

**UNIVERSIDAD TÉCNICA FEDERICO SANTA
MARÍA SEDE CONCEPCIÓN-REY BALDUINO
DE BÉLGICA**

“INTRANET DEPARTAMENTO ELECTRÓNICA E INFORMÁTICA”

Trabajo de titulación para optar al título
de Técnico universitario en
TELECOMUNICACIONES Y REDES

Alumno:

Joaquín Ignacio Riffo Agurto

Profesor guía:

Sr. Israel Figueroa Pedreros

Profesional co-referente:

Sr. Milton Marín

RESUMEN

La universidad Federico Santa María se de Concepción es una distinguida casa universitaria con una trayectoria de casi 50 años. Esta sede consta de varios espacios y departamentos, dentro de los cuales, se encuentra el departamento de electrónica e informática, que cuenta con varios lugares de trabajo como laboratorios y salas. Son estos sitios en los que se basará el proyecto de “Intranet departamento electrónica e informática”, con el fin de proveer un mejoramiento del esquema de red actual de la universidad para que sea más estable, con una mejor conexión, mejor comunicación y cuente con mayor seguridad.

Teniendo en cuenta lo anteriormente comentado, podrían existir falencias que afecten principalmente la topología de red de la sede. Se debe investigar y hacer un levantamiento de requerimientos para crear un plan de trabajo conjunto a la UTI (Unidad de tecnologías de la información) de la sede Concepción en las distintas áreas de trabajo dentro del departamento. Algunos de estos requerimientos serán exigencias en gran medida a la incorporación de equipamiento nuevo y el desarrollo de una estructura completa para que, la sede, de manera ambiciosa las pueda incorporar a futuro, aportando una mejora en gran parte a la conectividad.

Eventualmente el proyecto se enfocará diversamente en buscar problemas ya sean capa 1 del modelo OSI (cableado, switch, router,) y/o por su configuración de equipos, que están conectados directamente a la red de la universidad, teniendo énfasis en el direccionamiento de IP y configuración de VLAN (capa 2 modelo OSI). Al realizar una investigación de cada uno de los equipos adquiridos por la sede se ayudará a dar un enfoque más amplio al proyecto a realizar, y para finalizar cabe mencionar el respaldo asignado de la ISP utilizado como enlace principal de la sede es de Gtd Teleductos S.A.

PALABRAS CLAVE: INTRANET, TOPOLOGÍA DE RED, ISP, CONECTIVIDAD, MODELO OSI.

ÍNDICE

INTRODUCCIÓN	1
DESCRIPCIÓN DEL PROBLEMA	2
OBJETIVOS GENERALES	3
OBJETIVOS ESPECÍFICOS	3
MARCO TEÓRICO	4
ALCANCE	6
CAPÍTULO I: LABORATORIOS Y EQUIPOS	8
1. ESPACIOS FÍSICOS DEPARTAMENTO ELECTRÓNICA E INFORMÁTICA Y ESPACIOS PRINCIPALES DE COMUNICACIÓN DE LA UNIVERSIDAD	10
1.1. LABORATORIOS DE INFORMÁTICA	11
1.1.1. Laboratorio redes.	11
1.1.2. Laboratorio 1.	11
1.1.3. Laboratorio 2.	11
1.1.4. Laboratorio memoristas.	12
1.2. LABORATORIO 209 TELECOMUNICACIONES Y REDES	12
1.3. LABORATORIO ELECTRÓNICA	12
1.4. LABORATORIOS DE MECATRÓNICA	13
1.4.1. Laboratorio metrología.	13
1.4.2. Laboratorio resistencia.	13
1.4.3. Laboratorio proyecto.	13
1.4.4. Laboratorio computación.	13
1.5. SALA DE DATOS	14
1.6. SALA DE ENLACE INFORMÁTICA	14
2.-EQUIPOS DE COMUNICACIONES	14
2.1. SWITCHES SALA DE DATOS	15
2.1.1. Switch Catalyst 3850-24P-S:	15
2.1.2. Switch Dell PowerConnect 6248(core):	15
2.1.3. Switch Cisco Catalyst 3560G:	16
2.2. SWITCHES INFORMÁTICA	17
2.2.1. Switch Cisco SG200-26:	17
2.2.2. Switch Cisco SG200-50:	17
2.3. SWITCHES LAB. 209 TELECOMUNICACIONES Y REDES	18
2.3.1. Switch Cisco Catalyst 2960X-24TS:	18
2.3.2. Switch Cisco SF300-24P:	19
2.4. SWITCH ELECTRÓNICA	19
2.4.1. Switch DELL N2024:	19
2.5. SWITCHES MECATRÓNICA	20
2.5.1. Switch DELL N2048:	20
2.5.2. Switch DES-1024D:	21
2.6. SERVIDOR LAB. 209	22
2.6.1 PowerEdge R540:	22
CAPÍTULO II: RED, SEGURIDAD Y PROPUESTA UTFSM	24

1. ESTADO DE RED	26
1.1. VLAN	26
1.1.1. VLAN 21:	26
1.1.2. VLAN 15:	26
1.1.3. VLAN 18:	27
1.2. IP	27
1.2.1. Informática:	27
1.2.2. Telecomunicaciones y redes:	27
1.2.3. Electrónica:	29
1.2.4. Mecatrónica:	29
1.3. RESUMEN DE ESTRUCTURA DEL DEPARTAMENTO	30
2. SITUACIÓN ACTUAL UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA SEDE CONCEPCIÓN	31
2.1. ENLACE PRINCIPAL	31
2.2. EQUIPOS DE LA RED INTERNA DEL DEPARTAMENTO	32
2.2.1. Switches Administrables	33
2.2.2. Switches no Administrables	33
2.3. MAPA DE ESPACIOS FÍSICOS DENTRO DE LA SEDE	34
2.4. ANÁLISIS DE ESPACIOS DEL DEPARTAMENTO	35
3. SEGURIDAD EN LA RED EN CONTEXTO DE CIBERSEGURIDAD	36
3.1. ¿QUE ES CIBERSEGURIDAD?	36
3.2. FORMAS DE MEJORAR LA SEGURIDAD	37
3.3. FORMAS DE MEJORA DE SEGURIDAD EN SEDE CONCEPCIÓN	38
4. PROPUESTA MEJORAMIENTO DE LA RED INTERNA PARA EL DEPARTAMENTO DE ELECTRÓNICA E INFORMÁTICA	39
4.1. PROPUESTA DE ESTRUCTURA SEDE CONCEPCIÓN	39
CONCLUSIONES	42
BIBLIOGRAFÍA	43
ANEXO	46
ANEXO 1: CONVENIO DE LA UNIVERSIDAD CON GTD	46

ÍNDICE DE FIGURAS

Figura 1-1. Cisco Catalyst 3850-24P-S Switch..... 15

Figura 1-2. PowerConnect 6248.....16

Figura 1-3. Cisco Catalyst 3560G-24TS Switch.....16

Figura 1-4. Cisco SG200-26 26-port Gigabit Smart Switch.....17

Figura 1-5. Cisco SG200-50P 50-port Gigabit PoE Smart Switch.....18

Figura 1-6. Cisco Catalyst 2960X-24TS-LL Switch.....18

Figura 1-7. Cisco SF300-24P 24-Port 10/100 PoE Managed Switch with
Gigabit Uplinks.....19

Figura 1-8. Dell Networking N2024.....19

Figura 1-9. Dell Networking N2048.....20

Figura 1-10. DES-1024D.....21

Figura 1-11. Servidor en rack PowerEdge R540.....22

Figura 2-1. Diagrama interno Lab. 209.....28

Figura 2-2. Estructura resumida de equipos. 30

Figura 2-3. Mapa de emplazamiento.....34

Figura 2-4. Propuesta de red UTFSM.....40

Figura 2-5. Servicio de datos.....46

Figura 2-6. Servicio de datos página 2.....47

Figura 2-7. Servicio de datos página 3.....48

Figura 2-8. Servicio de internet.....49

Figura 2-9. Servicio de internet página 2.....50

Figura 2-10. Servicio de internet página 3.....51

Figura 2-11. Servicio de data center.....52

Figura 2-12. Servicio de data center página 2.....53

ÍNDICE DE TABLAS

Tabla 2-1. Resumen de red UTFSM.....31

Tabla 2-2. Switches Administrables.....33

Tabla 2-3. Switches no Administrables.....33

Tabla 2-4. Resumen espacios sede Concepción.....35

SIGLA Y SIMBOLOGÍA

ISP	:	Internet Service Provider (Proveedor de Servicios de Internet)
UTP	:	Unshielded Twisted Pair (Par Trenzado no Blindado)
VLAN	:	Virtual Local Area Network (Red Virtual de Área Local)
UTI	:	Unidad de Tecnologías de la Información
IP	:	Internet Protocol (Protocolo de Internet)
DNS	:	Domain Name System (Sistema de Nombres de Dominio)
PLC	:	Programmable Logic Controller (Controlador Lógico Programable)
LAN	:	Local Area Network

INTRODUCCIÓN

Para generar una conexión viable y de calidad, que sea segura y oportunamente sea estable para la universidad, se deben considerar varios aspectos los cuales en el siguiente proyecto se darán a conocer.

Este proyecto busca la mejora en la seguridad y conectividad del departamento de electrónica e informática. Para ello se investigará a profundidad los enlaces y conexiones que hay actualmente en el departamento al igual que los equipos y espacios de trabajo asignados.

La investigación plantea como complemento el generar propuestas que mejoren el perfeccionamiento de la conectividad a equipos que son vulnerables a causa de la antigüedad o que actualmente no puedan ser configurados, provocando que sean mal administrados en las áreas de trabajo y en consecuencia se obtiene una mala calidad de conexión para el personal y alumnado de la universidad.

Se hablará de VLAN para el desarrollo de la configuración correspondiente de los equipos, también de nateo y ruteo, determinando así el proceso de configuración o adaptación en los equipos en diversos espacios de la universidad, ya sea, en centrales de comunicación, laboratorios, salas de trabajo, etc. Con el fin de tener una conexión estable y segura, mejorando lo que vendría siendo el estado actual en la sede Concepción.

DESCRIPCIÓN DEL PROBLEMA

La ciberseguridad hoy en día es un tema que genera gran importancia para cualquier organización, en temas como resguardar la información personal o información confidencial para una empresa. Es por ello por lo que al usar la ciberseguridad como herramienta “nuestro sistema estará mejor protegido de los ataques informáticos, hackeos o cualquier robo de datos o identidad” [OBS Business School, 2019].

Un ejemplo claro del problema que se presenta en la red UTFSM principal sede concepción es la seguridad en sus conexiones, que se puede ver afectada por falencias que se encuentran presentes en los equipos de comunicaciones, ya sea porque están mal configurados o no poseen las características adecuadas.

El equipamiento de mecatrónica es un caso particular de mala administración, ya que en sus laboratorios no cuentan con equipos administrables capaces de ser configurados para un óptimo trabajo en sus salas.

OBJETIVOS GENERALES

Rediseñar una estructura de red que permita mejor seguridad en el departamento de electrónica e informática, conjunto un plan de trabajo que ayude a mejorar la conectividad y estabilidad para el departamento y en lo posible con configuraciones que ayuden a poder incorporar una intranet en las áreas de trabajo más vulnerables en la sede. Finalmente crear propuestas que permitan una mejor administración por parte del departamento en sus redes y establecer criterios para el tráfico de esta.

OBJETIVOS ESPECÍFICOS

- 1.-Determinar los equipos de comunicaciones y sus características, los cuales actualmente se están ocupando en el departamento de electrónica e informática.
- 2.-Generar un diagrama de la topología física de la red de la sede. En particular, sobre las subredes que ocupan el departamento de electrónica e informática.
- 3.-Identificar posibles equipos de comunicaciones que no posean las capacidades para generar dominios de difusión separados para las redes del departamento.
- 4.-Proponer una configuración de red para el departamento que permita mejorar su seguridad y conectividad dentro de sus diferentes espacios en la sede.

MARCO TEÓRICO

En este proyecto se utilizará como conceptos los siguientes términos a lo largo de todo esta investigación y desarrollo. Para el estudio completo de la topología de la universidad.

Modelo OSI: Es una normativa formada por siete capas, que define las diferentes fases por las que deben pasar los datos para viajar de un dispositivo a otro sobre una red de comunicaciones.

Topología de red: Es el arreglo físico o lógico en el cual los dispositivos o nodos de una red (computadoras, impresoras, servidores, hubs, switches, enrutadores, etc.) se interconectan entre sí sobre un medio de comunicación.

Ciberseguridad: Se conoce como la seguridad de la tecnología de la información.

Segmentación de redes: Consiste en dividir la red en subredes para poder aumentar el número de ordenadores conectados a ella y así aumentar el rendimiento, tomando en cuenta que existe una única topología, un mismo protocolo de comunicación y un solo entorno de trabajo.

Firewall: Un firewall llamado también cortafuego, es un sistema que permite proteger a una computadora o una red de computadoras de las intrusiones que provienen de una tercera red (expresamente de Internet).

VLAN: Es un método que permite crear redes que lógicamente son independientes, aunque estas se encuentren dentro de una misma red física.

Intranet: Una intranet es una red de computadoras similar a internet, aunque para uso exclusivo de una determinada organización, es decir que solamente los equipos de la empresa u organización pueden acceder a ella.

Ruteo: Básicamente consiste en mover paquetes, o en otras palabras información a nivel de una red de Internet desde una red a otra.

Nateo: Es un mecanismo utilizado por routers y equipos para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados siendo necesario editar los paquetes para permitir la operación de protocolos, los que incluyen información de direcciones dentro de la conversación del protocolo.

ALCANCE

En el siguiente proyecto, se planea dar a conocer las formas de cómo mejorar la ciberseguridad en el departamento de electrónica e informática además de la investigación de la estructura de la red y de cómo influye principalmente en la estabilidad para los usuarios. Así mismo se establecerá un reordenamiento de la topología actual de la sede que generará una mejora en ella, que en lo posible sea posteriormente incorporada para una mejor administración y uso de estos.

Este proyecto culminará ayudando tanto al alumnado que se encuentre en el campus de la universidad, como también a el profesorado y a todo funcionario que desee ocupar algunos de los equipos presentes en todo el campus.

CAPÍTULO I: LABORATORIOS Y EQUIPOS

1. ESPACIOS FÍSICOS DEPARTAMENTO ELECTRÓNICA E INFORMÁTICA Y ESPACIOS PRINCIPALES DE COMUNICACIÓN DE LA UNIVERSIDAD

La actual organización física de informática consta de tres laboratorios, una sala de memoristas, oficina de profesores y la sala de enlace. Los espacios de electrónica son tres laboratorios en los cuales el laboratorio 1 cuenta con la llegada de un equipo de comunicaciones, permitiendo un acceso a la red a los 16 equipos ahí establecidos. Por otra parte, la carrera de telecomunicaciones y redes cuenta con un laboratorio de trabajo hasta el momento. Por último, los espacios de mecatrónica son cuatro laboratorios en los que se trabaja sin equipos administrativos siendo los principales espacios en riesgo para la seguridad de la universidad y el departamento.

Cada uno de estos espacios cuenta con equipos que son administrados por la universidad y que ayudaran a ver de mejor manera como está conectada. El espacio asignado para los bastidores principales o rack que se encuentren por departamento serán descritos para una mayor contextualización de la topología de red.

En el primer caso se hablará de los laboratorios de informática en los cuales se establece la conexión y configuración de los equipos, así como también en el proceso de gestión en toda la universidad a los equipos de comunicaciones administrables.

Para finalizar con la idea y presentar los puntos específicos de cada laboratorio se realizaron cambios de categoría en el cableado de algunos equipos de manera que la conexión sea aún más estable, permitiendo así que no se vean afectado por un cuello de botella debido a las altas velocidades que entregan algunos switch y que a su vez puedan generar una conexión más segura sin que la red pierda la eficiencia.

1.1. LABORATORIOS DE INFORMÁTICA

Informática consta de tres laboratorios en los cuales la red suministrada por la universidad llega a un bastidor principal que está ubicado en la sala de enlace de informática, el cual mediante switches Cisco SG200-26 se encarga de dar red a los distintos espacios dentro del departamento.

En los switches se trabajó la configuración de IP y VLAN. Cabe señalar que la llegada de la conexión troncal o principal es directa a la sala de datos mediante fibra óptica y con un conector SFP al switch principal de la sala de enlace.

1.1.1. Laboratorio redes.

En este laboratorio se encuentran conectados 33 equipos mediante cableado a un switch Cisco SG200-50 ubicado en un rack en la misma sala. Este rack tuvo un mantenimiento por parte de alumnos de la carrera telecomunicaciones y redes para un manejo óptimo de él.

1.1.2. Laboratorio 1.

El laboratorio 1 de informática tiene una conexión de 33 equipos a un switch Cisco SG200-50 ubicado en un rack de la misma sala. En este laboratorio se hizo un cambio de equipos y cableado, el cual se concentró principalmente en la configuración de IP y VLAN del switch para darle conectividad a los ordenadores asignados a esta sala.

1.1.3. Laboratorio 2.

El laboratorio 2 de informática cuenta al igual que los dos laboratorios anteriores con 33 equipos conectados a un switch Cisco SG200-50 mediante un cableado categoría 6 ubicado en el rack del mismo laboratorio. En él, al igual del laboratorio 1 se trabajó en la configuración de IP y VLAN en el switch, dando conectividad a los computadores.

1.1.4. Laboratorios memoristas.

La sala de memoristas cuenta con 4 equipos conectados directamente al bastidor principal mediante puntos, con la función de establecer un área para los alumnos de impresión y de desarrollo de proyectos.

1.2. **LABORATORIO 209 TELECOMUNICACIONES Y REDES**

Esta carrera consta de un laboratorio equipado con bastidores, equipos y servidores, los cuales dan la conexión hacia los equipos de trabajo. El enlace llega a un bastidor principal en el cual está conectado un servidor, que está configurado para dar DHCP a las estaciones de trabajo mediante configuraciones vía consola.

El laboratorio está conectado directamente por cableado al rack ubicado en el hall central y este se encuentra conectado con la sala de datos principal. Los equipos de comunicaciones que se maneja en el laboratorio serán descritos más adelante para dar la información necesaria de sus características.

1.3. **LABORATORIO ELECTRÓNICA**

El laboratorio de electrónica 1 es el espacio en donde se encuentra el rack de comunicaciones principal de la sala y desde él salen las conexiones hacia los equipos del laboratorio, a través de un switch Dell N2026. Junto a él trabaja un rack de talleres, el que es el encargado de dar conectividad completa a ese sector de la universidad.

En este laboratorio hay una cantidad de 16 equipos conectados, los cuales tienen conectividad entre sí.

1.4. LABORATORIOS DE MECATRÓNICA

Los laboratorios de mecatrónica se encuentran actualmente con una red no segura de conexión, lo que significa que están trabajando con switches no administrables dentro de sus salas. Esto determina que la conectividad de sus equipos no se adapte específicamente a sus quehaceres tales como implementar su propia intranet para integrar equipos específicos y poder comunicarse entre sí dentro de sus laboratorios.

1.4.1. Laboratorio metrología.

El laboratorio de metrología cuenta con 2 switch no administrables, lo cual no permite tener una conexión privada y que sólo sea administrada por la UTI, que es la encargada de suministrar estos laboratorios con la llegada de un enlace al rack de mecatrónica.

1.4.2. Laboratorio resistencia.

Posee incorporado 2 equipos los que son switches no administrables, que a su vez no logran al igual que las demás salas una conexión segura que permite la interconectividad dentro del laboratorio.

1.4.3. Laboratorio proyecto.

Al igual que los demás laboratorios cuenta con 2 switches no administrables integrados para la conectividad del lugar, siendo ineficaz la seguridad en él.

1.4.4. Laboratorio computación.

El laboratorio de computación de mecatrónica cuenta con 10 equipos conectados a 2 switches no administrables destacando la inseguridad total de todos los demás laboratorios de mecatrónica.

1.5. SALA DE DATOS

La sala de datos es el espacio principal de la universidad que cuenta con la llegada del enlace primario contratado, este espacio posee variados equipos que están establecidos para la comunicación entre los diversos departamentos. Su función es suministrar la red en toda la sede y los equipos de comunicaciones ubicados en esta sala son esenciales para la conectividad, debido a que presentan una configuración para determinar las VLAN y asignarlas así a los demás equipos de la sede mediante telnet, web o consola.

1.6. SALA DE ENLACE INFORMÁTICA

La sala de enlace informática cuenta con un bastidor principal, conectado directamente por medio de fibra óptica a la sala de datos. Proporciona conectividad a todos los laboratorios de informática y sus alrededores, también cuenta con equipos de telecomunicaciones administrables que generan una conexión mediante cableado UTP.

2.-EQUIPOS DE COMUNICACIONES

La universidad cuenta con una gama diversa de equipos funcionales, a los que este proyecto se enfocará dando sus respectivas configuraciones y las localizaciones de estos de manera que se ayude a determinar cómo están administrados y cómo funcionan en el departamento.

La conexión principal de los equipos y más importante está en la sala de datos, conectada con la ISP contratada GTD Teleductos S. A. (Ver Anexo 1) mediante fibra óptica, lo que genera conexiones veloces para la transmisión de datos hacia la universidad.

2.1. SWITCHES SALA DE DATOS

2.1.1. Switch Catalyst 3850-24P-S:

El equipo adquirido por el convenio de la ISP es un switch catalyst 3850-24P-S (ver Figura 1-1.). Este equipo es capaz de realizar conexiones muy altas de 10/100/1000 Mbps y su función es conectar el enlace proveniente de GTD mediante una cabecera de fibra óptica hacia un convertidor HUAWEI S5700-LI-AC que se conecta a el switch, estableciendo la conexión hacia los switches principales que hablaremos a continuación.



Figura 1-1. Cisco Catalyst 3850-24P-S Switch. Extraído de CISCO (2019).

2.1.2. Switch Dell PowerConnect 6248(core):

Este equipo es el encargado de establecer la conexión a los demás equipos principales de toda la universidad, la configuración de cada una de las bocas pertenece a las VLAN de cada enlace troncal de los departamentos. Este equipo soporta enlaces 10/100/1000 y permite conexiones 10 Gb opcionales (ver Figura 1-2.)



Figura 1-2. PowerConnect 6248. Extraído de DELL (2019).

2.1.3. Switch Cisco Catalyst 3560G:

Este equipo actualmente está conectado a una red paralela mediante un cable UTP y pasando a un convertidor de fibra óptica proveniente del switch Cisco Catalyst 3850 (ver Figura 1-1.). Este equipo no está incorporado dentro de la red del departamento, es por ello por lo que solo la nombraremos y se procederá a examinar más a fondo los demás equipos del respectivo departamento de electrónica e informática. Sin embargo, es un equipo capaz pudiendo incorporarlo a laboratorios de mecatrónica sin ningún problema.



Figura 1-3. Cisco Catalyst 3560G-24TS Switch. Extraído de CISCO (2019).

2.2. SWITCHES INFORMÁTICA

2.2.1. Switch Cisco SG200-26:

La sala principal de informática cuenta con 3 equipos los cuales están conectados entre sí para dar conexión a los distintos laboratorios de informática y además a sus funcionarios. Lo realiza con un enlace directo a la sala de datos principal de la universidad mediante fibra óptica a un módulo sfp. El equipo principal es un Cisco SG200-26 (ver Figura 1-4.) que cuenta con 26 puertos gigabit de alta velocidad 10/100/1000 para una conexión estable hacia los laboratorios y salas de profesores.



Figura 1-4. Cisco SG200-26 26-port Gigabit Smart Switch. Extraído de CISCO (2019).

2.2.2. Switch Cisco SG200-50:

El siguiente equipo se encuentra ubicado en los distintos laboratorios del departamento de informática. Cada uno de estos equipos se encuentra configurado en un rango de IP y VLAN determinado que es suministrado por la UTI. Cuenta con 50 puertos gigabit de alta velocidad 10/100/1000 para una mayor capacidad y conexión en los equipos de los laboratorios de informática.



Figura 1-5. Cisco SG200-50P 50-port Gigabit PoE Smart Switch. Extraído de CISCO (2019).

2.3. SWITCHES LAB. 209 TELECOMUNICACIONES Y REDES

Los siguientes equipos de comunicaciones están establecidos en el laboratorio 209 con la única función de dar conexión a los puestos de trabajo y no influyen directamente en el enlace principal del departamento.

2.3.1. Switch Cisco Catalyst 2960X-24TS:

El siguiente equipo de comunicaciones tiene una conexión directa con la sala de datos y actualmente se trabaja con dos de estos equipos en el laboratorio, están además configurados para establecer la conexión de los puestos de trabajo, servidores, routers y demás switches que cuenta el laboratorio. Estos equipos son altamente eficaces para conexiones 10/100/1000, con módulos sfp para transmisión de fibra óptica.



Figura 1-6. Cisco Catalyst 2960X-24TS-LL Switch. Extraído de CISCO (2019).

2.3.2. Switch Cisco SF300-24P:

Este equipo de comunicaciones, establecido en los bastidores de trabajo del laboratorio 209 soporta conexiones 10/100 siendo su principal uso dar conectividad a los servidores y demás equipos de los puestos de trabajo.



Figura 1-7. Cisco SF300-24P 24-Port 10/100 PoE Managed Switch with Gigabit Uplinks. Extraído de CISCO (2019).

2.4. SWITCH ELECTRÓNICA

2.4.1. Switch DELL N2024:

Este switch establece la conexión a todos los equipos del laboratorio de electrónica 1 y a diferentes puntos de red dentro del mismo laboratorio, soporta conexiones 10/100/1000 y también trabaja en conjunto a otro switch que establece conexión con todos los laboratorios y talleres el cual será nombrado más adelante (Switch Talleres).



Figura 1-8. Dell Networking N2024. DELL (2019).

2.5. SWITCHES MECATRÓNICA

2.5.1. Switch DELL N2048:

El siguiente equipo de comunicaciones se encuentra ubicado en el rack de mecatrónica, posee un soporte 10/100/1000 y es el principal equipo de comunicaciones.

Es el encargado de dar conectividad a los distintos laboratorios de mecatrónica, sin embargo, existen otros equipos establecidos que no incorporan el software de configuración en los laboratorios, lo cual hace más difícil poder interactuar con ellos y ser configurarlos a medida según los requerimientos que puedan solicitar los alumnos o el personal. Este equipo en comparación a los establecidos en los demás departamentos es el único que no está conectado directamente con la sala de datos y eso en gran parte afecta mucho el tema de la conectividad.



Figura 1-9. Dell Networking N2048. DELL (2019).

2.5.2. Switch DES-1024D:

El siguiente equipo de comunicaciones establecido en diferentes espacios de mecatrónica es el principal problema que afecta a los distintos laboratorios. En ellos no se pueden crear dominios de difusión para la administración y en gran medida es lo que causa riesgos en ámbitos de seguridad, por lo cual la adquisición de nuevo equipamiento mejoraría de manera positiva la conectividad y se podrían generar subredes capaces de albergar todos los equipos establecidos en los laboratorios y agregar nuevos para un futuro. Soporta solo conexiones 10/100 y no cuenta con puertos de alta velocidad.



Figura 1-10. DES-1024D. D-LINK (2019).

2.6. SERVIDOR LAB. 209

2.6.1 PowerEdge R540:

El servidor PowerEdge R540 ubicado en la sala 209 de la carrera de telecomunicaciones y redes, es el equipo de comunicaciones principal, siendo el encargado de almacenar todos los datos e información establecida de todo el laboratorio como los accesos y reglas, que permitan una navegación segura y confiable para los equipos con los que se trabajan.

Hasta el momento la capacidad de almacenamiento está limitada en 4 terabytes que se utilizan con un software llamado VMware que permite la creación de máquinas virtuales capaces de incorporar reglas de conexión y sistemas de monitoreo en tiempo real.



Figura 1-11. Servidor en rack PowerEdge R540. DELL (2019).

CAPÍTULO II: RED, SEGURIDAD Y PROPUESTA UTFSM

1. ESTADO DE RED

El estado de red en el que actualmente se encuentra la universidad es administrado por la UTI que por medio de los equipos de comunicaciones podemos establecer la topología interna de nuestras redes. La universidad en tanto se segmenta en distintas VLAN que mediante equipos administrables se pueden hacer las configuraciones pertinentes. Sin embargo, algunos de los equipos establecidos en la universidad no poseen las características necesarias para incorporar tales configuraciones.

A su vez la universidad cuenta con IP's públicas designadas para dar conexión a toda la red de la sede, mediante diferentes rangos creando dominios de difusión.

1.1. VLAN

La universidad cuenta con una serie de VLAN administradas para los diferentes espacios de trabajo que en el caso del departamento de electrónica e informática cuenta con 4 que son los siguientes:

1.1.1. VLAN 21:

La VLAN presentada está asignada para el departamento de informática y para el laboratorio 209 de telecomunicaciones y redes, actualmente es la que se trabaja en toda el área, y en sus equipos.

1.1.2. VLAN 15:

La VLAN 15 está asignada para los laboratorios de mecatrónica en los cuales no se encuentran equipos administrables, por lo que la red es suministrada directamente configurando las IP estáticas a los equipos.

1.1.3. VLAN 18:

La VLAN 18 está actualmente trabajando con los laboratorios de electrónica permitiendo así, una completa red administrada por switch programables dando conectividad principalmente a equipos como PLC y circuitos. Estos equipos son administrados por el personal.

1.2. IP

En el caso de IP hablaremos sobre el ruteo o routing que se establece a lo largo de la sede como también el nateo que es incorporado por la implementación de IP públicas y privadas que abarca la universidad. Es importante conocer el rango de los distintos departamentos y de cómo se trabaja en forma general en la sede.

1.2.1. Informática:

Informática cuenta con un rango de IP 10.4.10.X con VLAN 21, este rango es generado por los equipos de comunicaciones que mediante las configuraciones hechas por la UTI incluidas también en los enlaces troncales de los demás equipos de comunicaciones. Logran dar conexiones estables en los laboratorios y oficinas del departamento.

1.2.2. Telecomunicaciones y redes:

El estado actual de la red será mostrado a continuación por medio de un diagrama que representa las conexiones a través de enlaces y equipos, con la implementación de máquinas virtuales. Aquí igualmente se puede determinar cómo es que se trabaja por medio de un servidor, el cual está diseñado para administrar toda la información y recursos que emplean los equipos a través del programa VMware vSphere Client. Este programa tiene la función de crear todas estas redes virtuales que ayudan a generar los distintos rangos y accesos para el funcionamiento interno del laboratorio.

Se cuenta también con un acceso hacia la red de internet otorgada por la UTI, que en este caso está en funcionamiento con el rango 200.1.31.237 con VLAN 21.

El rango actualmente se encuentra funcionando en servidor local del laboratorio, como también se cuenta con un rango 10.4.11.2 con VLAN 21 para el acceso a la red interna de la universidad.

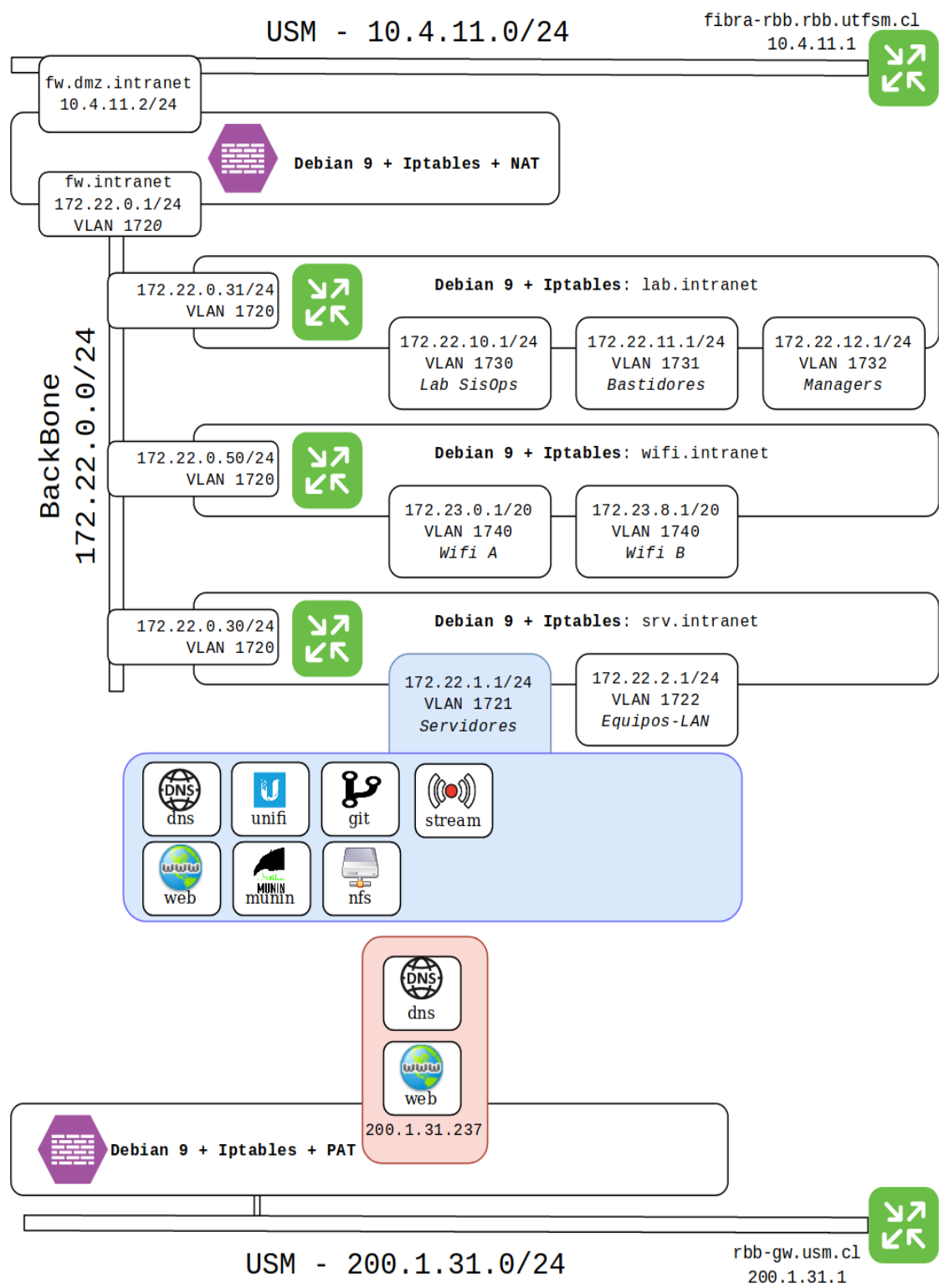


Figura 2-1 . Diagrama interno Lab. 209. DEI (2019).

1.2.3. Electrónica:

El estado de red actual de los laboratorios y espacios del departamento de electrónica establecidos por los equipos de comunicaciones configurados y de manera que le fue otorgada por la UTI son del rango 10.4.8.X con VLAN 18, estos rangos asignados son esenciales para el correcto funcionamiento de máquinas y ordenadores presentes en todo el departamento.

Para una conexión directa con el rack de talleres y del laboratorio 1 de electrónica, se modificaron ciertos puntos críticos, como el cambio de rack en el sector del laboratorio 1, también los cambios de equipos de comunicaciones establecidos en el lugar debido a las múltiples falencias y actualización de estos equipos.

A fin de mejorar la conexión de manera que sea más efectiva y de mejor calidad pudiendo así permitir la incorporación de más equipos para el desarrollo de las variadas actividades de trabajo para el departamento.

1.2.4. Mecatrónica:

En mecatrónica se aprecian varios aspectos que se generan a partir de lo investigado, en primer lugar, la conexión troncal hacia los distintos laboratorios establecidos, mediante equipos de comunicaciones administrables y no administrables no es fiable y por este motivo las redes locales del departamento causan problemas en la seguridad de los enlaces. El rango con el cual trabajan en los laboratorios es 10.4.5.X con VLAN 15.

En los distintos laboratorios se establecen equipos no administrables que no son capaces de crear difusiones de red lo que no permite administrar los distintos equipos y configurarlos para el desarrollo del proyecto en el cual se buscará la mejora actual de la sede que en gran parte buscará ser administrada de manera apartada por el departamento en conjunto con la UTI.

En el caso de mecatrónica se hizo una investigación de los distintos equipos que no son capaces de poder establecer difusiones de red como en los demás espacios para dar a conocer los beneficios que traería consigo la mejor actualización de equipamiento y poder desarrollar un plan de trabajo con el departamento para incorporar más subredes que permitan un óptimo trabajo en las distintas salas y laboratorios del lugar.

1.3. RESUMEN DE ESTRUCTURA DEL DEPARTAMENTO

En el esquema se logran apreciar las conexiones troncales a los distintos equipos del departamento con sus respectivos rangos de IP que en gran medida cuentan con configuraciones establecidas por el departamento de tecnologías de la información o UTI en la sede concepción. El cual trabaja directamente con casa central la cual proporciona los enlaces correspondientes para la sede.

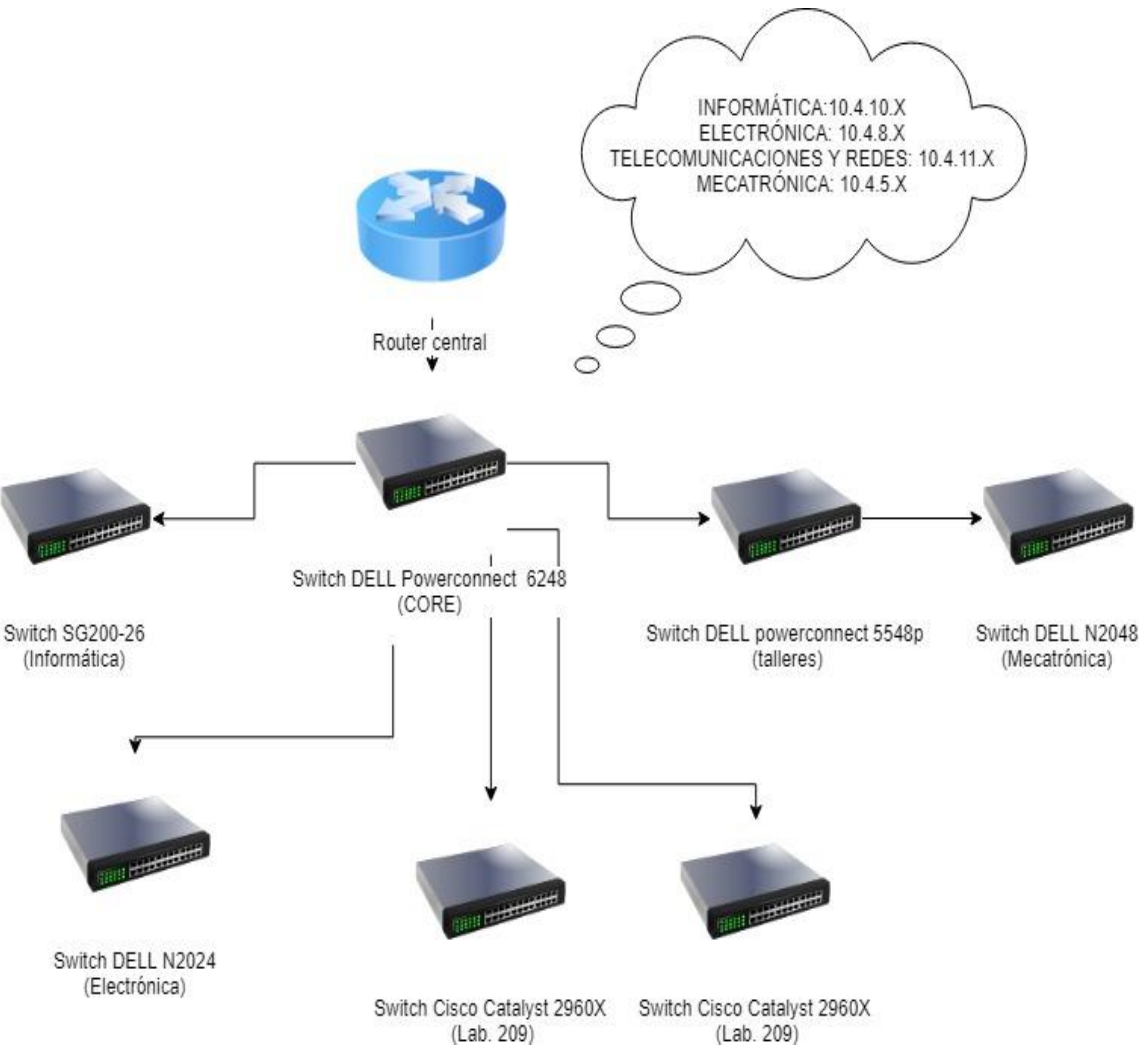


Figura 2-2. Estructura resumida de equipos. Elaboración propia. Extraído de [VERGARA, 2019].

ESPACIOS DEPARTAMENTO	IP	VLAN
INFORMÁTICA	10.4.10.X	21
TELECOMUNICACIONES Y REDES	10.4.11.X	21
ELECTRÓNICA	10.4.8.X	18
MECATRÓNICA	10.4.5.X	15

Tabla 2-1. Resumen de red UTFSM. Elaboración propia. Extraído de [VERGARA, 2019].

2. SITUACIÓN ACTUAL UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA SEDE CONCEPCIÓN

En el siguiente punto se dará a conocer de manera general los enlaces establecidos para el departamento y de cómo es el funcionamiento de la sede hoy en día por medio de diagramas y tablas que indiquen equipos y espacios del departamento de electrónica e informática.

2.1. ENLACE PRINCIPAL

Uno de los aspectos más importantes en el desarrollo de este proyecto es la red principal actual de la universidad, esta cuenta con dos enlaces trabajando en conjunto en la sede Concepción.

Un enlace es con la empresa GTD TELEDUCTOS S.A. la cual tiene un contrato vigente desde el 1 de marzo de 2018 y el otro enlace con contrato es CLARO que se asigna en un espacio en la conexión general de la universidad.

A partir de un esquema realizado podremos ver que la seguridad de la red es bastante vulnerable ya que no contamos con un firewall necesario para la protección de la red en nuestra sede. Cabe señalar que cada enlace cuenta con velocidades de conexión las cuales son 2 Gbps en conexión local y 1 Gbps en conexión a reuna que conecta y comunica entre universidades, centros de formación superiores, etc. las cuales nos solo

estarían en territorio nacional, sino que también está presente en servidores que se encuentran internacionalmente conectados.

La sala de datos principal es gestionada por la UTI que aloja los equipos de comunicaciones principales para la conexión hacia toda la universidad. En esto podemos decir que la estructura de red actual está operativamente funcionando a excepciones de algunos problemas que se podrían ir desarrollando a medida de las observaciones hechas en el lugar. Cabe señalar que en varios sectores de la universidad se cuenta con equipos AP (Access point) los que otorgan conexiones inalámbricas, generando distintas redes y rangos para el trabajo de funcionarios, profesores, alumnos, visitas y otras subredes que actualmente se trabajan en la sede, como por ejemplo la red reuna que admite conexiones internacionales que adquieren una mejor conectividad a lo largo del país y de manera segura.

2.2. EQUIPOS DE LA RED INTERNA DEL DEPARTAMENTO

La red interna de nuestra universidad cuenta con varios equipos capaces de ser configurados a partir de rangos de IP, VLAN y otros tipos de configuraciones capaces de administrar distintas redes y subredes de la sede, pero sin embargo hay otro tipo de problemas en los cuales encontramos equipos que no son capaces de poder dar administración segura a los distintos laboratorios establecidos en la universidad es por ello que se nombraran los equipos que son administrables y no administrables para establecer así una propuesta a futuro para la mejora e implementación de estos equipos de comunicaciones, a continuación se nombraran de manera resumida los distintos equipos que dan conexión al departamento.

2.2.1. Switches Administrables

MODELO	MARCA	SOPORTE	N° PUERTO S	TIPOS DE ENLACE	UBICACIÓN	N° EQUIPOS
Catalyst 3850	CISCO	10/100/1000	24	Fibra Óptica	Sala de datos	1
SF300	CISCO	10/100	24	UTP	Lab. 209	8
Catalyst 2960X	CISCO	10/100/1000	24	Fibra Óptica	Lab. 209	2
PowerCon nect 6248	DELL	10/100/1000	48	UTP	Sala de datos	1
SG200	CISCO	10/100/1000	24	Fibra Óptica	Sala enlace informática	3
N2048	DELL	10/100/1000	48	UTP	Mecatrónica	1
N2024	DELL	10/100/1000	24	Fibra Óptica	Lab. electrónica	1
SG200	CISCO	10/100/1000	48	UTP	Sala informática	3
Catalyst 3560	CISCO	10/100/1000	24	UTP	Sala de datos	1

Tabla 2-2 . Switches Administrables. Elaboración propia. Extraído de [VERGARA, 2019].

2.2.2. Switches no Administrables

MODELO	MARCA	SOPORTE	N° DE PUERTOS	TIPOS DE ENLACE	UBICACIÓN	CANTIDAD
DES-1024D	D-LINK	10/100	24	UTP	Mecatrónica	8

Tabla 2-3. Switches no Administrables. Elaboración propia. Extraído de [VERGARA, 2019].

Los equipos señalados anteriormente no cumplen con los requisitos ya sea por configuración o no posee características adecuadas para ser administrados de manera fácil y segura por lo que un plan de trabajo como el cambio de equipos sería ideal para

garantizar una mejora en la seguridad y conectividad de la intranet. Por lo que también se podrían configurar más subredes las cuales permiten conectar más equipos y se trabaje de forma más concisa en los laboratorios.

2.3. MAPA DE ESPACIOS FÍSICOS DENTRO DE LA SEDE

Considerando que los espacios en los que se encuentran los distintos equipos de comunicaciones son variados y establecidos a lo largo de toda la sede. Se podrán observar a continuación por un mapa de emplazamiento de la universidad señalando la ubicación generalizada de todos los espacios del departamento con los cuales se trabaja en conjunto por medio de equipos de comunicaciones para dar conexión a las áreas de trabajo.

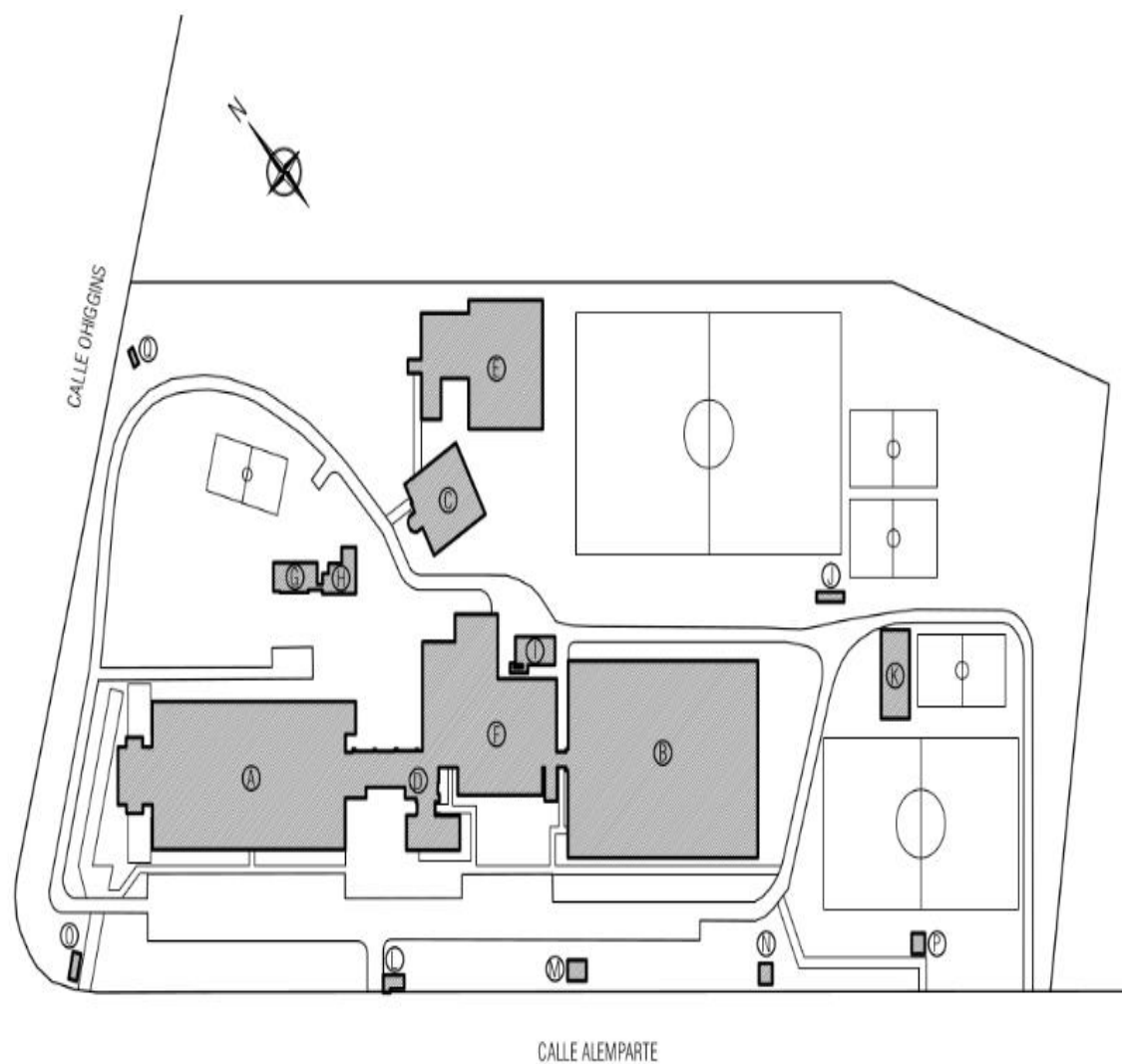


Figura 2-3 . Mapa de emplazamiento. Extraído de [PLANIMETRÍA USM SEDE CONCEPCIÓN, 2019]

ESPACIOS FÍSICOS	SECTOR	PISO
INFORMÁTICA	A	1
ELECTRÓNICA	B	1
MECATRÓNICA	B	1 y 2
TELECOMUNICACIONES Y REDES	A	2

Tabla 2-4. Resumen espacios sede Concepción. Elaboración propia. Extraído de [VERGARA, 2019].

2.4. ANÁLISIS DE ESPACIOS DEL DEPARTAMENTO

La inseguridad de la red es un análisis de los espacios establecidos dentro de la universidad, pues se ve afectada en gran parte por los laboratorios de mecatrónica, que en efecto son los que cuentan con una red menos segura comparados con los laboratorios de informática. Los equipos administrables son configurados para su correcto funcionamiento, otorgando VLAN y rangos de IP para los distintos espacios, funcionarios y alumnos, en cambio los equipos no administrables solo se rigen por un enlace troncal no configurado para dar conexión directa a dispositivos conectados.

El laboratorio 209 de la carrera de telecomunicaciones y redes al igual que los laboratorios de informática utiliza equipos administrables los cuales utilizando una

máquina virtual configurada con un servidor de nateo que trabaja segmentando las redes de los equipos, servidores y switches, verificando un orden que permita incluirlo en los demás espacios del departamento y a futuro dentro de los espacios completos de la universidad.

Mecatrónica en cambio tiene un sistema débil que no admite estas configuraciones lo cual implica un trabajo mediocre en sus equipos que si bien están conectados a la red de la universidad no logran administrar sus propias redes.

3. SEGURIDAD EN LA RED EN CONTEXTO DE CIBERSEGURIDAD

Para hablar de seguridad en la red de la universidad primero hay que ver varios aspectos que abordan este tema en ámbitos de conexión y ciberseguridad en las que la universidad claramente presenta falencias y en ese sentido investigar la base que es sumamente importante para determinar posibles mejoras a futuro o la implementación de equipamiento actualizado para el desarrollo seguro de las actividades en línea.

3.1. ¿QUE ES CIBERSEGURIDAD?

La ciberseguridad se define como la capa de protección para los archivos de información, que, a partir de ella, se trabaja para evitar cualquier tipo de amenaza, las cuales ponen en riesgo la información de todo tipo de empresas.

Para determinar el estado de seguridad se trabaja con sistemas robustos capaces de actuar antes, durante y después, esto no solo sirve para prevenir, sino también para poder darle confianza a los clientes en cualquier tipo de empresa pudiendo así reducir el riesgo de exposición del usuario y de los sistemas.

3.2. FORMAS DE MEJORAR LA SEGURIDAD

Existen distintos métodos de mejorar la seguridad, una de ellas es adquirir software de detección de intrusos o malwares que es imprescindible para cualquier organización. Estos programas ayudan a tener un mejor control en los sistemas y resguardar la información que es una de las cosas más importantes para los usuarios. Se tiene que tener en cuenta que los programas o softwares deben mantenerse siempre actualizados ya que gracias a esto buscan vulnerabilidades nuevas que vayan adquiriendo los malwares o virus de internet.

Una segunda opción de mejora es contar con gente capacitada que pueda otorgar los conocimientos necesarios a sus usuarios para la navegación segura en la red, para evitar el conocido phishing o fraude informático que hoy en día es el más conocido por la mayoría de las organizaciones ya que consta de vulnerar al usuario en específico vía mails o links de páginas fraudulentas lo que causa la pérdida de información confidencial de cualquier organización.

La tercera herramienta es ser preventivo en cualquier sistema, con la idea de siempre tener respaldo de la información en otros dispositivos externos o guardar estos datos en nubes de almacenamiento que permitan recuperar cierta información en casos de vulnerabilidades mayores.

Por último y no menos importante es la protección de comunicaciones que se basa prácticamente en proteger a una organización de cualquier grupo de amenazas, por ejemplo, un ataque de denegación de servicios, accesos no autorizados o la interceptación de las comunicaciones. También se debe considerar que las amenazas no solo vienen de internet, si no, también desde la misma organización por lo que es importante tener este tipo de seguridad cuando existen conexiones entre varias sedes u oficinas en varias partes del mundo o de un país.

3.3. FORMAS DE MEJORA DE SEGURIDAD EN SEDE CONCEPCIÓN

Para un mejor control en la seguridad de la universidad se determinan varios aspectos, uno de ellos es investigar los casos más comunes de vulneraciones, principalmente casos específicos que ocurren a funcionarios, profesores o alumnos.

Como la investigación se realizó a lo largo del pasado semestre se consideraron las siguientes causas:

- Correos con información delicada enviada en bandeja de spam por virus.
- Links de mail engañosos a funcionarios de la universidad (phishing).
- Malwares en equipos por falta de actualización de antivirus.
- Error de actualizaciones en equipos con Windows 10.

Las soluciones a todas estas problemáticas fueron resueltas meticulosamente, esto mediante la organización generada por la UTI, que realizó cada una de las solicitudes, de esta manera se observaron distintas situaciones permitiendo así el estudio de cada uno de estas.

En primer lugar los correos enviados por funcionarios a empresas para solicitar cotizaciones u otro tipo de servicios, son claramente necesarios, pero generan vulneraciones importantes a los equipos por lo que si no se cuenta con un buen antivirus o las actualizaciones de Windows necesarias es posible que se vea afectado de manera importante y genere ese tipo de acciones en los correos electrónicos, también está la posibilidad de que archivos enviados entre sí por estas organizaciones contengan archivos infectados y sean perjudiciales. Al tener archivos ya infectados estos se pueden propagar por la universidad mediante correos si es que no se tiene el cuidado de mantener las actualizaciones y una mantención al día de los equipos.

En segundo lugar, los correos engañosos o el tan conocido phishing es algo muy relacionado en cómo interactúa el usuario con la navegación en internet por lo cual estos engaños son responsabilidad de las personas que visitan páginas no confiables o entran a links de mails engañosos causando una entrega de datos ya sea IP, tarjetas de crédito, información personal, etc. Esto hace muy difícil la recuperación de los datos perdidos por lo que sería necesario bloquear cuentas o tarjetas las cuales se haya vinculado en algún momento para la compra online.

En tercer lugar, los responsables de fallas en los equipos son virus, malwares, etc. que son capaces de enviar sin necesidad de hacer clic, páginas malintencionadas que llevan al punto número 2 (phishing) por ello sin no se tienen las últimas versiones de los antivirus instalados sería muy difícil detectar posibles cambios que generan estos agentes malintencionados.

Por último, contar con equipos no actualizados puede causar grandes problemas de seguridad incluso provenientes de los mismos fabricantes en el caso de la universidad se opta por la recuperación de la información en los ordenadores afectados y un plan de trabajo que incorporó formatear con programas como clonezilla de manera más rápida y bloquear todas las actualizaciones con problemas, para permitir futuras versiones que implementen mejor soporte de software.

4. PROPUESTA MEJORAMIENTO DE LA RED INTERNA PARA EL DEPARTAMENTO DE ELECTRÓNICA E INFORMÁTICA

A fin de establecer un mejoramiento en la calidad y el funcionamiento de la red se tuvo que decretar una evaluación, la cual permitiera el mejor planteamiento del departamento con sus respectivos rangos de IP, VLAN, equipos y espacios. Con el objetivo de crear una intranet segura y de calidad para los distintos laboratorios y salas, en especial los laboratorios de mecatrónica, en los cuales los equipos de comunicaciones establecidos no tienen la capacidad de tener configuraciones administrables causando serios problemas de seguridad.

4.1. PROPUESTA DE ESTRUCTURA SEDE CONCEPCIÓN

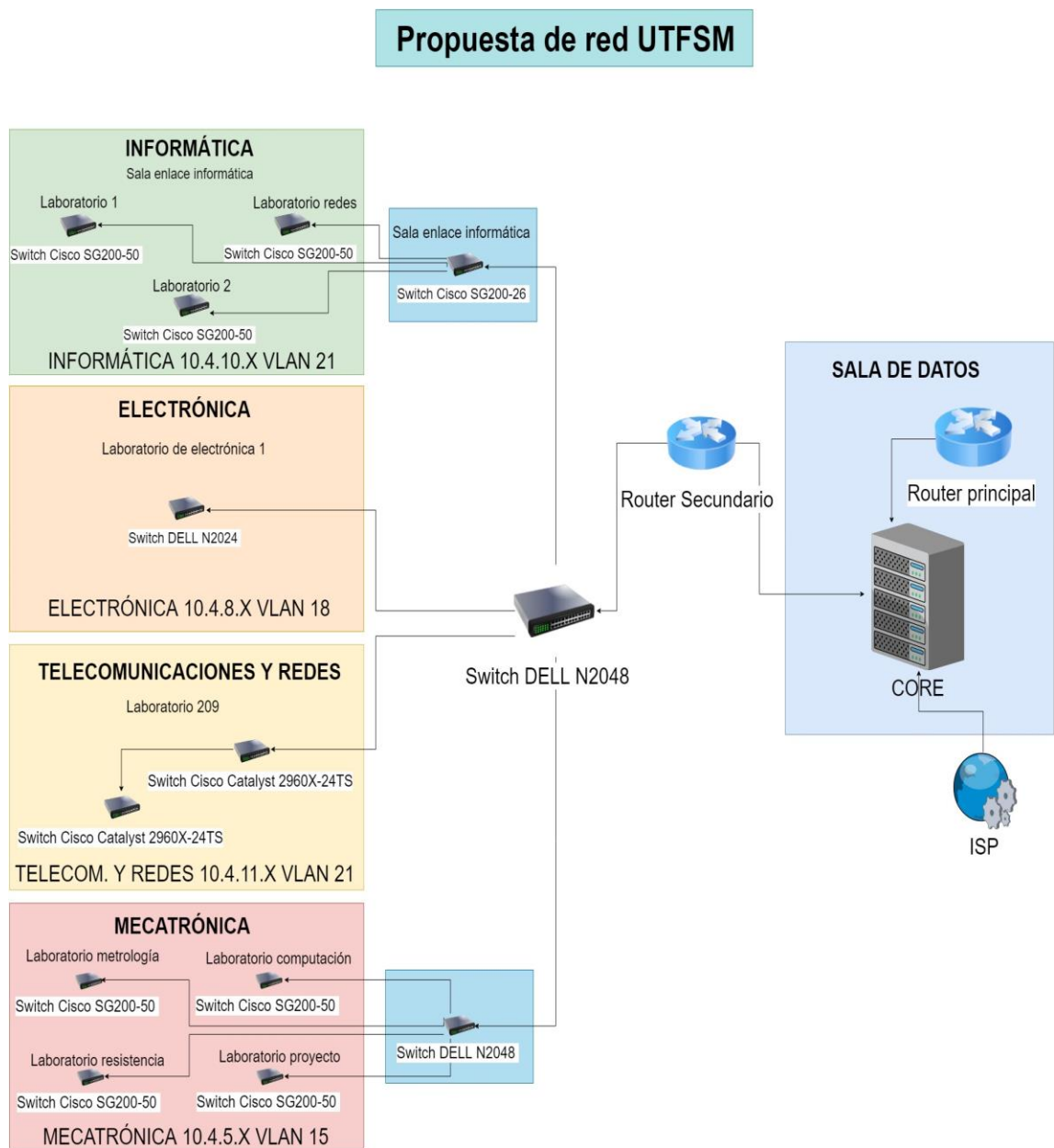


Figura 2-4 . Propuesta de red UTFSM. Elaboración propia (2019)

La idea de esta propuesta es generar una nueva estructura de red capaz de soportar diversas subredes especialmente en sectores donde la conexión es deficiente o los equipos no tienen las características necesarias para realizar dichas funciones de configuración, esto se da especialmente en el caso de mecatrónica que posee diversos equipos de comunicaciones no administrables, los cuales causan un efecto negativo en la conectividad y seguridad del departamento.

Este esquema busca la mejor alternativa de conexión para el departamento incluyendo equipos, rangos y otras medidas que puedan ser beneficiosas para los espacios con los equipos actuales establecidos.

La estructura de red se basa una intranet más segura para el departamento de electrónica e informática incluyendo nuevos equipos administrables para los laboratorios de mecatrónica y generando una red en conjunto con la UTI que sea administrada por la carrera de telecomunicaciones y redes.

El diagrama consta de diversos enlaces que son capaces de generar comunicación entre sí por medio de equipamiento apto de capa 3.

La idea de la estructura señalada es tener un router secundario actuando de forma conjunta con el router actual y generar una difusión para el departamento de electrónica e informática que se encargaría de los enlaces y mantener un orden en las VLAN y rangos de IP en laboratorios, salas, oficinas.

CONCLUSIONES

Se puede concluir que gracias a una minuciosa investigación se determinó las diversas falencias que afectan a la conexión y seguridad de la sede, principalmente al departamento de electrónica e informática. Se concretaron planes de trabajo en la búsqueda de la información de cada espacio y equipos con los cuales se trabaja. Todos estos datos fueron adquiridos con anterioridad por la UTI y por los encargados de cada departamento.

Gracias a la información conseguida se pudieron determinar las configuraciones de red, enlaces, equipos y espacios del departamento lo que permite la elaboración de un sistema cuyo propósito fue el mejoramiento de la seguridad y conectividad de forma que se administra de mejor manera la intranet del departamento.

Finalmente se permite implementar la idea de la estructura realizada de forma futura para el departamento y que incluya mejoras a lo largo del tiempo, teniendo en cuenta los diversos cambios de equipos y espacios que se asignen parcialmente en la sede.

BIBLIOGRAFÍA

1. CISCO. Cisco SG200-26 26-port Gigabit Smart Switch. [en línea]. <<https://www.cisco.com/c/en/us/support/switches/sg200-26-26-port-gigabit-smart-switch/model.html>>. [consulta: 2 de Julio de 2019].
2. CISCO. Cisco SG200-50P 50-port Gigabit PoE Smart Switch. [en línea]. <<https://www.cisco.com/c/en/us/support/switches/sg200-50p-50-port-gigabit-poe-smart-switch/model.html>>. [consulta: 2 de Julio de 2019].
3. CISCO. Cisco Catalyst 3850-24P-S Switch. [en línea]. <https://www.cisco.com/c/es_mx/support/switches/catalyst-3850-24p-s-switch/model.html>. [consulta: 3 de Julio de 2019].
4. CISCO. Cisco SF300-24P 24-Port 10/100 PoE Managed Switch with Gigabit Uplinks. [en línea]. <https://www.cisco.com/c/es_mx/support/switches/sf300-24p-24-port-10-100-poe-managed-switch-gigabit-uplinks/model.html>. [consulta: 3 de Julio de 2019].
5. CISCO. Cisco Catalyst 2960X-24TS-LL Switch. [en línea]. <https://www.cisco.com/c/es_mx/support/switches/catalyst-2960x-24ts-ll-switch/model.html#~tab-documents>. [consulta: 3 de Julio de 2019].
6. CISCO. Cisco Catalyst 3560G-24TS Switch. [en línea]. <<https://www.cisco.com/c/en/us/support/switches/catalyst-3560g-24ts-switch/model.html>>. [consulta: 6 de Julio de 2019].
7. CRESPO, Adrián. VLANs: Qué son, tipos y para qué sirven. [en línea]. <<https://www.redeszone.net/2016/11/29/vlans-que-son-tipos-y-para-que-sirven/>>. [consulta: 13 junio de 2019].
8. DEI. Wiki Departamento Electrónica e Informática. [en línea]. <<https://wiki.dei.usm.cl>>. [consulta: 15 de agosto de 2019].
9. DELL. PowerConnect 6248. [en línea]. <https://www1.la.dell.com/la/es/corp/Empresarial/pwcnt_6248/pd.aspx?refid=pwcnt_6248&s=corp>. [consulta: 6 de Julio de 2019].
10. DELL. Servidor en rack PowerEdge R540. [en línea]. <<https://www.dell.com/cl/empresas/p/poweredge-r540/pd>>. [consulta: 10 de Julio de 2019]

11. DELL. PowerConnect 5548P Switch. [en línea]. <<https://www.dell.com/en-us/work/shop/cty/powerconnect-5548p-switch/spd/powerconnect-5548p>>. [consulta: 10 de Julio de 2019].
12. D-LINK. Switch 24 Puertos 10/100Mbps no Gestionable DES-1024D. [en línea]. <<https://eu.dlink.com/es/es/products/des-1024d-24-port-10-100mbps-desktop-switch>>. [consulta: 12 Julio de 2019].
13. DOMINGUEZ, Antonio. ¿Qué es el Routing?. [en línea]. <<https://openwebinars.net/blog/que-es-el-routing/>>. [consulta: 27 mayo de 2019].
14. ECURED.CU. Enciclopedia Colaborativa Cubana. [en línea]. <https://www.ecured.cu/Topolog%C3%ADa_de_red>. [consulta: 10 junio de 2019].
15. GTD TELEDUCTOS S.A. y UTFSM. CONTRATO DE PRESTACIÓN DE SERVICIOS. [Documento]. Santiago, Chile. 2018. 21 Hojas. Contrato N° 17-7555.
16. OBS Business School. ¿Qué es ciberseguridad y de qué fases consta? [en línea]. <<https://www.obs-edu.com/int/blog-investigacion/sistemas/que-es-ciberseguridad-y-de-que-fases-consta>>. [consulta: 27 mayo de 2019].
17. Oficina de Seguridad del Internauta [OSI]. ¿Qué son los ataques DoS y DDoS?. [en línea]. <<https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos>>. [consulta: 17 agosto de 2019].
18. PEREZ, Alonso. NAT. [en línea]. <<http://www.ajpdsoft.com/modules.php?name=Encyclopedia&op=content&tid=790>>. [consulta: 14 junio de 2019].
19. PLANIMETRÍA USM SEDE CONCEPCIÓN. Diego Alejandro Toro Silva. Sin escala, blanco y negro, plano de emplazamiento. Hualpén 2018.
20. SOLANO, José. El modelo OSI. [en línea]. <http://dis.um.es/~lopezquesada/documentos/IES_1213/LMSGI/curso/xhtmll/xhtmll22/index.html>. [consulta: 17 de abril de 2019].
21. VENEGAS, Guillermo y SALAZAR, Graciela. Que es un Firewall y cómo funciona. Tipos de firewall. [en línea]. <<https://tecnologia-informatica.com/que-es-firewall-como-funciona-tipos-firewall/>>. [consulta: 13 junio de 2019].

22. VENEGAS, Guillermo y SALAZAR, Graciela. ¿Qué es una Intranet? ¿Para qué sirve? Intranet y empresa. [en línea]. <<https://tecnologia-informatica.com/que-es-una-intranet/>>. [consulta: 13 junio de 2019].
23. VERGARA, Tharsis. UTFSM. (Entrevista Personal). Hualpén. 2019.
24. WINEX. Segmentación y Direccionamiento IP. [en línea]. <<http://www.winex.com.py/2017/03/05/segmentacion-y-direccionamiento-ip/>>. [consulta: 21 de mayo de 2019].

ANEXO

ANEXO 1: CONVENIO DE LA UNIVERSIDAD CON GTD

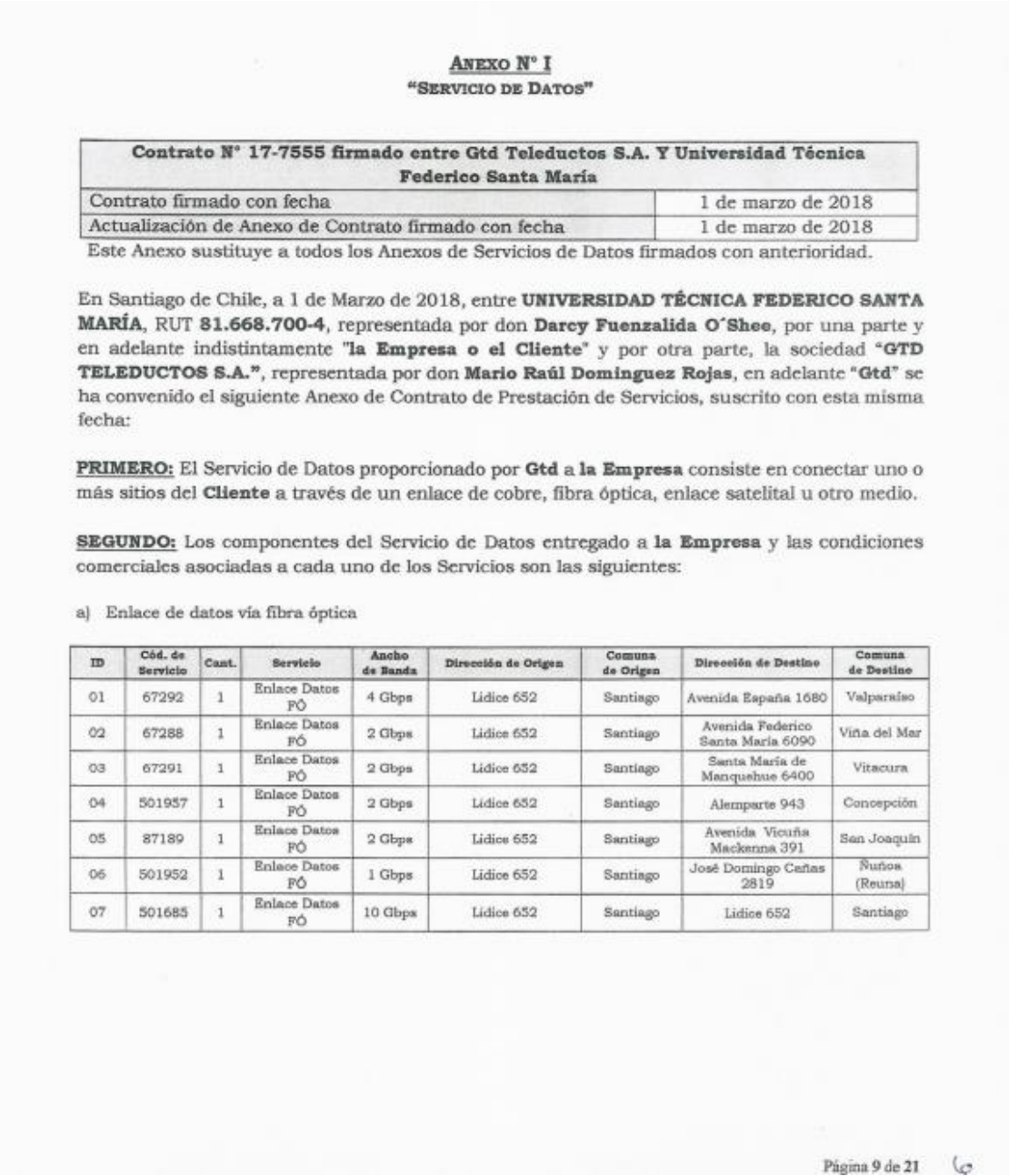


Figura 2-5. Servicio de datos. Extraído de [GTD TELEDUCTOS S.A. y UTFSM, 2018].

b) Equipos

ID	Cód. de Servicio	Cant.	Equipo	Dirección de Instalación	Comuna
01	501632	1	Switch Cisco 3850	Avenida España 1680	Valparaíso
02	501631	1	Switch Cisco 3850	Avenida Federico Santa María 6090	Vina del Mar
03	501629	1	Switch Cisco 3850	Santa María de Manquehue 6400	Vitacura
04	501959	1	Switch Cisco 3850	Alemparte 943	Concepción
05	501624	1	Switch Cisco 3850	Avenida Vicuña Mackenna 3919	San Joaquín
06	501956	1	Switch Cisco 3850	José Domingo Cañas 2819	Ñuñoa
07	501947	2	Switch Cisco 3850	Lidice 652	Santiago
08	501940	3	Switch Cisco 2960	Lidice 652	Santiago

TERCERO: Las condiciones comerciales generales asociadas al Servicio de Datos contratado por la Empresa son las siguientes:

Valor Habilitación	Renta Mensual Total
Sin Costo	270 UF + IVA
Plazo de Instalación del servicio	60 días
Plazo de contratación del servicio	36 meses
Fecha de inicio	1 de abril de 2018

Gtd se compromete a mantener una disponibilidad del Servicio contratado del 99,5% del tiempo Anual. Por lo que Gtd se obliga a solucionar cualquier falla dentro de un tiempo máximo de 4 horas en Santiago y 6 horas en regiones. Las interrupciones debido a causas no fortuitas en el Servicio para los que aplica un compromiso de disponibilidad, podrán ser sujeto de descuentos en la renta mensual detallada según la siguiente tabla:

Tiempo mensual máximo acumulado de interrupción de los servicios contratados	Porcentaje descuento a renta mensual del servicio afectado
0 a 3,6 horas	0%
3,61 a 10 horas	10%
10.01 a 24 horas	20%
24 horas o más	100%

Nota: La compensación será evaluada por la degradación y/o indisponibilidad, de acuerdo a la renta del servicio afectado y no por la totalidad del contrato.

CUARTO: La Empresa no podrá manipular, intervenir ni alterar el equipamiento instalado de dominio de Gtd, individualizados en la cláusula segunda del presente Anexo, quedándole expresamente prohibido modificar la configuración de los mismos, siendo la Empresa la responsable del uso, custodia y conservación de los equipos, hasta la restitución de los mismos a Gtd, en el mismo estado en que los recibió, teniendo en consideración el desgaste natural de

Figura 2-6. Servicio de datos página 2. Extraído de [GTD TELEDUCTOS S.A. y UTFSM, 2018].

los equipos, producto del uso a que tuvo derecho la **Empresa** durante la vigencia del presente contrato.

QUINTO: Se faculta al portador de copia del presente instrumento firmada por las partes contratantes, para requerir todo lo que en derecho corresponda en conjunto con el contrato principal.

Previa lectura, se ratifican y firman.

 MARIO RAÚL DOMÍNGUEZ ROJAS GTD TELEDUCTOS S.A.	 DARCY FUENZALIDA O'SHEE UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
--	--



Figura 2-7. Servicio de datos página 3. Extraído de [GTD TELEDUCTOS S.A. y UTFSM, 2018].

ANEXO N° II
"SERVICIO DE INTERNET"

Contrato N° 17-7555 Firmado Entre Gtd Teleductos S.A. y Universidad Técnica Federico Santa María	
Contrato firmado con fecha	1 de marzo de 2018
Actualización de Anexo de Contrato firmado con fecha	1 de marzo de 2018

Este Anexo sustituye a todos los Anexos de Servicios de Internet firmados con anterioridad.

En Santiago de Chile, a 1 de marzo de 2018, **UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA**, RUT **81.668.700-4**, representada por don **Darcy Fuenzalida O'Shee**, por una parte y en adelante indistintamente **"la Empresa o el Cliente"** y por otra parte, la sociedad **"GTD TELEDUCTOS S.A."**, representada por don **Mario Raúl Domínguez Rojas**, en adelante **"Gtd"** se ha convenido el siguiente Anexo de Contrato de Prestación de Servicios, suscrito con esta misma fecha:

PRIMERO: El Servicio de Internet proporcionado por **Gtd** a **la Empresa** consiste en brindar acceso a internet a través de enlaces de fibra óptica, cobre, u otro medio, con dos anchos de banda, uno nacional y otro internacional. Adicional al acceso a internet, **Gtd** puede brindar una serie de servicios adicionales como webhosting, correo electrónico, arriendo de direcciones IP, entre otros.

SEGUNDO: Los componentes y condiciones comerciales del Servicio de Internet entregado a **la Empresa** son las siguientes:

a) Servicios de Internet:

Tipo de Servicio	Descripción de Servicio	
ID	01	
Servicio de Acceso Dedicado	Código de Servicio: 501922	
	Acceso dedicado mediante un enlace FO de Gtd	
	Servicio instalado en:	
	Calle: Lidice 652	
	Comuna: Santiago	
	Plan de Acceso Dedicado: Empresa	
	Servicio entregado mediante enlace de Red IP en FO, con equipo terminal de red con interfaz ethernet y puerta con conector RJ-45	
	Ancho de Banda Internet Nacional	2 Gbps
	Ancho de Banda Internet Internacional	1 Gbps
	Garantía Ancho de Banda Acceso Nacional	Asegurado 1:1
Garantía Ancho de Banda Acceso Internacional	Asegurado 1:1	
8 Direcciones IP v4 válidas asociadas al servicio dedicado		
1 Bloque /48 IP v6 (65.536 subredes) asociada al servicio dedicado		
1 Switch Cisco 3850		

Gtd se compromete a mantener una disponibilidad del Servicio contratado del 99,8% del tiempo Anual. Por lo que **Gtd** se obliga a solucionar cualquier falla dentro de un tiempo máximo de 4 horas en Santiago y 6 horas en regiones. Las interrupciones debido a causas no fortuitas en el

Figura 2-8. Servicio de internet. Extraído de [GTD TELEDUCTOS S.A. y UTFSM, 2018].

Servicio para los que aplica un compromiso de disponibilidad, podrán ser sujeto de descuentos en la renta mensual detallada según la siguiente tabla:

Tiempo mensual máximo acumulado de interrupción de los servicios contratados	Porcentaje descuento a renta mensual del servicio afectado
0 a 3,6 horas	0%
3,61 a 10 horas	10%
10.01 a 24 horas	20%
24 horas o más	100%

Nota: La compensación será evaluada por la degradación y/o indisponibilidad, de acuerdo a la renta del servicio afectado y no por la totalidad del contrato

TERCERO: Las condiciones comerciales asociadas a los servicios contratados por la Empresa e individualizados en este anexo son las siguientes:

Valor Habilitación	Renta Mensual Total
Sin Costo	200 UF + IVA
Plazo de Instalación del servicio	30 días
Plazo de contratación del servicio	36 meses
Fecha de inicio	1 de marzo de 2018

La fecha de inicio de la vigencia del Plazo Mínimo de Contratación, para cada servicio, comenzará a regir cuando éstos se encuentren operativos.

CUARTO: Gtd no se hace responsable en ningún caso de la pérdida de información contenida en los servidores del usuario, provocada por manejos realizados por la Empresa en la administración y mantención de los programas y aplicaciones de su propiedad, así como daños o perjuicios que pudieren resultar de la utilización inadecuada de la red, o daños que pudieren ocurrir respecto de los datos de la Empresa por parte de otros usuarios de Internet o por parte de terceros.

QUINTO: La Empresa deberá velar por que los servicios contratados sean utilizados adecuadamente y ella será completamente responsable de las consecuencias que tenga la utilización de dichos servicios.

En caso que la Empresa sea denunciada por terceros por el ejercicio de malas prácticas, como por ejemplo, el envío de correos masivos (SPAM), la suplantación de identidad para un sitio web (phishing) o cualquier otra actividad dolosa que ponga en riesgo la integridad de los recursos dispuestos como parte de los servicios contratados, Gtd estará facultada desde ya primeramente para suspender en forma temporal el suministro de los servicios contratados hasta que se aclare el problema suscitado, y si ello persiste, regirá lo dispuesto en la cláusula décima del contrato principal.

En el caso específico del ejercicio de prácticas de envío de correo masivo (SPAM) y por ese motivo quedaran las direcciones IP asociadas a los servicios contratados bloqueadas en listas negras

Figura 2-9. Servicio de internet página 2. Extraído de [GTD TELEDUCTOS S.A. y UTFSM, 2018].

públicas confeccionadas por organismos responsables, tanto nacionales como internacionales, como por ejemplo SpamCop o Spamhaus, **la Empresa** será la única responsable de esta situación, siendo responsable también de gestionar el proceso de remoción de las direcciones IP desde las listas negras en las que se encuentren bloqueadas, debiendo asumir también de su cargo, en caso que existan, los costos que tenga el proceso de remoción.

SEXTO: **La Empresa** declara conocer íntegramente las implicaciones de la utilización de Internet, y libera y exime expresamente a **Gtd** de toda responsabilidad directa o indirecta, presente o futura que pudiese ocurrir a causa o consecuencia de infracciones a la ley de propiedad intelectual o derecho de autor N° 17.336 y sus modificaciones presentes y futuras como asimismo a los tratados, acuerdos o convenciones internacionales sobre propiedad intelectual que Chile haya suscrito y reconocido como ley de la República; como también deberá observar las disposiciones legales y aquellas normas internacionales que emanen sobre lo mismo, que se dicten o acuerden con posterioridad a la suscripción del presente contrato. La exención de responsabilidad de **Gtd** comprende cualquier acción u omisión de terceros respecto de las cuales, **Gtd.** y sus proveedores carezcan de autoridad para impedir que se cometan actos que pudieren causar daños o perjuicios a los usuarios de la red.

SÉPTIMO: En ningún caso **Gtd** garantiza la posibilidad de uso o la disponibilidad de acceso a los diferentes servicios existentes en Internet, acceso que será de entera responsabilidad de los proveedores de cada uno de dichos servicios. **Gtd** no asume ninguna responsabilidad por los contenidos, su origen o destino, o el uso de las comunicaciones de todo tipo, recibidas o enviadas mediante Internet.

Debido a que gran parte de los servicios y sistemas que componen la Red Internet dependen de terceras personas, **Gtd** no se responsabiliza de las variaciones de velocidad de transmisión que pudieran apreciarse al acceder a los distintos servidores que componen la Red.

OCTAVO: **Gtd** no asume responsabilidad alguna al prestar servicios a **la Empresa** respecto de las siguientes situaciones.

- a) Veracidad de la información que **la Empresa** obtenga a través de Internet
- b) Daños o perjuicios que pudieren resultar por la utilización de la red o daños que pudieren ocurrir respecto de los datos de **la Empresa** por parte de otros usuarios de Internet.

NOVENO: Se faculta al portador de copia del presente instrumento firmada por las partes contratantes, para requerir todo lo que en derecho corresponda en conjunto con el contrato principal.

Prevía lectura, se ratifican y firman.


MARIO RAÚL DOMÍNGUEZ ROJAS
GTD TELEDUCTOS S.A.



DARCY FUENZALIDA O'SHEE
UNIVERSIDAD TÉCNICA FEDERICO
SANTA MARÍA

Página 14 de 21 

Figura 2-10. Servicio de internet página 3. Extraído de [GTD TELEDUCTOS S.A. y UTFSM, 2018].

ANEXO N° III
"SERVICIO DE DATA CENTER"

Contrato N° 17-7555 firmado entre Gtd Teleductos S.A. y Universidad Técnica Federico Santa María	
Contrato firmado con fecha	1 de marzo de 2018
Actualización de Anexo de Contrato firmado con fecha	1 de marzo de 2018

Este Anexo sustituye a todos los Anexos de Servicios de Data Center firmados con anterioridad.

En Santiago de Chile, a 1 de marzo de 2018, **UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA**, RUT **81.668.700-4**, representada por don **Darcy Fuenzalida O’Shee**, por una parte y en adelante indistintamente **"la Empresa o el Cliente"** y por otra parte, la sociedad **"GTD TELEDUCTOS S.A."**, representada por don **Mario Raúl Domínguez Rojas**, en adelante **"Gtd"** se ha convenido el siguiente Anexo de Contrato de Prestación de Servicios, suscrito con esta misma fecha:

PRIMERO: El Servicio de Data Center proporcionado por **Gtd a la Empresa** consiste en el alojamiento de equipos, tales como servidores, equipos de red, entre otros, en el edificio Lídice II ubicado en Calle Lídice #652, comuna de Santiago.
Este edificio cuenta con la Certificación Tier III en Diseño y Construcción, la cual es adjudicada por la organización Uptime Institute.

SEGUNDO: Los componentes y condiciones comerciales del Servicio de Data Center entregado a **la Empresa** son las siguientes:

Tipo de Servicio	Descripción de Servicio		Valor Instalación UF + IVA	Valor Renta Mensual UF + IVA
Servicio de Housing	Modalidad de Housing	Alojamiento en 2 Rack Cerrado Exclusivo instalado en Lídice 652 Cada rack dispone de 44U útiles (1U = 4,3 cm)	Sin Costo	90
	Propiedad del Equipamiento	El equipamiento detallado anteriormente es de propiedad de Universidad Técnica Federico Santa María		
	Propiedad del licenciamiento de software	El software y su licenciamiento utilizado en el equipamiento detallado anteriormente es de propiedad de Universidad Técnica Federico Santa María		
	Administración de Equipamiento	El equipamiento detallado anteriormente será administrado Por Universidad Técnica Federico Santa María		
	Otros Servicios			
Consumo Eléctrico Housing	Habilitación de dos circuitos eléctricos Bus A de 32 Amperes con 1 bloque de 20 enchufes C-13 por Bus.		Sin Costo	Sin Costo
	Instalación en Lídice 652, Data Center Gtd			

Figura 2-11. Servicio de data center. Extraído de [GTD TELEDUCTOS S.A. y UTFSM, 2018].

Descripción Consumo Eléctrico	Rango Consumo	Valor UF/mes
Energía Base (Valor variable mensual, en función del consumo promedio de todos los circuitos asociados al rack del cliente)	0 - 5 KW	4,3 UF + IVA
Sobreconsumo	Mayor a 5 KW	13,6 UF + IVA

Nota: La Renta Mensual asociada al servicio de energía eléctrica, considerada por KW consumido, se reajustará semestralmente, en función de las variaciones que experimente la tarifa cobrada por el proveedor de energía.

TERCERO: El resumen de las condiciones comerciales asociadas al Servicio de Data Center contratado por la **Empresa** son las siguientes:

Valor Habilitación	Renta Mensual Total
Sin Costo	90 UF + IVA
Plazo de instalación del servicio	30 días
Plazo de contratación del servicio	36 meses
Fecha de inicio	1 de abril de 2018

CUARTO: Gtd se obliga a proporcionar a la **Empresa** lo siguiente:

- a) Seguridad: Física, eléctrica y ambiental. Acceso controlado con personal de guardia 7x24, tarjetas de aproximación para cada recinto crítico, y alojamiento del equipamiento de la **Empresa** en racks o gabinetes especialmente diseñados con este fin.
- b) Climatización: Ambiente adecuado para la operación del equipamiento de la **Empresa**, mediante equipos de climatización precisa en configuración N+1.
- c) Energía: Sistema de respaldo UPS y distribución de energía respaldada y redundante en configuración 2N.
- d) Conectividad: Rutas y proveedores respaldados, tanto en enlaces de datos como enlaces a Internet,
- e) Incendios: Sistemas de detección temprana de incendios con tecnología Láser y sistema de extinción automática y con extintores de CO2.
- f) Servicio de Soporte en modalidad 7 x 24.

QUINTO: La **Empresa** por su parte, en relación con los servicios contratados de Data Center se obliga a lo siguiente:

- a) A respetar íntegramente la normativa del Reglamento de Data Center Grupo **Gtd**, el cual forma parte integral de este contrato.
- b) A respetar el horario que fije **Gtd** para el acceso al Data Center, el horario que se fije de permanencia dentro de él, como también el número de personas, y condiciones comerciales en caso de requerir trabajos en horarios especiales.
- c) A avisar oportunamente por escrito sus cambios de domicilio para recibir avisos y notificaciones que le deba efectuar **Gtd**.
- d) En el evento de que la **Empresa** deba cambiar de domicilio o físicamente a otro lugar, primeramente éste nuevo lugar o domicilio debe ser factible para que **Gtd** pueda trasladar e

Figura 2-12. Servicio de data center página 2. Extraído de [GTD TELEDUCTOS S.A. y UTFSM, 2018].