-desarrollo/**

**Topología:** La topología de la red define la estructura de una red. Una parte de la definición física, que es la disposición real de los cables o medios. La otra parte es la topología lógica, que define la forma en que los hosts acceden a los medios para enviar datos. (Esteban Asenjo, 2006, pag. 15)

**ROUTER:** Dispositivo físico o lógico que permite encaminar la conexión entre redes TCP/IP, es el encargado de que los paquetes de información lleguen a su destino. (Deyvid Pinilla, 2013, pag. 11)

**Fuente: https://www.xataka.com/ordenadores/como-saber-si-el-router-de-mi-operadora-es-bueno-o-si-debo-cambiarlo**

**SWITCH:** Dispositivo capaz de enlazar físicamente varios ordenadores de forma activa, enviando los datos exclusivamente al ordenador al que van destinados. (Deyvid Pinilla, 2013, pag. 11)

**Fuente: https://www.magens.cl/Product/switch-cisco-gigabit-50-sin-poe-administrable-slm2048t-na-p-5359**

**LAN: (**Local Área Network) Red de Área Local. Como su nombre indica, es una red de ordenadores de tamaño pequeño/medio localizada en un edificio (como máximo). Se conectan los ordenadores a través de tarjetas de red, y las arquitecturas más conocidas son Ethernet y Token-Ring. (Deyvid Pinilla, 2013, pag. 12)

**Biométrica:** El término biometría proviene de las palabras: BIOS (vida) y metrón (medida). "La biometría es la ciencia que estudia las características únicas que posee una persona" tales como: rostro facial, mano, huella, dactilar, voz, silueta e iris, mediante el uso de métodos estadísticos y algoritmos para conseguir la detección del individuo. Dichos métodos "presentan un pequeño margen de error en la realización de la identificación de la persona." (Luis Chuqui, 2014, pág. 1)

**Huellas dactilares:** Las huellas dactilares son patrones constituidos por las crestas papilares de los dedos de las manos, se localizan en la dermis y se reproducen en la epidermis, generando configuraciones diversas. Se forman en el periodo fetal, a partir del sexto mes, manteniéndose invariables a través de la vida del individuo, a menos que sufran alteraciones debido a accidentes tales como cortes o quemaduras. Las impresiones dactilares son las reproducciones resultantes de las huellas sobre una superficie plana, quedando almacenada en formato

analógico (papel) o digital (digital (archivo), en estas las crestas papilares se aprecian como las líneas más oscuras y los surcos o valles inter-papilares como las líneas más claras. (Victoria Hidalgo, 2010, Pag. 28)

Fuente: https://www.consejosytrucos.co/salud/nuestras-huellas-dactilares-pueden-decirnos-mucho-sobre-nosotros-mismos/

**Ethernet:** es un estándar de redes de computadoras de área local con acceso al medio por contienda CSMA/CD (*"Acceso Múltiple por Detección de Portadora con Detección de Colisiones"*), es una técnica usada en redes Ethernet para mejorar sus prestaciones. El nombre viene del concepto físico de ether. Ethernet define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI. (Ethernet, 2016).

**Autentificación:** La identificación es la capacidad de identificar de forma exclusiva a un usuario de un sistema o una aplicación que se está ejecutando en el sistema. La autenticación es la capacidad de demostrar que un usuario o una aplicación es realmente quién dicha persona o aplicación asegura ser. (Autentificación, 2016).

**Telecomunicaciones:** Abarca todas las formas de comunicación a distancia. La palabra incluye el prefijo griego tele, que significa "distancia" o "lejos". Por lo tanto, la telecomunicación es una técnica que consiste en la transmisión de un mensaje desde un punto hacia otro, usualmente con la característica adicional de ser bidireccional. La telefonía, la radio, la televisión y la transmisión de datos a través de computadoras son parte del sector de las telecomunicaciones.

Las Telecomunicaciones también se pudieran definir como el Conjunto de medios de comunicación a distancia o transmisión de palabras, sonidos, imágenes o datos en forma de impulsos o señales electrónicas o electromagnéticas. (Telecomunicaciones, 2018).

**Infraestructura tecnológica:** es el conjunto de sistemas (ordenadores, equipos de electrónica de red, equipos de almacenamiento, y demás elementos físicos) junto con la manera que se ha elegido para gestionarlos (lo que incluye procesos y herramientas de gestión de los equipos, de medición de su rendimiento, de seguridad ante incidencias y catástrofes además de los sistemas operativos básicos). (La infraestructura tecnológica, 2018).

## Hipótesis

Con el Análisis y diseño de la seguridad para la empresa aduanas D&M permitirá que la seguridad dentro de la empresa mencionada sea más precisa y a su vez los datos de mayor importancia y la infraestructura dentro de esta se mantenga protegidas y aisladas, con esto también habrá una mejora sustancial en el rendimiento de la red de datos dentro de dicha institución gracias al diseño el cual acarrea la seguridad para dicha empresa.

**Diseño metodológico: metodología y técnicas de investigación cuantitativa y/o cualitativa**

**Enfoque de Investigación**

El enfoque de investigación que se implementará será mixto, los cuales son:

- Cuantitativa
- Cualitativa

**Tipo de Estudio:**

El tipo de estudio que vamos a usar es el Descriptivo en el cual ya como se describirá cual topología de red se va a usar o diseñar, también de vamos a describir la función específica de trabajo de los sistemas biométricos en las diversas áreas y de cómo esto van de la mano con una infraestructura cableada dentro de esa infraestructura cableada detallaremos por qué y para que se usan cada elemento que conlleva dicha estructura y su respectivo beneficio en la empresa.

**Método de Investigación**

El método de investigación a usar es el método descriptivo con el cual nos centraremos en el análisis, estudio y posterior descripción a la solución del problema planteado anteriormente, a su vez dentro de dicha descripción detallaremos cada pormenor orientado a esto dejando con claridad cada idea con base científica planteada en el documento final.

Con esa información se resolverá dicho problema planteado y servirá como posible referencia para una posible evolución futura dentro de la institución o referencia para otro posible trabajo o estudio en el área.

**Fuentes y técnicas para recolección de información**

La técnica que utilizaremos la investigación descriptiva, explicativa lo cual estaremos comunicando con nuestro cliente para que este nos facilite información sobre los parámetros necesarios para iniciar el análisis y diseño del sistema en cuestión.

Como métodos secundarios de recolección de información nos auxiliamos de revistas, libros, tesis, documentos y proyectos anteriores que estén validados y sean de temas relacionados al nuestro para así obtener la información necesaria para este trabajo.

**Tratamiento de la información**

Para el tratamiento de información usaremos gráficas, tablas referenciales y el uso de programas para el diseño óptimo de red. Estas herramientas permitirán la presentación clara, organizada y concisa de los datos recolectados al analizar y que permitirán una mejor presentación de nuestro diseño/solución a la problemática planteada.

## Referencias:


Giménez, A. J. F. (2014). Seguridad en equipos informáticos (mf0486_3). Retrieved from https://ebookcentral.proquest.com

Gómez, V. Á. (2014). Seguridad en equipos informáticos. Retrieved from https://ebookcentral.proquest.com

Castaño, R. R. J., & López, F. J. (2013). Redes locales. Retrieved from https://ebookcentral.proquest.com

Hillar, G. C. (2004). Redes: diseño, actualización y reparación. Retrieved from https://ebookcentral.proquest.com

Díaz, G., Mur, F., & Sancristóbal, E. (2004). Seguridad en las comunicaciones y en la información. Retrieved from https://ebookcentral.proquest.com

Escrivá, G. G., Romero, S. R. M., & Ramada, D. J. (2013). Seguridad informática. Retrieved from https://ebookcentral.proquest.com

Santos, G. M. (2014). *Diseño de redes telemáticas*. Retrieved from https://ebookcentral.proquest.com

Ansejo, E. A. (2006). *Cybertesis*. Obtenido de http://cybertesis.uach.cl/tesis/uach/2006/bmfcia816o/doc/bmfcia816o.pdf

Campo, A. A. (2017). *poligran*. Obtenido de http://repository.poligran.edu.co/bitstream/handle/10823/934/Aguilar%20campo%20FINAL.PDF?sequence=1&isAllowed=y

Escobar, R. F. (2016). Obtenido de http://repository.udistrital.edu.co/bitstream/11349/3430/1/VargasGarciaCristianGerman2016.pdf

Gamez, D. A. (2012). *unilibre*. Obtenido de https://repository.unilibre.edu.co/bitstream/handle/10901/6372/GamezPrietoDanielAlberto%202012.pdf?sequence=1&isAllowed=y

Gutierrez, J. E. (2007). *lasalle*. Obtenido de http://repository.lasalle.edu.co/bitstream/handle/10185/2158/T91.07%20G985e.pdf?sequence=1

Isabel, J. R. (2013). *Orff.uc3m*. Obtenido de https://orff.uc3m.es/bitstream/handle/10016/19246/TFG_GONZALEZ_ISABEL_JOSE_%20RAMON.pdf

Jacomes, V. A. (2010). *espoch*. Obtenido de http://dspace.espoch.edu.ec/bitstream/123456789/376/1/38T00185.pdf

Montaña, D. (2017). *Unilibre*. Obtenido de https://repository.unilibre.edu.co/bitstream/handle/10901/10557/Proyecto%20de%20grado%20Daniel%20Felipe%20Monta%C3%B1a%20Duque.pdf?sequence=1&isAllowed=y

Parra, P. (2014). *usta*. Obtenido de https://repository.usta.edu.co/bitstream/handle/11634/742/Propuesta%20de%20mejoramiento%20del%20desempeno%20de%20la%20red%20de%20Telecomunicacione.pdf?sequence=1&isAllowed=y

Pinilla, D. (2013). *unilibre*. Obtenido de https://repository.unilibre.edu.co/bitstream/handle/10901/8878/Proyecto%20Final%20CISCO%202013.pdf?sequence=1

# Esquema preliminar de contenido de Trabajo de Grado

**AGRADECIMIENTOS**

**DEDICATORIAS**

**RESUMEN EJECUTIVO**

**INTRODUCCIÓN**

**ASPECTOS METODOLÓGICOS**

**Capítulo 1. Antecedentes de Gestiones de Aduanas D&M**

1.1. Antecedentes de Gestiones de Aduanas D&M
1.2. Actividad Económica
1.3. Gestión Administrativa
1.4. Misión, Visión, Valores
1.5. Organigrama

**Capítulo 2. Tecnología Biométrica**

2.1. Conceptos de Tecnología Biométrica
2.2. Tipos de Tecnología Biométrica
2.3. Importancia de las Tecnología Biométrica
2.4. Ventajas de las tecnologías Biométrica
2.5. Tecnología Biométrica Huella Dactilar
2.6. Características de dicha tecnología
2.7. Justificación de dicha tecnología en la compañía Gestiones de Aduanas D&M

**Capítulo 3. Conceptos de Redes y Seguridad**

3.1. Conceptos de Redes y Seguridad
3.2. Ventajas de las Redes y Seguridad
3.3. Tipos de Redes y Seguridad
3.4 Características
3.4 Firewall
3.5 Tipos de firewall
3.4. Características del firewall
3.5. Proxy
3.6 Importancia del Proxy
3.7 Políticas de seguridad
3.8 Políticas del sistema
3.9 Topologías de redes
3.10 Importancia de la topología de red
3.6. Seguridad Biométricas

**Capítulo 4. Propuesta de Diseño e Implementación de un Sistema Biométrico para la empresa Gestiones de Adunas D & M**

4.1. Situación Tecnológica De Gestiones de Aduanas D & M
4.2. Diagrama de red actual
4.3. Propuesta de desarrollo e implementación de un Data center
4.4. Fundamento de la propuesta
4.5 Objetivos de la propuesta
4.6. Ubicación del Data center
4.7. Diseño de la nueva red
4.8. Propuesta de implementación de la nueva red
4.9. Fundamentos de la propuesta
4.10 Objetivos de la propuesta.
4.11. Inversión del proyecto
4.12. Cálculo de retorno de inversión.
4.13. Cronograma del Proyecto.

**CONCLUSIÓN**

**RECOMENDACIÓN**

**BIBLIOGRAFÍA**

**GLOSARIO**

**ANEXOS**