TIJUANA, B.C. ABRIL, 2019





**UNIVERSIDAD TECNOLÓGICA DE TIJUANA**

**TÍTULO DEL PROYECTO**

IMPLEMENTACIÓN DE SERVIDORES DE RESPADLO Y DE APLICACIONES

**TRABAJO RECEPCIONAL**

**TÍTULO A OTORGAR**

**INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN**

PRESENTA

EDGAR ANTONIO RODÍGUEZ CHÁVEZ

**UNIVERSIDAD TECNOLÓGICA DE TIJUANA**

**TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN**



**TÍTULO A OTORGAR**

Ing. en Tecnologías de la Información y Comunicación

**TRABAJO RECEPCIONAL**

Implementación de servidor de respaldos y aplicaciones

**Realizada por**

Edgar Antonio Rodríguez Chávez

**En la empresa**

Poder Judicial del estado de Baja California Tecate B.C

**Director de Trabajo Recepcional**

M.E. José Antonio Reyes Pérez

**Tijuana, B.C. abril, 2019**

# DEDICATORIA Y AGRADECIMIENTOS

Agradezco principalmente a mis padres y familiares por el apoyo incondicional que me brindaron en los momentos que lo necesitaba, ya sea económico o psicológico para que pudiera seguir adelante, les doy las gracias por estar pendientes de mí, motivándome a seguir adelante en mi vida personal y profesional.

Agradezco a mis profesores, Maestros y Doctores por brindarme el conocimiento y por el apoyo que nos brindaron aun fuera de su horario, también a mis amigos, compañeros que me ayudaron y me motivaron a seguir adelante en mi vida social y en cada complicación que se presentó en la elaboración de las actividades realizadas en clase.

Dedico esta memoria a mi familia y a Dios por estar conmigo en todo momento, y a la escuela por mostrar profesionalismo y respeto hacia mí.

# RESUMEN

Párrafo que resume en 150 palabras la problemática analizada. Se utilizan enunciados simples e ideas concretas. Evita rodeos e información superflua.

El resumen se redacta en idioma español e idioma inglés y aparece en ese orden en la cuartilla.

**ABSTRACT**

# ÍNDICE

Página

[Dedicatoria y agradecimientos 3](#_Toc503818755)

[Resumen 4](#_Toc503818756)

[índice 5](#_Toc503818757)

[Capítulo I. Introducción 7](#_Toc503818758)

[Capítulo II marco teórico 8](#_Toc503818759)

[Capítulo III. Marco contextual 9](#_Toc503818760)

[Capítulo IV. Estrategia metodológica y resultados 10](#_Toc503818761)

[Capítulo V. Conclusiones y recomendaciones 11](#_Toc503818762)

[Referencias 12](#_Toc503818763)

[Anexos 13](#_Toc503818764)

**ÍNDICE DE TABLAS**

[Tabla 1. Recursos Técnicos 13](#_Toc2940327)

[Tabla 2. Características de servidores 14](#_Toc2940328)

[Tabla 3. Recursos Tecnológicos 15](#_Toc2940329)

[Tabla 4. Comparativa de S.O. Windows Server 34](#_Toc2940330)

[Tabla 5.Comparación de los S.O. Linux 36](#_Toc2940331)

[Tabla 6. Características del Hardware 45](#_Toc2940332)

**ÍNDICE DE ILUSTRACIONES**

[Ilustración 1. Modelo en cascada 17](#_Toc2940320)

[Ilustración 2. Grafica de Gantt 21](https://d.docs.live.net/b820b4acecfb238c/11%20B%20Rodriguez%20Antonio/Memoria%20Ingenieria.docx#_Toc2940321)

[Ilustración 3. Relaciones de la seguridad 24](https://d.docs.live.net/b820b4acecfb238c/11%20B%20Rodriguez%20Antonio/Memoria%20Ingenieria.docx#_Toc2940322)

[Ilustración 4. Ciclo de la administración de la seguridad 26](https://d.docs.live.net/b820b4acecfb238c/11%20B%20Rodriguez%20Antonio/Memoria%20Ingenieria.docx#_Toc2940323)

[Ilustración 5. Modelo relacional simple 31](#_Toc2940324)

[Ilustración 6. Organigrama del departamento de TI 42](#_Toc2940325)

[Ilustración 7.Topología de Redes 46](#_Toc2940326)

# CAPÍTULO I. INTRODUCCIÓN

En la actualidad el mundo se ha adaptado a la tecnología de manera satisfactoria ya que esta ha sido la principal fuente de evolución en las empresas, debido a su cambio constante cada una de ellas se encuentran en búsqueda de las mejores herramientas informáticas siendo estas las que brindan facilidades a los usuarios, estableciendo a quienes utilizan la tecnología en un mejor nivel competitivo en comparación con quienes no la han utilizado, además los tiempos de ejecución en las distintas actividades se reducen y existe un menor margen de error según lo muestran las estadísticas de cada empresa.

Aquellas empresas que se dedican a brindar servicios de forma gratuita no son la excepción al momento de buscar los mejores recursos para su administración, es por esto que el Poder Judicial de Tecate está considerando mejorar sus servicios en cuanto al uso de tecnología teniendo esperando como resultado una automatización de sus procesos, de tal manera que puedan alcanzar sus principales objetivos y ofrecer un mejor servicio a la comunidad.

El presente proyecto se elaborara en el área de sistemas como prácticas profesionales con el fin de mejorar la seguridad y optimización de la información que se llevan a cabo en el juzgado penal tales como: la información de cada persona inculpada, la búsqueda de dicha información en el menor tiempo posible y la optimización de recursos para el sistema (software) que se maneja ya que se va a tener un servidor de respaldos y un servidor de aplicaciones autónomo, obteniendo la información de manera eficaz, lo cual se reflejará en cada audiencia que se maneje.

Para facilitar la lectura y comprensión sobre el desarrollo de este trabajo se ha dividido en capítulos, los cuales a continuación se hacen mención:

En el primer capítulo se contempla la introducción del proyecto que se abordó para la realización de las prácticas profesionales por lo que se da contexto al tema del proyecto que se va a desarrollar.

En el segundo capítulo se ha desarrollado un marco teórico donde se detallarán las bases teorías necesarias para entender las razones del desarrollo de este proyecto.

En el tercer capítulo de ha desarrollado el marco contextual en él se describe el lugar donde se ubica el problema y los antecedentes relacionados con otros trabajos de investigación relacionados con el tema, considerando los métodos y técnicas utilizaron y los resultados que obtuvieron.

En el cuarto capítulo que corresponde al tema estrategias, metodológicas y resultados, se presenta el desarrollo del proyecto. Se describe la manera en que se realizaron las actividades y la solución de la problemática identificada. Se incluye, también, el reporte de los resultados obtenidos.

El quinto y último capítulo y se presentan las conclusiones y recomendaciones obtenidas a lo largo del trabajo en este proyecto.

## **1.1 Enunciado de la problemática**

El Juzgado penal de Tecate conocido como el poder judicial de sector público donde se llevan a cabo las denuncias y demandas ciudadanas, se cuentan con una alta saturación de información que se maneja a diario por lo que es muy indispensable la seguridad de la información de las denuncias presentadas, los casos y todo el procedimiento que se lleva, por lo que es indispensable que no se pierda ningún dato ya que puede afectar a las partes involucradas en dichos tramites.

En el presente juzgado se percataron que no se cuenta con algún procedimiento o método para resguardar la información de una manera segura y sin temor a que llegue a pasar algo ya que es un gran problema el hecho que no hay seguridad en la información y pueda a llegar a perderse dicha información pudiendo llegar afectar a las personas quienes podría generar grandes multas por el Poder Judicial de Baja california. Se han generado alrededor de 200 multas al año que son entre 5mil a 24 mil pesos por multa, por afectación de las personas que están involucradas en esa información perdida, por lo tanto que se requiere de alguna solución para eliminar las multas generadas y mantener seguridad de la información que se maneja.1.2 Objetivos: general y específicos

Basándonos en la problemática expuesta y los requerimientos que se necesitan para poder realizar el proyecto se establecieron objetivos generales y específicos que se quieres llegar a alcanzar.

### 1.2.1 Objetivo general.

Automatizar y agilizar procesos de respaldo de información y mejorar la seguridad de esta, mediante la configuración de la red y la creación de servidores de respaldo y aplicación.

### 1.2.2 Objetivos específicos

* Mejorar el tiempo de respaldo y búsqueda de información
* Administración de la información respaldada
* Agilizar el rendimiento de las aplicaciones
* Aumentar la seguridad de la información a respaldar

## 1.3 Justificación

Muchas empresas, ignoran la seguridad de sus computadoras por completo porque nunca han tenido un problema. Pero eso no significa que no pueda pasar un día. Ya que es un riesgo de que ocurra (y que pierdas una enorme cantidad de datos) lo que debería llevarte a plantearte hacer respaldos de seguridad de tus archivos. Algunas empresas, conscientes que deben realizar respaldos de seguridad, han fallado y eso que al parecer resulta muy fácil hacer copias de seguridad cuando tenemos a nuestra disposición un CD, HD o dispositivo USB. El problema es que este tipo de dispositivos, aparte de ser dispositivos físicos que pueden extraviarse, robarse o dañarse, no tienen las características adecuadas de seguridad.

Generalmente, se realiza las copias de seguridad de manera espontánea o sin programarlas, lo que al final depende de cada empleado, es una fuente de riesgos que te puede dar lugar también a la pérdida de datos. Otro de los motivos para hacer copias de seguridad es porque te ayuda por tanto a ahorrar tiempo y a optimizar el proceso de migración de datos cuando cambias de computadora.

Por lo tanto, este proyecto de implementación de servidor de respaldos y de aplicaciones contribuye a lo antes mencionado, con él se garantizará la seguridad de la información que se maneja en el juzgado y la administración tanto del sistema que utilizan así como la información misma a la hora de requerirlo.

## 1.4 Factibilidad

Después de haber identificado los principales problemas de la empresa, estos serán analizados de manera detallada, para identificar las causas y soluciones al problema presentado. En esta etapa se procede a analizar la factibilidad técnica, económica y operacional para las soluciones encontradas.

### 1.4.1 Factibilidad Técnica

En el juzgado penal consta de varios departamentos entre ellos el área de sistemas la cual tiene el equipo y herramientas necesarias para cumplir con la labor del día al día, dispone de equipo de cómputo, servidores, routers, equipos de audio y de video, cableado entre otras cosas; considerando todo este equipo que se encuentra almacenado no habría necesidad de adquirir algún otro para poder realizar este proyecto, solo se contemplará los costos de los servicios necesarios para la realización del proyecto los cuales serán contemplados en la factibilidad económica.

Se muestra en la siguiente tabla las características tanto de Hardware como de Software que se necesitan para el desarrollo y funcionamiento del sistema:

Tabla 1. Recursos Técnicos

|  |  |  |  |
| --- | --- | --- | --- |
| Recursos técnicos para el desarrollo del proyecto | | | |
| Tipo de Recurso | Nombre del recurso | Descripción | Cantidad |
| RH | Sistemas | N/A | 1 |
| Hardware | Servidores | Dell PowerEdge T30 | 2 |
| Software | Windows Server 2012 | Sistema operativo de Microsoft | 1 |
| Software | Inuvika | Gestión de aplicaciones remotas | 1 |
| Software | Ubuntu | Sistema Operativo de Linux | 1 |
| Hardware | Switch de 24 puertos | Switch Linksys Gigabit Ethernet 24 Puertos | 4 |
| Hardware | Router | Router MikroTik Gbt Ethernet | 2 |

Como parte de los recursos que se necesitan para la realización del proyecto se requieren de dos servidores, los cuales presentan con las siguientes características:

|  |  |
| --- | --- |
| Características de Servidores | |
| Características | Descripción |
| Marca | Servidor Dell |
| Modelo | PowerEdge T30 |
| Procesador | Intel Xeon de 3.2 GHz Octa-Core |
| Memoria RAM | 12 GB Ddr3 |
| Disco duro | 2 T |
| Disco duro | 512GB SSD |
| Tarjeta de Video | Nvdia 1060 Ti PCiExpress |
| Tarjeta Madre | ASUS ATX PRIME B250M-A, |
| Fuente de poder | Corsair CX650M de 650 Watts |

Tabla 2. Características de servidores

Como se ha visto la empresa cuenta con la tecnología necesaria para llevar a cabo la implementación de este proyecto por lo tanto podemos decir que este es técnicamente viable.

### 1.4.2 Factibilidad Económica

En el estudio de la factibilidad económica, se determinó el presupuesto de costos de los recursos técnicos, humanos y materiales tanto para el desarrollo como para la implementación del Proyecto. Además, ayudará a realizar el análisis costo-beneficio de del proyecto, el mismo que permitirá determinar si es factible.

A continuación, se describe los costos de los recursos necesarios para el desarrollo del sistema:

Tabla 3. Recursos Tecnológicos

|  |  |  |  |
| --- | --- | --- | --- |
| Recursos Tecnológicos | | | |
| Cantidad | Descripción | Costo | Costo Total |
| 1 | Licencia de Windows Server | $5799.99 | $5,799.99 |
| 1 | Servidor Virtual Azure | $325,422.78 | $325,422.78 |
| 1 | Inuvika 18.5 | $559.89 | $559.89 |
|  | | Total | $331,782.66 |

\*Costos por año

Si tomamos en cuenta que las multas originadas anualmente por perdida de información corresponden a $2, 900,000.00 pesos y la inversión de este proyecto que es de $331,782.66 pesos equivale a menos de una octava parte de lo que equivale al total de las multas anuales. Con estos beneficios especificados, se ha estimado que el total de ahorro que la empresa obtendrá por el funcionamiento del proyecto que sería aproximadamente de $2, 568,217.34 pesos al año.

### 1.4.3 Factibilidad Operacional

### La factibilidad operativa se midió evaluando el impacto que tendrá el proyecto, en la empresa y en el personal que laboran en ella (impacto sobre las impresiones de cada uno del personal). Esta determinación se observó por medio de entrevistas y recomendaciones con el personal del juzgado penal.

### El sistema propuesto inducirá cambios importantes en los procedimientos de la empresa, aunque no afectará al personal actual, sino más bien la forma en que se realizan las cosas. Una vez terminado el proyecto, se procederá a su implementación y utilización, donde el personal para poder hacer uso el sistema será por otro medio al habitual, por lo que se les dará una breve capacitación, de la nueva forma de acceso al sistema ya que lo demás es el mismo procedimiento, a pesar del pequeño cambio de utilización del sistema existe apoyo muy notable por parte de los usuarios, pues han participado en la planificación del proyecto.

### Se ha analizado el impacto que tendrá el sistema sobre todas las distintas áreas, y es favorable que se mejorará el control y seguridad de la documentación y se agilizará la obtención de información.

### La capacitación que es para todo el personal tiene una duración de 20 minutos, para dar la introducción de lo que es y cómo utilizarla, para la familiarización con el sistema y para la confianza en el uso de este. Los beneficios se verán a corto plazo, pues se optimizarán los tiempos de realización de ciertas actividades con esto se mejorará la productividad del personal.

### 1.5 Presentación de la metodología seguida

La metodología es fundamental en la utilización de un proyecto ya que es el conjunto de procedimientos y gestión del proyecto a desarrollar, funciona como base y guía de cómo se va a realizar el proyecto y de qué manera se desarrolló, para tener un control de este.

La metodología por utilizar para la gestión de este proyecto es la llamada modelo en cascada donde es un proceso secuencial, en el que el desarrollo del sistema se ensambla de un conjunto de etapas que se ejecutan una tras otra. Se utiliza este modelo por las posiciones que ocupan las diferentes fases que componen el proyecto, colocadas una encima de la otra y siguiendo un flujo de ejecución de arriba hacia abajo, como su nombre lo dice en cascada.

Para esta metodología se han establecido pasos o fases que se llevaran de manera consecutiva, las cuales podemos observar en la siguiente ilustración:

Ilustración 1. Modelo en cascada

Como primera fase se implementan los requisitos del proyecto: que se necesita, con que se cuenta y de qué manera se obtendrá ya que es fundamental para poder comenzar el proyecto.

La segunda fase es el diseño de cómo va la estructurar el proyecto tomando en cuenta las alternativas que se tienen sus ventajas y desventajas.

La tercera fase es la implementación, donde todo lo analizado anteriormente se llevará a la ejecución teniendo los recursos y el diseño ya establecido.

La cuarta fase es la verificación como su propio nombre lo indica, una vez que termina la fase de implementación se verifica que todo lo que compone el proyecto se esté ejecutando de una forma satisfactoria.

La última fase corresponde a la de mantenimiento, donde todas las funcionalidades del proyecto estén estables, es asegurarse que el proyecto trabaje de manera óptima contando con los diferentes tipos de mantenimientos ya se preventivo o correctivo planeando que tanto tiempo se debe establecer dichos mantenimientos.

Por lo que esta metodología se adapta a las necesidades del proyecto para una buena funcionalidad y un buen alcance del proyecto.

## 1.6 Plan de trabajo y cronograma de actividades

El plan de trabajo y el cronograma de actividades es algo fundamental dentro de la realización del proyecto para poder saber cómo se llevará a cabo el plan de trabajo así como las actividades que se realizaran para poder tener un control de los tiempos que se manejaran.

### 1.6.1 Plan de Trabajo

El proyecto busca encontrar resultados que permitan mejorar la seguridad de la información y la optimización de la utilización del sistema por lo que por medio de una gráfica de Gantt se realizó el plan de trabajo para la elaboración del proyecto que se describirán a continuación:

La primera actividad a realizar es el análisis y diseño de la estructura de la red, antes de realizar cualquier cosa se necesita realizar un análisis de lo que se cuenta, de lo que se ocupa y de lo que se debe hacer utilizando las herramientas correspondientes para poder plasmar de una mejor manera el análisis y diseño a desarrollar para poder tener definido el alcance, el método a utilizar , las técnicas e instrumentos utilizados en la recolección de la información del análisis y diseño de la estructura de la red.

La segunda actividad es el cableado de la estructura de la red tomando en cuenta la obtención de los recursos y teniendo el plan que se desarrolló en el análisis y diseño de la red para poder realizar esta actividad, para cumplir con el objetivo planteado y continuación del proyecto.

La tercera actividad por desarrollar es la configuración de la red por medio de vlans, teniendo los requerimientos necesarios para la implementación de la configuración a la red.

La cuarta actividad por realizar es el Análisis de los requerimientos del servidor de respaldos tomando en cuenta las herramientas y de las especificaciones de los servidores obtenidos para la realización del proyecto.

La quinta consiste en la creación de servidor de respaldos (Windows server) se realiza después de tener el análisis y los requerimientos para la elaboración de la actividad.

La sexta actividad corresponde al análisis de los requerimientos del servidor de aplicaciones, viendo que servicios necesitamos para contemplarlo en la creación del servidor, así como el personal que tendrá acceso a él.

La séptima actividad involucra la creación del servidor de aplicaciones (Linux) se realiza después de tener el análisis y los requerimientos para la elaboración de esta actividad.

La octava actividad para realizar es la de configuración y cableado de equipo de cómputo, donde teniendo todas las partes fundamentales completas se integran para poder obtener el sistema completo y operando de una manera eficiente

La última actividad para es la documentación del proyecto donde se describe lo que se realizó, y elaborando un reporte de todo el proceso que se llevó a cabo para la realización del proyecto.

Utilizando la metodología antes mencionada se podrá obtener los resultados esperados de la elaboración del proyecto.

### 1.6.2 Cronograma de actividades

Para la realización del proyecto se requiere tener un orden para las actividades que se realizaran, para esto se ha utilizado la herramienta de gestión gráfica de Gantt que consiste en un software visual para la planificación y programación de actividades o tareas sobre una línea del tiempo, que permite establecer tiempos como la duración y comienzo de cada actividad que ayudaran para que se pueda llevar un control y guía para el complimiento del proyecto en tiempo y en forma.

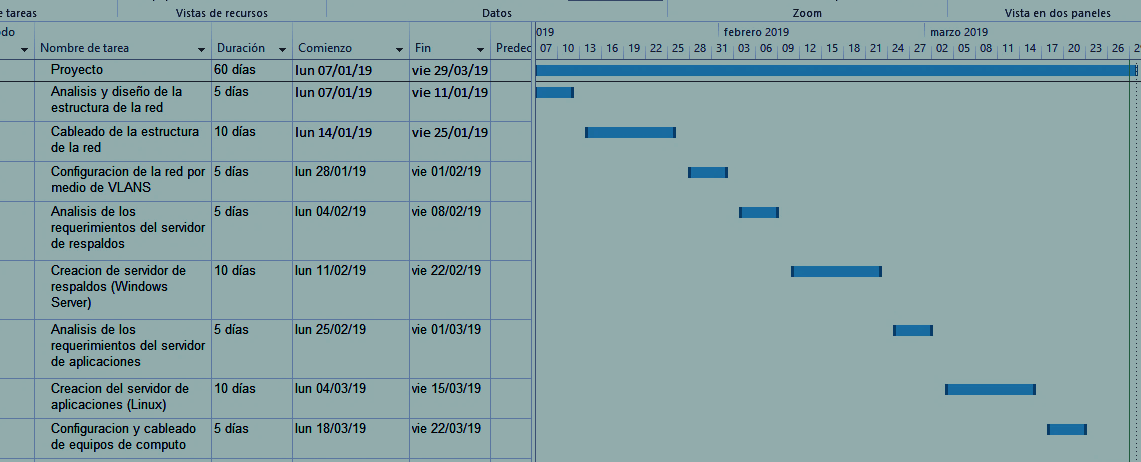
En la siguiente ilustración se muestra la planificación de las actividades o tareas a realizar para la realización del proyecto:

Ilustración 2. Grafica de Gantt

# CAPÍTULO II MARCO TEÓRICO

En esta sección se hace una revisión de los conceptos básicos que son relevantes para la realización de este proyecto. Se detallarán las teorías necesarias para entender las razones del desarrollo de este proyecto.

## 2.1 Seguridad informática

La seguridad informática es un conjunto de protecciones (reglas, herramientas, recomendaciones, etc.…) para proteger la información, dispositivos y los procesos que forman parte de una red de datos (informática, 2019).

Para poder brindar la seguridad optima es necesario implementar herramientas y mecanismos de seguridad que ayuden a alcanzar el objetivo que es la seguridad de la información. Se tienen que elegir las mejores herramientas y métodos para cumplir con el objetivo de proporcionar máxima seguridad a la infraestructura de IT de la organización que se requiere. Es necesario tener una serie de pasos que ayuden a contestar las siguientes preguntas: ¿Qué es lo que se quiere proteger?, ¿Qué podría pasar?, ¿Qué tan frecuentemente podría pasar? ¿De quiénes se van a proteger?, ¿Cómo se van a proteger?

Se deben seguir una serie de pasos que lleven a obtener las respuestas a las preguntas antes mencionadas.

* ¿Qué es lo que se quiere proteger?

Se identificarán los recursos a los que se requieren proteger y a lo que es denominado entorno de seguridad. En el entorno de seguridad es necesario identificar los diferentes tipos de riesgos. Este proceso tiene que ser desarrollado formalmente por un grupo de todas las áreas de la organización, con el objeto de tener una visión más amplia sobre el valor de lo que se requiere protección y las consecuencias que pueden llegar de que se vea comprometida la confidencialidad, integridad o disponibilidad. Para obtener está información es necesario contestar las siguientes preguntas:

* ¿Qué podría pasar?

Esta pregunta tiene como objeto identificar los bienes existentes para la compañía (software, hardware, datos, personas, etc…) y los eventos amenazantes.

* ¿Qué tan frecuentemente podría pasar?

Esta pregunta tiene como objeto cuantificar la frecuencia de ocurrencia potencial de los eventos amenazantes.

Con las respuestas anteriores se identifican claramente los riesgos sensibles para la empresa y las posibles consecuencias que pueden ser comprometidos para la seguridad, se podrá tener un nivel de conocimiento sobre los bienes con que se cuenta y lo que representan para la organización, así como el conocer cuál sería el impacto en caso de que sufran algún incidente.

* ¿De quiénes se van a proteger?

Al resolver esta pregunta se identifican las amenazas, los riesgos y las vulnerabilidades a las que se encuentra expuesto el entorno identificado.

En una organización se debe de garantizar la seguridad de la información que se maneja, tomando en cuenta quienes son las personas autorizadas para manejar la misma, así como los recursos que necesita cada uno de los empleados para realizar las tareas diarias como capacitación.

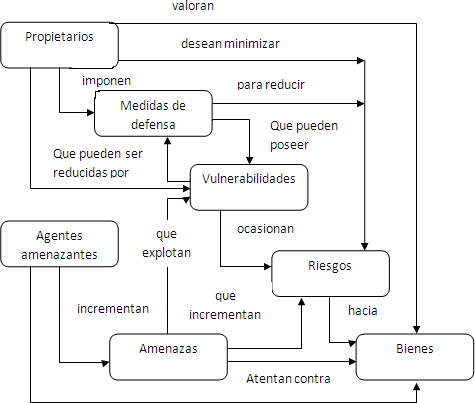
La seguridad se enfoca en dar protección a los bienes que están expuestos a riesgos considerados como una potencial amenaza. Se debe prestar mucha atención a las actividades malignas o a las actividades humanas, donde en la siguiente ilustración se muestra una relación de la seguridad de la información.

Ilustración 3. Relaciones de la seguridad

**Fuente: (Álvarez Marañón & Pérez García, 2004)**

Los responsables de sus áreas o departamentos de la empresa son quienes estiman y valoran los bienes, que desean minimizar los riesgos informáticos implementando medidas de seguridad para reducir las vulnerabilidades informáticas.

Los responsables de los bienes con ayuda del departamento de seguridad informática son encargados de analizar todas las amenazas que podrían presentarse para determinar cuáles son los que aplican en la empresa. Los resultados de este análisis se conocen como riesgos que ayudan en la selección de las medidas de seguridad para reducir éstos a un nivel considerable.

Las medidas de seguridad deben seleccionarse e implementarse para reducir puntos débiles y cumplir las políticas de seguridad de los encargados de la empresa. Después de la creación de las medidas de defensa es posible que aún queden puntos vulnerables, de manera que éstos pueden ser utilizados por personal amenazantes que representan un nivel mínimo de riesgo para los bienes; sin embargo, es necesario que la empresa implemente política o restricciones adicionales para minimizar los riesgos.

* ¿Cómo se van a proteger?

Esto lleva a determinar las políticas de seguridad informática para el entorno analizado, ya que las normas ayudan a debilitar las amenazas y vulnerabilidades identificadas a fin de proteger su entorno.

El plantear y dar analizar a estas preguntas será lo que dará la oportunidad de seleccionar de manera formal y segura las herramientas de seguridad necesarias para proteger la información en riesgo.

**2.1.1 Administración de la seguridad.**

Para que un esquema de seguridad quede completo, es necesario que se lleve a cabo la administración de la seguridad, para realizar esto, se recomienda contar con un Departamento de Seguridad en Cómputo, el cual está conformado por personal especializado en seguridad informática; así como la del equipo de trabajo que se encargará de administrar la seguridad informática.

A continuación, se mostrará una ilustración del ciclo de administración de la seguridad ideal para una empresa.

Ilustración 4. Ciclo de la administración de la seguridad

La administración de la seguridad se refiere a gestionar y dirigir todas las acciones que se lleven a cabo con el fin de proteger la información (Toro, P. 2019). La administración consta de cuatro etapas que son:

Etapa 1: Planeación. Se debe llevar a cabo una revisión de las políticas de seguridad, por lo que hay que revisar el esquema de seguridad desarrollado para identificar si se requiere actualizar, remover y modificar las que ya existe.

Etapa 2: Protección. Después de revisar y actualizar las políticas de seguridad del entorno y hacer uso de nuevas tecnologías, ya que estas nuevas formas de protección elevan el nivel de seguridad del entorno.

Etapa 3: Detección. Es necesario contar con sistemas que permitan realizar actividades de monitoreo de forma continua en toda la información, áreas y sistemas que sean considerados dentro de las políticas; y así mismo, generar reportes que permitan detectar alguna falla para tomar las medidas adecuadas.

Etapa 4: Reacción. En ésta etapa se toman las decisiones que toman las acciones para proteger los bienes informáticos de la empresa u organización, esto con base en la información obtenida de la etapa anterior, se realiza de manera continua un análisis para tomar una decisión de cambio de políticas o métodos.

A continuación, se explicará lo que es el análisis de riesgos, las metodologías que se tienen para realizar el análisis de riesgos y los tipos esenciales del análisis de riesgos para más adelante entender los resultados obtenidos.

## 2.2 Políticas de Seguridad.

Toda organización, tiene la necesidad y por qué no, la obligación de definir políticas de seguridad. La necesidad surge porque existe un fallo en la seguridad de la información, la cual pone en riesgo a la misma y a la seguridad a la hora de proteger los datos, que implican significantes sumos de dinero y tiempo.

El estándar ISO 17799 contiene diez secciones de seguridad. Cada sección cubre un asunto o área, las cuales son utilizadas como base para la determinación de los riesgos de seguridad y la aplicación de controles de seguridad para el manejo de la seguridad de la información. La que se menciona a continuación, es la que corresponde a las políticas de seguridad (Iso-actual.com, 2019).

Las políticas de seguridad son un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad de la información dentro de la misma. Las políticas definen la seguridad de la información en el sistema central de la organización, por lo tanto, un sistema central es seguro si cumple con las políticas de seguridad impuestas para esa organización. Las políticas de seguridad especifica qué propiedades de seguridad el sistema debe de proveer.

# 2.3 Análisis de riesgos.

# El análisis de riesgo es el estudio de las causas de las posibles amenazas y probables eventos no deseados y los daños y consecuencias que éstas puedan producir, este tipo de análisis es ampliamente utilizado como herramienta de gestión en estudios financieros y de seguridad para identificar riesgos y otras para evaluar riesgos.

Los resultados obtenidos del análisis, van a permitir aplicar alguno de los métodos para el tratamiento de los riesgos, que involucra identificar el conjunto de opciones que existen para tratar los riesgos, evaluarlas, preparar planes para este tratamiento y ejecutarlos.

Se definen algunos términos de suma importancia para el análisis de riesgos:

* **Bienes.** Es todo aquello que tiene valor para la organización y necesita protección.
* **Riesgo.** Todo aquello que representa la posibilidad de sufrir algún daño o pérdida.
* **Análisis de riesgos.** Uso sistemático de información disponible para identificar las fuentes y para estimar la frecuencia en la que determinados eventos no deseados pueden ocurrir y la magnitud de sus consecuencias.
* **Manejo de riesgo.** Proceso de identificación, control y minimización o eliminación de riesgos de seguridad – que pueden afectar a los sistemas de información – por un costo aceptable.
* **Evaluación del riesgo.** Comparación de los resultados de un análisis de riesgo con los criterios, estándares u otros criterios de decisión.
* **Impacto.** Pérdidas como resultado de la actividad de una amenaza (destrucción, modificación, revelación, denegación de servicios). El impacto generalmente se expresa en las áreas de impacto mencionadas.
* **Amenaza.** Todo aquello que puede, intenta o pretende destruir o dañar algo.
* **Vulnerabilidad.** Son las debilidades pertenecientes a algo.
* **Ataque.** La realización de una amenaza. Cuando una amenaza explota una vulnerabilidad y se logra el objetivo.
* **Riesgo residual.** Nivel de riesgo que queda después de la consideración de todas las medidas necesarias.
* **Control.** Protocolos y mecanismos de protección que permiten el cumplimiento de las políticas de seguridad de la organización.

**2.2.1 Tipos de Análisis de Riesgos.**

Existen dos tipos de análisis de riesgos:

**1. Cuantitativo.**

Todos sus recursos y controles se identifican, y se evalúan en términos monetarios. Todas las amenazas potenciales se identifican y se estima la frecuencia de su ocurrencia, estas amenazas se comparan con las vulnerabilidades potenciales del sistema de tal forma que se identifiquen las áreas que son sensibles. Esta metodología hace uso del término Expectativa de Pérdida Anual (ALE) o también llamado Costo Anual Estimado (EAC). La forma de calcularlo para un evento en concreto se realiza mediante la multiplicación de la ocurrencia de la amenaza por el valor del activo o clasificación del daño (Es.wikipedia.org, 2019).

De esta forma se puede determinar si los controles existentes son adecuados o se requiere la implementación de otros, esto se observa cuando el producto obtenido tras multiplicar el valor del activo por la frecuencia de ocurrencia de la amenaza en un periodo de tiempo determinado por la duración del control es menos que el costo de dicho control.

**2. Cualitativo.**

Teóricamente es posible situar acontecimientos en el orden del riesgo ALE y posteriormente tomar las decisiones más convenientes. Los problemas de este tipo de análisis de riesgos se asocian generalmente a la falta de fiabilidad (probabilidad del buen funcionamiento de una cosa) y exactitud de los datos, debido a que es difícil lograr una figura representativa de la pérdida o daño que se tiene como resultado de las brechas de seguridad. (Es.wikipedia.org, 2019).

En esta otra, en lugar de establecer los valores exactos se asignan niveles de alto, bajo y medio que representan la frecuencia de ocurrencia y el valor de los bienes. Ambos análisis de riesgos hacen uso de tres elementos interrelacionados:

**Amenazas**

Son aquellos eventos que pueden causar daño a algo y están siempre presentes en cada sistema.

**Vulnerabilidades**

Son todos aquellos puntos de un sistema que están propensos a ser explotados por una amenaza y que pueden desencadenar en que dicha amenaza tenga mayor probabilidad de tener éxito.

**Controles**

Son las medidas precautorias que se toman para contrarrestar los ataques y reducir las vulnerabilidades. Existen cuatro tipos de controles:

* Los controles disuasivos reducen la probabilidad de un ataque deliberado.
* Los controles preventivos protegen vulnerabilidades haciendo que los ataques fracasen o que reduzcan su impacto.
* Los controles correctivos reducen el efecto de un ataque.
* Los controles detectores descubren ataques y disparan controles preventivos o correctivos.

Estos tres elementos pueden ser ilustrados mediante un modelo relacional simple que se aprecia en la ilustración.

Ilustración 5. Modelo relacional simple

**2.3 Servidores**

Un servidor es un ordenador u otro tipo de equipo informático encargado de suministrar información a una serie de clientes, que pueden ser tanto personas como otros dispositivos conectados a él. La información que puede transmitir es múltiple y variada: desde archivos de texto, imagen o vídeo y hasta programas informáticos, bases de datos, etc.

El servidor actúa como el gran cerebro del sistema informático de la empresa, capaz de almacenar la información necesaria para el funcionamiento de cada departamento. El servidor tiene una gran utilidad en el funcionamiento de la empresa, ya que es capaz de llevar a cabo funciones tanto de carácter físico (funcionamiento de las máquinas y los aparatos necesarios para la actividad empresarial) como a nivel de información, ya que registra, almacena y envía la información que los distintos clientes le van solicitando. (Rodriguez, P. 2019)

**2.1 Tipos de servidores**

En el campo de la informática existen muchísimos tipos de servidor según su función y su contenido, cada día más. Estos son algunos de los tipos más comunes de servidores que podemos encontrar en el área laboral:

* **Servidor de impresiones:** controla una o más impresoras y acepta trabajos de impresión de otros clientes de la red, poniendo en cola los trabajos de impresión.
* **Servidor de correo:** almacena, envía, recibe, enruta y realiza otras operaciones relacionadas con email para los clientes de la red.
* **Servidor de fax:** almacena, envía, recibe, enruta y realiza otras funciones necesarias para la transmisión, la recepción y la distribución apropiadas de los fax.
* **Servidor de la telefonía:** realiza funciones relacionadas con la telefonía, como es la de contestador automático, almacenando los mensajes de voz, encaminando las llamadas y controlando también la red o el Internet.
* **Servidor proxy:** realiza un cierto tipo de funciones a nombre de otros clientes en la red para aumentar el funcionamiento de ciertas operaciones, también proporciona servicios de seguridad.
* **Servidor del acceso remoto:** controla las líneas de módem de los monitores u otros canales de comunicación de la red para que las peticiones conecten con la red de una posición remota, responde llamadas telefónicas entrantes y reconoce la petición de la red.
* **Servidor web:** almacena documentos HTML, imágenes, archivos de texto, escrituras, y demás material Web compuesto por datos y distribuye este contenido a clientes que la piden en la red.
* **Servidor de base de datos:** provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor.
* **Servidor de Seguridad:** Tiene software especializado para detener intrusiones maliciosas, normalmente tienen antivirus, antispyware, antiMadware, además de contar con cortafuegos redundantes de diversos niveles y/o capas para evitar ataques, los servidores de seguridad.

**Servidores de respaldos**

Un servidor de respaldo es un tipo de servidor que tiene un software de respaldo instalado y tiene mucha capacidad de almacenamiento en discos duros (u otros medios) disponible para ser usado con el propósito de asegurar que no ocurra pérdida de información.

**Servidor de aplicaciones**

El servidor de aplicaciones se trata de un dispositivo de software que proporciona servicios de aplicación a las computadoras cliente. Un servidor de aplicaciones generalmente gestiona la mayor parte (o la totalidad) de las funciones de lógica de negociación y de acceso a los datos de las aplicaciones. ("Servidor de aplicaciones", 2019)

**2.3.2 Sistemas Operativos para Servidores.**

En el mercado existen diversos sistemas operativos especializados para funcionar como servidores, los más utilizados son los de las familias de Microsoft Windows o alguna distribución de Linux.

**Sistemas Operativos de la familia Microsoft.**

Microsoft es conocida por el desarrollo del popular sistema operativo Microsoft Windows. Este sistema operativo ha evolucionado mucho desde la aparición de su primera versión en 1985 hasta tener toda una gama de productos orientados a cubrir las necesidades de los diferentes tipos de usuarios.

Actualmente Microsoft Windows cuenta con versiones para usuarios domésticos, para empresas y para dispositivos móviles.

**Microsoft Windows Server**

El sistema operativo Microsoft Windows Server cuenta con varias versiones recientes que se pueden encontrar en muchas organizaciones, entre ellas las versiones 2003, 2016 y 2019.

En la tabla que se muestra abajo se enlistan algunas características importantes de estas tres versiones de Microsoft Windows Server.

Tabla 4. Comparativa de S.O. Windows Server

|  |  |  |  |
| --- | --- | --- | --- |
| Características | Microsoft Windows  2003 Server. | Microsoft Windows  Server 2016. | Microsoft Windows  Server 2019. |
| Sistema de Archivos. | FAT 32 y NTFS. | NTFS. | NTFS. |
| Soporte HTTP. | Si. | Sí | Sí. |
| Soporte DNS. | Sí. | Sí. | Sí. |
| Soporte FTP. | Sí. | Sí. | Sí. |
| Soporte HTTPS. | Sí. | Sí. | Sí. |
| Soporte SSH. | Sí. | Sí. | Sí. |
| Soporte DHCP | Sí. | Sí. | Sí. |
| Soporte RAID. | Sí. | Sí. | Sí. |
| Fecha de Lanz. | Febrero 2003. | 2015. | Febrero 2018. |
| Precio promedio. | $199-$5,999 USD | $199-$7,999 USD | $199-$9,750 USD |
| Soporte. | Sólo Actualizaciones | Sí. | Sí. |
| Licencia. | Propietaria. | Propietaria. | Propietaria |

Microsoft Windows Server 2019 es el sistema operativo más reciente para servidores que ha sacado al mercado Microsoft, por lo que cuenta con todo el soporte y respaldo de Microsoft. Si se compara con otros sistemas operativos, su costo es muy elevado, ya que según la versión que se quiera, va desde los 199 hasta los 9,750 USD.

**Sistemas Operativos de la familia Linux**

El sistema operativo Linux cuenta con muchas distribuciones, algunas de las cuales son: Mandriva, Debian, Red Hat, SuSE, Gentoo, Ubuntu, Fedora, BSD, entre otras.

**Comparativa entre distribuciones del Sistema Operativo Linux**

Fedora es un Sistema Operativo Linux que cuenta con una amplia aceptación por parte de la industria, con lo último y lo más nuevo en software libre y de código abierto.

Ubuntu Server también es una distribución Linux que va ganando adeptos como Sistema Operativo para servidores.

Por su parte Red Hat (la distribución en la que se basa Fedora), es una distribución de Linux ya probada y con un amplio mercado en la industria, cuenta con un soporte continuo y amplio que permite a las empresas implementar las soluciones que requieren de una manera robusta.

Finalmente otra distribución de Linux muy utilizada para el servicio de aplicaciones y de bases de datos es CentOs Linux, que es una distribución desarrollada por la compañía Novell, cuenta con herramientas muy poderosas que facilitan la gestión de aplicaciones.

En la siguiente tabla se hace una comparativa de las características más importantes de las distribuciones de Linux más utilizadas para servidores.

Tabla 5.Comparación de los S.O. Linux

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Características | Fedora Core | Ubuntu Server | RedHat Enterprise | CentOS |
| Sistema de Archivos | Ext3 | Ext3 | Ext3 | Ext3 |
| Versiones | 12 | 9.10 | 5.3 | 11 |
| Licencia | GPL. | GPL. | Propietaria | Propietaria |
| Precio Promedio | Gratuito. | Gratuito. | $349.00 USD -  $18,000.00 USD | Gratuito |
| Principales Servicios | HTTP,  SSH, DHCP, | HTTP,  SSH, DHCP, | FTP, DNS, | HTTP, SSH,  DHCP, |

# CAPÍTULO III. MARCO CONTEXTUAL

El problema de seguridad informática es un tema que comúnmente existe en muchas empresas, más si se trata de empresas pequeñas y medianas debido a que no le toman la importancia de la seguridad informática para poder contar con medidas de seguridad adecuadas y poder evitarse pérdidas o problemas a futuro, a lo largo del tiempo y de las actualizaciones de las tecnologías se han creado muchas medidas alternas para dar solución a este cotidiano problema de seguridad por lo que existen diversas maneras de contrarrestar el problema y muchas maneras dependen de lo económico, de la eficiencia y automatización ya que entre mayor es la inversión de la solución mucho mayor es la probabilidad de fallas en la seguridad, por lo que se realizó la investigación de otros proyectos similares.

## 3.1 Antecedentes del proyecto

El tema de la seguridad informática ha dado pie al desarrollo de proyectos relacionados con las tecnologías de la información con la finalidad de agilizar , actualizar y automatizar los procesos ………… uno de los trabajos relacionados a este campo de investigación es el que presenta Alciviades, E. ( 2009) en su tesis de titulación “-.-----------------------“ en la cual busca

Otro proyecto similar es el que presenta ……….. titulado ………… en el encontró ……….

Dentro de una empresa privada se desarrolló un problema situado en la seguridad informática por lo que se emplearon varias medidas de seguridad para contrarrestar dicho problema por medio de un servidor de respaldo que dio solución permanente a dicho problema, proyecto desarrollado por Enrique Alciviades Rodas Ron realizado dicho proyecto en el año 2009, realizando la implementación de una herramienta automatizada de respaldos para buscar muchos beneficios, tanto en el orden administrativo , operativo como económico. Este proyecto busco Brindar una guía básica, para que los profesionales de TI puedan en su momento justificar la implementación de una herramienta de este tipo. Los beneficios que brinda este tipo de proyectos siempre serán positivos, poniendo especial énfasis en el tema económico que en nuestro medio generalmente tiene la mayor prioridad sobre cualquier otro aspecto de una solución.

Todo proyecto debe manejarse de manera formal, aplicando estándares definidos y aceptados formalmente. Algo que ha quedado muy bien aprendido es que los proyectos deben dividirse en fases y aplicar un manejo profesional que garantice un buen manejo del tiempo, costos y recursos, características que siempre deben ser equilibradas para asegurar un producto final con calidad.

En proyectos como este trabajo se puede apreciar que es mucho más eficiente el buscar herramientas que solucionen problemas puntuales en corto tiempo, con probada calidad, tal vez con un costo mayor si lo comparamos contra un desarrollo local al inicio, pero que se va diluyendo a medida que pasa el tiempo del proyecto. A veces es necesario hacer el ejercicio de cálculo y comparación entre herramientas ya fabricadas, contra el tiempo, costo y calidad de realizar una propia. Las empresas normalmente deben dedicarse a ser especialistas en su negocio y Sistemas debe convertirse en un área de servicio que brinde soluciones rápidas alineadas a la estrategia.

Proyecto realizado en una universidad de Ecuador el año de 2017 por Geovanny Daniel Jiménez Caraguay con el título de Implementar una solución de respaldos de archivos de configuración de los sistemas, servidores, equipamiento de red y bases en el centro de datos de la Universidad Nacional de Loja

El presente Proyecto consiste en la implementación de una solución de respaldos automatizados en el centro de datos de la Universidad Nacional de Loja, para los principales servidores, sistemas, equipos de red y bases de datos, contando de esta manera con un mecanismo que ayude a garantizar la integridad y disponibilidad de la información en caso que ocurra algún evento adverso que pueda producir perdida de información, para de esta manera obtener una recuperación confiable. Para el desarrollo del proyecto, se ha planteo una metodología compuesta por cinco fases, realizado primeramente un análisis de la situación actual del centro de datos, para conocer su estructura y la situación actual de respaldos, en la fase 2 se realizó una revisión de herramientas software de respaldos para realizar un análisis comparativo de las principales herramientas de respaldo de información, llegando a plantear una solución con el software de respaldo en red Bacula para los servidores, sistemas y bases de datos, mientras que para los dispositivos de red se planteó la implementación de un servidor TFTP, para que los dispositivos de red envíen mediante una tarea automática su configuración.

Luego, en la fase 3 se realizó la experimentación en un escenario de pruebas tomando tres servidores como clientes y el servidor de pruebas de la UTI como el servidor de respaldos, en el cual también se instaló el servicio TFTP para las pruebas de los dispositivos de red. En la siguiente fase se realizó el dimensionamiento del hardware requerido, tomando en cuenta la información a respaldar de todos los servidores existentes, para finalmente en la fase 5, realizar la implementación de la solución planteada en el servidor designado para respaldos en el centro de datos de la UTI, logrando de esta manera aumentar el grado de disponibilidad e integridad de la información dentro de la institución, así como la continuidad del servicio.

La implementación de la solución planteada contribuye de gran manera a mantener la integridad y disponibilidad de la información de los principales servidores del centro de datos, ya que permite tener un backup de toda la información considerada crítica, y poder restaurarla sin ningún problema cuando sea requerido.

La automatización de las tareas de respaldo permite a los funcionarios de la UTI tener un respaldo programado de toda la información que es relevante para esta área; además, permite garantizar en mayor porcentaje la continuidad de los servicios que brindan a la comunidad universitaria. (Jiménez Caraguay, 2019)

El tercer proyecto implementado en un instituto con el nombre de Implantación de una solución de respaldo en el año 2016 realizado por el Director General de Informática Manuel Escudero Sanchez, Jefe de Servicio de sistemas Informáticos Elena Gonzales Arnal, Técnico de Gestión Informática Joaquin Matas Gambin y el Subdirector General de Calidad de Servicios Manuel Frutos Mirete donde todo el directivo General de Informática desarrollo una estrategia de modernización y unificación de las infraestructuras para dar respuesta a las necesidades en el manejo de la información de los sistemas corporativos del Gobierno Regional.

La Dirección General ha planteado un proyecto de integración de los servicios críticos en un sistema unificado de almacenamiento, salvaguarda y seguridad, que permita una solución de alto valor, que garantice los requisitos planteados por estos sistemas de información y permita una flexibilidad y escalabilidad adecuadas para el funcionamiento, desarrollo y crecimiento de dichos entornos.

La solución planteada ha constado de los procesos de estudio de la información crítica y sus necesidades de manejo, definición y diseño de un sistema de almacenamiento de alta disponibilidad, adecuación y redefinición de las estrategias de seguridad (políticas de backup, planes de contingencia) e integración y migración de los sistemas críticos al nuevo entorno.

Se ha podido constatar en la realización de este proyecto, que es muy interesante la opción de abordar soluciones de respaldar, copia de datos, restauración y continuidad de servicios de una manera integral, ya que es una buena forma de conseguir un sistema robusto en el que los Acuerdos de Calidad de Servicio que se pueden ofrecer no se ven limitados por el “eslabón más débil de la cadena”, cuestión que puede suceder en los enfoques realizados por la integración de sistemas independientes, sino que se pueden definir de una manera global. (Sanchez et al., 2019)

## 3.2 Características Temporales

El Juzgado penal oral de Baja California se encuentra ubicado en la ciudad de Tecate Baja California México, en Calle Misión san Francisco s/n, Col. El Descanso. Este fue inaugurado en el año 1995 y se crea con el propósito de ofrecer servicios gratuitos para atender y dar seguimiento a las penas y mediadas de seguridad a los inculpados en un proceso criminal. Se crearon varios juzgados penales orales en toda Baja california como: Ensenada, Tijuana, Tecate, Mexicali, Rosarito, etc., para poder brindar el servicio a toda la comunidad que carece de servicios y equipos básicos indispensables para el desarrollo de los juzgados, siendo que en Tecate la población es alrededor de 72,860 habitantes y la atención diaria de alrededor de 100 personas y en cuanto a las audiencias orales son 50 por día, cantidad muy considerable para la unidad operativa.

El poder judicial en Tecate tiene 3 salas para audiencias: Sala Unitaria, Auxiliar y adolescentes donde día tras días se realizan audiencias para llevar los casos que la población expone, donde dichas salas cuentan con un sistema de grabación y monitoreo para tener evidencia de todo lo expuesto en la audiencia y en caso de requerirlo solicitarlo para analizar lo sucedido en dicha audiencia.

El juzgado penal está conformado por los departamentos de Recursos Humanos, Nominas, Sistemas, Coordinación entre otras áreas, donde por medio de un sistema se lleva el control de cada interno o caso que se presente en los juzgados penales.

En el departamento de sistemas que es el área que se asignó para la realización de las actividades del proyecto, hay tres computadoras, una de ellas es un servidor de streaming, y las otras dos son computadoras de escritorio para la gestión de archivos y/o herramientas necesarias.

El ambiente laboral de la empresa es excelente. Las oficinas son amplias y accesibles, se cuenta con un almacén de equipo de cómputo, y consumibles para el mismo juzgado, y con un site donde están los servidores y equipo electrónico de Redes y telecomunicaciones, el equipo que tienen para trabajar es una computadora de escritorio como herramienta principal que tiene tres monitores para tener una mayor visión y agilidad, como herramientas se cuenta con un cuarto con cajoneras en el cual hay diferentes tipos de instrumentos y herramientas de trabajo por ejemplo: desarmadores de todos tipos y tamaños, instrumentos de medición como multímetro, voltímetro, checador de fuente de poder, . etc. También tapetes antiestáticos , cables utp, conectores Jack Rj-45, ponchadora de cable , repuestos de equipos de cómputo, diferentes tipos de cable de video de audio , adaptadores de todo tipo , cautino, pinzas de corte de diferente medida,, etc…..

El departamento de TI realiza todo el soporte que requiere la empresa, tomando en cuenta la realización del mantenimiento preventivo, correctivo a cada computadora para cuidar el estado de los equipos, se realizan las configuraciones necesarias a cada computadora para que casa usuario que la necesite pueda acceder a ella.

El departamento de sistemas tiene 3 personas que a través de un organigrama se mostrará el nombre y el puesto que desempeña cada personal.

Ilustración 6. Organigrama del departamento de TI

El departamento de TI está compuesto por 3 personas encargadas de realizar sus propias actividades para poder llevar a cabo la operación correcta del juzgado en el ámbito informático, las cuales se mencionan a continuación:

El encargado de sistemas se encarga de una gran variedad de tareas que incluyen la construcción del plan para supervisar la seguridad de las redes a dirigir las operaciones en internet, también la parte de la planeación, coordinación, dirigen investigaciones y facilitan las actividades relacionadas con la informática, se encarga de determinar las metas de la empresa que ayuden a mejorarla.

El encargado de soporte técnico realiza diferentes actividades en la empresa, entre las tareas principales que maneja son las siguientes:

* Detección y eliminación de virus y/o programas espías.
* Instalación y configuración de componentes internos o externos.
* Realización y control de copias de seguridad de la información sensible de la empresa.
* Desarrollo de planes de mantenimiento preventivo y correctivo.

El encargado de redes y telecomunicaciones tienen la responsabilidad de controlar una o más redes, son responsables que los trabajadores realicen tareas rutinarias, además de supervisar el rendimiento de la red para asegurarse de que todos los sistemas funciones de la manera más óptima y eficiente.

Entre las principales tareas que desempeña son:

* Proporcionar servicios de soporte.
* Asegurarse de que la red sea utilizada eficientemente.
* Cableado estructurado.
* Mantenimiento preventivo y correctivo en la estructura.

El técnico de audio y video es el encargado en sistemas de televisión y acondicionamiento de recintos de audio e imagen. Este profesional ejerce su actividad en productoras audiovisuales, emisoras de radio, estudios de doblaje, de grabación, etc. Se encarga de controlar los sistemas de videograbación y los equipamientos de los estudios, la acústica y el tratamiento de las imágenes y sonidos.

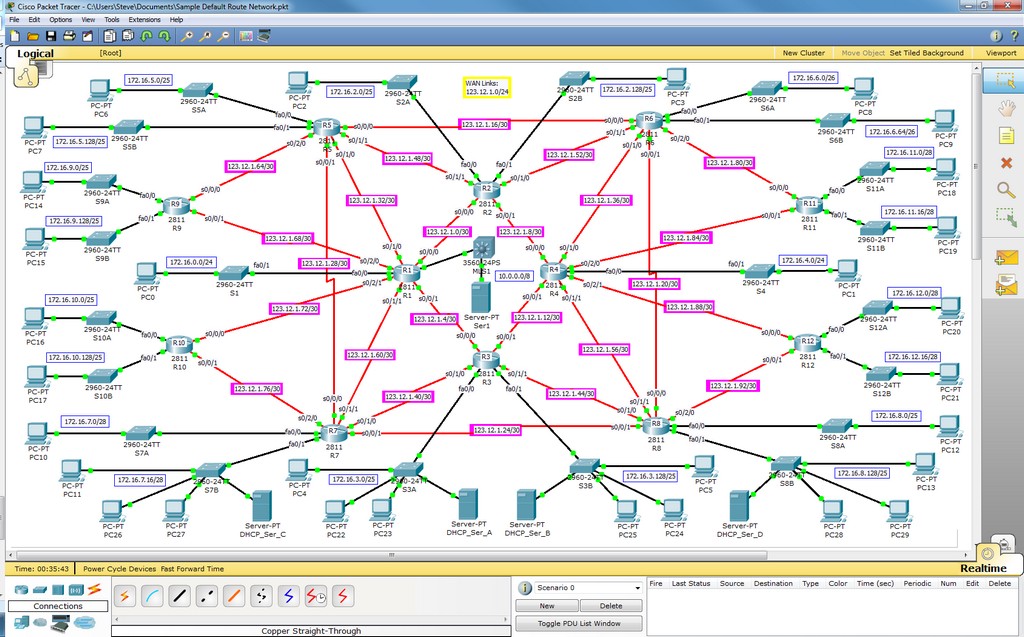
# CAPÍTULO IV. ESTRATEGIA METODOLÓGICA Y RESULTADOS

Para la realización del proyecto se requiere de un análisis y diseño de lo que se quiere llegar a realizar por medio de herramientas, se realizó un análisis para ver de qué manera se podrá administrar la red sin tener colisiones o fallas utilizando la herramienta de Packet Tracer, para poder realizar una simulación e ilustración de qué manera se puede realizar la estructura de la red tomando en cuenta las configuraciones de los routers, switches y la distribución de las IPs para cada equipo de cómputo que requiera ser conectado, se realizó un análisis de los routers a utilizar proporcionados por el gobierno de BC para ver de qué manera trabajan, las especificaciones y que tecnologías soportan, es fundamental saber las características del Hardware de los equipos electrónicos para determinar si son útiles a la hora de requerirlos donde se muestra una tabla de las características del hardware del switch

Switch Administrables TP-Link -SL3428

Tabla 6. Características del Hardware

|  |  |
| --- | --- |
| CARACTERÍSTICAS DE HARDWARE | |
| Estándares y Protocolos | IEEE 802.3I, IEEE 802.3U, IEEE 802.3AB, IEEE 802.3Z, IEEE 802.3X, IEEE 802.1D, IEEE 802.1S, IEEE 802.1W |
| Interfaz | 24 puertos RJ45 10/100Mbps, 4 puertos RJ45 10/100/1000Mbps, 2 Ranuras SFP 100/1000MBps, 1 puerto de consola |
| Medios de Red | 10Base-T UTP categoría 3, 4, 5cables (100m máximo) |
| Fuente de alimentación | 100 ~ 240VAC, 50/60Hz |
| Consumo de energía | Máximo: 11.9W (220V/50Hz) |
| Dimensiones | 17.32\*8.7\*1.73 plug.(400\*220\*44 mm) |

Ilustración 7.Topología de Redes

* Cableado de la estructura de red
* Configuración de la red por medio de vlans
* Análisis de los requerimientos del servidor de respaldos
* Creación de servidor de respaldos (Windows server)
* Análisis de los requerimientos del servidor de aplicaciones
* Creación del servidor de aplicaciones (Linux)
* Configuración y cableado de equipos de computo
* Documentación del proyecto

# CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

# REFERENCIAS

Álvarez, G., & Pérez, P. (2004). Seguridad informática para empresas y particulares. Madrid: McGraw-Hill/Interamericana.

Es.wikipedia.org. (2019). Análisis de riesgo. [online] Available at: https://es.wikipedia.org/wiki/Análisis\_de\_riesgo [Accessed 22 Feb. 2019].

Hernández, J. (2019). Técnico/a de imagen y sonido. Retrieved from https://treball.barcelonactiva.cat/porta22/es/fitxes/T/fitxa5901/tecnicoa-de-imagen-y-sonido.do

Informática, S. (2019). *Significado de Seguridad informática*. [online] Significados. Available at: https://www.significados.com/seguridad-informatica/ [Accessed 22 Feb. 2019].

Iso-actual.blogspot.com. (2019). ISO/IEC 17799. [online] Available at: http://iso-actual.blogspot.com/p/isoiec-17799.html [Accessed 22 Feb. 2019].

Jiménez Caraguay, G. (2019). Implementar una solución de respaldos de archivos de configuración de los sistemas, servidores, equipamiento de red y bases de datos en el centro de datos de la Universidad Nacional de Loja [Ebook]. Ecuador. Retrieved from http://dspace.unl.edu.ec/jspui/bitstream/123456789/19097/1/Jiménez%20Caraguay%2C%20Geovanny%20Daniel.pdf

Rodríguez, J. (2019). Qué es un servidor y para qué sirve - Infortelecom. Retrieved from https://infortelecom.es/blog/que-es-un-servidor-y-para-que-sirve/

Sánchez, M., González, E., Matas, J. and Frutos, M. (2019). *Implantación de una solución de respaldo*. [ebook] Available at: http://file:///E:/proyecto%20similar%20de%20directores.pdf [Accessed 8 Mar. 2019].

Servidor de aplicaciones. (2019). Retrieved from https://es.wikipedia.org/wiki/Servidor\_de\_aplicaciones

Toro, R. (2019). *ISO 27001: La Seguridad de la Información en la Administración General del Estado*. [online] PMG SSI - ISO 27001. Available at: https://www.pmg-ssi.com/2015/03/iso-27001-la-seguridad-de-la-informacion-en-la-administracion-general-del-estado/ [Accessed 22 Feb. 2019].

(2019). [Ebook]. Retrieved from https://www.dspace.espol.edu.ec/bitstream/123456789/7845/1/Implementación%20de%20una%20solución%20automatizada%20de%20respaldos.pdf

# ANEXOS (opcional)

Los anexos se pueden respetar su presentación original.