



INGENIERÍA EN REDES Y TELECOMUNICACIONES

PROYECTO DE GRADO

**DISEÑO DE UN SISTEMA DE CONTROL
DE ACCESO Y ACTIVOS PARA LOS
LABORATORIOS DE COMPUTACIÓN DE
LA UNIVERSIDAD PRIVADA DOMINGO
SAVIO**

Luis Alberto Carballo Sánchez

**Proyecto de grado para optar al grado de licenciatura en
Ingeniería en Redes y Telecomunicaciones**

Tarija-Bolivia

2019

AGRADECIMIENTO

A mi madre, porque gracias a su trabajo y paciencia pude culminar esta etapa de mi formación académica.

Al tutor de mi proyecto, por ser un guía de este trabajo tanto como de mi formación personal además de apoyarme en los momentos más difíciles.

A mis amigos en general, por haberme dado tantos buenos recuerdos que me ayudaron a seguir adelante.

DEDICATORIA

Dedico este trabajo a mi madre por el apoyo que me brindó a través de los años, su amor incondicional y la confianza que tiene en mí, que es fundamental para seguir formándome como humano y profesional.

TITULO: DISEÑO DE UN SISTEMA DE CONTROL DE ACCESO Y ACTIVOS PARA LOS LABORATORIOS DE COMPUTACIÓN DE LA UNIVERSIDAD PRIVADA DOMINGO SAVIO

AUTOR: Luis Alberto Carballo Sanchez

RESUMEN

Este trabajo tiene como objetivo investigar dos problemas importantes que tienen los laboratorios de computación de la Universidad Privada Domingo Savio.

El primero, es el acceso libre que tienen las personas a los laboratorios de computación, como no existe un control sobre quien entra y sale de los mismos esto puede dar origen a muchos percances dentro de los laboratorios de computación, el segundo problema tiene que ver con fortalecer la seguridad dentro de los laboratorios de computación, aunque no fueron demasiados los robos de equipos, es importante resguardar todos los activos dentro de los laboratorios de computación ya que varios tienen precios elevados.

Dado que existen varios sistemas de control de acceso, para determinar la mejor solución se comparará varios de los mismos para ver cual se ajusta mejor a las necesidades de los laboratorios de computación de la universidad.

En el desarrollo de este trabajo se puede ver a la tecnología RFID (identificación por radiofrecuencia) como una de las mejores opciones para el control de acceso.

CARRERA: INGENIERÍA EN REDES Y TELECOMUNICACIONES

PROFESOR GUÍA: GONZALO TARIFA RODRIGUEZ

DESCRIPTORES O TEMAS: Sistema de control de acceso

PERIODO DE INVESTIGACIÓN: 90 días

E-MAIL DEL AUTOR: lcarballo56@gmail.com

ÍNDICE GENERAL

CAPÍTULO I : INTRODUCCIÓN

1.1. ANTECEDENTES	1
1.2. DELIMITACIÓN	3
1.2.1. Límite Sustantivo.....	3
1.2.2. Límite Espacial.....	3
1.2.3. Límite Temporal	3
1.3. PLANTEAMIENTO DEL PROBLEMA.....	4
1.4. FORMULACION DEL PROBLEMA.....	4
1.5. SISTEMATIZACIÓN DEL PROBLEMA Y SOLUCIÓN.....	5
1.6. OBJETIVOS.....	6
1.6.1. Objetivo General	6
1.6.2. Objetivos Específicos	6
1.7. JUSTIFICACIÓN.....	7
1.7.1. Científico – Tecnológica	7
1.7.2. Socio – Económica	7
1.7.3. Metodológica.....	7
1.8. METODOLOGÍA	8
1.8.1. Descriptiva	8
1.8.4. Población, muestra y muestreo	8
1.8.5. Fuentes de información.....	8

CAPÍTULO II: MARCO TEÓRICO

2.1. DEFINICION DE RED DATOS	9
2.2. CLASIFICACIÓN DE LAS REDES.....	10
2.2.1. Redes LAN.....	10
2.2.2. Redes MAN.....	11
2.2.3. Redes WAN	12
2.3. TOPOLOGÍAS DE RED.....	13
2.3.1. Red en Estrella.....	13
2.4. COMPONENTES DE UNA RED DE DATOS	14
2.4.1. Servidores (Hardware)	14
2.4.2. Router	15
2.4.3. Switch.....	16
2.4.4. Adaptadores de Red (Tarjetas de Red).....	17
2.4.5. Puestos de Trabajo (Terminales)	18
2.4.6. Firewall.....	19
2.5. MEDIOS DE TRANSMISIÓN	19
2.5.1. Medios Guiados de Cobre.....	20
2.5.2. Par Trenzado	20
2.5.2.1. Cable UTP	20
2.5.2.2. Cable STP	21
2.5.2.3. Categorías.....	22
2.6. ARQUITECTURA DE RED DE DATOS.....	23
2.7. DISEÑO JERÁRQUICO DE RED CISCO.....	24

2.7.1. Capa de Acceso	25
2.7.2. Capa de Distribución	25
2.7.3. Capa de Núcleo	26
2.8. REQUISITOS DE LA RED	27
2.9. PRINCIPIOS DE INGENIERÍA ESTRUCTURADA.....	27
2.10. IEEE 802.1Q	28
2.11. VLAN	28
2.12. CONTROL DE ACCESO	29
2.12.1. Control de Acceso Basado en Algo que Usted Conoce	29
2.12.2. Control de Acceso Basado en Algo que Usted Tiene	30
2.12.3. Control de Acceso Basado en Algo que Usted es.....	31
2.13. TECNOLOGÍAS PARA CONTROL DE ACCESO	32
2.13.1. Código de Barras	32
2.13.2. Tarjetas Magnéticas.....	33
2.13.3. Sistemas biométricos	34
2.13.4. Acceso con Tarjetas de RFID (Identificación por Radiofrecuencia)	35
2.13.5. Acceso con Memorias de Contacto.....	36
2.14. CONCEPTOS BASICOS DE RFID	37
2.15. APLICACIONES RFID.....	37
2.16. ARQUITECTURA DE UN SISTEMA MEDIANTE RFID.....	39
2.16.1. Funcionamiento de un Sistema RFID	42
2.16.2. Etiquetas RFID.....	43
2.16.2.1 Etiquetas Activas	44

2.16.2.2. Etiquetas Pasivas	45
2.16.2.3. Etiquetas Semipasivas	45
2.16.3. Etiquetas de Lectura y Escritura	46
2.16.4. Frecuencia de Velocidades de Transmisión.....	46
2.16.5. Lector/Escritor de Tarjetas RFID.....	47
2.16.6. Componentes de Software RFID	49
2.16.6.1. Software de Sistemas RFID	49
2.16.6.2. RFID Middleware.....	50
2.16.6.3. Aplicación de Computador	51
2.16.7. Estándares	53
2.16.7.1. ISO	53
2.16.7.1.1. ISO/IEC 14443	53
2.16.7.2. EPC	53
2.16.7.3. ONS.....	54
2.16.7.4. EPC GEN 2	54
2.16.7.4.1. Capa Física EPC GEN 2	55
2.16.7.4.2. Capa de Identificación de Etiquetas de EPC GEN 2.....	56
2.16.8. Otros Estándares RFID	58
2.16.9. Métodos de Conexión para Administración de Dispositivos RFID	58
2.16.10. Seguridad en Sistemas RFID	59
2.16.11. Espectro Electromagnético	62

2.16.11.1. Rango del Espectro Electromagnético	62
--	----

CAPÍTULO III: INGENIERÍA DE PROYECTO

3.1. FASE DE PREPARACIÓN 67

3.1.1. Descripción de la Situación Actual	67
---	----

3.1.2. Disposición Tecnológica de los Laboratorios de Computación	68
---	----

3.1.3. Factores de Riesgo Tecnológico	68
---	----

3.2. FASE DE PLANIFICACIÓN..... 69

3.2.1. Datos Técnicos de la Red de Datos de los Laboratorios de Computación..	69
---	----

3.2.1.1. Equipos de Red	70
-------------------------------	----

3.2.1.2. Capas del Modelo de Red Jerárquico de Cisco	70
--	----

3.2.1.3. Equipos de Computación	71
---------------------------------------	----

3.2.1.4. Descripción de Conexiones Lógicas	71
--	----

3.2.1.5. Descripción de Conexiones Físicas	71
--	----

3.2.1.6. Direccionamiento IP	72
------------------------------------	----

3.2.1.7. Topología Lógica Actual de la Red de Datos	73
---	----

3.2.2. Sistema de Cámaras IP Interlogix	74
---	----

3.2.2.1. Software TruVision Navigator	74
---	----

3.2.2.2. Video Grabadora en Red TruVision NVR 22	75
--	----

3.2.2.3. Cámara IP TruVision Turret IR	75
--	----

3.2.2.4. Topología Lógica de la Red de Vigilancia	76
---	----

3.2.2.5. Direcciones IP de las Cámaras de Vigilancia	76
--	----

3.2.3. Comparativa de Tecnologías de Control de Acceso	77
3.2.3.1. Tecnologías de Control de Acceso.....	77
3.2.3.2. Factores de Comparación de Tecnologías de Control de Acceso..	77
3.2.3.3. Análisis de Comparativa de Tecnologías de Control de Acceso	79
3.2.4. Fabricantes de Sistemas de Control de Acceso RFID	83
3.2.4.1. SUPREMA.....	83
3.2.4.1.1. Ventajas	83
3.2.4.1.2. Desventajas	83
3.2.4.1.3. Modelo de Arquitectura de Sistema de Control de Acceso SUPREMA	84
3.2.4.2. INTERLOGIX.....	84
3.2.4.2.1. Ventajas	84
3.2.4.2.2. Desventajas	85
3.2.4.2.3. Modelo de Arquitectura de sistemas de Control de Acceso INTERLOGIX	85
3.2.4.3. ZKTEKO	86
3.2.4.3.1. Ventajas	86
3.2.4.3.2. Desventajas	86
3.2.4.3.3. Modelo de Arquitectura de Sistema de Control de Acceso ZKTEKO.....	86
3.2.5. Selección del Fabricante	87

3.3. Fase de Diseño	88
3.3.1. Topología lógica del sistema RFID	88
3.3.1.1. Topología Lógica de Sistema de Control de Acceso y Activos.....	89
3.3.1.2. Proceso Logístico de Funcionamiento de Sistema de Control de Acceso y Activos RFID	90
3.3.1.3. Proceso de Autenticación de Usuarios y Resguardo de Activos	91
3.3.1.4. Descripción del Equipamiento a Utilizar	92
3.3.2. Integración del Sistema de Control de Acceso y Activos a la Red de Laboratorios de Computación	93
3.3.2.2. Nueva Red de los Laboratorios de Computación	95
3.3.3. Costos de la Implementacion del Sistema de Control de Acceso y Activos	95
3.4. FASE DE OPERACIÓN	97
3.4.1. Software BIO STAR 2.	97
3.4.2. Base de Datos.....	99
 CAPÍTULO IV: CONCLUSIONES Y RECOMENDACIONES	
4.1. CONCLUSIONES	101
4.2. RECOMENDACIONES.....	102
 BIBLIOGRAFIA	
 ANEXOS	

INDICE DE IMÁGENES

FIGURA Nº I.1: ÁRBOL DE PROBLEMAS	5
FIGURA Nº II.1: RED LAN.....	10
FIGURA Nº II.2: RED MAN	11
FIGURA Nº II.3: RED WAN.....	12
FIGURA Nº II.4: TOPOLOGÍA EN ESTRELLA	13
FIGURA Nº II.5: SERVIDOR	14
FIGURA Nº II.6: ROUTER.....	15
FIGURA Nº II.7: SWITCH.....	16
FIGUR A Nº II.8: TARJETA DE RED	17
FIGURA Nº II.9: COMPUTADOR PERSONAL	18
FIGURA Nº II.10: FIREWALL.....	19
FIGURA Nº II.11: CABLE UTP	21
FIGURA Nº II.12: CABLE STP	22
FIGURA Nº II.13: CÓDIGO DE BARRAS.....	32
FIGURA Nº II.14: LECTOR MAGNÉTICO.....	33
FIGURA Nº II. 15: SISTEMA BIOMÉTRICO	34
FIGURA Nº II.16: MEMORIA DE CONTACTO.....	37
FIGURA Nº II.17: ARQUITECTURA DE UN SISTEMA RFID	40
FIGURA Nº II.18: FUNCIONAMIENTO DE UN SISTEMA RFID	43

FIGURA N° II.19: DIAGRAMA LECTOR/ESCRITOR RFID	48
FIGURA N° II.20: DIAGRAMA DE FUNCIONAMIENTO EPC GEN 2	57
FIGURA N° II.21: ESPECTRO ELECTROMAGNÉTICO.....	64
FIGURA N° III.1: TOPOLOGÍA LÓGICA DE LA RED DE LOS LABORATORIOS DE COMPUTACIÓN.....	70
FIGURA N° III.2: TOPOLOGÍA LOGICA ACTUAL DE LA RED DE DATOS DE LOS LABORATORIOS DE COMPUTACIÓN	73
FIGURA N° III.3: SOFTWARE TRUVISION NAVIGATOR	74
FIGURA N° III.4: TRUVISION NVR 22.....	75
FIGURA N° III.5: TRUVISION TURRET IR	75
FIGURA N° III.6: TOPOLOGÍA LÓGICA DE RED DE VIGILANCIA.....	76
FIGURA N° III.7: MODELO DE SISTEMA DE CONTROL DE ACCESO SUPREMA	84
FIGURA N° III.8:MODELO SISTEMA DE CONTROL DE ACCESO INTERLOGIX85	
FIGURA N° III.9: MODELO DE SISTEMA DE CONTROL DE ACCESO ZKTEKO87	
FIGURA N° III.10: TOPOLOGÍA FÍSICA DE SISTEMA DE CONTROL DE ACCESO Y ACTIVOS.....	88
FIGURA N° III.11:TOPOLOGÍA LÓGICA SISTEMA DE CONTROL DE ACCESO Y ACTIVOS RFID.....	89
FIGURA N° III.12: FLUJO DE SISTEMA DE CONTROL DE ACCESO	90
FIGURA N° III.13: NUEVA RED DE LOS LABORATORIOS DE COMPUTACIÓN95	
FIGURA N° III.14: ASISTENTE DE INSTALACIÓN SOFTWARE BIOSTAR 2	97

FIGURA Nº III.15: INTERFAZ PRINCIPAL SOFTWARE BIOSTAR 2	98
FIGURA Nº III.16: INTERFAZ BIOSTAR PARA BUSCAR LECTORES RFID	98
FIGURA Nº III.17: ADMINISTRADOR DE CONFIGURACIÓN DE SERVIDOR SQL	99

ÍNDICE DE TABLAS

TABLA Nº III.1: SWITCHES DE LA CAPA DE ACCESO DE LA RED DE DATOS DE LOS LABORATORIOS DE COMPUTACIÓN	70
TABLA Nº III.2: CANTIDAD DE EQUIPOS DE COMPUTACIÓN EN CADA LABORATORIO DE COMPUTACIÓN.....	71
TABLA Nº III.3: DIRECCIONES IP DE LA RED DE LOS LABORATORIOS DE COMPUTACIÓN	72
TABLA Nº III.4: DIRECCIONES IP DE LAS CÁMARAS DE VIGILANCIA	76
TABLA Nº III.5: FIABILIDAD DE LOS SISTEMAS DE CONTROL DE ACCESO..	79
TABLA Nº III.6: FACILIDAD DE USO DE LOS SISTEMAS DE CONTROL DE ACCESO.....	79
TABLA Nº III.7: ESTABILIDAD DEL MEDIO DE IDENTIFICACIÓN DE LOS SISTEMAS DE CONTROL DE ACCESO	80
TABLA Nº III.8: TIEMPO DE ACCESO DE LOS SISTEMAS DE CONTROL DE ACCESO.....	80
TABLA Nº III.9: MANTENIMIENTO DE LOS SISTEMAS DE CONTROL DE ACCESO.....	81
TABLA Nº III.10: PRECIO DE LOS SISTEMAS DE CONTROL DE ACCESO.....	81

TABLA Nº III.11: COMPARATIVA DE TECNOLOGÍAS DE CONTROL DE ACCESO	82
TABLA Nº III.12: DISPOSITIVOS DE SISTEMA DE CONTROL DE ACCESO.....	92
TABLA Nº III.13: DISEÑO DE RED.....	94
TABLA Nº III.14: RED DE CONTROL DE ACCESO Y CÁMARAS IP	94
TABLA Nº III.15: COSTO DE IMPLEMENTACIÓN	96

CAPÍTULO I

INTRODUCCIÓN

1.1. ANTECEDENTES

En una sociedad que está evolucionando cada vez más hacia la automatización y seguridad, utilizando la tecnología como punta de lanza, los sistemas de control de acceso se hacen cada vez más populares en el día a día, para la gestión de personal o para el control de entrada y salida de personas en áreas restringidas. El control de acceso es la parte principal de la pirámide de criticidad de sistemas de seguridad. Así que la elección de una solución fiable es clave y este tipo de sistemas, surgieron para resolver algunos problemas relacionados con el uso de llaves, cerraduras y cerrojos mecánicos, ya que el uso de la llave metálica convencional, tal y como se la conoce hoy, tiene varios factores negativos para una organización y es de vital importancia tener un control de seguridad respecto a las personas que ingresan a sus instalaciones; es por ello que cada organización debe analizar sus necesidades específicas y determinar el nivel de seguridad que desean; por lo tanto, es necesario crear un plan de seguridad; además, es importante que las instalaciones sean accedidas únicamente por personas autorizadas.

Adquirir un Sistema de Control de Accesos en el cual se tiene un control de accesos de personal y de visitas a las instalaciones, tiene el objetivo de mantener una serie de auditorías de los accesos efectuados por distintas personas en las diferentes instalaciones, utilizando esta información para obtener estadísticas para la empresa. Con dichas estadísticas se puede obtener muchos beneficios para una empresa, ya que, esta información se puede obtener al instante con el objetivo de realizar análisis de diferentes tipos. La seguridad en el acceso a instalaciones privadas gestionadas por las respectivas empresas provee una solución para el control adecuado de las personas que acceden a las instalaciones, aparte que son muchas las empresas que manejan tanto información como materiales muy valiosos que, en el caso de atentar contra estos objetos, generaría un problema de dimensiones mayores a la empresa.

La universidad de Antioquia sede Medellín, fue pionera al ser la primera Universidad que cuenta con un sistema de control de acceso. Fue implementado para agilizar el

ingreso y egreso de los estudiantes con resultados positivos y ahora es referente para otras universidades que deseen implementar un sistema de control de acceso. (tecnoseguro, 2015).

Acorde a (Pitán), en el ingreso a la USAC por el Anillo Periférico y la avenida Petapa, está previsto el ingreso y salida de personas por medio de un sistema digital. En cada acceso habrá molinetes digitales. Los estudiantes tendrían que pasar una especie de gafete en un lector y los visitantes tendrían que registrarse.

Wendy López, Directora General de Administración de la USAC, explicó que no hay un registro de control de ingreso a las instalaciones, entonces es muy difícil brindar condiciones de seguridad.

“Estamos creando la base técnica para controlarlo, no estamos cerrando el campus, no se va a privar el ingreso a nadie. Lo que se quiere únicamente es tener conocimiento de quién nos visita, para poder tener un Campus Universitario más seguro”, explicó Harry Ochaeta, del Departamento de Diseño, Urbanización y Construcciones.

El sistema que tiene previsto implementar la USAC, incluye el sistema de vigilancia y alertar al centro de operaciones si alguien cruza líneas peatonales o si alguna persona se parquea en áreas prohibidas. También se podrán identificar objetos olvidados, grabar placas de carros y detectar rostros. (Prensa Libre, 2019)

Actualmente, la universidad cuenta con 8 laboratorios de computación, por lo que mejorar las políticas de acceso a estos recintos es importante. Lo que se plantea con el presente proyecto, es mejorar la seguridad física de los laboratorios de computación, controlando el ingreso y egreso y, así también, resguardando los activos dentro de los mismos.

Tomando en cuenta el crecimiento de la Universidad Privada Domingo Savio Sede Tarija y el flujo de personas que transitan sus instalaciones a diario, es de vital importancia contar con un sistema de control de acceso a los laboratorios de

computación. La implementación de este Sistema permitirá validar que las personas que ingresan a los laboratorios de computación tengan un vínculo con la Universidad, ya sea en calidad de estudiante, docente, funcionario o visitante.

1.2. DELIMITACIÓN

1.2.1. Límite Sustantivo

El proyecto comprende el diseño de una red de control de acceso perimetral para los laboratorios de computación, que interactúe con un servidor a través de la red local y a su vez funcione en conjunto con las cámaras de seguridad, para conformar un historial de ingreso y egreso del personal de dichos recintos, así también, debe contar con una alarma en caso de posibles atentados contra los activos fijos en los laboratorios de computación dentro de las instalaciones de la Universidad Privada Domingo Savio sede Tarija.

1.2.2. Límite Espacial

El actual proyecto se realizará en el Departamento de Tarija (Bolivia), Provincia Cercado, ciudad de Tarija, dentro de las instalaciones de la Universidad Privada “Domingo Savio”, ubicadas en el Barrio “German Bush”, Av. Los Sauces esq. Fabián Ruiz (-21.536826,-64.741630).

1.2.3. Límite Temporal

El presente proyecto se desarrollará durante la gestión 2019, durante 90 días tomando en cuenta gestiones pasadas para indagar y tomar las respectivas precauciones que conllevara la investigación del problema.

1.3. PLANTEAMIENTO DEL PROBLEMA

El Departamento de Sistemas de la Universidad Privada Domingo Savio Sede Tarija, se encarga de la administración de toda la tecnología inmersa en el Campus Universitario. El personal de soporte técnico se encarga de administrar la infraestructura tecnológica de los ocho laboratorios de computación, ubicados en el tercer y cuarto piso del edificio bloque B.

Considerando el valor económico de los activos alojados en los mencionados ambientes, no existe un control integral; es decir, que la seguridad tanto como la integridad del equipamiento depende únicamente de controles manuales que el personal realiza en diferentes horarios, de acuerdo a los turnos académicos, apoyado en cámaras de seguridad ya que tampoco tienen personal activo vigilando o administrando las cámaras de manera constante. Si bien éste es un método parcialmente efectivo, donde se provee un cierto nivel de seguridad, no completa la integralidad que se requiere para proporcionar un control efectivo, las cámaras por sí solas no pueden obtener información del activo que está siendo sustraído, ni tampoco determinar con precisión el nombre de la persona que ingresa o sale del ambiente en particular.

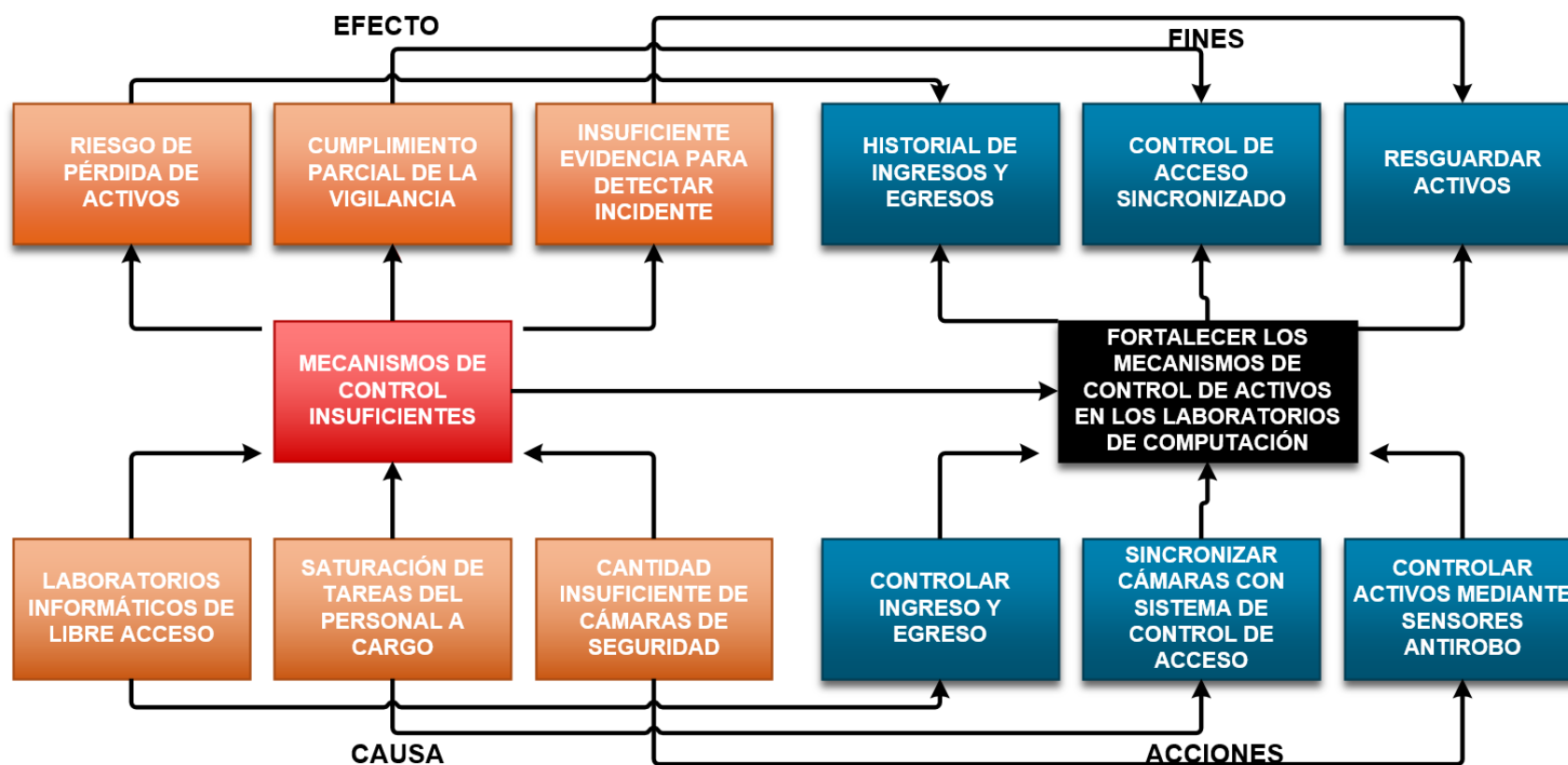
En función a lo anteriormente expuesto y tomando como referencia el riesgo de los activos alojados, se requiere fortalecer los mecanismos de control para proporcionar vigilancia integral efectiva, mediante un sistema de control de acceso y activos que funcionen en conjunto con las cámaras de vigilancia y así mejorar la seguridad en los laboratorios de computación de la Universidad Privada “Domingo Savio”.

1.4. FORMULACION DEL PROBLEMA

Para la investigación del siguiente problema se plantea la pregunta: ¿Cómo puede un sistema de control de acceso y activos, mejorar la seguridad de los laboratorios en la Universidad Privada Domingo Savio, para disminuir el riesgo a la seguridad física del activo tecnológico?

1.5. SISTEMATIZACIÓN DEL PROBLEMA Y SOLUCIÓN

FIGURA Nº I.1: ÁRBOL DE PROBLEMAS



Fuente: Elaboración propia

1.6. OBJETIVOS

1.6.1. Objetivo General

Diseñar un sistema de control de acceso que permita mejorar los mecanismos de control y la seguridad de los laboratorios de computación de la Universidad Privada Domingo Savio Sede Tarija.

1.6.2. Objetivos Específicos

- Realizar un diagnóstico para conocer la situación técnica actual de los laboratorios de computación de la Universidad Privada Domingo Savio.
- Seleccionar la tecnología de control de acceso y diseñar la topología de red del sistema de control de acceso y activos, que más se adecúe a las necesidades de seguridad actuales de la Universidad.
- Determinar el segmento de red que usará la red de controladores del sistema de control de acceso.
- Integrar la red de dispositivos del sistema de control de acceso a la infraestructura actual de red de datos de la universidad.
- Realizar la estimación de costos para la adquisición de los dispositivos que forman parte del sistema de control de acceso y activos.
- Utilizar la metodología de ciclo de vida PPDIO para realizar el diseño del proyecto.

1.7. JUSTIFICACIÓN

1.7.1. Científico – Tecnológica

La finalidad del proyecto es automatizar el apartado de control de acceso para mejorar la seguridad de los laboratorios de computación de la Universidad, no solo con el fin de controlar y asegurar activos; sino, para la entidad en general aplicando la tecnología idónea de acuerdo a las necesidades del Campus Universitario.

1.7.2. Socio – Económica

Se pretende beneficiar a los estudiantes de la universidad al autenticar el acceso a los laboratorios de computación, dado que cualquier persona tiene acceso a los mismos, sin importar si tiene o no relación con la Universidad, para lo que un atentado contra los activos en los laboratorios de computación se podría realizar no solo por parte de estudiantes de la Universidad; sino, de cualquier individuo.

Mediante la implementación del sistema de control de acceso para los laboratorios de computación, la pérdida de activos reduciría al mínimo erradicando los hechos delictivos y así contribuyendo con la seguridad de estos; además, de ser un ahorro significativo en gastos de seguridad al automatizar el control de acceso a dichos recintos.

1.7.3. Metodológica

El análisis de funcionamiento tanto de la Universidad como de los laboratorios de computación es de vital importancia para la implementación de dicho proyecto y así determinar la efectividad del sistema, recolectando datos del área de sistemas y soporte técnico.

1.8. METODOLOGÍA

1.8.1. Descriptiva

La investigación es descriptiva, porque es necesario recopilar información del funcionamiento de los laboratorios de computación analizando la situación actual, para determinar que la tecnología se adhiere mejor al funcionamiento actual de los laboratorios de computación.

1.8.4. Población, muestra y muestreo

Para el presente proyecto se tomará en cuenta como población a la Universidad Privada Domingo Savio sede Tarija, para conocer a fondo el funcionamiento de los laboratorios de computación de la Universidad. La muestra estará compuesta por los laboratorios de computación.

1.8.5. Fuentes de información

Fuentes de Información Primaria – tomando en cuenta al tutor y al plantel de soporte técnico a cargo de los laboratorios de computación de la Universidad, se realizará entrevistas al encargado de soporte técnico que pueda proveer conocimiento sobre el tema en cuestión.

Fuente de Información Secundaria – se hará uso de toda la información disponible en libros y páginas web, como videos de la red o ebooks relacionados con el tema.

CAPÍTULO II

MARCO TEÓRICO

2.1. DEFINICIÓN DE RED DATOS

La fusión de las computadoras y las comunicaciones ha tenido una profunda influencia en cuanto a la manera en que se organizan los sistemas de cómputo. El concepto una vez dominante del “centro de cómputo” como un salón con una gran computadora a la que los usuarios llevaban su trabajo para procesarlo, es ahora totalmente obsoleto (aunque los centros de datos que contienen miles de servidores de Internet se están volviendo comunes).

El viejo modelo de una sola computadora para atender todas las necesidades computacionales de la organización se ha reemplazado por uno en el que un gran número de computadoras separadas pero interconectadas, realizan el trabajo. A estos sistemas se les conoce como redes de computadoras.

La red de datos es un conjunto de computadoras autónomas interconectadas mediante una sola tecnología. Se dice que dos computadoras están interconectadas si pueden intercambiar información. La conexión no necesita ser a través de un cable de cobre; también se puede utilizar fibra óptica, microondas, infrarrojos y satélites de comunicaciones. Las redes pueden ser de muchos tamaños, figuras y formas.

Como resultado del vertiginoso progreso tecnológico, estas áreas están convergiendo con rapidez en el siglo XXI y las diferencias entre recolectar, transportar, almacenar y procesar información, están desapareciendo rápidamente. Las organizaciones con cientos de oficinas esparcidas sobre una amplia área geográfica dan por sentado como algo rutinario la capacidad de examinar el estado actual, aún de su oficina más remota, con sólo presionar un botón. A medida que aumenta nuestra habilidad para recopilar, procesar y distribuir la información, la demanda por un procesamiento aún más complejo de la información aumenta rápidamente. (Tanenbaum & Wetherhall, 2015)

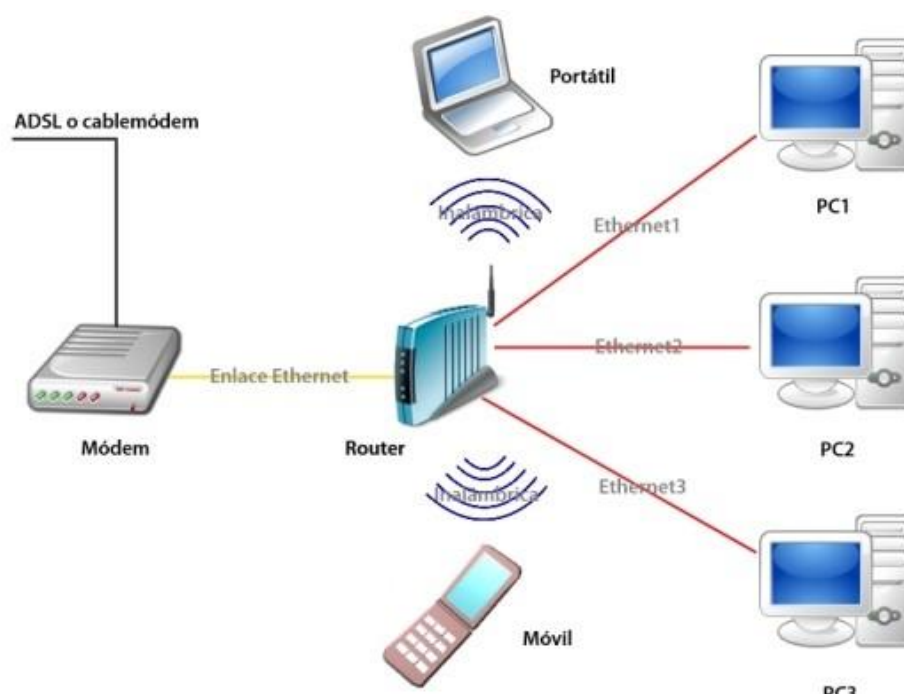
2.2. CLASIFICACIÓN DE LAS REDES

La principal clasificación que se hace actualmente de las redes telemáticas es en función del ámbito o alcance geográfico de la red y en función de este factor se puede distinguir entre tres tipos de redes: LAN, MAN y WAN.

2.2.1. Redes LAN

El término LAN (Local Área Network o red de área local), se aplica a una red de datos cuando los dispositivos unidos en dicha red se encuentran ubicados en un área geográfica limitada. Las distancias entre dispositivos conectados a una red de área local pueden variar entre unos pocos metros hasta varios cientos de metros o incluso kilómetros. En este caso, lo importante es que los equipos conectados pertenezcan a una misma unidad organizativa, por ejemplo, una empresa, institución educativa, organismo público, etc.

FIGURA Nº II.1: RED LAN



Fuente: (www.milcomos.com, s.f.)

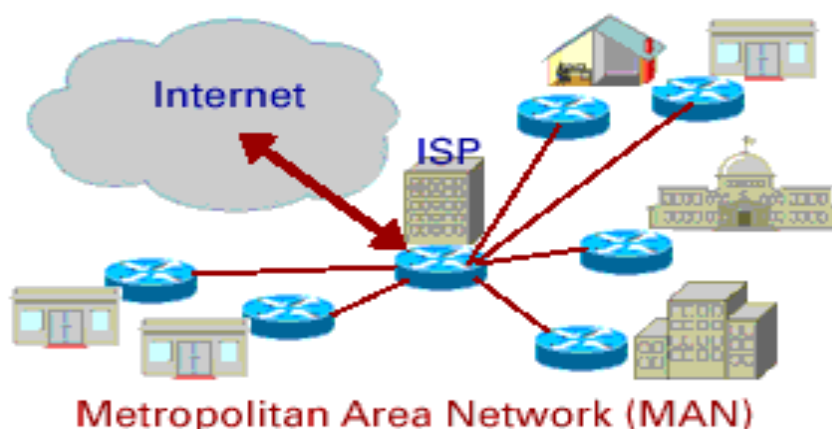
Se han desarrollado tecnologías específicas para implementar este tipo de redes; por ello, otro criterio habitual de identificación de una red LAN es el uso de una tecnología específica para redes LAN. Los estándares actuales de redes LAN son Ethernet y Wi-Fi (González, 2014, págs. 20,21).

2.2.2. Redes MAN

(Montañana, 2015), considera que una MAN abarca una distancia de unas pocas decenas de kilómetros, que es lo que normalmente se entiende como área metropolitana. El término MAN suele utilizarse también en ocasiones para denominar una interconexión de LANs, ubicadas en diferentes recintos geográficos (por ejemplo, diferentes campus) cuando se dan las siguientes circunstancias:

- La interconexión hace uso de enlaces telefónicos de alta o muy alta velocidad (comparable a la de las propias LANs interconectadas).
- La interconexión se efectúa de forma transparente al usuario, que aprecia el conjunto como una única LAN por lo que se refiere a servicios, protocolos y velocidades de transmisión.
- Existe una gestión unificada de toda la red.

FIGURA Nº II.2: RED MAN

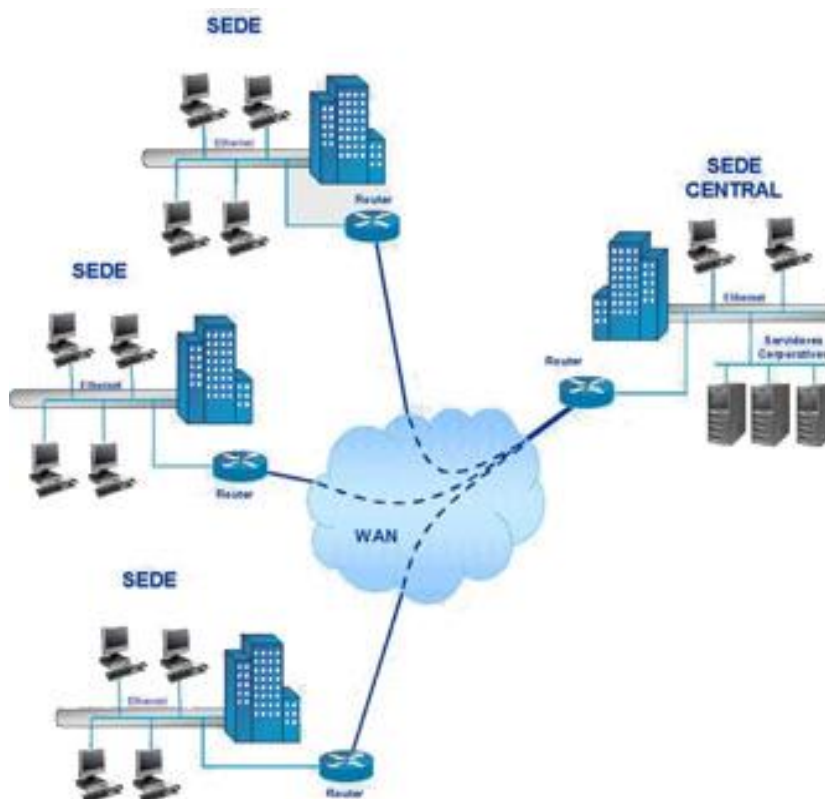


Fuente: (sistemas.com, s.f.)

2.2.3. Redes WAN

Generalmente, se considera como redes de área amplia, a todas aquellas que cubren una extensa área geográfica, requieren atravesar rutas de acceso público y utilizan, al menos parcialmente, circuitos proporcionados por una entidad proveedora de servicios de telecomunicación. Generalmente, una WAN consiste en una serie de dispositivos de conmutación interconectados. La transmisión generada por cualquier dispositivo se encaminará a través de estos nodos internos hasta alcanzar el destino. A estos nodos (incluyendo los situados en los contornos), no les concierne el contenido de los datos; al contrario, su función es proporcionar el servicio de conmutación, necesario para transmitir los datos de nodo en nodo hasta alcanzar su destino final. (Stallings, 2004).

FIGURA Nº II.3: RED WAN



Fuente: (galileo.edu, s.f.)

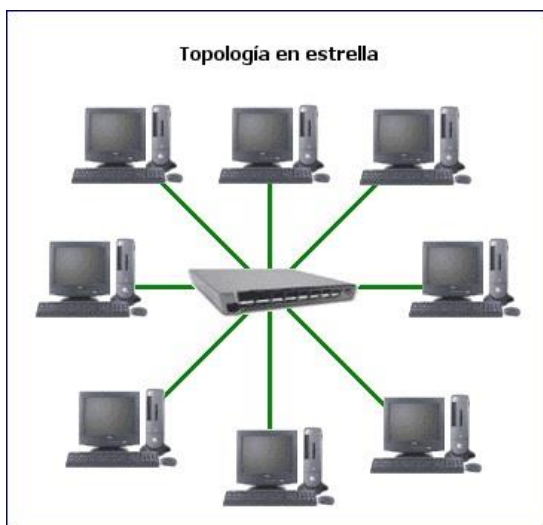
2.3. TOPOLOGÍAS DE RED

Para (González, 2014), en el contexto de las redes de comunicaciones, la topología se refiere a la forma en que está diseñada la red, bien físicamente o bien lógicamente. Dos o más dispositivos se conectan a un enlace. Dos o más enlaces forman una topología. Por tanto, en función de cómo estén conectados los diferentes dispositivos que forman una red, existen varias topologías de las cuales solo se mencionará la que se usará en el proyecto.

2.3.1. Red en Estrella

Son aquellas en las que todos los que acceden a la red, conectan con un punto central. Este elemento central puede ser un ordenador, un concentrador, una central de conmutación, etc. Este equipo permite que a través suyo se puedan comunicar todos los dispositivos conectados. (Viñé, 2000).

FIGURA Nº II.4: TOPOLOGÍA EN ESTRELLA



Fuente: (arquitecturabsicaderedes, s.f.)

2.4. COMPONENTES DE UNA RED DE DATOS

Los principales componentes físicos que forman una red de área local son:

2.4.1. Servidores (Hardware)

Son dispositivos encargados de dar determinados servicios a las demás estaciones o puestos que forman la red. Estos equipos son generalmente ordenadores de alto rendimiento, que garantizan altas velocidades de acceso y seguridad. Los servidores pueden ser dedicados si se utiliza un ordenador exclusivamente para realizar esas funciones, o bien no dedicados (redes de igual a igual), cuando las funciones de servir a otras estaciones de la red las realizan también los equipos de usuario. Esta configuración es común, cuando se trata de redes con pocas estaciones. (Viñé, 2000).

FIGURA Nº II.5: SERVIDOR



Fuente: (gerardoveliz.files.wordpress, s.f.)

2.4.2. Router

Un router es un dispositivo de interconexión utilizado para unir redes y encaminar el tráfico entre ellas. El direccionamiento IP permite disponer de rangos de direcciones asignados a diferentes redes interconectadas entre sí. La arquitectura de la interconexión de redes está basada fundamentalmente en el uso de estos dispositivos.

Uno de los principales usos de los routers, es unir redes de diferentes tecnologías; por ejemplo, los routers que unen una red LAN con una red WAN. El ejemplo más común sería el router que proporcionan los ISP para proporcionar conexión a Internet a sus clientes. Dicho router se encarga de unir la red del cliente (red LAN) con la red del ISP (red WAN). (González, 2014).

FIGURA Nº II.6: ROUTER



Fuente: (redestelematicas, s.f.)

2.4.3. Switch

El switch reemplazó la combinación de hubs y puentes. Puede tener varios puertos, lo que permite ampliar la red fácilmente y su funcionamiento es similar al de un puente. Podría definirse al switch como un puente multipuerto. Para su funcionamiento, se basa en las direcciones MAC, generando una tabla con aquellas que se encuentran conectadas a cada uno de los puertos. Es posible conectar dos o más switches entre sí y cada uno aprenderá del otro sus respectivas tablas de MAC (tablas de conmutación). Al igual que sucede con el puente, para su funcionamiento, el switch se encarga de comparar, de las tramas recibidas, la dirección MAC de destino con su tabla de conmutación, y luego, reenvía las tramas al puerto correspondiente. (Carballeiro, 2014).

FIGURA Nº II.7: SWITCH



Fuente: (ds3comunicaciones, s.f.)

2.4.4. Adaptadores de Red (Tarjetas de Red)

Son componentes que permiten a los puestos de trabajo, conectarse a la red. También se las denomina tarjetas de interfaz de red (NIC, Network Interface Card). Estas tarjetas se instalan en los puestos de trabajo y se conectan al medio de transmisión de la red. Existen distintas tarjetas que se utilizan en función del tipo de red y del cableado utilizado. (Viñé, 2000).

FIGUR A Nº II.8: TARJETA DE RED



Fuente: (startech, s.f.)

2.4.5. Puestos de Trabajo (Terminales)

Son los equipos con los que el usuario accede a la red para poder comunicarse con otros usuarios o con los servidores. Estos equipos normalmente son ordenadores personales (PC), a los que se conecta una tarjeta de red o bien estaciones de trabajo. En cualquiera de los casos, lo normal es que sean equipos con capacidad de proceso. (Viñé, 2000).

FIGURA Nº II.9: COMPUTADOR PERSONAL



Fuente: (vichaunter, s.f.)

2.4.6. Firewall

Si bien el router posee algunas funciones de seguridad, estas son limitadas en comparación con las de un firewall. Este dispositivo examina cada paquete de la red y decide si enviarlo o bloquear su acceso, para permitir solo el tráfico seguro. Es utilizado principalmente en entidades bancarias como complemento para efectuar transacciones. (Carballeiro, 2014).

FIGURA Nº II.10: FIREWALL



Fuente: (CISCO, 2016)

2.5. MEDIOS DE TRANSMISIÓN

Los datos son transportados a través de un material que canaliza la señal que transporta. Es lo que se conoce habitualmente como medios cableados o simplemente cables. Cuando se conecta dos dispositivos mediante un cable, la información viaja de un dispositivo a otro canalizada en dicho cable. Existen dos tipos de señales que se pueden utilizar para transportar datos a través de un medio guiado: las señales eléctricas y las señales ópticas. Cada uno de estos tipos de señales utiliza un material diferente. (González, 2014).

2.5.1. Medios Guiados de Cobre

El cobre es el material que se emplea para transportar señales eléctricas. Sin ninguna duda, es el medio actualmente más utilizado en las redes telemáticas y, en general, en cualquier sistema que necesite transportar señales eléctricas. Sus principales propiedades son:

- Conductividad. El cobre es el mejor conductor de la corriente eléctrica que se conoce.
- Ductilidad o capacidad para dividirse en finos hilos, sin romperse.
- Maleabilidad o facilidad para darle forma.

En las redes telemáticas se utilizan dos tipos de cableado de cobre, el cable de par trenzado y el cable coaxial. (González, 2014).

2.5.2. Par Trenzado

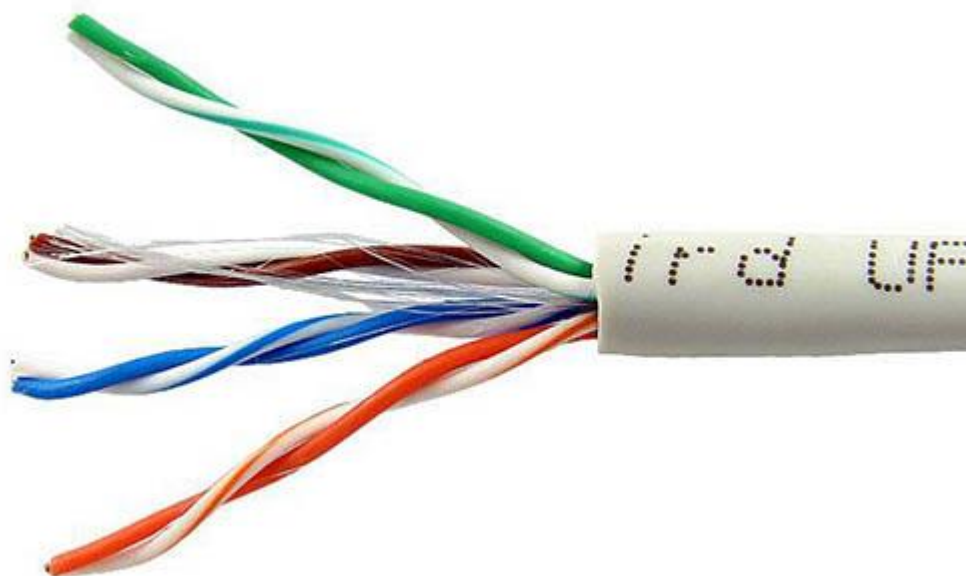
El cable de par trenzado es un elemento importante en las redes. Está formado por dos conductores eléctricos aislados que son entrelazados para anular interferencias externas y además, para transportar la señal en modo diferencial. Un conductor es positivo y el otro negativo, es el medio universal para la conexión de redes cableadas. (Carballeiro, 2014).

2.5.2.1. Cable UTP

El cable UTP (Unshielded Twisted-Pair) o cable de par trenzado sin apantallar, es el medio de transmisión más empleado en redes de área local. La razón principal de su extenso uso es que es el medio cableado más barato para transmitir datos. Es flexible y, por lo tanto, sencillo de instalar (otros tipos de cables son más rígidos y, por lo tanto, más difíciles de manipular). El conector utilizado en este tipo de cable es también barato. Es relativamente ligero y de poco diámetro, las velocidades soportadas se ajustan a las necesidades de la mayor parte de las redes. El cable UTP está formado por cuatro pares trenzados (ocho hilos de cobre), cada uno de los hilos está cubierto por una funda protectora de un color determinado para

identificar su función. Además, todo el conjunto está cubierto por otra funda plástica exterior. (González, 2014).

FIGURA N° II.11: CABLE UTP



Fuente: (tuelectronica, s.f.)

2.5.2.2. Cable STP

El cable STP (Shielded Twisted-Pair) o cable de par trenzado apantallado, es otro tipo de cable de cobre utilizado en redes telemáticas, aunque su uso en la actualidad es más bien escaso. Al igual que el cable UTP, está formado por cuatro pares trenzados y cada par está recubierto de una malla metálica o pantalla, cuya función es reducir el efecto de las interferencias. Además, todo el conjunto lleva otra malla o lámina metálica para aumentar su inmunidad frente al ruido eléctrico y las interferencias. Existe además un tipo de cable STP que solo lleva la lámina metálica exterior; es decir, los pares no van apantallados. La inmunidad que presenta este tipo de cable mejora sus prestaciones; pero, por el contrario, proporciona algunos inconvenientes, como mayor costo y mayor dificultad de instalación.

Hay que tener en cuenta que el blindaje metálico debe estar conectado a tierra, y si esto no se hace correctamente, el efecto puede ser justo el contrario, ya que los blindajes metálicos sin conexión a tierra son muy sensibles a las interferencias. En la práctica, solo es justificable utilizar cable STP en instalaciones con fuerte nivel de interferencias y lo cierto es que en la actualidad muy pocas instalaciones están preparadas para el uso de cables STP y éste apenas se utiliza. (González, 2014).

FIGURA Nº II.12: CABLE STP



Fuente: (iamjurgo, s.f.)

2.5.2.3. Categorías

Los cables utilizados para la transmisión de señales se diferencian en categorías para su uso. A continuación, se comenta sus características:

- **Categoría 5e:** es la versión mejorada de la categoría 5. Se utiliza para velocidades de 100 Mbps y 1 Gbps.
- **Categoría 6:** se usa para velocidades de 1 Gbps. En su interior, incluye un separador plástico, que aísla a cada par trenzado.
- **Categoría 6e:** utilizado para un futuro, en conexiones de hasta 10 Gbps.
- **Categoría 7:** está diseñado para transmitir en 10 Gbps. Es compatible con las categorías 5/5e/6/6e. Se diferencia de los anteriores, porque cada par está aislado y una malla recubre todos los pares, lo que reduce las interferencias que podrían afectarlo.

- **Categoría 8:** soporta frecuencias de hasta 1200 MHz. Es un cable multipropósito; es decir, se lo puede implementar para conexiones de telefonía convencional y para de banda ancha. En su interior posee un alambre de drenaje, que en contacto con la pantalla de aluminio (que se encarga de recubrir a todos los pares), reduce la impedancia. (Carballeiro, 2014).

2.6. ARQUITECTURA DE RED DE DATOS

Las dos arquitecturas de redes más importantes en la actualidad son los protocolos OSI (Open Systems Interconnection) y TCP/IP (Transmission Control Protocol/Internet Protocol).

Conviene destacar que la arquitectura es una entidad abstracta, más general que los protocolos o las implementaciones concretas en que luego se materializan éstos. Típicamente para cada capa de una arquitectura existirán uno o varios protocolos y para cada protocolo habrá múltiples implementaciones. Las implementaciones cambian continuamente; los protocolos ocasionalmente se modifican o aparecen otros nuevos que coexisten con los anteriores o los dejan anticuados; sin embargo, una vez definida una arquitectura, ésta permanece esencialmente intacta y muy raramente se modifica. (Montañana, 2015).

Las funciones básicas de cualquier protocolo son:

- **Detección de errores:** debido a que las líneas de transmisión pueden ser ruidosas y los sistemas de comunicaciones imperfectos, los protocolos han de poder detectar los posibles errores que se produzcan durante el intercambio de datos.
- **Identificación del camino:** puesto que muchas comunicaciones, se multiplexan por la misma vía de comunicación, los protocolos han de tener un mecanismo para identificar los distintos caminos lógicos para poder tratar las comunicaciones separadamente.
- **Control del flujo de la información:** los participantes en una comunicación pueden tener distintas velocidades de procesamiento de la información, por lo

que, si no existe un control alguno de los participantes, se podría llegar a saturar perdiendo datos. Por lo tanto, los protocolos tienen que tener un mecanismo que regule el flujo de la transferencia de información.

- **Codificación del tipo de mensaje:** los datos que viajan entre dos sistemas pueden ser de dos tipos: De información, que se transmiten entre dichos sistemas (la información efectiva) y de control de las comunicaciones. Estos dos tipos de mensajes deberán estar codificados conforme a unos formatos establecidos en cada protocolo. (Viñé, 2000).

2.7. DISEÑO JERÁRQUICO DE RED CISCO

En la tecnología de redes, un diseño jerárquico implica dividir la red en capas independientes. Cada capa (o nivel) en la jerarquía, proporciona funciones específicas que definen su función dentro de la red general. Esto ayuda al diseñador y al arquitecto de red, a optimizar y seleccionar las características, el hardware y el software de red adecuados para llevar a cabo las funciones específicas de esa capa de red.

Un diseño típico de red LAN jerárquica de campus empresarial, incluye las siguientes tres capas:

- **Capa de acceso:** proporciona acceso a la red para los grupos de trabajo y los usuarios.
- **Capa de distribución:** proporciona una conectividad basada en políticas y controla el límite entre las capas de acceso y núcleo.
- **Capa de núcleo:** proporciona un transporte rápido entre los switches de distribución dentro del campus empresarial.

El beneficio de dividir una red plana en bloques más pequeños y fáciles de administrador local. Sólo el tráfico destinado a otras redes se traslada a una capa superior. Los dispositivos de Capa 2 en una red plana, brindan pocas oportunidades de controlar broadcasts o filtrar tráfico no deseado. A medida que se agregan más

dispositivos y aplicaciones a una red plana, los tiempos de respuesta se degradan hasta que la red queda inutilizable. (CISCO, 2016).

2.7.1. Capa de Acceso

En un entorno LAN, la capa de acceso otorga acceso a la red para las terminales. En el entorno WAN, puede proporcionar acceso a la red empresarial para los trabajadores a distancia o los sitios remotos a través de conexiones WAN. La capa de acceso cumple varias funciones, incluido lo siguiente:

- Switching de capa 2.
 - Alta disponibilidad.
 - Seguridad del puerto.
 - Clasificación y marcación de QoS y límites de confianza.
 - Inspección del protocolo de resolución de direcciones (ARP).
 - Listas de control de acceso virtual (VACL).
 - Árbol de expansión.
- (CISCO, 2016)

2.7.2. Capa de Distribución

La capa de distribución agrega los datos recibidos de los switches de la capa de acceso antes de que se transmitan a la capa núcleo para el enrutamiento hacia su destino final. El dispositivo de capa de distribución, es el centro en los armarios de cableado. Para segmentar los grupos de trabajo y aislar los problemas de la red en un entorno de campus, se utiliza un router o un switch multicapa.

Un switch de capa de distribución, puede proporcionar servicios ascendentes para muchos switches de capa de acceso. La capa de distribución puede proporcionar lo siguiente:

- Agregación de enlaces LAN o WAN.

- Seguridad basada en políticas en forma de listas de control de acceso (ACL) y filtrado.
- Servicios de routing entre redes LAN y VLAN, y entre dominios de routing (p.ej., EIGRP a OSPF).
- Redundancia y balanceo de carga.
- Un límite para la agregación y la sumarización de rutas que se configura en las interfaces hacia la capa de núcleo.
- Control del dominio de difusión, ya que ni los routers ni los switches multicapa reenvían difusiones. El dispositivo funciona como punto de demarcación entre los dominios de difusión.

2.7.3. Capa de Núcleo

La capa de núcleo también se conoce como “backbone de red”. La capa de núcleo consta de dispositivos de red de alta velocidad, Estos están diseñados para conmutar paquetes lo más rápido posible e interconectar varios componentes de campus, como módulos de distribución, módulos de servicio, el centro de datos y el perímetro de la WAN.

Algunas de las consideraciones en cuanto a la capa de núcleo incluyen lo siguiente:

- Debe proporcionar switching de alta velocidad; es decir, un transporte rápido.
- Debe proporcionar confiabilidad y tolerancia a fallas.
- Debe lograr la escalabilidad mediante equipos más rápidos, no con más equipos.
- Debe evitar la manipulación de paquetes que implica una gran exigencia para la CPU a causa de la seguridad, la inspección, la clasificación de la calidad de servicio (QoS) u otros procesos. (CISCO, 2016).

2.8. REQUISITOS DE LA RED

Cuando se analiza el diseño de red, es útil categorizar las redes según la cantidad de dispositivos que se atienden:

- **Red pequeña:** proporciona servicios para hasta 200 dispositivos.
- **Red mediana:** proporciona servicios para 200 a 1000 dispositivos.
- **Red grande:** proporciona servicios para más de 1000 dispositivos.

Los diseños de red varían según el tamaño y las necesidades de las organizaciones. (CISCO, 2016).

2.9. PRINCIPIOS DE INGENIERÍA ESTRUCTURADA

Independientemente del tamaño o los requisitos de la red, un factor fundamental para la correcta implementación de cualquier diseño de red es seguir buenos principios de Ingeniería Estructurada. Estos principios incluyen lo siguiente:

- **Jerarquía:** un modelo de red jerárquico es una herramienta útil de alto nivel para diseñar una infraestructura de red confiable. Divide el problema complejo del diseño de red en áreas más pequeñas y más fáciles de administrar.
- **Modularidad:** al separar en módulos las diversas funciones que existen en una red, esta es más fácil diseñar. Cisco identificó varios módulos, incluido el campus empresarial, el bloque de servicios, el centro de datos e internet perimetral.
- **Resistencia:** la red debe estar disponible para que se pueda utilizar tanto en condiciones normales como anormales. Entre las condiciones normales se incluyen los flujos y los patrones de tráfico normales o esperados, así como los eventos programados, como los periodos de mantenimiento. Entre las condiciones anormales se incluyen las fallas de hardware o de software, las cargas de tráfico extremas, los patrones de tráfico poco comunes, los eventos de denegación de servicio (DoS), ya sean intencionales o involuntarios y otros eventos imprevistos.

- **Flexibilidad:** la capacidad de modificar partes de la red, agregar nuevos servicios o aumentar la capacidad sin necesidad de realizar actualizaciones de gran importancia (es decir, reemplazar los principales dispositivos de hardware).

Para cumplir con estos objetivos fundamentales del diseño, la red se debe armar sobre la base de una arquitectura de red jerárquica que permita la flexibilidad y el crecimiento. (CISCO, 2016).

2.10. IEEE 802.1Q

Los enlaces troncales se utilizan para llevar el tráfico que pertenece a los VLAN múltiples entre los dispositivos sobre el mismo enlace. Un dispositivo puede determinar a qué VLAN el tráfico pertenece por su identificador de VLAN. El identificador de VLAN es una etiqueta que se encapsula con los datos, el 802.1Q es la norma IEEE para marcar las tramas con etiqueta en un enlace troncal y soporta hasta 4096 VLANs. En el 802.1Q, el dispositivo troncal inserta una etiqueta 4-byte en la trama original y recalcula la Secuencia de verificación de tramas (FCS) antes de que el dispositivo envíe la trama sobre el link de troncal.

2.11. VLAN

Las VLAN (redes de área local virtuales), pueden considerarse como dominios de difusión lógica. Una VLAN divide los grupos de usuarios de la red de una red física real, en segmentos de redes lógicas. Esta implementación proporciona soporte al estándar de identificación IEEE 802.1Q VLAN, con la posibilidad de permitir que en los adaptadores Ethernet se ejecuten varios ID de VLAN. Cada ID de VLAN está asociado a las capas superiores (IP, etc.) con una interfaz de Ethernet independiente y crea instancias lógicas del adaptador Ethernet para cada VLAN. Por ejemplo, ent1, ent2 y así sucesivamente. El soporte de VLAN IEEE 802.1Q puede configurarse a través de cualquier adaptador Ethernet soportado. Los adaptadores deben conectarse a un conmutador que proporcione soporte a IEEE 802.1Q VLAN.

Es posible configurar varios dispositivos lógicos VLAN en un solo sistema. Cada dispositivo lógico VLAN constituye una instancia adicional del adaptador Ethernet. Estos dispositivos lógicos pueden utilizarse para configurar las mismas interfaces IP de Ethernet que se utilizan con los adaptadores Ethernet físicos. En este caso, el valor ifsize de la opción no (0 por omisión), debe aumentarse para incluir no sólo las interfaces Ethernet para cada adaptador; sino, los dispositivos lógicos VLAN que estén configurados.

2.12. CONTROL DE ACCESO

Según (Tejada, 2012, págs. 18,19), el control de acceso es la habilidad de permitir o denegar el uso de un recurso físico (áreas restringidas según rango del visitante) o virtual (acceso a información) a personas o entidades.

El control de acceso físico está enfocado en tres preguntas: ¿quién?, ¿cuándo? y ¿cómo?, es decir, ¿quién está autorizado a entrar o salir?, ¿cuándo entrar o saldrá del área? y ¿cómo lo realizará?

2.12.1. Control de Acceso basado en algo que Usted conoce

Es el mecanismo de autenticación más popular en la industria y el más barato, por lo que se convierte en la técnica más utilizada en entornos que no precisan de una alta seguridad.

Consiste en decidir si un usuario es quien dice ser, simplemente basándose en una prueba de conocimiento que a priori, sólo ese usuario puede superar. La prueba de conocimiento no es más que una contraseña que en principio es secreta, lo que la hace más vulnerable a todo tipo de ataques, debido a que los usuarios de la misma con el afán de no olvidarla utilizan contraseñas fáciles de recordar como, por ejemplo: la edad, fecha de nacimiento, nombre de sus familiares, etc., lo que las hace predecibles para el atacante. En todos los esquemas de autenticación basados en contraseñas, se cumple el mismo protocolo. Las entidades que participan en la autenticación acuerdan una clave, clave que han de mantener en

secreto si desean que la autenticación sea fiable. Cuando una de las partes desea autenticarse ante otra, se limita a mostrarle su conocimiento de esa clave común y si ésta es correcta, se otorga el acceso a un recurso. Lo habitual es que existan roles preestablecidos, con una entidad activa que desea autenticarse y otra pasiva que admite o rechaza a la anterior. Para incrementar la seguridad en el uso de contraseñas, existen sistemas que utilizan password de una sola vez (One-Time Password). También se utiliza como complemento a otros mecanismos de autenticación. Por ejemplo, en el caso del Número de Identificación Personal (PIN) a la hora de utilizar cajeros automáticos. (Paredes, 2007).

2.12.2. Control de Acceso basado en algo que Usted tiene

Hace más de veinte años, un periodista francés llamado Roland Moreno, patentaba la integración de un procesador en una tarjeta de plástico. Sin duda, no podía imaginar el abanico de aplicaciones de seguridad que ese nuevo dispositivo, denominado chipcard¹³, estaba abriendo. Desde entonces, cientos de millones de esas tarjetas han sido fabricadas y son utilizadas a diario para fines que varían desde las tarjetas monedero más sencillas, hasta el control de accesos a instalaciones militares y agencias de inteligencia de todo el mundo.

Cuando a las chipcards se les incorporó un procesador inteligente, nacieron las smartcards, una gran revolución en el ámbito de la autenticación de usuarios. Cuando el usuario poseedor de una smartcards desea autenticarse, necesita introducir la tarjeta en un hardware lector; los dos dispositivos se identifican entre sí con un protocolo a dos bandas, en el que es necesario que ambos conozcan la misma clave, lo que elimina la posibilidad de utilizar tarjetas de terceros para autenticarse ante el lector de una determinada compañía. (Paredes, 2007).

2.12.3. Control de Acceso basado en algo que Usted es

La biometría, es una tecnología de seguridad basada en el reconocimiento de una característica física e intransferible de las personas. En el siglo XIX, comenzaron las investigaciones científicas acerca de la biometría, con el fin de buscar un sistema de identificación de personas con fines judiciales.

Con estas investigaciones se producen importantes avances y se empieza a utilizar los rasgos morfológicos únicos en cada persona para la identificación. Ya en el siglo XX, la mayoría de los países del mundo utiliza las huellas digitales como sistema práctico y seguro de identificación.

Con el avance tecnológico, nuevos instrumentos aparecen para la obtención y verificación de huellas digitales. Actualmente, la biometría se presenta en un sinnúmero de aplicaciones, demostrando ser el mejor método de identificación humana, debido a que se tienen características morfológicas únicas que nos diferencian, como por ejemplo la forma de la cara, la geometría de partes de nuestro cuerpo como las manos, nuestros ojos y tal vez la más conocida, la huella digital.

Los dispositivos biométricos tienen tres partes principales: por un lado, disponen de un mecanismo automático que lee y captura una imagen digital o analógica de la característica a analizar; además, disponen de una entidad para manejar aspectos como la compresión, almacenamiento o comparación de los datos capturados, con los guardados en una base de datos y; también, ofrecen una interfaz para las aplicaciones que los utilizan. El proceso general de autenticación sigue pasos comunes a todos los modelos de autenticación biométrica:

- Captura o lectura de los datos que el usuario a validar presenta.
- Extracción de ciertas características de la muestra.
- Comparación de estas características con las guardadas en una base de datos.
- Decisión de si el usuario es válido o no.

(Paredes, 2007)

2.13. TECNOLOGÍAS PARA CONTROL DE ACCESO

En la actualidad, se cuenta con una gran variedad de tecnologías que pueden ayudar a suplir esta necesidad, entre las cuales están:

2.13.1. Código de Barras

Los Códigos de Barras son una técnica de codificación gráfica que representa datos en forma de barras y espacios de diferentes dimensiones y representaciones que ha ayudado a los comerciantes en la identificación de productos y precios. Las imágenes son leídas por equipos especiales de lectura óptica, a través de los cuales se puede comunicar información al computador.

La principal ventaja del Código de Barras es que su implementación es muy barata, pues la creación de códigos no es muy compleja y es de fácil aplicación a las tarjetas que contendrán los códigos. Sus desventajas son de gran variedad; pero, las que más priman son: la vulnerabilidad a falsificaciones y los problemas en las lecturas, cuando la superficie se encuentra sucia, borrosa o manchada. Estas razones pueden ser incluso significativas para descartar esta tecnología en sistemas de control de acceso. (Sánchez, 2008).

FIGURA Nº II.13: CÓDIGO DE BARRAS



Fuente: (Tejada, 2012)

El Código de Barras, consiste en un sistema de codificación creado a través de series de líneas y espacios paralelos de distinto grosor. Generalmente se utiliza como sistema de control, ya que facilita la actividad comercial del fabricante y del distribuidor, por lo que no ofrece información al consumidor; sino, datos de operaciones aplicados a identificar productos, llevar control de inventarios, carga y descarga de mercancías, disminuir tiempos de atención en ventas.

2.13.2. Tarjetas Magnéticas

Son tarjetas que contienen una banda magnética que posee un código que permite identificarse rápidamente. Este sistema utiliza señales electromagnéticas para registrar y codificar la información.

Una de las aplicaciones más comunes de esta tecnología, son las tarjetas de crédito. Las tarjetas magnéticas poseen una alta difusión y popularidad; además, son de bajo costo. Sin embargo, su uso continuo las deteriora físicamente, debido a la fricción en el momento de la lectura; también si la tarjeta es acercada a una fuente electromagnética, relativamente fuerte, la información contenida en ella puede ser modificada, con lo cual pierde su utilidad. (Green, 2007).

FIGURA Nº II.14: LECTOR MAGNÉTICO



Fuente: (mitarjeta, s.f.)

2.13.3. Sistemas biométricos

Estos sistemas fundamentan sus decisiones de reconocimiento mediante una característica personal, donde los lectores reconocen automáticamente la característica física de la persona, eliminando por completo el uso de tarjetas electrónicas o magnéticas.

Las principales características físicas que se trabajan en el reconocimiento de las personas son: reconocimiento de iris, reflexión retina, geometría de la mano, geometría facial, termografía mano facial, huellas dactilares y patrón de la voz. La biometría ofrece una ventaja significativa: el alto grado de seguridad, ya que sólo identifica la característica de la persona autorizada; por tanto, es difícil la suplantación de información, ya que los rasgos físicos son únicos e intransferibles. Las desventajas de este sistema son su alto costo de implementación (por los lectores que se manejan para detectar los rasgos de la persona), la reducida velocidad de lectura (comparada con la de otros sistemas) y la carencia de una eficiencia necesaria para grandes corporaciones, pues los retardos en las lecturas de personal, disminuirían tiempos en las labores minorista como dispositivo antirrobo.

FIGURA Nº II. 15: SISTEMA BIOMÉTRICO



Fuente: (grabaseg.jimdo, s.f.)

Este tipo de identificación se realiza a través del análisis y/o medición de características físicas.

Algunas de las técnicas biométricas que existen son:

- Reconocimiento de iris.
- Reflexión retinal.
- Geometría de la mano.
- Termografía mano, facial.
- Huellas dactilares.
- Patrón de voz.

(Sánchez, 2008, págs. 9,10).

2.13.4. Acceso con Tarjetas de RFID (Identificación por Radiofrecuencia)

La tecnología de radiofrecuencia se desarrolló en 1940, como medio para la identificación de los aviones aliados y enemigos durante la Segunda Guerra Mundial.

Años más tarde evolucionó, logrando así ser utilizada en la industria ferroviaria para el seguimiento de los coches del ferrocarril y para los años 60's y 70's, su uso se enfocó en la seguridad de materiales nucleares.

En la actualidad RFID se utiliza principalmente en el rubro de seguridad, como es el caso de los cruces fronterizos, credenciales de identidad, en el control vehicular, identificación de ganado, envío de paquetes, control de equipaje en los aeropuertos y de artículos para renta o préstamo (películas y libros) en videoclubes y bibliotecas, en la industria automotriz, para los procesos de automatización y seguimiento, en el sector agrícola y en el de administración de flora y fauna para rastrear al ganado y a los animales, así como en el mercado. La Tecnología de Identificación por Radiofrecuencia, es un método electrónico que consiste en asignar un código de información a un producto, proceso o persona y usar esta información para identificar o acceder a información adicional al respecto. Los sistemas de

identificación por radiofrecuencia consisten generalmente de dos componentes:

- El “transponder”, que es una pequeña etiqueta electrónica (tag) que contiene un minúsculo microprocesador y una antena de radio. Esta etiqueta contiene un identificador único que puede ser asociado a una persona o producto.
- El “lector”, que obtiene el identificador del “transponder”.

El receptor se puede activar por medio de una batería incorporada (transponder activo) o puede ser alimentado por la señal enviada por el lector (transponder pasivo). El lector genera un campo magnético cuya señal de RF, es captada por el receptor del chip. Éste, a su vez activará al transmisor, el cual enviará un mensaje codificado único. Este mensaje es decodificado por el lector y procesado por la computadora. (Sánchez, 2008).

2.13.5. Acceso con Memorias de Contacto

Los botones de Memoria de Contacto son un tipo específico de tecnología de auto identificación, que requiere un contacto físico con el botón para leer los datos de la etiqueta. La adopción ha sido muy limitada, comparada con la pequeña inversión a realizar y las innovaciones que ha habido en esta área.

La Memoria de Contacto, no ha tenido una amplia adopción como solución de auto identificación. Una de las principales preocupaciones al respecto, es que los tres mayores sistemas conocidos de esta tecnología en la actualidad son propietarios y si cualquiera de estos es descontinuado, será complicado encontrar un sustituto.

Pero entre sus ventajas están la de ser dispositivo de múltiples lecturas y escrituras, además de ser muy resistentes, ya que pueden ser empleados en entornos hostiles y con vibraciones propias de aplicaciones de manufactura. (Sánchez, 2008)

FIGURA N° II.16: MEMORIA DE CONTACTO



Fuente: (electrónica.mercadolibre, s.f.)

2.14. CONCEPTOS BASICOS DE RFID

(Wen-chung, Bae-Ling, & Lih-Chyan, 2013), afirman que RFID es una tecnología sin contacto, que usa señales de radiofrecuencia para intercambiar información entre un objeto etiquetado y, un lector para identificar y rastrear al objeto. Un sistema básico RFID consiste en:

- Etiquetas RF.
- Lectores RF.
- servidor de base de datos.

Para empezar, la identificación un lector RF manda una señal para solicitar la información dentro de las etiquetas RF, tras recibir dicha señal cada tarjeta responde transmitiendo la información correspondiente, luego el lector la pasa al servidor para su posterior proceso.

2.15. APLICACIONES RFID

(RFID:Tecnología, aplicaciones y perspectivas) Se muestra las siguientes aplicaciones de la tecnología RFID:

- Los grandes almacenes Wal-Mart y el Departamento de Defensa (DOD) de los Estados Unidos, fueron los que comenzaron a implantar RFID en sus procesos, obligando a sus distribuidores a etiquetar todos los productos, con el objetivo de mejorar la cadena de suministro. Varias veces se pospuso el plazo límite para su implantación; pero, actualmente ya se observan los beneficios obtenidos. Wal-Mart, que recibe 3 millones de productos etiquetados al mes, ha logrado una reducción en rotura de stocks del 16% y una mejora en el tiempo de reemplazo de los productos fuera de stock del 300%.
- A partir de la iniciativa del DOD, las fuerzas aliadas de la OTAN están incorporando tecnología RFID a su logística.
- En el campo de la moda, Mark & Spencer está obteniendo buenos resultados al etiquetar sus prendas de vestir a nivel de ítem. Al igual que esta, Levi Strauss & Co, evalúa los resultados obtenidos al aplicar RFID EPC a sus pantalones.
- Gillette estima en un 25% los ahorros en coste de operaciones, al identificar con etiquetas EPC sus productos en fabricación.
- No sólo American Express; sino, también Visa y MasterCard, han incluido transponders RFID dentro de sus tarjetas de crédito. McDonald's, en EEUU, ha empezado a aceptar este medio de pago, para reducir el tiempo de espera de sus clientes.
- El Departamento de Seguridad Nacional (DHS), Aeropuerto Internacional de San Francisco, Organización de Aviación Civil Internacional, así como los aeropuertos de Singapur y Australia, están participando en un proyecto piloto promovido por el gobierno de los EEUU, para incluir en los pasaportes: nombre, nacionalidad, fecha y lugar de nacimiento, fotografía y huella dactilar.
- Otro gran beneficiario del uso de la tecnología RFID, es la industria farmacéutica. Tras 2 años de proyectos piloto y la colaboración de cientos de empresas de tecnología y de la industria farmacéutica, la Food and Drug Administration (FDA), emitirá un pliego con recomendaciones para asegurar la cadena de suministro de medicamentos y evitar falsificaciones mediante tecnología RFID.

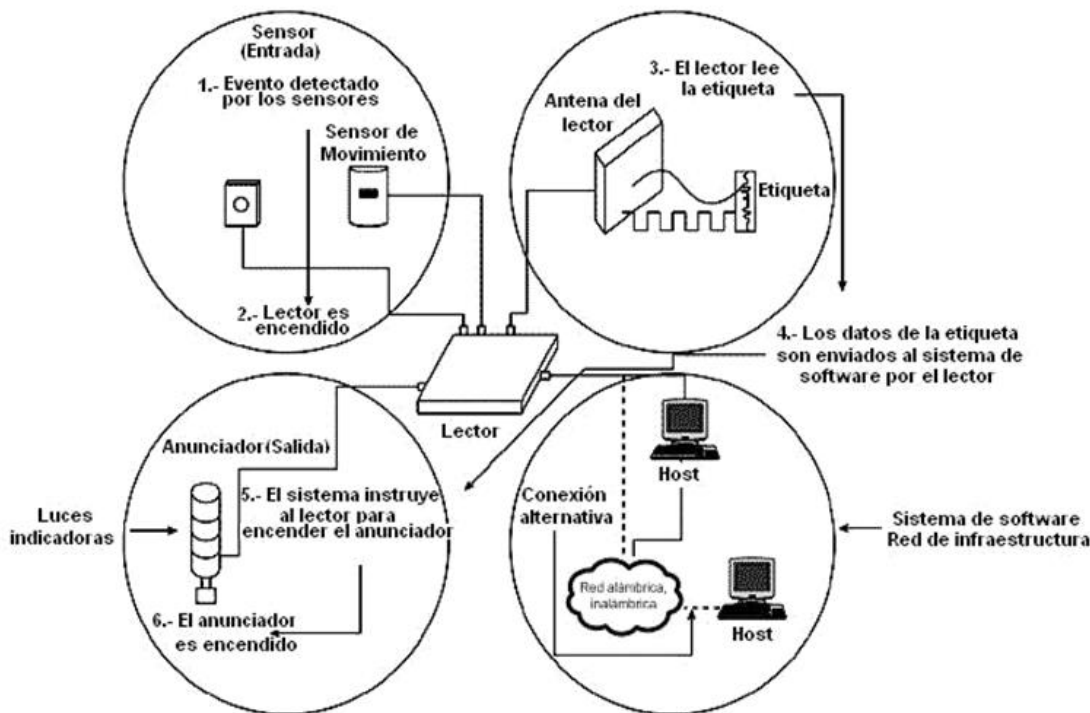
- En Europa, la Comisión Europea ha aprobado la concesión de 7,5 millones de euros en 3 años para el programa BRIDGE (“Building Radio frequency Identification solutions for the Global Environment”), un consorcio formado por 31 empresas, con el objetivo de llevar a cabo investigación dirigida a aplicaciones de negocio y el desarrollo de aplicaciones software y hardware RFID.
- Como último ejemplo, recordar que todas las entradas usadas en la pasada copa del mundo de fútbol de Alemania contaron con un transponder RFID, como medida de autenticación para reforzar la seguridad en los estadios y poder contrastar los datos del comprador en tiempo real contra los datos de compra almacenados en los sistemas de la organización. (pág. 18)

2.16. ARQUITECTURA DE UN SISTEMA MEDIANTE RFID

(Sánchez, 2008) muestra 3 componentes básicos en un sistema de RFID:

1. El tag, etiqueta o transponder de RFID. Consiste en un pequeño circuito, integrado con una pequeña antena, capaz de transmitir un número de serie único hacia un dispositivo de lectura, como respuesta a una petición. Algunas veces puede incluir una batería.
2. El lector (el cual puede ser de lectura o lectura/escritura), está compuesto por una antena, un módulo electrónico de radiofrecuencia y un módulo electrónico de control.
3. Un controlador o un equipo anfitrión, comúnmente un pc o workstation, en la cual corre una base de datos y algún software de control.

FIGURA Nº II.17: ARQUITECTURA DE UN SISTEMA RFID



Fuente: (Ávila & Pupiales)

La tecnología de identificación por radiofrecuencia puede ser dividida principalmente en 3 categorías:

1. **Sistemas Pasivos:** en los cuales las etiquetas de RFID no cuentan con una fuente de poder. Su antena recibe la señal de radiofrecuencia enviada por el lector y almacena esta energía en un capacitor. La etiqueta utiliza esta energía para habilitar su circuito lógico y para regresar una señal al lector. Estas etiquetas pueden llegar a ser muy económicas y pequeñas; pero, su rango de lectura es muy limitado.
2. **Sistemas Activos:** utilizan etiquetas con fuentes de poder integradas, como baterías. Este tipo de etiquetas integra una electrónica más sofisticada, lo que incrementa su capacidad de almacenamiento de datos, interfaces con sensores, funciones especializadas, Además de que permiten que exista una mayor distancia entre lector y etiqueta (20 m a 100 m). Este tipo de etiquetas son más

costosas y tienen un mayor tamaño. Pueden permanecer dormidas hasta que se encuentran dentro del rango de algún lector, o pueden estar haciendo broadcast constantemente.

3. **Sistemas Semi Activos:** emplean etiquetas que tienen una fuente de poder integrada, la cual energiza al tag para su operación. Sin embargo, para transmitir datos, una etiqueta semi activa, utiliza la potencia emitida por el lector. En este tipo de sistemas, el lector siempre inicia la comunicación. La ventaja de estas etiquetas es que al no necesitar la señal del lector para energizarse (a diferencia de las etiquetas pasivas), pueden ser leídas a mayores distancias, y como no necesita tiempo para energizarse, estas etiquetas pueden estar en el rango de lectura del lector por un tiempo substancialmente menor para una apropiada lectura. Esto permite obtener lecturas positivas de objetos moviéndose a altas velocidades.

Tanto los tags activos como los pasivos pueden adicionalmente ser clasificados de la siguiente forma:

- **Solo Lectura (ro):** en estos dispositivos, los datos son grabados en el tag durante su fabricación, para esto, los fusibles en el microchip del tag son quemados permanentemente, utilizando un haz láser muy fino. Después de esto, los datos no podrán ser reescritos. Este tipo de tecnología se utiliza en pequeñas aplicaciones, pero resulta poco práctico para la mayoría de las aplicaciones más grandes, que intentan explotar todas las bondades de RFID.
- **Una escritura, muchas lecturas (worm):** un tag worm, puede ser programado sólo una vez; pero, esta escritura generalmente no es realizada por el fabricante; sino, por el usuario justo en el momento que el tag es creado. Este tipo de etiquetas puede utilizarse en conjunto con las impresoras de RFID, las cuales escriben la información requerida en el tag.
- **Lectura y escritura (rw):** estas etiquetas, pueden ser reprogramadas muchas veces. Típicamente este número varía entre 10,000 y 100,000 veces, incluso mayores. Esta opción de reescritura ofrece muchas ventajas, ya que el tag puede ser escrito por el lector, e inclusive por sí mismo en el caso de los tags

activos. Estas etiquetas regularmente contienen una memoria flash o fram para almacenar los datos. (págs. 14,15).

2.16.1. Funcionamiento de un Sistema RFID

(Ruiz Zamarreño & Ochoa Eneriz, 2015) Nos dice que un sistema RFID está basado en la comunicación bidireccional entre un lector (interrogador) y un tag, mediante señales de radiofrecuencia. Durante su funcionamiento, el lector y el tag están en constante comunicación siempre y cuando éste se encuentre en el rango de distancia requerido. Cuando el tag ingresa en el área de cobertura del sistema, el lector envía señales de radiofrecuencia hacia el tag, el cual las recibe a través de su antena y envía su información hacia el lector. El lector al recibir la señal de identificación, la decodifica y procesa con el objetivo de extraer la información. Tanto el lector como el tag envían señales de radiofrecuencia, cuya frecuencia de operación debe ser la misma, con el fin de establecer una comunicación permanente entre ambos. Las frecuencias más empleadas van desde 125 KHz hasta la banda ISM de 2,4 GHz.

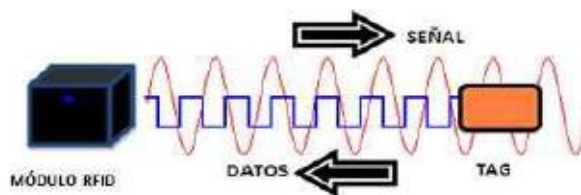
En primer lugar, el lector RFID mediante su antena transmisora emite una interrogación; es decir, una señal de radiofrecuencia de baja potencia que permite la creación de un campo electromagnético. Este campo electromagnético funciona como una señal “portadora” de energía del lector hacia el tag, que está compuesto por una antena, también en forma de bobina y, un circuito integrado. Este circuito integrado necesita una pequeña cantidad de energía para poder funcionar, por lo que la antena contenida en éste es la que funciona como medio para obtener esta energía que se encuentra presente en el campo electromagnético producido por el lector RFID. En este proceso de comunicación, el tag se introduce en el campo electromagnético que emite el lector, por lo que en la antena del tag se induce energía eléctrica, la cual es almacenada para poder permitir que el circuito integrado del tag funcione y los datos contenidos en su memoria sean transmitidos. Para ello lo que hace es modular la señal en torno a los datos que desea transmitir, siendo

las más frecuentes ASK (Amplitude Shift Keying), FSK (Frequency Shift Keying) y PSK (Phase Shift Keying).

La señal electromagnética emitida por el tag es adquirida por la antena receptora del lector RFID y convertida a una señal eléctrica. Este lector tiene un sistema de recepción diseñado para detectar y procesar esta señal débil que proviene del tag.

Una vez que los datos del tag han sido demodulados por el lector, su módulo digital comprueba que éstos han sido recibidos correctamente. Así, el lector utiliza la información redundante del código transmitido por el tag para realizar el proceso de validación (CRC). Cuando éste comprueba que no existen errores y certifica la información recibida, los datos están listos para posteriormente ser procesados o enviados a la unidad de control a la que esté conectado el lector. (págs. 26,27,28)

FIGURA Nº II.18: FUNCIONAMIENTO DE UN SISTEMA RFID



Fuente: (Ruiz Zamarreño & Ochoa Eneriz, 2015)

2.16.2. Etiquetas RFID

Para (Delgadillo Rodriguez & Ortiz Corvera, 2011) una etiqueta RFID o transponder, es un microchip combinado con una antena en un paquete compacto, de tal manera que éste pueda ser unido al objeto a rastrear. La antena de la etiqueta recoge señales de un lector RFID o scanner y regresa la señal, usualmente con algo de información adicional (como un serial único u otra información personalizada). Las etiquetas RFID pueden ser del tamaño de un grano de arroz o de un pequeño libro de bolsillo.

Las características que comparten las etiquetas son:

- Una memoria no volátil donde se almacenan los datos.
- Una memoria ROM donde se almacenan instrucciones básicas para su funcionamiento (temporizadores, controladores de flujo de datos, etc.).
- Memoria RAM para almacenar datos durante la comunicación con el lector.
- Una antena con la que se detecta el campo creado por el lector, y con el cual se energiza para poder comunicarse.

Existen 3 tipos de etiquetas: activas, pasivas y semipasivas. El tamaño de éstas depende del tamaño de la antena, el cual se incrementa con el rango y disminuye con la frecuencia (pág. 32).

2.16.2.1 Etiquetas Activas

Estas etiquetas poseen su propia fuente autónoma de energía, que utilizan para dar corriente a sus circuitos integrados y propagar su señal al lector. Estas etiquetas son mucho más fiables (tienen menos errores) que las pasivas, debido a su capacidad de establecer sesiones con el lector. Gracias a su fuente de energía, son capaces de transmitir señales más potentes que las de las etiquetas pasivas, lo que los lleva a ser más eficientes en entornos difíciles para la radiofrecuencia como el agua (incluyendo humanos y ganado, formados en su mayoría por agua), metal (contenedores, vehículos). También son efectivos a distancias mayores pudiendo generar respuestas claras a partir de recepciones débiles. Por el contrario, suelen ser de mayor tamaño y más caras, y su vida útil es en general mucho más corta.

Muchas etiquetas activas tienen rangos efectivos de cientos de metros y una vida útil de sus baterías de hasta 10 años. Algunas de ellas integran sensores de registro de temperatura y otras variables que pueden usarse para monitorizar entornos de alimentación o productos farmacéuticos. Otros sensores asociados con RFID incluyen humedad, vibración, luz, radiación, temperatura y componentes atmosféricos como el etileno. Las etiquetas activas, además de tener un rango mucho mayor (500 m), tienen capacidades de almacenamiento mayores y la

habilidad de guardar información adicional enviada por el transceptor. (Delgadillo Rodriguez & Ortiz Corvera, 2011).

2.16.2.2. Etiquetas Pasivas

Las etiquetas pasivas no poseen alimentación eléctrica. La señal que les llega de los lectores induce una corriente eléctrica pequeña y que es suficiente para operar el circuito integrado CMOS de la etiqueta, de forma que puede generar y transmitir una respuesta. La mayoría de las etiquetas pasivas utiliza retro dispersión sobre la portadora recibida; esto es, la antena ha de estar diseñada para obtener la energía necesaria para funcionar a la vez que para transmitir la respuesta por retro dispersión. Esta respuesta puede ser cualquier tipo de información, no sólo un código identificador. Una etiqueta puede incluir memoria no volátil, posiblemente reescribible (por ejemplo, EEPROM).

Las etiquetas pasivas suelen tener distancias de uso práctico comprendidas entre los 10 cm (ISO 14443) y llegando hasta unos pocos metros (EPC e ISO 18000-6), según la frecuencia de funcionamiento y el diseño y, tamaño de la antena. Por su sencillez conceptual, son obtenibles por medio de un proceso de impresión de las antenas. Como no precisan de alimentación energética, el dispositivo puede resultar muy pequeño: pueden incluirse en una estampa o insertarse bajo la piel (etiquetas de baja frecuencia). (Delgadillo Rodriguez & Ortiz Corvera, 2011).

2.16.2.3. Etiquetas Semipasivas

Las etiquetas RFID semipasivas son muy similares a las pasivas, salvo que incorporan además una pequeña batería. Esta batería permite al circuito integrado de la etiqueta estar constantemente alimentado. Además, elimina la necesidad de diseñar una antena para recoger potencia de una señal entrante. Por ello, las antenas pueden ser optimizadas para la señal de retro dispersión. Las etiquetas RFID semipasivas responden más rápidamente, por lo que son más eficientes en el radio de lectura comparadas con las etiquetas pasivas. (Delgadillo Rodriguez & Ortiz Corvera, 2011).

2.16.3. Etiquetas de Lectura y Escritura

Las etiquetas pueden ser de sólo lectura o de lectura-escritura. Las tarjetas de sólo lectura son aquellas que durante su fabricación o bien, antes de su primer uso, han sido programadas con un código de identificación único y que la información que contienen no puede ser cambiada. Con las tarjetas de lectura-escritura se tiene la posibilidad de cambiar los datos que contiene la tarjeta, incluso pueden ser modificados cada vez que ocurre determinado evento, por lo que son adecuadas para aplicaciones que requieren información variable. (Delgadillo Rodriguez & Ortiz Corvera, 2011).

2.16.4. Frecuencia de Velocidades de Transmisión

(Cervantes Nájera, Hernández Reyes, & Santiago Jacobo, 2008) dice que las frecuencias de RFID pueden ser divididas en 4 rangos:

- **Baja Frecuencia LF (Low Frequency):** en el rango de 120 kHz a 134 kHz. Estas etiquetas tienden a ser muy utilizados en accesos a edificios.
- **Alta Frecuencia HF (High Frequency):** en el rango de 13,56 MHz. La desventaja de estas etiquetas es que su frecuencia tiene un alcance de lectura bajo, generalmente del orden de 30 centímetros. Ofrecen como ventaja ser de lectura fácil y sin problemas en presencia de agua.
- **Ultra Alta Frecuencia UHF (Ultra High Frequency):** funcionan en el rango de 868 MHz a 956 MHz. Las etiquetas de RFID de UHF usualmente se emplean en la cadena de suministros. Uno de los beneficios más grandes de las etiquetas UHF pasivas, es que tienen un rango mayor a tres metros y pueden leer cientos de etiquetas simultáneamente. Sin embargo, no pueden ser leídas fácilmente en altas concentraciones de líquidos, como recipientes de bebida a través de seres vivos.
- **Microondas:** en el rango de 2,45 GHz. Se utilizan en el control de acceso en vehículos.

2.16.5. Lector/Escritor de Tarjetas RFID

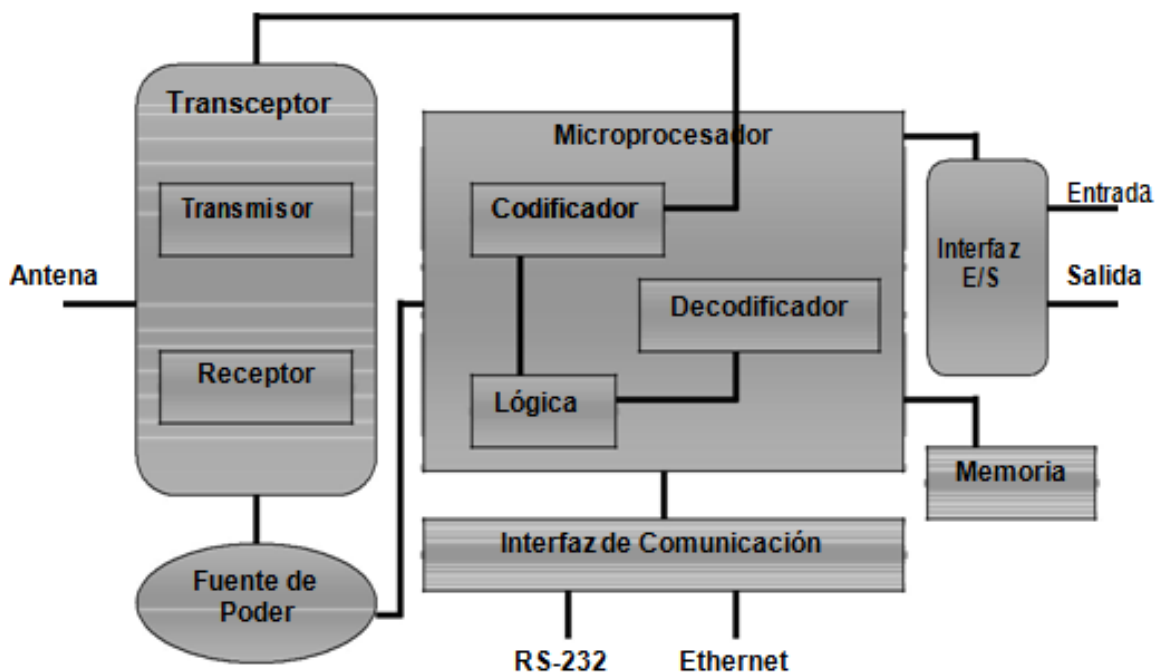
(Sánchez, 2008) muestra que el lector de RFID, es un dispositivo que puede leer y escribir datos hacia tags RFID compatibles.

El lector es el componente central del hardware en un sistema de RFID y tiene los siguientes componentes:

- **Transmisor:** el transmisor emite potencia y envía el ciclo de reloj a través de su antena hacia los tags que se encuentran dentro de su rango de lectura.
- **Receptor:** este componente recibe las señales analógicas provenientes del tag a través de la antena y envía estos datos al microprocesador, donde esta información es convertida en su equivalente digital.
- **Antena:** esta antena va conectada directamente al transmisor y al receptor. Existen lectores con múltiples puertos para antenas, lo que les permite tener múltiples antenas y extender su cobertura.
- **Microprocesador:** este componente es responsable de implementar el protocolo de lectura empleado para comunicarse con tags compatibles. Decodifica y realiza verificación de errores a las señales recibidas. Adicionalmente, puede contener cierta lógica para realizar filtrado y procesamiento de bajo nivel de los datos leídos, esto es, eliminar lecturas duplicadas o erróneas.
- **Memoria:** la memoria es utilizada para almacenar información como los parámetros de configuración del lector; además, de una lista de las últimas lecturas realizadas, de modo tal que, si se pierde la comunicación con el pc, no se pierdan todos los datos.
- **Canales de entrada/salida:** estos canales permiten al lector interactuar con sensores y actuadores externos. Estrictamente hablando, es un componente opcional, pero incluido en la mayoría de los lectores comerciales de la actualidad.

- **Controlador:** el controlador es el componente que permite a una entidad externa, sea un humano o un software de computadora, comunicarse y controlar las funciones del lector. Comúnmente los fabricantes integran este componente como un firmware.
- **Interfaz de comunicación:** esta interfaz provee las instrucciones de comunicación, que permiten la interacción con entidades externas, mediante el controlador, para transferir datos y recibir comandos. Un lector puede tener distintos tipos de interfaz como se discute más adelante, por ejemplo: rs-232, rs-485, interfaz de red, entre otras.
- **Fuente de alimentación:** este componente provee de alimentación eléctrica a los componentes del lector y regularmente consiste en un cable con un adaptador de voltaje, conectado hacia la toma de corriente. Pero en los últimos años se han incrementado el número de lectores de tipo pistola, los cuales son móviles y su fuente de alimentación es una batería recargable. (págs. 16,17).

FIGURA Nº II.19: DIAGRAMA LECTOR/ESCRITOR RFID



Fuente: (Sánchez, 2008)

2.16.6. Componentes de Software RFID

Las características y funcionalidades de los componentes de software varían de un sistema RFID a otro, dependiendo de los requerimientos de la aplicación. Estos componentes caen dentro de las siguientes categorías:

- Software de Sistemas RFID.
- RFID middleware.
- Aplicaciones de computador.

(Paredes, 2007)

2.16.6.1. Software de Sistemas RFID

El software de sistemas RFID es una colección de funciones necesarias para habilitar la interacción básica entre un tag y un lector. En la forma más básica, la comunicación ocurre a un nivel de procesamiento de las señales de radio. Esto requiere de hardware, software de bajo nivel, y un buen sistema de software para administrar el flujo de datos entre el tag y el lector.

- **Lectura / Escritura:** éstas son las funciones más básicas de un tag. Un lector toma un tag para leer o escribir datos. El acceso a la memoria del tag para leer los datos se da el momento en que el tag ingresa al campo de acción del lector, entonces se transmiten los datos contenidos en el tag hacia el lector. El tag también puede ser abastecido de datos por el lector (desde la aplicación del computador) escribiendo en su memoria, con tal de que el tag tenga capacidad de escritura.
- **Anti-Colisión:** el software anticolidión, se utiliza cuando múltiples tags actúan en el campo de radiofrecuencia del lector y deben ser identificados simultáneamente. Este comportamiento es típico en la mayoría de las aplicaciones de la cadena de suministros. Es el caso de realizar un inventario en un supermercado. Cientos o incluso miles de objetos pueden estar dentro del campo de lectura, que puede ser de varios pies de radio. Las funciones de

anticolisión requieren cooperación entre el tag y el lector para disminuir el riesgo en que muchos tags respondan a la vez. En algunos casos el algoritmo puede ser simple en el que cada tag espera una cantidad de tiempo aleatorio antes de responder la petición del lector.

- **Detección / Corrección de errores:** el lector puede emplear un sofisticado software para detectar y corregir errores de transmisión del tag. Tal software puede incluir programación para detectar y descartar información duplicada o incompleta.
- **Encriptación, Autorización y Autenticación (Seguridad):** estos parámetros se utilizan cuando el intercambio de información entre el tag y el lector debe ser seguro; para esto, tanto el tag como el lector deben cooperar y ejecutar el protocolo necesario con el fin de conseguir el nivel deseado de seguridad en el transporte de los datos. Por ejemplo, para prevenir que un lector no autorizado recupere datos de un tag determinado, éste y el lector deben ejecutar un protocolo de autorización, intercambiando un código secreto. Luego de que esta información compartida ha sido intercambiada y validada, el tag transmite datos al lector de forma segura. Desde luego esta funcionalidad en el tag requiere de un diseño sofisticado, el cual puede significar impacto en el costo de un tag pasivo. (Paredes, 2007).

2.16.6.2. RFID Middleware

RFID Middleware consiste en un conjunto de componentes de software que actúan como un puente entre los componentes de un sistema RFID (tag y el lector) y el software de aplicación del computador.

Éste tiene dos funciones primarias:

- **Monitoreo:** esta función consiste en realizar una supervisión central e informar el estado de los lectores dentro de una aplicación RFID-habilitada. Ésta es una función muy importante en ambientes donde múltiples lectores son distribuidos por uno o múltiples escenarios y el supervisar visual o manualmente no es

práctico. Por ejemplo, considerando el entorno de un almacén grande con múltiples artículos y docenas de lectores ubicados estratégicamente que recogen datos automáticamente de los artículos etiquetados. En este caso, es importante ser alertado tan rápidamente como sea posible a desperfectos del lector o funcionamientos defectuosos. Esto ayuda a dirigirse al problema rápidamente y reparar cualquier error que pudo haber ocurrido, de modo oportuno. En una situación ideal, el software supervisor debe poder ocuparse de otros dispositivos lectores (por ejemplo, de lectores de código de barras o impresora/codificadora de etiqueta inteligentes RFID).

- **Gestión del flujo de datos:** en una palabra, esta función consiste en codificación, colección, proceso, filtración y agregación de datos transmitidos, entre las etiquetas y lectores para la integración con la aplicación del computador. Ésta es una función muy significativa en un ambiente donde los lectores pueden recoger grandes ráfagas o cadenas constantes de datos de la etiqueta (como en una aplicación de la cadena de suministros). Los datos de la etiqueta necesitan ser limpiados; por ejemplo, eliminando mensajes duplicados, o filtrándolos y las alarmas pueden necesitar ser levantadas, basadas en ciertas reglas predefinidas para la colección de los datos. Otra función importante realizada en esta fase es la normalización de los datos. En la ausencia de normas, el formato de los datos y los protocolos de comunicación del lector con el computador, son normalmente propietarios. En ambientes del multi vendedor, el software RFID middleware es responsable de traducir varios formatos de datos del lector en uno solo, normalizando el formato para facilitar la integración a nivel de la aplicación del computador. (Paredes, 2007).

2.16.6.3. Aplicación de Computador

La aplicación del computador recibe datos procesados y normalizados enviados de la etiqueta, vía el lector y el software RFID middleware. La aplicación del computador es típicamente un software previamente existente en una empresa, tal como un control de inventario o un sistema de administración de un almacén. Dependiendo de lo sofisticado del software RFID middleware y las capacidades de

la aplicación del computador, el software de aplicación puede no necesitar saber la fuente real de los datos, ni siquiera espera recibirlos. Por ejemplo, una aplicación de control de inventario puede rastrear todos los productos con éxito en los estantes de una tienda, sin "saber" cómo los datos son ingresados. Antes de que el sistema RFID fuera instalado, estos datos pueden haber sido ingresados manualmente o a través de un sistema del código de barras. Con tal que la interfaz tenga un protocolo bien definido para ingresar los datos, el software RFID middleware necesitará sólo un proceso y estructura de los datos originales de la etiqueta y usar el protocolo definido por la aplicación del computador, para pasar en éste datos. Sin embargo, algunas aplicaciones pueden necesitar ser modificadas para aceptar un conjunto nuevo de datos del RFID middleware, porque les falta definir un protocolo del interfaz totalmente apropiado. Este escenario es más probable si la aplicación es más antigua o propia. En otras situaciones, un software diferente debe ser escrito o adquirido como la aplicación del computador, porque una solución completamente nueva se ha desplegado dentro de la empresa. Por ejemplo, considere un sistema de control de acceso basado en RFID, llevado a cabo en un negocio donde el control de acceso se logró previamente a través de llaves metálicas. En este caso, el software de aplicación nuevo exige controlar, autenticar, y proporcionar el acceso del usuario. Es importante notar que existe un significativo desafío, sin tener en cuenta que si una aplicación existente puede ocuparse de datos RFID o una nueva aplicación o la interfaz tiene que ser desarrollada. En muchos casos, RFID representa los nuevos datos para una empresa. Es poco probable que la empresa tenga un modelo de negocio existente que pueda influir totalmente en estos datos. Por ejemplo, en una solución RFID habilitada de una típica cadena de suministros, los artículos son identificados por EPC. La cadena de suministros existente, los modelos de negocios y aplicaciones originalmente desarrolladas para usar los datos de UPC ahora tienen el acceso a nuevos y extendidos datos del EPC que ellos pueden y deben manejar. Esto es lo que se llama la identificación única o serialización. Los negocios tendrán de hecho una re-arquitectura de sus modelos de negocios y aplicaciones, para ser capaces de comprender los beneficios de estos datos adicionales generados a través de los sistemas RFID. (Paredes, 2007)

2.16.7. Estándares

La tecnología RFID, debe cumplir con estándares creados por organizaciones como: ISO y EPC.

2.16.7.1. ISO

ISO tiene 3 estándares para RFID: ISO 14443 (para sistemas sin contacto), ISO15693 (para sistema de proximidad) e ISO 18000 (para especificar la interfaz aérea para una variedad de aplicaciones). (Sánchez, 2008).

2.16.7.1.1. ISO/IEC 14443

ISO/IEC 14443, es una tecnología de lectura sin contacto, con un rango de aproximadamente diez centímetros. Esta tecnología de lectura de alta frecuencia (13,56 MHz), fue diseñada principalmente para su uso en tickets electrónicos y dinero digital. Para estas aplicaciones, la lectura de corto alcance y la velocidad en transacciones es crítica. Dado que otros mercados tenían los mismos requerimientos, eso hizo que la ISO/IEC 14443 fuera adoptada para tránsito, compras fuera de línea y más actualmente para el control de acceso. (Smart Card Alliance, 2002).

2.16.7.2. EPC

EPC global es una organización sin fines de lucro que ha desarrollado una amplia gama de estándares para la identificación de productos. Los estándares EPC están enfocados a la cadena de suministro y particularmente definen la metodología para la interfaz aérea. El formato de los datos almacenados en una etiqueta RFID, para la identificación de un producto, captura, transferencia, almacenamiento y acceso de estos datos; así como el middleware y la base de datos que almacena esta información.

Las funciones de EPC o código electrónico de producto, son similares a las de UPC o código de producto universal encontrado en la tecnología de código de barras.

EPC es un esquema de identificación para identificar objetos físicos de manera universal por medio de etiquetas RFID. El código EPC en una etiqueta RFID puede identificar al fabricante, producto, versión y número de serie y, adicionalmente provee un grupo de dígitos extra para identificar objetos únicos.

La red de EPC global es un grupo de tecnologías que habilita la identificación automática e inmediata de elementos en la cadena de suministro y la compartición de dicha información.

La tecnología RFID involucra colocar las etiquetas RFID en los objetos, la lectura de etiquetas (idealmente sin intervención humana) y el paso de la información a un sistema dedicado de infraestructura de tecnologías de la información. Con dicha infraestructura se pueden identificar objetos automáticamente, rastrear, monitorear y activar eventos relevantes. (Sánchez, 2008).

2.16.7.3. ONS

EPC global ha desarrollado un sistema llamado ONS (object naming service), que es similar al DNS (domain name service) utilizado en internet. ONS actúa como un directorio para las organizaciones que desean buscar números de productos en internet. (Sánchez, 2008).

2.16.7.4. EPC GEN 2

EPC global ha trabajado con un estándar internacional para el uso de RFID y EPC, en la identificación de cualquier artículo, en la cadena de suministro para las compañías de cualquier tipo de industria; esto, en cualquier lugar del mundo. El Consejo Superior de la Organización, incluye representantes de EAN International, Uniform Code Council, The Gillette Company, Procter & Gamble, Walmart, Hewlett Packard, Johnson & Johnson, Checkpoint Systems y Auto ID Labs. El estándar gen 2 de EPC global, fue aprobado en diciembre de 2004 y es probable que llegue a formar la espina dorsal de los estándares en etiquetas RFID de ahora en adelante. EPC gen2 es la abreviatura de “EPC global UHF generation 2”. (Sánchez, 2008).

2.16.7.4.1. Capa Física EPC GEN 2

La capa física define cómo se envían los bits entre el lector RFID y las etiquetas. En su mayor parte se utilizan métodos para enviar señales inalámbricas que se presentó antes. En Estados Unidos, las transmisiones se envían en la banda ISM de 902 928 MHz sin licencia. Esta banda se encuentra dentro del alcance de UHF (Frecuencia Ultra Alta), por lo que las etiquetas se denominan etiquetas RFID de UHF. El lector realiza el salto de frecuencias por lo menos cada 400 mseg, para dispersar su señal a través del canal, para limitar la interferencia y cumplir con los requerimientos regulatorios. El lector y las etiquetas usan formas de modulación ASK (Modulación por Desplazamiento de Amplitud), para codificar bits, puesto que toman turnos para enviar bits, el enlace es half dúplex.

Existen dos diferencias principales en comparación con otras capas físicas que se han estudiado. La primera es que el lector siempre transmite una señal, sin importar que sea el lector o la etiqueta quien se está comunicando. Naturalmente, el lector transmite una señal para enviar bits a las etiquetas. Para que las etiquetas envíen bits al lector, éste transmite una señal portadora fija que no transmite bits. Las etiquetas recolectan esta señal para obtener la potencia que necesitan para operar; de no ser así, una etiqueta no podría transmitir en primer lugar. Para enviar datos, una etiqueta cambia entre la acción de reflejar la señal del lector, como una señal de radar, que rebota de un objetivo y la acción de absorberla. A este método se le conoce como retro dispersión. Es distinto a todos los demás métodos inalámbricos que se han visto hasta ahora, en donde el emisor y receptor nunca transmiten al mismo tiempo. La retro dispersión es una forma de bajo consumo de energía para que la etiqueta cree su propia señal débil y aparezca en el lector. Para que el lector decodifique la señal entrante, debe filtrar la señal de salida que está transmitiendo. Como la señal de la etiqueta es débil, las etiquetas sólo pueden enviar bits al lector a una tasa baja, y no pueden recibir ni detectar transmisiones de otras etiquetas.

La segunda diferencia es que se utilizan formas muy simples de modulación, de modo que se puedan implementar en una etiqueta que opere con muy poca potencia

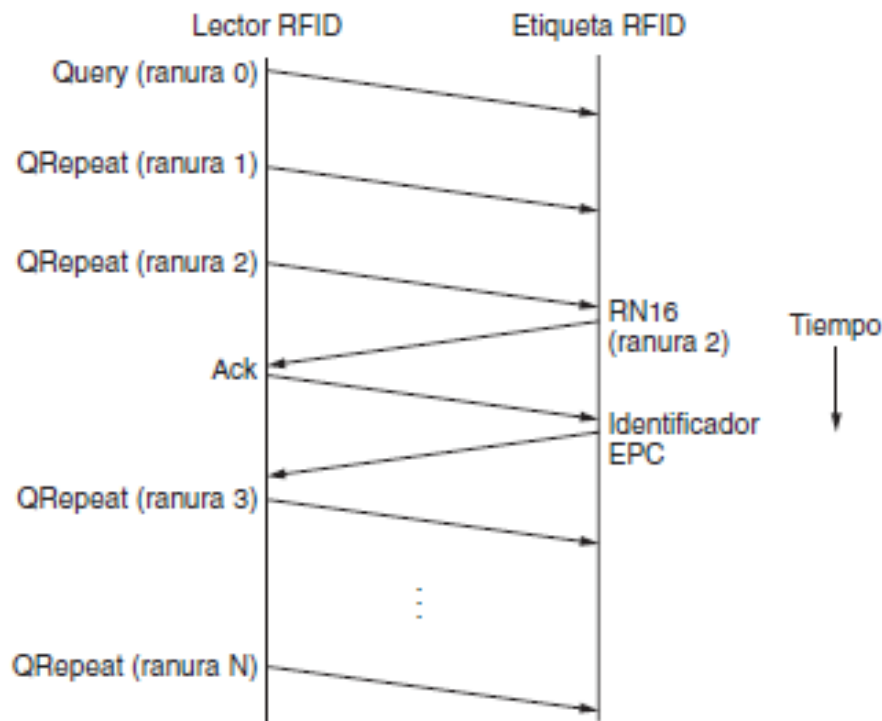
y su costo de fabricación sea de unos cuantos centavos. Para enviar datos a las etiquetas, el lector usa dos niveles de amplitud. Los bits se determinan para que sean un 0 o un 1, dependiendo de cuánto tiempo espere el lector antes de un periodo de baja potencia. La etiqueta mide el tiempo entre los periodos de baja potencia y compara este tiempo con una referencia que se mide durante un preámbulo. los 1s son más largos que los 0s. Las respuestas de las etiquetas consisten en que la etiqueta alterne su estado de retro dispersión a intervalos fijos, para crear una serie de pulsos en la señal. Se pueden usar desde uno hasta ocho periodos de pulsos para codificar cada 0 ó 1, dependiendo del grado de confiabilidad que se requiera. (Tanenbaum & Wetherhall, 2015).

2.16.7.4.2. Capa de Identificación de Etiquetas de EPC GEN 2

Para generar un inventario de las etiquetas circundantes, el lector necesita recibir un mensaje de cada etiqueta, en el cual se proporcione la identificación de la misma. Esta situación es un problema de acceso múltiple, en el cual se desconoce el número de etiquetas en el caso general. El lector podría difundir una consulta para pedir a todas las etiquetas que envíen sus identificadores. Sin embargo, las etiquetas que respondieran de inmediato tendrían una colisión en forma muy parecida a las colisiones de las estaciones en una red Ethernet clásica. El protocolo más apropiado para la situación actual, en la que las etiquetas no pueden escuchar las transmisiones de las demás, es el ALOHA ranurado. Este protocolo se adaptó para usarlo en el RFID Gen 2. En la primera ranura (ranura 0), el lector envía un mensaje Query (consulta) para iniciar el proceso. Cada mensaje QRepeat avanza a la siguiente ranura. El lector también indica a las etiquetas el rango de ranuras a través del cual deben aleatorizar las transmisiones. Es necesario usar un rango, ya que el lector sincroniza las etiquetas al iniciar el proceso; a diferencia de las estaciones en una red Ethernet, las etiquetas no despiertan con un mensaje en el momento que deseen. Las etiquetas seleccionan una ranura al azar para responder. La etiqueta responde en la ranura 2. Sin embargo, las etiquetas no envían sus identificadores cuando responden por primera vez. En cambio, una etiqueta envía un número aleatorio corto de 16 bits en un mensaje RN16. Si no hay colisión, el

lector recibe este mensaje y envía un mensaje ACK por su cuenta. En esta etapa, la etiqueta ha adquirido la ranura y envía su identificador EPC. La razón de este intercambio es que los identificadores EPC son largos, por lo que las colisiones en estos mensajes serían muy caras. En cambio, se usa un intercambio corto para probar si la etiqueta puede usar en forma segura la ranura para enviar su identificador. Una vez que se transmite con éxito su identificador, la etiqueta deja temporalmente de responder a los nuevos mensajes Query, de modo que se puedan identificar las etiquetas restantes. Un problema clave es que el lector ajuste el número de ranuras para evitar colisiones, pero sin usar tantas ranuras como para que se vea afectado el desempeño. Este ajuste es análogo al retroceso exponencial binario en Ethernet. Si el lector ve demasiadas ranuras sin respuestas, o demasiadas ranuras con colisiones, puede enviar un mensaje QAdjust para reducir o aumentar el rango de ranuras a través de las cuales responden las etiquetas. (Tanenbaum & Wetherhall, 2015)

FIGURA Nº II.20: DIAGRAMA DE FUNCIONAMIENTO EPC GEN 2



Fuente: (Tanenbaum & Wetherhall, 2015)

2.16.8. Otros Estándares RFID

Existen, así mismo, muchos más estándares, pero enfocados a industrias específicas. Por ejemplo: el AIAG b-11 (Automotive Industry Action Group), para identificación de llantas y ANSI mh10.8.4, para aplicaciones estándar de RFID con contenedores reutilizables. Las siguientes son algunas organizaciones que han producido algún estándar relacionado con RFID, o han desarrollado alguna función regulatoria al respecto:

- ANSI (American National Standards Institute).
- AIAG (Automotive Industry Action Group).
- EAN.UCC (European Article Numbering Association International, Uniform Code Council).
- EPC GLOBAL
- ISO (International Organization for Standardization).
- CEN (Comité Européen Normalisation).
- ETSI (European Telecommunications Standards Institute).
- ERO (European Radiocommunications Office).
- UPU (Universal Postal Union).
- ASTM (American Society for Testing Materials).

(Sánchez, 2008)

2.16.9. Métodos de Conexión para Administración de Dispositivos RFID

(Sánchez, 2008) se muestra las opciones siguientes:

- **RS-232:** este protocolo provee sistemas de comunicación confiables de corto alcance. Tiene ciertas limitaciones como una baja velocidad de comunicación, que va de 9600 bps a 115,2 kbps. El largo del cable está limitado a 30 metros, no cuenta con un control de errores y su comunicación es punto a punto.
- **RS-485:** el protocolo RS-485, es una mejora sobre RS-232, ya que permite longitudes de cable de hasta 1.200 metros. Alcanza velocidades de hasta 2,5

Mbps y es un protocolo de tipo bus, lo cual permite a múltiples dispositivos estar conectados al mismo cable.

- **Ethernet:** se considera como una buena opción, ya que su velocidad es más que suficiente para los lectores de RFID. La confiabilidad del protocolo TCP/IP sobre Ethernet, asegura la integridad de los datos enviados y finalmente al ser la infraestructura común para las redes, la mayoría de las instituciones ya cuentan con una red de este tipo, lo que permite una instalación más sencilla y menos costos de integración.
- **Wireless 802.11:** se utiliza en la actualidad en los lectores de RFID móviles. Además de que esta solución reduce los requerimientos de cables y, por lo tanto, de costos.
- **USB:** pensando desde la tendiente desaparición del puerto serial en las computadoras, algunos proveedores de lectores RFID han habilitado sus equipos para poder comunicarse mediante el puerto USB.

2.16.10. Seguridad en Sistemas RFID

(Instituto Nacional de tecnologías de la comunicación, 2010) Nos muestra los riesgos para el servicio. Se concretan en los tipos de “ataque” más habituales que puede sufrir la instalación, cada uno de ellos con una finalidad y un impacto diferente. La forma más simple de ataque a un sistema RFID, es evitar la comunicación entre el lector y la etiqueta, pero también existen otras formas de ataque más sofisticadas, cuyo blanco son las comunicaciones en radiofrecuencia:

- **Aislamiento de etiquetas:** el ataque más sencillo a la seguridad en RFID, consiste en impedir la correcta comunicación lector-etiqueta. Esto se puede conseguir introduciendo la etiqueta en una “jaula de Faraday” o creando un campo electromagnético que interfiera con el creado por el lector. Este ataque puede ser utilizado para sustraer productos protegidos por etiquetas RFID. También puede ser una medida de protección de usuarios ante lectores de etiquetas ilegales. Un ejemplo muy relevante de este caso es el del pasaporte

electrónico, para el que existen fundas especiales con hilos de metal que crean una “jaula de Faraday”, evitando lecturas incontroladas de su información.

- **Suplantación:** este ataque consiste en el envío de información falsa que parece ser válida. Por ejemplo, se podría enviar un código electrónico de producto (EPC) falso, cuando el sistema espera uno correcto. Este tipo de ataque puede servir para sustituir etiquetas, lo cual puede permitir la obtención de artículos caros con etiquetas suplantadas de productos más baratos. Además, aplicado a la cadena de distribución, puede llegar a acarrear un fraude de grandes dimensiones por la sustitución de grandes volúmenes de mercancías.
- **Jaula de Faraday:** es un espacio cerrado revestido metálicamente, que imposibilita la influencia de los campos eléctricos exteriores en el interior del mismo. Las ondas de radio no pueden adentrarse en el interior de la jaula. Este ataque puede utilizarse en otros entornos, como puede ser el del telepeaje.
- **Inserción:** este ataque consiste en la inserción de comandos ejecutables en la memoria de datos de una etiqueta donde habitualmente se esperan datos. Estos comandos pueden inhabilitar lectores y otros elementos del sistema. La finalidad de este tipo de ataque será la desactivación del sistema o la invalidación de parte de sus componentes, permitiendo algún tipo de fraude, o una denegación de servicio.
- **Repetición:** consiste en enviar al lector RFID, una señal que reproduce la de una etiqueta válida. Esta señal se habrá capturado mediante escucha a la original. El receptor aceptará como válidos los datos enviados. Este ataque permitirá suplantar la identidad que representa una etiqueta RFID.
- **Denegación de Servicio (DoS):** este tipo de ataque, satura el sistema enviándole de forma masiva más datos de los que éste es capaz de procesar. Por ejemplo, colapsando la funcionalidad de backscattering o señal de retorno de la tecnología RFID. Asimismo, existe una variante, el RF Jamming, mediante el cual se consigue anular o inhibir la comunicación de radiofrecuencia, emitiendo ruido suficientemente potente. En ambos, casos, se invalida el sistema para la detección de tags. Con este ataque se consigue que los objetos

etiquetados, escapen al control del sistema en su movimiento. Puede ser utilizado para la sustracción de mercancía a pequeña o gran escala.

- **Desactivación o Destrucción de Etiquetas:** consiste en deshabilitar las etiquetas RFID sometiéndolas a un fuerte campo electromagnético. Lo que hace este sistema, es emitir un pulso electromagnético que destruye la sección más débil de la antena, con lo que el sistema queda inutilizado. Si se dispone de los medios técnicos necesarios, se pueden inutilizar las etiquetas de protección antirrobo de los productos, favoreciéndose así su sustracción. Este ataque también se puede utilizar en los sistemas utilizados para la cadena de distribución.
- **Clonación de la tarjeta RFID:** a partir de la comunicación entre una etiqueta y el lector, se copian dichos datos y se replican en otra etiqueta RFID para ser utilizados posteriormente.
- **Riesgo de ataque mediante inyección de lenguaje de consultas SQL:** por medio de la comunicación entre la etiqueta y el lector, se pasa lenguaje SQL hacia el soporte físico que lee la etiqueta; el cual, debido a dicho ataque, ejecuta las órdenes incluidas en la etiqueta y esto puede ser introducido en una base de datos.
- **Código malicioso (malware):** otro posible riesgo de la tecnología RFID, consiste en la infección y transmisión de códigos maliciosos incluidos dentro de etiquetas RFID. Para ello el código malicioso debe entrar en la etiqueta, lo que supone un hecho complicado, dado que la capacidad de almacenamiento de algunas etiquetas no es muy grande.
- **Spoofing:** caso particular para etiquetas activas (de lectura y escritura). En este caso se escriben datos reales en una etiqueta RFID para suplantar la información original. Es más habitual en las etiquetas RFID de las prendas de vestir. Se puede suplantar la información tantas veces se requiera, siempre que éstas sean de lectura.
- **Ataques Man in the Middle (MIM):** vulnera la confianza mutua en los procesos de comunicación y reemplaza una de las entidades. Ya que la tecnología RFID

se basa en la interoperabilidad entre lectores y etiquetas, es vulnerable a este tipo de ataques.

- **Inutilización de etiquetas:** si se somete la etiqueta RFID a un fuerte campo electromagnético, ésta se inhabilita. Esta técnica es usada para sustraer productos ya que, si se dispone; por ejemplo, de una antena altamente direccional, se pueden inutilizar las etiquetas del producto.

La posibilidad de estos ataques y la facilidad técnica de alguno de ellos se debe a lo maduro de la tecnología que permite el acceso a lectores y grabadores de RFID a precio muy asequible. Por este motivo, la tecnología debe mejorar aún más, aumentando el nivel de protección de accesos y minimizando las posibilidades de fraude (págs. 31,32,33).

2.16.11. Espectro Electromagnético

El espectro electromagnético o simplemente espectro, es el rango de todas las radiaciones electromagnéticas posibles. El espectro de un objeto es la distribución característica de la radiación electromagnética de este objeto. El espectro electromagnético se extiende desde las bajas frecuencias usadas para la radio moderna (extremo de la onda larga), hasta los rayos gamma (extremo de la onda corta), que cubren longitudes de onda de entre miles de kilómetros y la fracción del tamaño de un átomo. Se piensa que el límite de la longitud de onda corta está en las cercanías de la longitud Planck; mientras que el límite de la longitud de onda larga es el tamaño del universo mismo, aunque en principio el espectro sea infinito. (espectrometria.com, s.f.).

2.16.11.1. Rango del Espectro Electromagnético

El espectro cubre la energía de ondas electromagnéticas que tienen longitudes de onda diferentes. Las frecuencias de 30 Hz y más bajas pueden ser producidas por ciertas nebulosas estelares y son importantes para su estudio. Se han descubierto

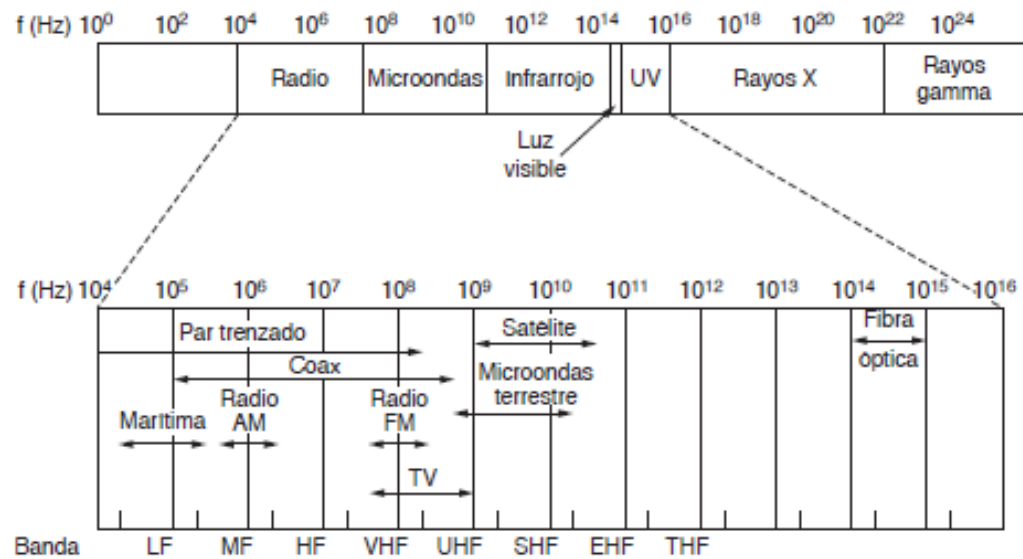
frecuencias tan altas como $2,9 \times 10^{27}$ Hz, a partir de fuentes astrofísicas. La energía electromagnética en una longitud de onda particular λ (en el vacío) tiene una frecuencia asociada f y una energía fotónica E ; así, el espectro electromagnético puede expresarse en términos de cualquiera de estas tres variables, que están relacionadas mediante ecuaciones. De este modo, las ondas electromagnéticas de alta frecuencia tienen una longitud de onda corta y energía alta; las ondas de frecuencia baja tienen una longitud de onda larga y energía baja. Siempre que las ondas de luz (y otras ondas electromagnéticas) se encuentran en un medio (materia), su longitud de onda se reduce. Las longitudes de onda de la radiación electromagnética, sin importar el medio por el que viajen, son por lo general, citadas en términos de longitud de onda en el vacío, aunque no siempre se declara explícitamente.

Generalmente, la radiación electromagnética se clasifica por la longitud de onda:

- Ondas de radio.
- Microondas.
- Infrarroja.
- Rayos ultravioletas.
- Rayos gama.

El comportamiento de la radiación electromagnética depende de su longitud de onda. Las frecuencias más altas tienen las longitudes de onda más cortas y las frecuencias inferiores tienen longitudes de onda más largas. Cuando la radiación electromagnética interacciona con átomos y moléculas, su comportamiento también depende de la cantidad de energía por cuanto que transporta. (espectrometria.com, s.f.)

FIGURA Nº II.21: ESPECTRO ELECTROMAGNÉTICO



Fuente: (Tanenbaum & Wetherhall, 2015)

CAPÍTULO III

INGENIERÍA DE PROYECTO

Para el abordaje de este capítulo se utilizará la metodología de ciclo de vida tecnológica PPDIO de Cisco, para complementar de forma precisa el desarrollo de la ingeniería de proyecto. A continuación, se especifica las actividades que se aplicarán en cada fase de la metodología, como sigue:

1. Fase de preparación:

- Descripción de la situación actual.
- Disposición tecnológica de los laboratorios de computación.
- factores de riesgo.

2. Fase de planificación:

- Relevamiento de información de las siguientes áreas (laboratorios de computación, cámaras de seguridad y red de datos).
- Comparativa de tecnologías de control de acceso para definir la tecnología a usar.
- Comparativa de fabricantes para optar por la mejor solución.

3. Fase de diseño:

- Diseño de topología de sistema de control de acceso y activos.
- Segmentación y direccionamiento ip a través de una propuesta nueva de diseño lógico de red.

4. Fase de operación:

- Configuración de software para administrar sistema.
- Configuración de servidor con base de datos.

3.1. FASE DE PREPARACIÓN

En la fase de preparación, se describirá el funcionamiento actual de los laboratorios de computación y los riesgos a los cuales están expuestos los activos tecnológicos de los mismos.

3.1.1. Descripción de la Situación Actual

La Universidad Privada Domingo Savio, recibe más de tres mil personas por día. Su categorización responde no solo a estudiantes sino también a funcionarios. El acceso al Campus es libre; es decir, que no se exige un documento de identidad para recorrer todas las instalaciones.

Asimismo, los Laboratorios de Computación, albergan entre cuatrocientas a quinientas personas por día. El acceso a los ambientes se controla mediante la apertura por parte del docente, a quien se le entrega una llave de acceso, misma que debe devolverse al finalizar su turno. Los estudiantes ingresan de manera libre cada vez que el docente proporciona el acceso utilizando su llave. A partir de esta situación se presentan varios factores de riesgo respecto a los activos tecnológicos donde se encuentran:

- Equipos de computación.
- Periféricos.
- Equipo multimedia.
- Para el resguardo y control de los activos, el Departamento de Soporte Técnico es el directo responsable de la administración de los laboratorios.

Las tareas de administración comprenden:

- Atención a los laboratorios.
- Instalación de software.
- Gestión del cableado de red.
- Reparación de equipos de computación.

Debido a la cantidad de equipamiento tecnológico y a la naturaleza del sistema de educación modular, las tareas de: gestión, administración y control, se vuelven complejas. Los controles de seguridad se realizan de manera manual, relevando los controles a los compañeros de trabajo de acuerdo a un informe previo. Como apoyo, se utilizan las cámaras de seguridad para evitar las susceptibilidades en los controles diarios; sin embargo, el control no es integral ni preciso.

3.1.2. Disposición Tecnológica de los Laboratorios de Computación

La Universidad cuenta con 8 laboratorios de computación, 6 de uso para materias (A, B, C, D, E, F) y 2 para cursos especializados (Cisco y Microsoft). Además, que el acceso al laboratorio B y F es a través del laboratorio A y E respectivamente.

Tomando en cuenta lo mencionado anteriormente, pudo notarse que dentro de los laboratorios en total hay más de cien equipos de computación, sin considerar todos los demás equipos usados en las distintas áreas de la Universidad. Aunque se coordinan los horarios como también el uso de los laboratorios mediante normativas, no es un control suficiente porque los laboratorios son importantes por su valor de inversión económica como también por el perjuicio académico que significa para un estudiante, no contar con su equipo de computación para realizar prácticas en su respectiva materia.

3.1.3. Factores de Riesgo Tecnológico

Según una entrevista realizada al Supervisor de Soporte Técnico referente a la administración de los laboratorios, se pudo notar las siguientes vulnerabilidades:

- La cantidad de equipos de computación y multimedia que se encuentran dentro de cada uno de los ocho laboratorios; además, de la cantidad de personas que transitan los mismos, aumenta la probabilidad de sufrir robos por parte de estudiantes que usan los laboratorios.

- La pérdida de activos de los laboratorios significaría una considerable pérdida económica para la Universidad, debido al alto costo de cada uno de los equipos dentro de dichos recintos.
- Actualmente, no hay una forma de controlar quién debería tener acceso a los laboratorios y quién no.
- Hay horarios en los que el personal de Soporte Técnico se ve limitado por la cantidad de tareas que deben cumplir y los laboratorios de computación se vuelven más propensos a sufrir robos de activos.

3.2. FASE DE PLANIFICACIÓN

En la fase de planificación, se realizará un diagnóstico del estado actual de la red de datos, laboratorios de computación y cámaras de seguridad; además, de una comparativa de tecnologías de control de acceso para determinar la tecnología que mejor se integra a la red de datos de la Universidad.

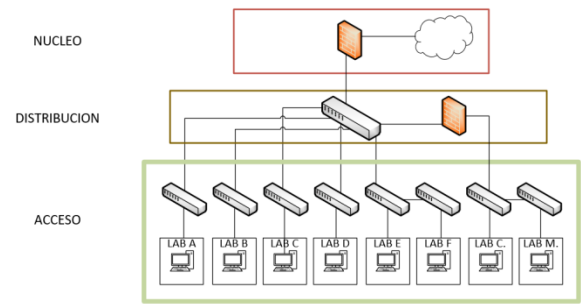
3.2.1. Datos Técnicos de la Red de Datos de los Laboratorios de Computación

A continuación, se detallarán todos los datos técnicos de la red de datos de los laboratorios de computación.

3.2.1.1. Equipos de Red

La distribución de los equipos de red de los laboratorios de computación cumple con los requisitos del diseño jerárquico de redes Cisco.

FIGURA Nº III.1: TOPOLOGÍA LÓGICA DE LA RED DE LOS LABORATORIOS DE COMPUTACIÓN



Fuente: elaboración propia

3.2.1.2. Capas del Modelo de Red Jerárquico de Cisco

- NÚCLEO: Firewall.
- DISTRIBUCIÓN: Switch principal L3 3650 24 p.
- ACCESO: Switches de laboratorios y computadoras.

TABLA Nº III.1: SWITCHES DE LA CAPA DE ACCESO DE LA RED DE DATOS DE LOS LABORATORIOS DE COMPUTACIÓN

EQUIPOS DE RED			
LAB	EQUIPO	MODELO	UBICACION
A	Switch	Cisco Sg220,224	Data Center
B	Switch	Cisco Sg224	Data Center
C	Switch	Cisco sg220	Gabinete Soporte Técnico
D	Switch	Cisco sg224	Gabinete Soporte Técnico
E	Switch	Cisco sg224	Gabinete lab E
F	Switch	Cisco sg220	Gabinete lab E
CISCO	Switch	TL-SG1024	Gabinete lab Cisco
MICROSOFT	Switch	TL-SG1024	Gabinete lab Cisco

Fuente: elaboración propia

3.2.1.3. Equipos de Computación

TABLA Nº III.2: CANTIDAD DE EQUIPOS DE COMPUTACIÓN EN CADA LABORATORIO DE COMPUTACIÓN

LISTA DE LABORATORIOS DE COMPUTACIÓN Y CANTIDAD DE COMPUTADORAS		
N	LABORATORIO	CANTIDAD
1	A	36
2	B	20
3	C	17
4	D	20
5	E	17
6	F	25
7	CISCO	12
8	MICROSOFT	14
TOTAL		161

Fuente: elaboración propia

3.2.1.4. Descripción de conexiones lógicas

Cada uno de los laboratorios de computación, cuenta con un switch y estos se conectan a un switch central en el data center para la comunicación local. Para la comunicación hacia internet, el dispositivo switch central se conecta a un firewall de red que se encarga de administrar las conexiones salientes.

3.2.1.5. Descripción de conexiones físicas

Los laboratorios B, F, E, D, C, Cisco y Microsoft, utilizan conexiones directas entre ambientes mediante cable UTP, en el caso de los laboratorios E y F, se utiliza fibra óptica. Para el cableado de red de los equipos de computación, se utiliza la categoría 6 en un 90%, solamente 2 laboratorios (A y D) todavía utilizan la categoría 5e.

3.2.1.6. Direccionamiento IP

La siguiente tabla representa el direccionamiento IP actual de la red de laboratorios:

TABLA N° III.3: DIRECCIONES IP DE LA RED DE LOS LABORATORIOS DE COMPUTACIÓN

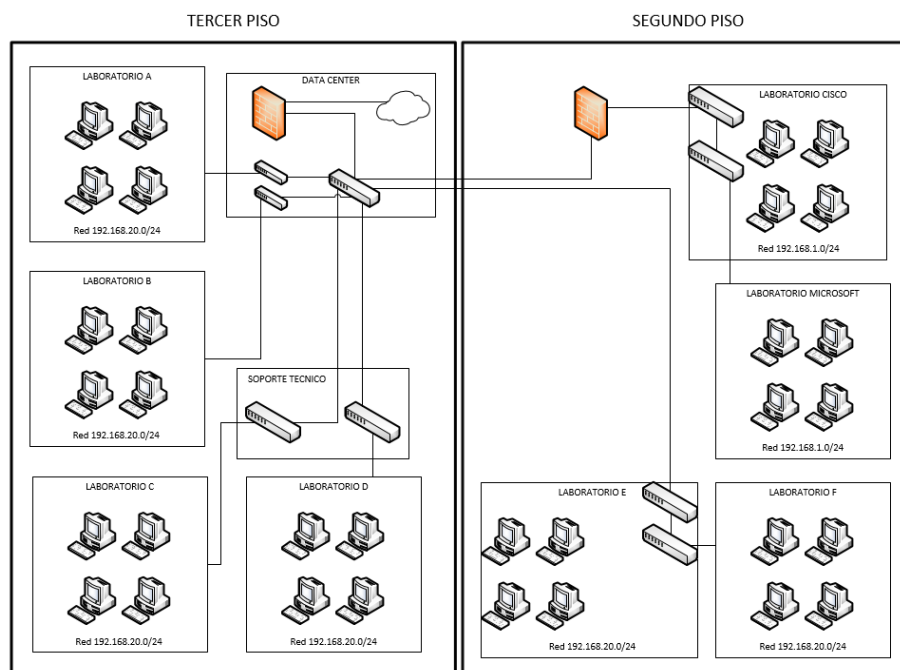
DIRECCIONAMIENTO IP ACTUAL DE LOS LABORATORIOS			
LAB	IP INICIAL	IP FINAL	MÁSCARA DE RED
A	192.168.20.66	192.168.20.108	255.255.255.0
B	192.168.20.47	192.168.20.67	255.255.255.0
C	192.168.20.5	192.168.20.25	255.255.255.0
D	192.168.20.26	192.168.20.46	255.255.255.0
E	192.168.20.109	192.168.20.129	255.255.255.0
F	192.168.20.130	192.168.20.154	255.255.255.0
CISCO	192.168.1.202	192.168.1.212	255.255.255.0
MICROSOFT	192.168.1.222	192.168.1.233	255.255.255.0

Fuente: elaboración propia

La topología de red que usan los laboratorios es de tipo estrella extendida, ya que es una de las más usadas y fácil de implementar; pero, también tiene ciertas desventajas, si el switch central falla, toda la red deja de funcionar; además, de ser un poco más costosa para su implementación que otras topologías.

3.2.1.7. Topología Lógica Actual de la Red de Datos

FIGURA N° III.2: TOPOLOGÍA LOGICA ACTUAL DE LA RED DE DATOS DE LOS LABORATORIOS DE COMPUTACIÓN



Fuente: elaboración propia

Basado en la gráfica anterior, se puede ver que el direccionamiento IP no es óptimo, dado que todos los laboratorios comparten una red plana, lo cual hace que la misma sea más propensa a colisiones innecesarias, que quizás en una red pequeña no sería un gran problema, Pero, considerando la cantidad de equipos con los que cuentan los laboratorios de computación en total, esto puede afectar el desempeño de la red. Es por eso que se tomará en cuenta la segmentación de la red, a manera de evitar tráfico de difusión innecesaria que disminuya la velocidad de la red y así simplificar la administración lógica de la red de laboratorios.

Para la integración del sistema de control de acceso y activos, se dividirá la red en dos segmentos de red principales: uno para los equipos de computación y otro para todos los dispositivos que conformarán el sistema de seguridad, que son las cámaras ip y el sistema de control de acceso y activos. La segmentación de la red optimizará el uso de los recursos de red, mejorando así su desempeño.

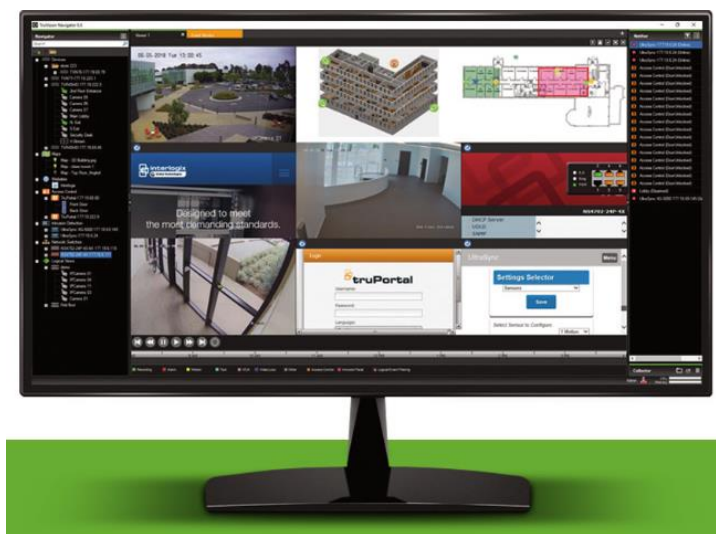
3.2.2. Sistema de Cámaras IP Interlogix

En el año 2018, se instalaron cámaras de seguridad en todos los laboratorios como medida preventiva de seguridad. Este sistema tiene tres partes:

- Software TruVision Navigator v7.0.
- Grabadora de video en red TruVSION NVR 22.
- Cámara IP TruVision Turret IR.

3.2.2.1. Software TruVision Navigator

FIGURA Nº III.3: SOFTWARE TRUVISION NAVIGATOR



Fuente: (interlogix, s.f.)

- Hasta 10 ventanas de video visibles a la vez.
- Vista de evento en vivo una vez accionada la cámara.
- Vista personalizada de todas las cámaras instaladas.

3.2.2.2. Video Grabadora en Red TruVision NVR 22

FIGURA N° III.4: TRUVISION NVR 22



Fuente: (interlogix, s.f.)

- Soporte para cámaras IP VGA de 8Mpx.
- Hasta 16 cámaras en tiempo real (30fps).
- Compresión h.264/h.265.
- Hasta 24TB de video guardado.
- Soporte para monitor triple.
- Archivado local mediante USB.

3.2.2.3. Cámara IP TruVision Turret IR

FIGURA N° III.5: TRUVISION TURRET IR

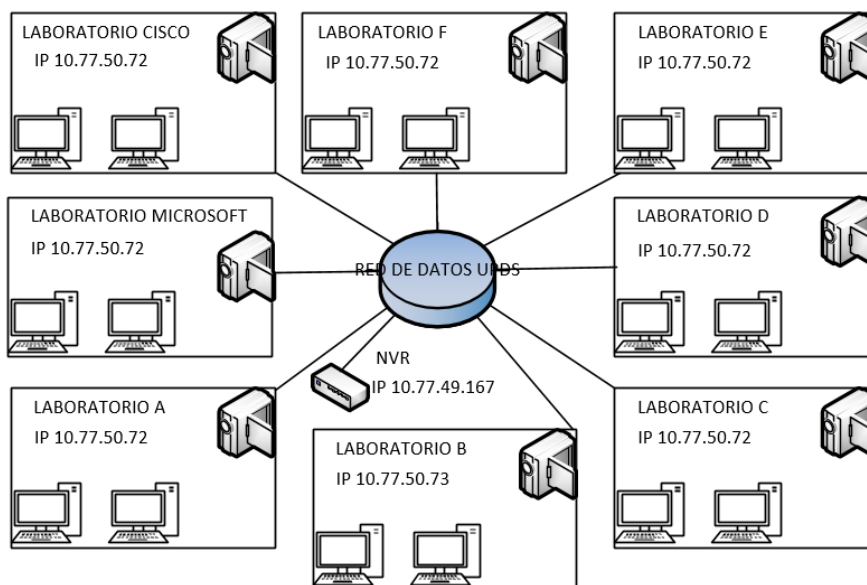


Fuente: (interlogix, s.f.)

- Resolución de 2MPx o 4MPx.
- Detector de movimiento integrado.
- Tecnología de Compresión h.264.

3.2.2.4. Topología Lógica de la Red de Vigilancia

FIGURA Nº III.6: TOPOLOGÍA LÓGICA DE RED DE VIGILANCIA



Fuente: elaboración propia

3.2.2.5. Direcciones IP de las Cámaras de Vigilancia

En la siguiente tabla se puede ver las direcciones IP y la ubicación de las cámaras IP en cada uno de los laboratorios de computación.

TABLA Nº III.4: DIRECCIONES IP DE LAS CÁMARAS DE VIGILANCIA

LABORATORIO	IP	UBICACION
A	10.77.50.72	Sobre la puerta de ingreso
B	10.77.50.73	Fondo con visión a la puerta de ingreso
C	10.77.50.74	Fondo con visión a la puerta de ingreso
D	10.77.50.75	Fondo con visión a la puerta de ingreso
E	10.77.50.76	Fondo con visión a la puerta de ingreso
F	10.77.50.77	Sobre la puerta de ingreso
CISCO	10.77.50.78	Sobre la pizarra
MICROSOFT	10.77.50.79	Fondo con visión hacia la pizarra

Fuente: elaboración propia

3.2.3. Comparativa de Tecnologías de Control de Acceso

A continuación, se realizará una comparación de tecnologías de control de acceso, para determinar la que mejor se integra con las necesidades de la universidad.

3.2.3.1. Tecnologías de Control de Acceso

Las tecnologías más usadas para un sistema de control de acceso se basan en dos categorías:

1. Sistemas biométricos:

Los sistemas biométricos reconocen rasgos de las personas como ser: huella dactilar, forma facial, iris o retina. Estos son unos de los muchos sistemas biométricos y se engloban dado que poseen características similares.

2. Sistemas basados en posesión:

- Tarjetas magnéticas.
- Código de barras.
- Memorias de contacto.
- RFID.

3.2.3.2. Factores de comparación de tecnologías de Control de Acceso

Siempre que se necesite realizar una autenticación segura del usuario, existen diferentes parámetros que son necesarios tomar en cuenta para elegir un sistema de control de acceso en particular. Los parámetros que se pudieron identificar son la fiabilidad, facilidad de uso, estabilidad del medio de identificación, tiempo de acceso, mantenimiento del lector y el precio de los componentes del sistema.

- Fiabilidad, se entiende como la probabilidad de que el sistema de autenticación rechace a un usuario; es decir, la probabilidad de identificar erróneamente a un usuario, concediendo o rechazando el acceso legítimo del mismo, porque no es capaz de identificarlo correctamente.
- La Facilidad de uso, se ve afectada por la poca relación que tienen algunas personas con la tecnología, además de la inexperiencia con la misma, por lo

que, para la implementación de cualquiera de estos sistemas de control de acceso, se requiere capacitar a todos los usuarios en el uso del sistema.

- La Estabilidad del Medio de Identificación, hace referencia a las posibles causas que pueden interferir y crear errores de lectura. Son factores ambientales (ruido, suciedad, clima, etc) y condiciones físicas (cortaduras, envejecimiento). La estabilidad para los sistemas basados en tarjetas hace referencia al desgaste que pueden sufrir las mismas y es un elemento importante a considerar, porque si el medio de identificación se desgasta, fácilmente el usuario tendrá problemas para identificarse.
- El Tiempo de Acceso, es uno de los factores más importantes para medir el rendimiento de un sistema de control de acceso, no solo por el valor del tiempo; sino, por la congestión que podría crear en distintas áreas de una organización. Es por esto que es necesario que los usuarios tengan identificación rápida para que puedan acceder a las instalaciones.
- El Mantenimiento, es importante para alargar la vida útil del dispositivo y evitar fallas en la identificación de usuarios. Sin embargo, esto implica un costo, lo cual influye en la elección de la tecnología.
- El Precio, es un factor muy importante debido a la inversión inicial que se requiere.

3.2.3.3. Análisis de comparativa de tecnologías de Control de Acceso

En las siguientes tablas se puede comparar todos los parámetros previamente nombrados, para determinar la tecnología a usar para el diseño del sistema de control de acceso y activos.

TABLA Nº III.5: FIABILIDAD DE LOS SISTEMAS DE CONTROL DE ACCESO

TECNOLOGÍA	FIABILIDAD
SISTEMAS BIOMÉTRICOS	La fiabilidad de los sistemas biométricos es alta porque es difícil encontrar a dos individuos con rasgos faciales, huella dactilar, iris iguales.
TARJETAS MAGNÉTICAS	Es más fiable que el código de barras. Sin embargo, pueden ser duplicados y leídos por otro lector fácilmente.
CÓDIGO DE BARRAS	La fiabilidad es baja, dado que los códigos de barras pueden ser fotocopiados fácilmente.
MEMORIAS DE CONTACTO	La fiabilidad de las memorias de contacto es media ya que son más difíciles de duplicar que las tarjetas de código de barras, sin embargo, puede ser prestada a otra persona lo cual disminuye la fiabilidad.
RFID	La fiabilidad es mayor que las de banda magnética y código de barras porque las tarjetas poseen un código único de fábrica que no se repite además que son más difíciles de duplicar por la seguridad que tienen.

Fuente: elaboración propia

TABLA Nº III.6: FACILIDAD DE USO DE LOS SISTEMAS DE CONTROL DE ACCESO

TECNOLOGÍA	FACILIDAD DE USO
SISTEMAS BIOMÉTRICOS	Son fáciles de usar el único problema que tienen es al registrarse por problemas de alineación o especificaciones del lector.
TARJETAS MAGNÉTICAS	Son fáciles de usar; pero deben pasar por un lector provocando desgaste de las tarjetas.
CÓDIGO DE BARRAS	Son fáciles de usar; pero deben pasar por un lector provocando desgaste de las tarjetas.
MEMORIAS DE CONTACTO	Es de fácil manejo al igual que las tarjetas de magnéticas y código de barras.
RFID	es muy fácil de utilizar ya que no se necesita que la tarjeta pase por una ranura además que el uso de radio frecuencia permite que pueda ser leído a través de ropa billetera o una mochila.

Fuente: elaboración propia

TABLA Nº III.7: ESTABILIDAD DEL MEDIO DE IDENTIFICACIÓN DE LOS SISTEMAS DE CONTROL DE ACCESO

TECNOLOGÍA	ESTABILIDAD DEL MEDIO DE IDENTIFICACIÓN
SISTEMAS BIOMÉTRICOS	La estabilidad del medio es alta porque los rasgos faciales o huellas dactilares no cambian con el tiempo solamente en caso de producirse alguna lesión podría presentarse un problema.
TARJETAS MAGNÉTICAS	La estabilidad es baja porque el desgaste de la tarjeta es alto por el rozamiento continuo con el lector lo cual puede producir fallos.
CÓDIGO DE BARRAS	La estabilidad es baja porque el desgaste de la tarjeta es alto por el rozamiento continuo con el lector lo cual puede producir fallos.
MEMORIAS DE CONTACTO	La estabilidad es alta porque el desgaste es bajo ya que es altamente resistente porque la memoria no hace contacto con el lector.
RFID	La estabilidad es media ya que la lectura se hace mediante radio frecuencia por lo que las tarjetas no se desgastan sin embargo una flexión excesiva de la tarjeta puede dañar la misma.

Fuente: elaboración propia

TABLA Nº III.8: TIEMPO DE ACCESO DE LOS SISTEMAS DE CONTROL DE ACCESO

TECNOLOGÍA	TIEMPO DE ACCESO
SISTEMAS BIOMÉTRICOS	El tiempo de acceso es medio porque se debe posicionar correctamente para identificarse lo que puede ocasionar fallos y puede tardar desde 0,5 segundos hasta 3 segundos.
TARJETAS MAGNÉTICAS	Tomando en cuenta la posición de la banda que tiene la tarjeta al pasarla por el lector puede tardar 2 segundos
CÓDIGO DE BARRAS	Al posicionar la tarjeta con respecto al lector de código de barras por lo que el tiempo de acceso puede tardar hasta 3 segundos
MEMORIAS DE CONTACTO	Se realiza con contacto y puede tardar hasta 3 segundos
RFID	Con el radio de lectura y la capacidad de leer múltiples tarjetas al mismo tiempo el tiempo de lectura oscila entre los 0,05 segundos hasta 0.5 segundos

Fuente: elaboración propia

TABLA Nº III.9: MANTENIMIENTO DE LOS SISTEMAS DE CONTROL DE ACCESO

TECNOLOGÍA	MANTENIMIENTO
SISTEMAS BIOMÉTRICOS	El mantenimiento es alto porque es recomendable limpiar el hardware una vez cada 3 meses como mínimo dependiendo del sistema que se use.
TARJETAS MAGNÉTICAS	El mantenimiento es medio porque es necesario limpiar constantemente el lector porque el polvo y la suciedad afectan su rendimiento.
CÓDIGO DE BARRAS	El mantenimiento es medio porque el lente de enfoque puede ser dañado con el tiempo afectado por el polvo o la luz solar excesiva.
MEMORIAS DE CONTACTO	El mantenimiento es muy bajo porque el lector es de acero inoxidable.
RFID	Los lectores son unidades totalmente selladas y sin partes móviles, lo que garantiza un funcionamiento correcto sin límite de uso soporta altas y bajas temperaturas, ni la lluvia. Además, estos lectores tienen muy poco desgaste, ya que el lector no entra en contacto con las tarjetas como los lectores de tarjetas magnéticas o código de barras.

Fuente: elaboración propia

TABLA Nº III.10: PRECIO DE LOS SISTEMAS DE CONTROL DE ACCESO

TECNOLOGÍA	PRECIO
SISTEMAS BIOMÉTRICOS	El precio de estos sistemas es el más elevado de la lista por que tienen mayor seguridad.
TARJETAS MAGNÉTICAS	El costo es bajo porque solo debe imprimir la banda.
CÓDIGO DE BARRAS	Su costo es bajo dado que el código de barras es de fácil impresión.
MEMORIAS DE CONTACTO	El precio es alto con relación a las tarjetas magnéticas y código de barras porque las memorias de contacto no se desgastan.
RFID	Depende del fabricante, aunque en los últimos años bajaron los precios por el alto uso de esta tecnología en el control de inventarios y accesos.

Fuente: elaboración propia

TABLA Nº III.11: COMPARATIVA DE TECNOLOGÍAS DE CONTROL DE ACCESO

	SISTEMAS BIOMÉTRICOS	TARJETAS MAGNÉTICAS	CÓDIGO DE BARRAS	MEMORIA DE CONTACTO	RFID
FIABILIDAD	ALTA	MEDIO	BAJA	MEDIO	MEDIO
FACILIDAD DE USO	ALTA	ALTA	ALTA	ALTA	ALTA
ESTABILIDAD	ALTA	BAJA	BAJA	ALTA	MEDIO
TIEMPO DE ACCESO	MEDIO	BAJO	BAJO	BAJO	BAJO
MANTENIMIENTO	ALTO	MEDIO	MEDIO	BAJO	BAJO
PRECIO	ALTO	BAJO	BAJO	MEDIO	BAJO

Fuente: elaboración propia

Tomando en cuenta la tabla anterior, podemos ver las ventajas que ofrece RFID sobre las demás tecnologías:

- Tarjetas sin desgaste: dado que la tarjeta no hace contacto con el lector, no se desgasta y también se alarga su vida útil a comparación de las tarjetas de código de barras o tarjetas magnéticas, por lo que el resultado es la optimización de recursos.
- Los lectores no necesitan mantenimiento, porque las tarjetas nunca entran en contacto con el lector.
- El tiempo de acceso es más rápido; además de poder leer múltiples tarjetas al mismo tiempo.
- Tarjetas re escribibles: a comparación de las tarjetas magnéticas o de código de barras las tarjetas RFID se pueden reescribir.
- El precio ha reducido considerablemente en los últimos años, para poder competir con otras tecnologías de control de acceso.

Además, que RFID cuenta con sistemas de control de inventarios y antirobo, por lo que esta tecnología es la que mejor se integra a las necesidades de la Universidad Privada Domingo Savio.

3.2.4. Fabricantes de Sistemas de Control de Acceso RFID

Se comparará tres fabricantes de sistemas de control de acceso basados en tecnología RFID por las siguientes razones:

- Los años de experiencia que tiene en el mercado.
- El costo de la implementación del sistema de control de acceso.
- La arquitectura del sistema de control de acceso.

3.2.4.1. SUPREMA

Uno de los líderes en tecnología RFID y control de acceso a nivel mundial, cuenta con una gama de productos amplia aplicada a varios sectores de desarrollo para tecnología RFID; además, de formar parte del mercado hace más de quince años.

3.2.4.1.1. Ventajas

- Amplia gama de productos con el fin de ofrecer una solución personalizada a cada empresa, tomando en cuenta las necesidades de cada una.
- Partner de varias empresas distribuidoras y fabricantes de sistemas RFID, que también llevan mucho tiempo ofreciendo soluciones de control de acceso.
- Basta experiencia en soluciones de sistemas de seguridad, dado que trabaja con empresas de distintos tamaños.
- API de desarrollo; además, de un software especializado en gestión de control de acceso, que proveen una solución íntegra acorde a las necesidades de cada organización.

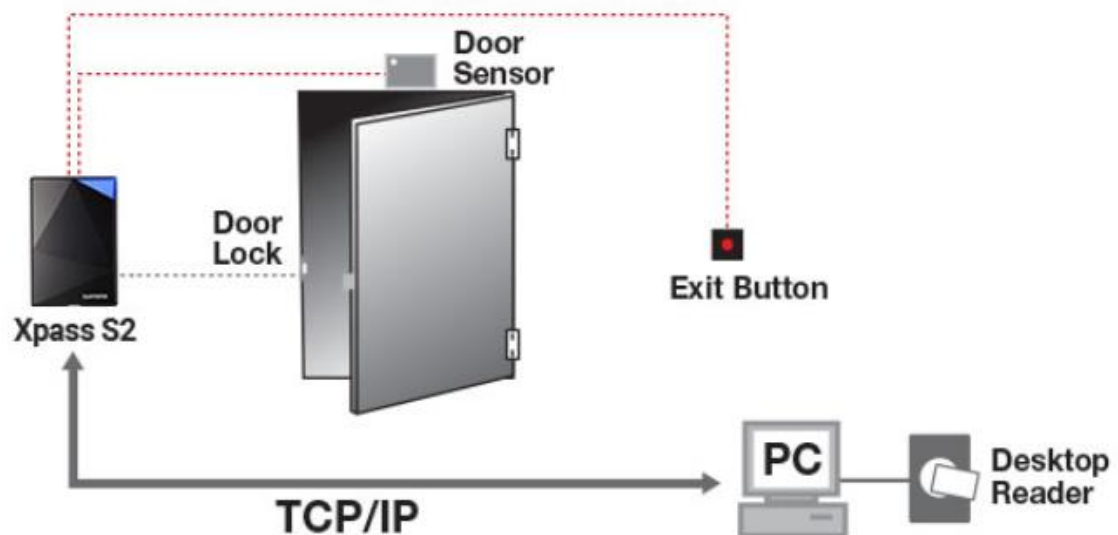
3.2.4.1.2. Desventajas

- No cuenta con sucursales en Latinoamérica y eso aumenta relativamente el costo de la implementación, por el valor agregado que sería la importación al país de la tecnología.

3.2.4.1.3. Modelo de Arquitectura de Sistema de Control de Acceso SUPREMA

El sistema de control de acceso Suprema, usa lectores RFID que pueden operar de manera autónoma o solicitar autenticación a través de la red de datos al servidor, donde estará instalado el software de control de acceso.

FIGURA Nº III.7: MODELO DE SISTEMA DE CONTROL DE ACCESO SUPREMA



Fuente: (supremainc, s.f.)

3.2.4.2. INTERLOGIX

Interlogix, ofrece soluciones de seguridad a pequeñas y medianas empresas, con énfasis en crear edificios inteligentes que se acomoden a las necesidades de cada organización en particular.

3.2.4.2.1. Ventajas

- Fácil integración del sistema de control de acceso, pagando una licencia que permite la interoperación de las cámaras y el sistema de control de acceso para que usen un solo software.

- Interlogix cuenta con sucursales en Latinoamérica, lo que facilita la cotización y economiza en el precio de la inversión.

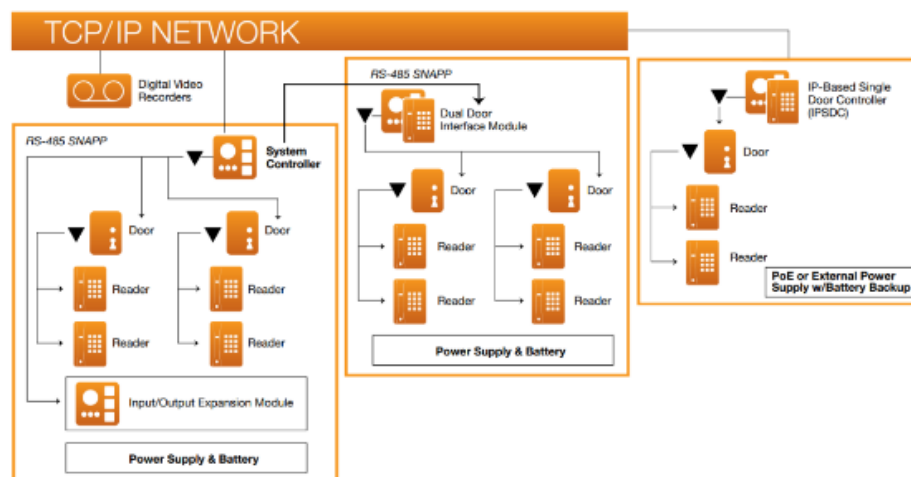
3.2.4.2.2. Desventajas

- Costo de licencias de operación de dispositivos y cámaras ip elevado.
- Costo de implementación relativamente elevado, a causa de que la integración de cada uno de los dispositivos y el uso de cada uno de sus softwares supone una inversión.
- Las extensiones de control de acceso para administrar un mayor número de dispositivos, ocupa demasiado espacio por el tamaño de cada una de las placas que se deben adherir a la placa principal.

3.2.4.2.3. Modelo de Arquitectura de sistemas de Control de Acceso INTERLOGIX

El sistema de control de acceso Interlogix, usa un controlador central que servirá para la interoperación de cada uno de sus lectores RFID con el servidor encargado de autenticar a los usuarios.

FIGURA Nº III.8: MODELO DE SISTEMA DE CONTROL DE ACCESO INTERLOGIX



Fuente: (interlogix, s.f.)

3.2.4.3. ZKTEKO

Es una multinacional que se especializa en la fabricación y desarrollo de tecnología para control de acceso. Sus productos están disponibles en varios países de Latinoamérica y el mundo, a precios justos además de tener una vasta experiencia en sistemas de seguridad, ya que forma parte del mercado hace más de diez años.

3.2.4.3.1. Ventajas

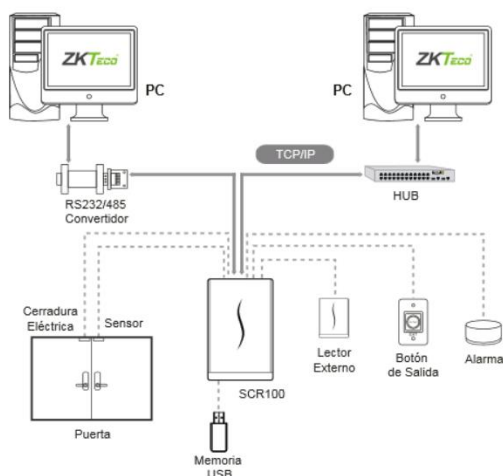
- El sistema es de fácil implementación, gracias a la cantidad de soluciones que ofrece y se acomodan a las necesidades de cada empresa.
- El costo de los equipos es bajo, ya que están disponibles en varios países de Latinoamérica, lo que facilita su compra.
- Productos confiables en base a la experiencia que tiene por los años que lleva, ofreciendo soluciones de control de acceso.

3.2.4.3.2. Desventajas

- Costo de licencia de software de control de acceso elevado.

3.2.4.3.3. Modelo de Arquitectura de Sistema de Control de Acceso ZKTEKO

El sistema de control de acceso Zkteko, usa lectores RFID que pueden operar de manera autónoma o solicitar autenticación a través de la red de datos al servidor, donde estará instalado el software de control de acceso.

FIGURA Nº III.9: MODELO DE SISTEMA DE CONTROL DE ACCESO ZKTEKO

Fuente: (zktecolatinoamerica, s.f.)

3.2.5. Selección del Fabricante

Se utilizará la solución Suprema por las siguientes razones:

- La ventaja de poder optar por una administración distribuida o centrada, ya que los equipos pueden funcionar individualmente o conectados a un servidor central. La independencia de cada uno de los lectores, reducirá el índice de fallos; dado que si el servidor central falla, no afectará el funcionamiento de los lectores.
- La utilización de lectores IP reduce los costos de instalación, operación e implementación, porque el nodo central que proveen otro tipo de soluciones ocupa mucho espacio y soporta un limitado número de lectores, por lo que en caso de tener que instalar varios lectores no solo es un mayor gasto; sino, que también se necesitará un espacio mayor, donde estos equipos puedan estar resguardados, por lo que el uso de lectores IP es más simple y beneficioso en todo sentido.
- Considerando la posibilidad en un futuro de implementar esta solución en todo el Campus Universitario, la ventaja que el sistema tenga una API, es valiosa. Una API proveerá la ventaja de desarrollar un software que se integre

mejor a las necesidades futuras de la Universidad, proveyendo una solución integra y óptima para todo el Campus Universitario.

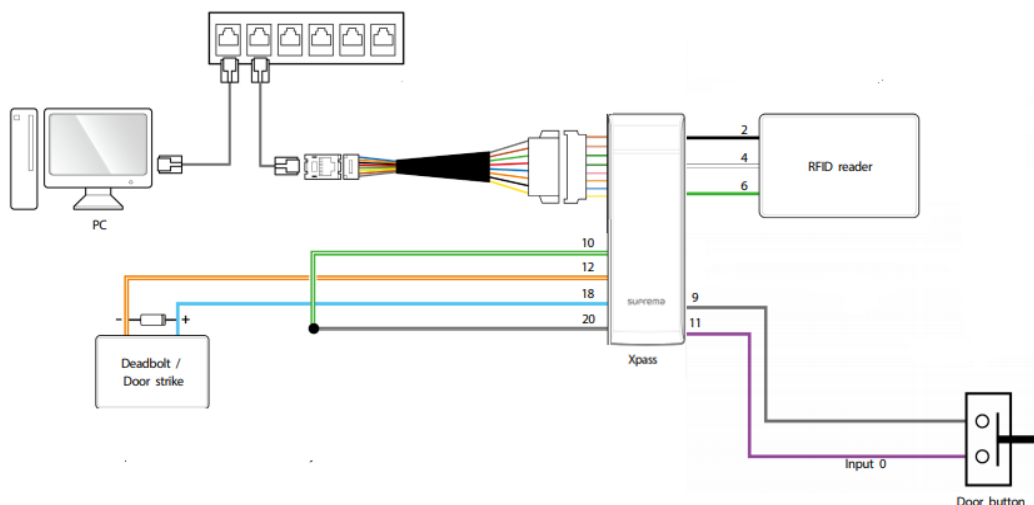
3.3. Fase de Diseño

En la fase de diseño una vez concluida la selección de tecnología y fabricante, se procederá con la presentación del diseño de la topología lógica del sistema, componentes y funcionamiento.

3.3.1. Topología lógica del sistema RFID

El componente principal del sistema de control de acceso y activos es el lector principal Suprema xpass, que estará ubicado afuera de cada uno de los laboratorios de computación y a su vez estará conectado a un lector dentro de los mismos, para poder resguardar los activos. Para autenticar usuarios, este se conectará a un servidor a través de la red de datos de los laboratorios de computación.

FIGURA Nº III.10: TOPOLOGÍA FÍSICA DE SISTEMA DE CONTROL DE ACCESO Y ACTIVOS

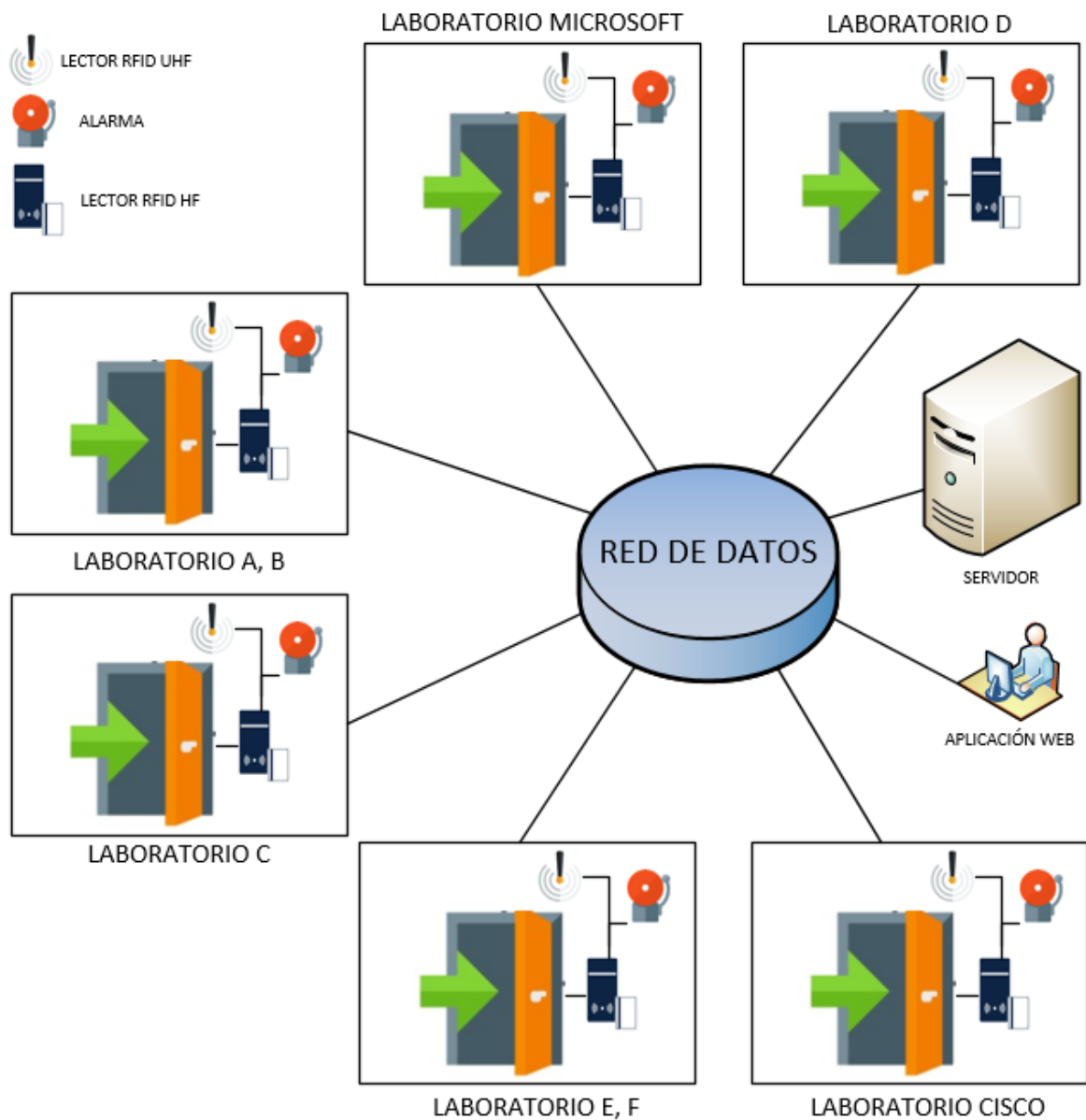


Fuente: elaboración propia

3.3.1.1. Topología Lógica de Sistema de Control de Acceso y Activos

El siguiente diseño comprende el uso de 6 lectores para 6 puertas, porque 2 el ingreso al laboratorio de computación B y F es a través del A y E respectivamente, que estarán conectados a la red de datos.

FIGURA Nº III.11: TOPOLOGÍA LÓGICA DE SISTEMA DE CONTROL DE ACCESO Y ACTIVOS RFID



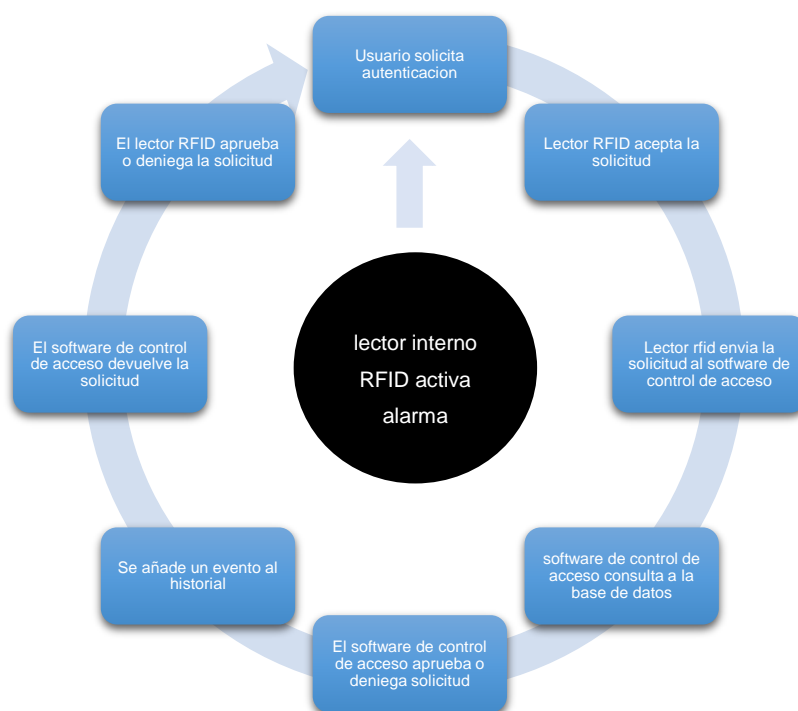
Fuente: elaboración propia

3.3.1.2. Proceso Logístico de Funcionamiento de Sistema de Control de Acceso y Activos RFID

Con el siguiente proceso logístico, se explicará la manera en la que los usuarios se podrán autenticar para acceder a los laboratorios de computación, una vez se cumplan las siguientes condiciones:

1. Registrar activos tecnológicos en el software de control de activos: mediante este proceso se registrarán todos los activos tecnológicos de los laboratorios de computación, de tal manera que cada activo esté asociado a un tag RFID.
2. Registrar a los usuarios en el software de control de acceso: cada una de las tarjetas RFID estará asociada a un estudiante, registrando sus datos en las mismas para que el lector RFID pueda autenticar al usuario y determinar si tiene permiso o no para entrar a los laboratorios de computación.

FIGURA Nº III.12: FLUJO DE SISTEMA DE CONTROL DE ACCESO



Fuente: Elaboración propia.

3.3.1.3. Proceso de Autenticación de Usuarios y Resguardo de Activos

1. El estudiante aproxima una tarjeta RFID al lector de control de acceso para ingresar al laboratorio de computación.
2. El lector de control de acceso procesa la solicitud.
3. El lector de control de acceso envía la solicitud a través de la red de datos, hasta llegar al servidor donde se está ejecutando el software de control de acceso y activos.
4. El software procesa la solicitud y consulta a la base de datos la información del estudiante.
5. Acorde a la información que se haya obtenido de la base de datos, se aceptará o denegará la solicitud.
6. Una vez que se haya aprobado o denegado la solicitud, el software de control de acceso agrega un evento al historial de eventos del sistema con el nombre y cédula de identidad del estudiante; además de incorporar si se aprobó o denegó la solicitud para el ingreso a los laboratorios de computación, fecha y hora.
7. El servidor devuelve la solicitud al lector de control de acceso, a través de la red de datos.
8. El lector RFID aprueba o deniega la solicitud acorde a la información que recibió del software de control de acceso y activos, accionando el relé para destrabar la chapa electromagnética o denegando la solicitud.
9. Cuando el lector interno de control de activos detecta un tag que pertenezca a uno de los activos tecnológicos que están dentro de los laboratorios de computación, activa la alarma y cualquier solicitud no se procesará hasta tomar medidas sobre dicho suceso.

3.3.1.4. Descripción del Equipamiento a Utilizar

Los siguientes dispositivos formaran parte del sistema de control de acceso:

TABLA Nº III.12: DISPOSITIVOS DE SISTEMA DE CONTROL DE ACCESO

DISPOSITIVO	DESCRIPCIÓN
TARJETA RFID PASIVA MIFARE 1K	Tarjeta pasiva de proximidad para control de acceso que se usará para identificar a todas las personas que deseen ingresar a los laboratorios de computación y servirá como carnet de estudiante.
TAG UHF RFID	Tag adhesivo de ultra alta frecuencia que se ubicará dentro de todos los activos tecnológicos de los laboratorios de computación que puedan sufrir algún atentado como ser case, monitor, teclado, ratón, sillas y proyectores.
LECTOR RFID HF SL500A USB	Lector/escritor para computadora con soporte para tarjetas pasivas de alta frecuencia (13,56 MHz), se usará para asociar la información de un estudiante a una tarjeta pasiva RFID que será usada como carnet de estudiante.
LECTOR RFID UHF RT400A	Lector/escritor para computadora con soporte para etiquetas UHF (840-960 MHz) que se usará para adjuntar el nombre del activo a una tarjeta adhesiva UHF y así poder controlar los activos dentro de los laboratorios de computación.
CHAPA ELECTROMAGNÉTICA YM-280	Cerradura electromagnética de puerta que mantiene su hoja de hierro unida a la puerta. Una vez se corta el paso de corriente a través del relé de activación esta se separará de su hoja de hierro para abrir la puerta.
FUENTE DE ALIMENTACIÓN CHAPA ELECTROMAGNÉTICA ADP 16.5V 1.21A	Fuente de alimentación continua de 16 voltios para cerradura electromagnética.
BOTON DE SALIDA ABK-800A	Botón que estará ubicado dentro del laboratorio, una vez presionado abrirá la puerta.
LECTOR UHF INTEGRADO SL130	El lector tendrá la función de sonar la alarma y evitar la activación del relé de apertura de chapa cuando detecte que uno de los tags UHF que estarán ocultos dentro de los activos tecnológicos de los laboratorios de computación.
LECTOR HF XPASS XPM-POE	Los lectores estarán ubicados al lado de las puertas de los laboratorios de computación y serán utilizados para autenticar a los estudiantes que deseen ingresar a los mismos presentando sus carnets además de añadir un evento al historial de ingresos del software de control de acceso.
SOFTWARE RFID BIOSTAR 2	Software de administración de lectores RFID vía web que autorizará o denegará el acceso además de mantener un historial de todas las solicitudes para ingresar a los laboratorios.
CABLE UTP CAT 6 BRAND REX	Cable de red que se usará para cablear toda la instalación del sistema.

Fuente: elaboración propia

3.3.2. Integración del Sistema de Control de Acceso y Activos a la Red de Laboratorios de Computación

Para una óptima integración del sistema de control de acceso y activos, se debe optimizar los recursos de red, ya que el estado actual de la red de datos de los laboratorios de computación, no cumple con los requisitos para poder integrar de manera efectiva y dar prioridad a los datos que envíe el sistema de control de acceso y activos, es por eso que se propone usar el modelo de tres capas de CISCO; además de implementar Vlans y VLSM para segmentar las redes en todos los switches. Así también, el protocolo de conexión estándar IEEE 802.1.Q, ya que es compatible con switches no administrables y se usa para el etiquetado Vlan. A manera de centralizar la administración, también se implementará un dominio de Vlans VTP en el switch de capa 3, con la implementación de este protocolo, se puede modificar las Vlans y transmitir toda la configuración a todos los switches, que serán parte del dominio VTP o sea de la red de los laboratorios de computación. La aplicación de estos cambios en la red de laboratorios de computación optimizará el ancho de banda local, segmentando las redes lógicamente y dando prioridad al tráfico del sistema de control de acceso y activos.

3.3.2.1. Propuesta de Diseño de Red

Usando la técnica de segmentación VLSM, se realizará el direccionamiento IP para cada laboratorio dentro de la red (192.168.1.0).

La siguiente asignación de redes, segmentación IP y VLANs, se usará para los laboratorios y permitirá una óptima integración del sistema de control de acceso y activos.

TABLA Nº III.13: DISEÑO DE RED

LAB	EQUIPOS	IPs	SEGMENTO DE RED	IP FINAL	VLAN
A	36	64	192.168.1.0/26	192.168.1.63	10
B	20	32	192.168.1.64/27	192.168.1.95	20
C	17	32	192.168.1.96/27	192.168.1.127	30
D	20	32	192.168.1.128/27	192.168.1.159	40
E	17	32	192.168.1.160/27	192.168.1.191	50
F	25	32	192.168.1.192/27	192.168.1.223	60
CISCO	12	16	192.168.1.224/28	192.168.1.239	N/A
MICROSOFT	14	16	192.168.1.240./28	192.168.1.254	N/A

Fuente: elaboración propia

El tráfico de la red de control de acceso y activos debe tener prioridad por sobre la red de los laboratorios, ya que se debe dar prioridad al tráfico de autenticación a estudiantes, por lo que la red 192.168.2.0 se segmentará usando la técnica VLSM. La red de cámaras IP y el sistema de control de acceso formarán parte de esta red.

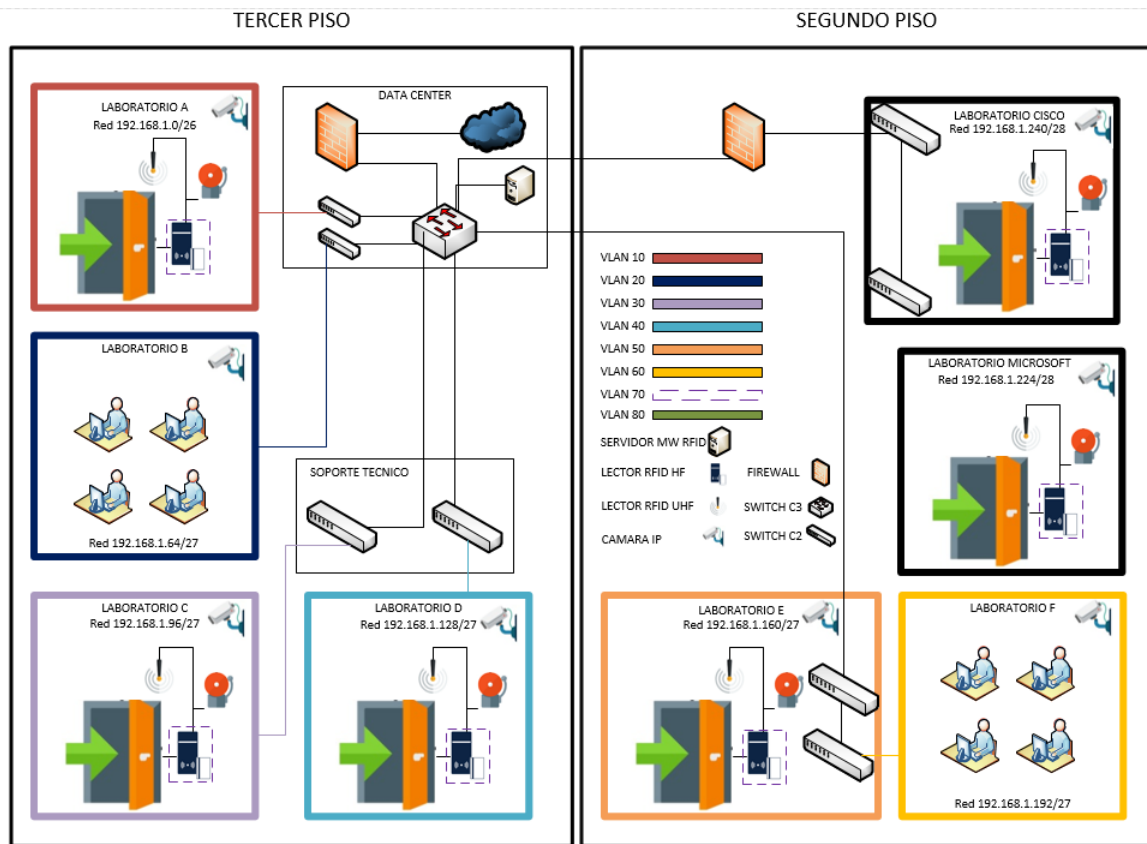
TABLA Nº III.14: RED DE CONTROL DE ACCESO Y CÁMARAS IP

RED	IPs	SEGMENTO DE RED	IP FINAL	VLAN
CONTROL DE ACCESO	16	192.168.2.0/27	192.168.2.15	70
CÁMARAS	16	192.168.2.0/27	192.168.2.31	80

Fuente: elaboración propia

3.3.2.2. Nueva Red de los Laboratorios de Computación

FIGURA N° III.13: NUEVA RED DE LOS LABORATORIOS DE COMPUTACIÓN



Fuente: elaboración propia

3.3.3. Costos de la Implementación del Sistema de Control de Acceso y Activos

La implementación de un sistema de control de acceso, cuenta con una placa base principal y varios lectores esclavos que conforman el sistema en general; es por eso que el costo de implementación es tan elevado, ya que, para controlar un mayor número de lectores, es necesario adjuntar módulos a la placa base además de tener que pagar una licencia en base a la cantidad de dispositivos que se desee controlar. Los lectores basados en tecnología IP, son una mejor inversión puesto que no necesitan de una placa base o un módulo para integrarse al sistema. Operan a través de la red de datos, lo cual abarata el costo de implementación; además, que

cada estudiante portará una tarjeta RFID que será el nuevo carnet de estudiante. Al elevar el precio del mismo en un 30%, no solo retornará el precio de inversión, sino, que generará beneficios a la Universidad. El costo para la implementación está basado en precios de tiendas locales como también de otros países, por lo que el presupuesto es un estimado porque para ciertos dispositivos se debe tomar en cuenta el precio de importación que tendrá.

TABLA Nº III.15: COSTO DE IMPLEMENTACIÓN

DESCRIPCION	CANT.	VALOR U. (Bs)	VALOR T. (Bs)
Licencia avanzada software BioStar 2.0	1	5.000	5.000
Controlador de acceso RFID Xpass S2	6	3600	21.600
Chapa electromagnética 280kg	6	360	2160
Fuente de poder de 15V	6	53	424
Lector/escritor de tarjetas UHF RT400A	1	5.850	5.850
Botón de salida de aluminio	6	72	432
Tarjetas pasivas MIFARE 1K	5.000	5	25.000
Cable UTP Grand Rex cat 6	200m	4.50	900
Lector UHF SL130	6	6.000	36.000
Tag UHF RFID inlay de corto alcance	1000	4	4.000
Lector HF SL500A USB	1	3500	3500
TOTAL		104.866	

Fuente: elaboracion propia

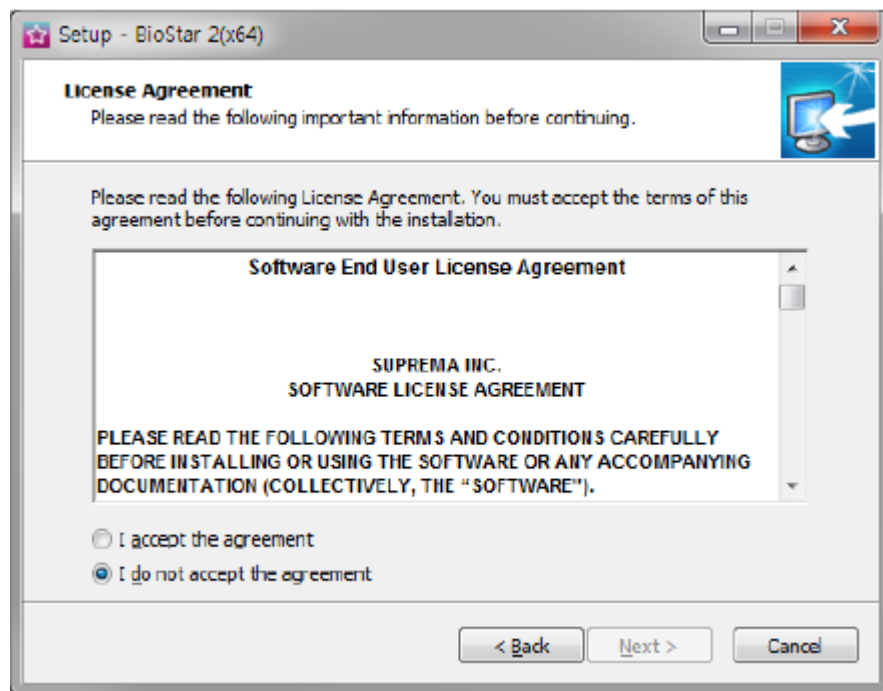
3.4. FASE DE OPERACIÓN

En la fase de operación, se procederá con la instalación del software para la administración del sistema.

3.4.1. Software BIO STAR 2

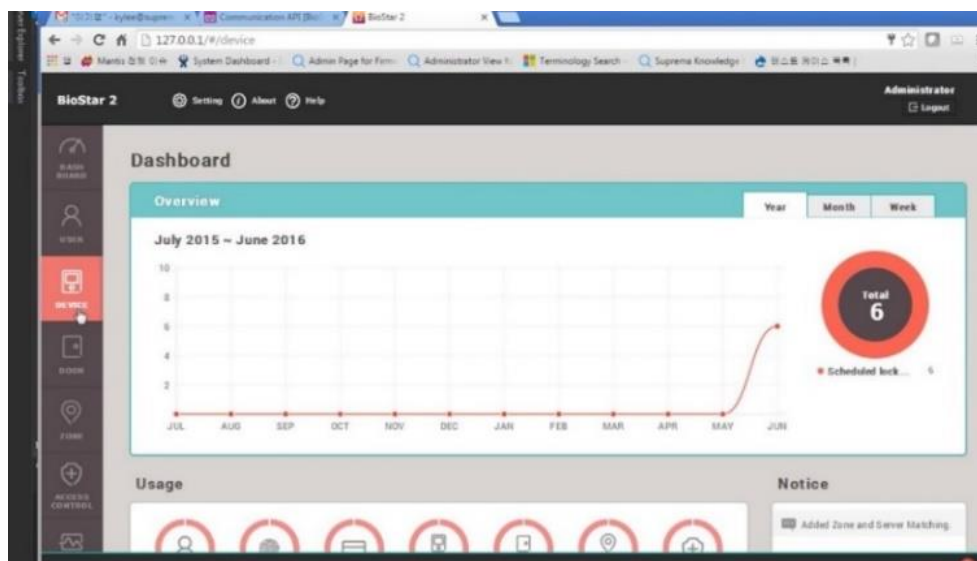
El software Biostar 2, será instalado en uno de los servidores que están en el Data Center. Para instalar el software solo se debe seguir con el asistente de instalación.

FIGURA Nº III.14: ASISTENTE DE INSTALACIÓN SOFTWARE BIOSTAR 2



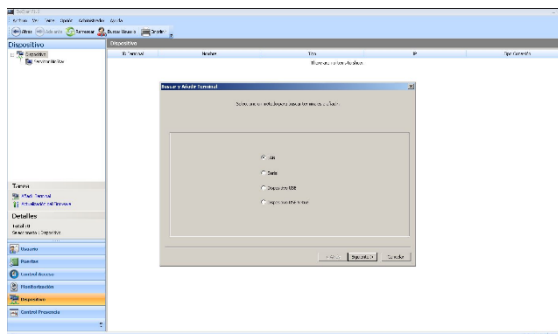
Fuente: (supremainc, s.f.)

Para entrar a la interfaz web del software, solo se debe ingresar la IP de loopback en un navegador web o sea (127.0.0.1), dado que los requerimientos del software son mínimos y se puede instalar en cualquier servidor que esté funcionando dentro del data center.

FIGURA Nº III.15: INTERFAZ PRINCIPAL SOFTWARE BIOSTAR 2

Fuente: (supremainc, s.f.)

Para la configuración inicial, conectar el lector directamente al servidor. Una vez que está conectado, directamente iniciar el software Biostar 2.0 para reconocer el lector.

FIGURA Nº III.16: INTERFAZ BIOSTAR PARA BUSCAR LECTORES RFID

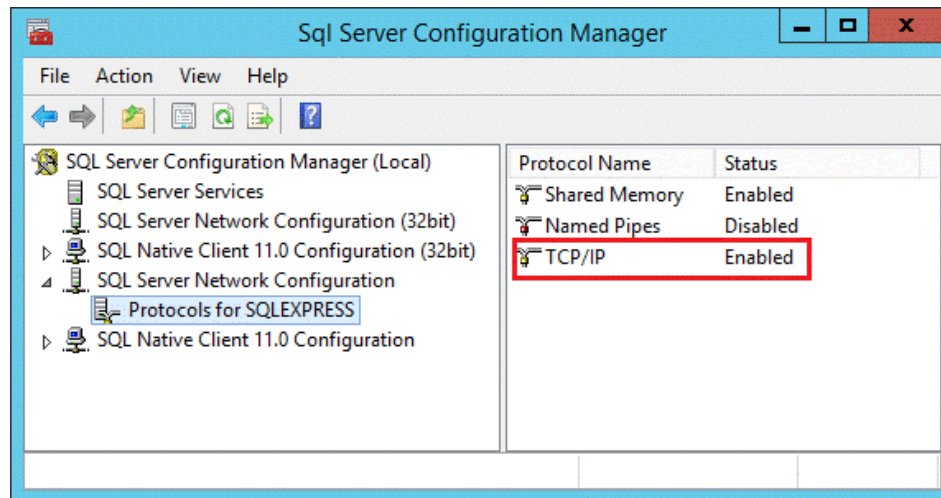
Fuente: (supremainc, s.f.)

El software configurará automáticamente el lector. Si el servicio DHCP falla la IP por defecto es (169.254.0.1) para configurar manualmente.

3.4.2. Base de Datos

Para conectar a la base de datos, se debe ejecutar el administrador de configuración SQL y configurar el protocolo TCP/IP para protocolos SQL EXPRESS.

FIGURA Nº III.17: ADMINISTRADOR DE CONFIGURACIÓN DE SERVIDOR SQL



Fuente: (webhosting, s.f.)

Una vez conformada la base de datos, se usarán los lectores/escritores SL130 y RT400A para adjuntar la información de un estudiante y un activo tecnológico a una tarjeta pasiva RFID y tag RFID respectivamente.

Se registrará en el software usuarios y activos siendo los activos usuarios con acceso denegado por defecto.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1. CONCLUSIONES

Durante la elaboración de carácter investigativo del presente proyecto, se pudo llegar a las siguientes conclusiones y recomendaciones:

- Tomando en cuenta todas las tecnologías aplicables al sector de control de acceso RFID, es la tecnología más apropiada a usar por su confiabilidad y seguridad.
- Aunque parezca que la tecnología RFID sigue teniendo un costo elevado para su implementación, conforme pasan los años la tecnología se está volviendo más accesible, dado que cada vez más empresas optan por su implementación, gracias a los beneficios que brinda conforme estén presentes las necesidades de cada una de ellas.
- RFID es una de las mejores alternativas no solo para el control de acceso; sino, también para transporte, administración de inventarios, automatización de empresas, control de acceso vehicular, tickets electrónicos y tiendas de ropa.
- En el área de control de acceso RFID, se debe complementar con el uso de cámaras y personal de seguridad, ya que por sí solo no es una solución completa.
- Se logró definir el proceso de integración de las tecnologías de control de acceso y activos para obtener un control preciso, automático y eficiente de los activos de la Universidad.
- La segmentación de la red permitirá, mejorar el rendimiento de la misma para futuras integraciones con otras tecnologías como WIFI.
- Existe la posibilidad de implementar varias aplicaciones, además del control de acceso que mejoren la calidad de servicio que ofrece el Campus para todos sus estudiantes.

4.2. RECOMENDACIONES

Una vez concluido el proyecto y tomando en cuenta todo lo investigado en relación a la tecnología RFID, considerando las ventajas que provee, se mencionan las siguientes recomendaciones:

- Realizar actualizaciones semanales de la base de datos, para mantener un registro actualizado de estudiantes.
- Aplicar las recomendaciones de segmentación de la red, para que los tiempos de respuesta sean adecuados.
- Extender el sistema de control de acceso y activos a todo el Campus Universitario.
- Empezar la extensión del sistema por áreas críticas como ser el parqueo de motocicletas y el ingreso al Campus.
- Elaborar políticas de seguridad para optimizar la logística de administración de la infraestructura de los laboratorios de computación.

También es de vital importancia para el mantenimiento del proyecto, designar un encargado que se dedique a la administración para un funcionamiento óptimo del mismo.

BIBLIOGRAFÍA

BIBLIOGRAFÍA

Angeles, R. (2004). *EMERGING TECHNOLOGIES:RFID*. (L. A. Sanchez, Trad.) Auerbach Publications.

Ávila, N., & Pupiales, P. (s.f.). *Diseño de un sistema de control de acceso utilizando la tecnología de identificación RFID para la empresa SOLUCIONES G CUATRO DEL ECUADOR CIA. LTDA*. Quito.

Carballeiro, G. (2014). *Redes: Dispositivos e instalación*.

Castel, J. (2017). <http://www.la-razon.com>. Obtenido de <http://www.la-razon.com>: http://www.la-razon.com/suplementos/el_financiero/Rfid-permite-control-rapido-empresas-financiero_0_2659534082.html

Cervantes Nájera, a., Hernández Reyes, P., & Santiago Jacobo, M. (2008). *sistema de informacion y control de acceso basado en tecnologia RFID*. Mexico, D.F.

CISCO. (2016). *CCNA Routing and Switching. Introduction to Networks*.

Delgadillo Rodriguez, S., & Ortiz Corvera, J. A. (2011). *DISEÑO DE UN SISTEMA DE CONTROL DE ACCESO MEDIANTE TECNOLOGIA RFID CON IMPLEMENTACION DE UN SERVIDOR WEB EMBEBIDO EN UN PIC*. Zacatecas.

Domínguez, H. M., & Saéz Vacas, F. (2006). *Domótica:Un enfoque sociotécnico*. madrid: Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones.

[espectrometria.com](http://www.espectrometria.com). (s.f.). Obtenido de https://www.espectrometria.com/espectro_electromagntico

González, M. S. (2014). *DISEÑO DE REDES TELEMÁTICAS*. RA-MA.

Guarango, M. J. (2013). *ESTUDIO Y DISEÑO INMÓTICO PARA EL EDIFICIO DE BIBLIOTECA DE LA UNIVERSIDAD POLITECNICA SALESIANA SEDE CUENCA, IMPLEMENTANDO LA TECNOLOGIA KONNEX PARA EL CONTROL DE ILUMINACION, CONTROL DE ACCESOS Y CONTROL DE SEGURIDAD TECNICA*. CUENCA.

Hancke, G. P. (s.f.). *Practical Attacks on Proximity Identification Sstems*. (L. A. Sanchez, Trad.) reino unido: university of cambridge.

Hassan Habibi, M., Gardeshi, M., & Alaghband, M. (2011). *Practical Attacks on a RFID Authentication Protocol Conforming to EPC C-1 G-2 Standard*. (L. A. Sanchez, Trad.) Iran : international journal of ubicomp.

<http://arquitecturabsicaderedes.blogspot.com>. (s.f.). Obtenido de http://arquitecturabsicaderedes.blogspot.com/2012/02/arquitectura-basica-de-red-de-tipo_9246.html

<http://iamjurgo.blogspot.com/>. (s.f.). Obtenido de <http://iamjurgo.blogspot.com/>

<http://internetmagic-capb.blogspot.com>. (s.f.). Obtenido de http://internetmagic-capb.blogspot.com/2010/09/tipos-de-topologias-de-red-red-en_22.html

<http://redestelematicas.com>. (s.f.). Obtenido de <http://redestelematicas.com/wp-content/uploads/2013/06/Figura-03.-Cisco-28001.jpg>

<http://revisaryaprender100.blogspot.com>. (s.f.). Obtenido de <http://revisaryaprender100.blogspot.com/2014/07/redes-multipunto-definicion-en-una-red.html>

http://www.aprendiendopc.com. (s.f.). Obtenido de *http://www.aprendiendopc.com/wp-content/uploads/2011/05/red-punto-a-punto.jpg*

http://www.digicorp.com.bo. (s.f.). Obtenido de *http://www.digicorp.com.bo/shop/product/adp-16-5v1-21a-2902*

http://www.ds3comunicaciones.com. (s.f.). Obtenido de *http://www.ds3comunicaciones.com/cisco/images/SG220-50-K9-NA_front.jpg*

http://www.javiergarzas.com. (s.f.). Obtenido de *http://www.javiergarzas.com/2013/09/tcpip-se-impuso-a-osi-2.html*

http://www.steren.com.do. (s.f.). Obtenido de */catalogo/prod.php?f=3&sf=27&c=1515&p=3192*

http://www.stronglink-rfid.com. (s.f.). Obtenido de *http://www.stronglink-rfid.com/en/rfid-readers/sl500.html*

https://gerardoveliz.files.wordpress.com. (s.f.). Obtenido de *https://gerardoveliz.files.wordpress.com/2015/07/server.jpg*

https://sites.google.com/a/galileo.edu. (s.f.). Obtenido de *https://sites.google.com/a/galileo.edu/proyectofinal8203/redes-de-computadoras/redes-wan*

https://store.emacs.es. (s.f.). Obtenido de *https://store.emacs.es/products/c6u-hf1-rlx-305vt*

https://tuelectronica.es. (s.f.). Obtenido de *https://tuelectronica.es/que-es-un-cable-de-red-utp-y-sus-mejoras/*

<https://worldmeforever.files.wordpress.com/2012/03/malla.png> (s.f.). Obtenido de <https://worldmeforever.files.wordpress.com/2012/03/malla.png>

<https://www.atlasrfidstore.com/alien-squig-rfid-white-wet-inlay-aln-9710-higgs-4> (s.f.). Obtenido de <https://www.atlasrfidstore.com/alien-squig-rfid-white-wet-inlay-aln-9710-higgs-4>

<https://www.indiamart.com/proddetail/mifare-1k-card-18062609473.html> (s.f.). Obtenido de <https://www.indiamart.com/proddetail/mifare-1k-card-18062609473.html>

<https://www.interlogix.com/video/product/truvision-nvr-22> (s.f.). Obtenido de <https://www.interlogix.com/video/product/truvision-nvr-22>

<https://www.orbitadigital.com/es/distribucion/cables-conectores/Conectores/2754-conector-bnc-macho-a-rca-hembra.html> (s.f.). Obtenido de <https://www.orbitadigital.com/es/distribucion/cables-conectores/Conectores/2754-conector-bnc-macho-a-rca-hembra.html>

<https://www.pccomponentes.com/ordenadores> (s.f.). Obtenido de <https://www.pccomponentes.com/ordenadores>

<https://www.startech.com/es/Industriales-ES/Adaptadores-Red/Tarjeta-de-Red-Ethernet-Gigabit-10-100-1000-a-PCI-de-32-Bits-de-1-Puerto-ST1000BT32> (s.f.). Obtenido de <https://www.startech.com/es/Industriales-ES/Adaptadores-Red/Tarjeta-de-Red-Ethernet-Gigabit-10-100-1000-a-PCI-de-32-Bits-de-1-Puerto-ST1000BT32>

https://www.supremainc.com/en/hardware/rfid_xpass-s2.asp (s.f.). Obtenido de https://www.supremainc.com/en/hardware/rfid_xpass-s2.asp

https://www.tvc.mx/shop/catalog/product_info.php?products_id=1452 (s.f.). Obtenido de https://www.tvc.mx/shop/catalog/product_info.php?products_id=1452

<https://www.vichaunter.org/informatica/que-es-un-pc> (s.f.). Obtenido de <https://www.vichaunter.org/informatica/que-es-un-pc>

Instituto Nacional de tecnologías de la comunicación. (2010). *guía sobre seguridad y privacidad de la tecnología RFID*. España: agencia española de protección de datos.

Mitrokotsa, A., Rieback, M., & Tanenbaum, A. (s.f.). *Classifying RFID Attacks and Defenses*.

Montañana, R. (2015). *Curso de Telemática y Redes de Ordenadores*.

O'Connor, M. C. (24 de mayo de 2010). *rfid journal*. Obtenido de <http://www.rfidjournal.com/articles/view?7628>

Paredes, M. C. (2007). *DISEÑO Y CONSTRUCCIÓN DE UN PROTOTIPO DE RED PARA EL CONTROL DE INGRESO A SITIOS DE ACCESO MASIVO UTILIZANDO LA TECNOLOGIA DE IDENTIFICACION POR RADIO FRECUENCIA (RFID)*.

RFID: Tecnología, aplicaciones y perspectivas. (s.f.). LIBERA whitepaper series.

Ruiz Zamarreño, C., & Ochoa Eneriz, C. (2015). *Gestión de Accesos mediante RFID*.

Sánchez, J. A. (2008). *Sistema de control de acceso con RFID*. Mexico, D.F.

sistemas.com. (s.f.). Obtenido de <https://sistemas.com/termino/wp-content/uploads/man.gif>

Smart Card Alliance. (2002). *Contactless Technology for Secure Physical Access: Technology and Standards Choices*. (L. A. Sanchez, Trad.)

Stallings, W. (2004). *COMUNICACIONES Y REDES DE COMPUTADORES*. (J. E. Verdejo, Trad.) Pearson Education.

Stronglink. (s.f.). *UHF RFID integrated reader software operation manual*.

Tanenbaum, A. S., & Wetherhall, D. J. (2015). *Redes de Computadoras*. (A. V. Elizondo, Trad.)

tecnoseguro. (7 de may de 2015). Obtenido de tecnoseguro.com:
<https://www.tecnoseguro.com/noticias/control-de-acceso/control-acceso-universidad-publica.html>

Tejada, D. S. (2012). *Prototipo de control de acceso peatonal al campus de la corporación universitaria*. Caldas, Colombia.

Vergara, Z. V. (2013). *Sistema de control de acceso y monitoreo con la tecnologia RFID para el departamento de sistemas de la universidad politécnica salesiana sede Guayaquil*. Guayaquil.

Viñé, J. C. (2000). *Introduccion a la Telematica y Redes de Datos*.

Ward, M., & Van kranenburg, R. (2006). *RFID:Frequency, standards, adoption and innovation*. Londres.

Wen-chung, K., Bae-Ling, C., & Lih-Chyan, w. (2013). *Secure Indefinite-Index RFID Authentication Scheme with Challege-Response Strategy*. (L. A. Sanchez, Trad.) Taiwan: information technology and control.

www.electrónica.mercadolibre.com.ve. (s.f.). Obtenido de www.electrónica.mercadolibre.com.ve

www.milcomos.com. (s.f.). Obtenido de <http://www.milcomos.com/configurar-un-router>

ANEXOS

ANEXO N°1: TIPO DE LICENCIAS SOFTWARE BIOSTAR 2

Access Control License

* BioStar 2.6.0 is applied

Item		Starter (free of charge)	Basic	Standard	Advanced	Professional	Enterprise
Users	Maximum No. of Cards per User	8	8	8	8	8	8
	Maximum No. of Fingerprints per User	10	10	10	10	10	10
	User Auto Sync	✓	✓	✓	✓	✓	✓
	Access-on-Card	✓	✓	✓	✓	✓	✓
	Security Credential Cards	✓	✓	✓	✓	✓	✓
	iCLASS Seos Card	✓	✓	✓	✓	✓	✓
	Inactivation User Reports	✓	✓	✓	✓	✓	✓
	Custom Field	✓	✓	✓	✓	✓	✓
Access Control	Maximum No. of Connected Devices	1,000	1,000	1,000	1,000	1,000	1,000
	No. of Doors	5	20	50	100	300	1,000
	Maximum No. of Access Levels	128	128	128	128	128	128
	Maximum No. of Access Groups	128	128	128	128	128	128
	Maximum No. of Access Groups per User	16	16	16	16	16	16
	Maximum No. of Doors per Access Level	128	128	128	128	128	128
	Access Group Auto Sync	✓	✓	✓	✓	✓	✓
Elevator Control	Maximum No. of Elevators	-	-	-	1,000	1,000	1,000
	Maximum No. of Floors per Elevator	-	-	-	192	192	192
	Maximum No. of Floor Levels	128	128	128	128	128	128
Zones	Anti-Passback	△(Door)	△(Door)	✓	✓	✓	✓
	Fire Alarm	-	-	✓	✓	✓	✓
	Schedule Lock/Unlock	-	-	✓	✓	✓	✓
	Guard Zone	-	-	✓	✓	✓	✓
	Interlock Zone	-	-	✓	✓	✓	✓
	Muster Zone	-	-	✓	✓	✓	✓
Advanced Features	Dashboard	✓	✓	✓	✓	✓	✓
	Cloud	-	-	✓	✓	✓	✓
	Server Matching	-	-	-	✓	✓	✓
	Audit Trail	✓	✓	✓	✓	✓	✓
	Daylight Saving Time	✓	✓	✓	✓	✓	✓
	Double mode	✓	✓	✓	✓	✓	✓
	No. of Mobile Cards	-	-	250	500	1,000	1,000+

Time & Attendance Management License

Item	Basic (free of charge)	Time & Attendance Management License
No. of Work Rules	Unlimited	Unlimited
No. of Schedules	1	Unlimited
No. of Users per Schedule	99	Unlimited
Shift Types	Fixed Shift and Flexible Shift	Fixed Shift and Flexible Shift
Calendar View	✓	✓

Video Log License

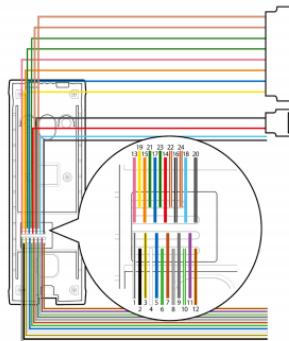
Item	Basic (free of charge)	Video License
Video Logs	-	✓

REQUERIMIENTOS

Item		Small	Medium	Enterprise
Environment	Total Devices	1 to 50	51 to 100	101 to 1,000
System requirement (Server)	OS	<ul style="list-style-type: none"> Windows 7 Home Basic 64bit SP1 or later Windows 7 Home Basic 32bit SP1 or later 	<ul style="list-style-type: none"> Windows Server 2008 R2 Standard 64bit SP2 or later Windows 7 SP1 Home Premium 64bit SP1 or later 	<ul style="list-style-type: none"> Windows Server 2008 R2 Standard 64bit SP2 or later Windows 7 SP1 Home Premium 64bit SP1 or later
	Database	MariaDB 10.1.10, MS SQL Server 2014 SP2, MS SQL Server 2014 SP2 Express, MS SQL Server 2016 SP1		
	CPU	2 GHz Dual Core	4 GHz Quad Core	4 GHz Quad Core
	RAM	6 GB	10 GB	16 GB
	HDD	500 GB	1 TB	4 TB
	Others	Java 1.8.0_201		
System requirement (Client)	CPU	1 GHz	1 GHz	1 GHz
	RAM	4 GB	4 GB	4 GB
	Web Browser	Google Chrome 49 or later		

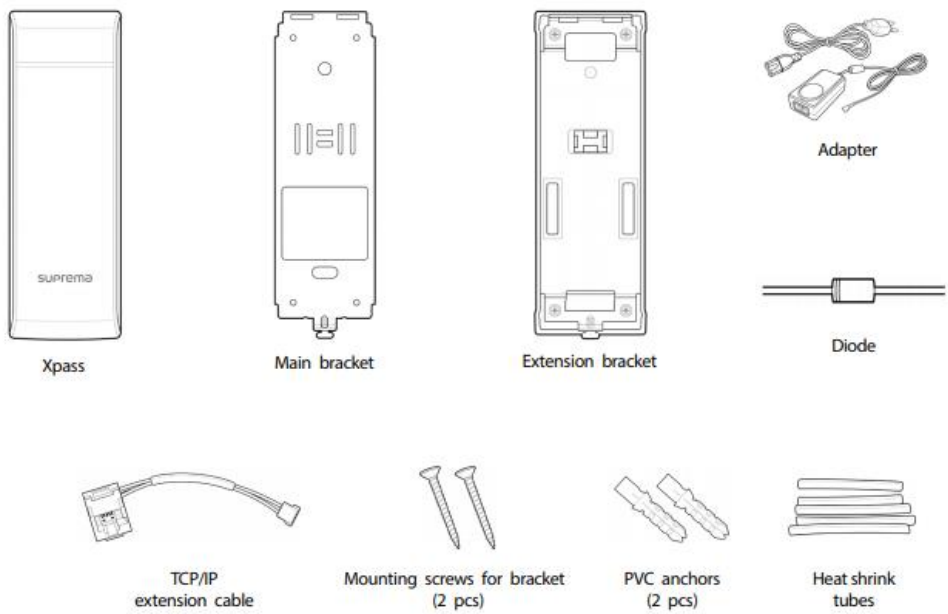
ANEXO N° 2: LECTOR RFID HF XPASS XPM-POE

CABLES Y CONECTORES



Pin	Pin name	Color
1	485 GND	White (Black stripe)
2	WG GND	Black
3	485 TRXN	Yellow (Black stripe)
4	WG D1	White
5	485 TRXP	Blue (White stripe)
6	WG D0	Green
7	TTL IN1	Brown
8	RLY NO	Gray (White stripe)
9	TTL GND	Gray
10	RLY COM	Green (White stripe)
11	TTL IN0	Purple
12	RLY NC	Orange (Black stripe)
13	ENET TXP	Pink
14	PWR +VDC	Red
15	ENET TXN	Orange
16	PWR GND	Black (White stripe)
17	ENET RXP	Blue
18	PWR OUT	Sky-blue
19	ENET RXN	Yellow
20	PWR GND	Black (White stripe)
21	VB1	Green (Black stripe)
22	VB2	Brown (White stripe)
23	VB1	Green (Black stripe)
24	VB2	Brown (White stripe)

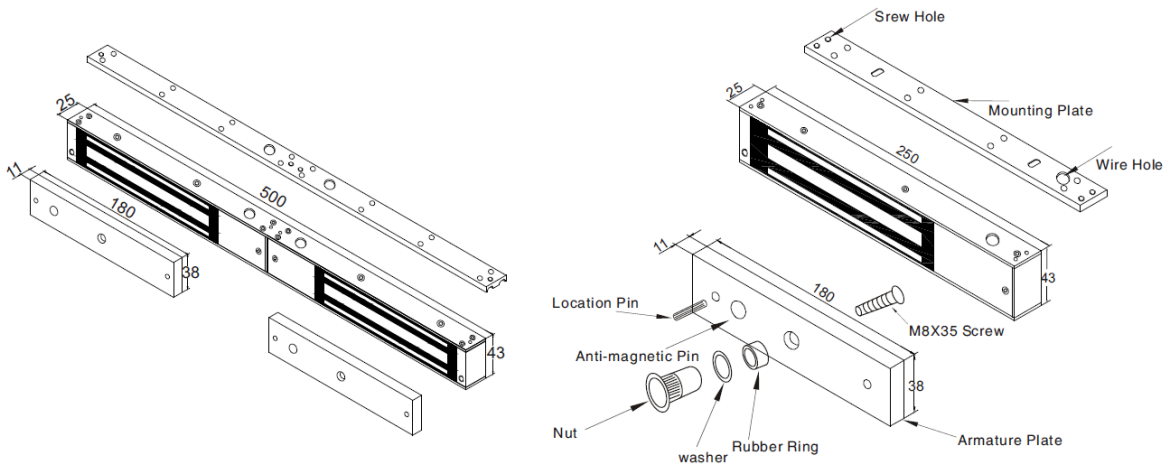
COMPONENTES




CARÁCTERÍSTICAS

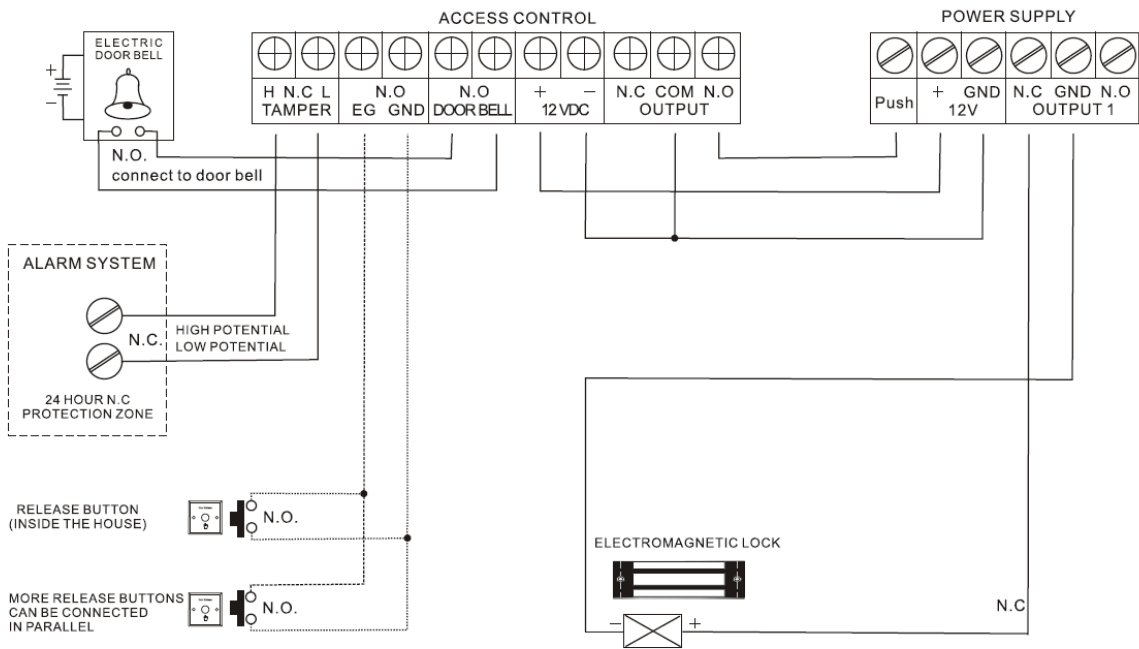
Category	Feature	Specification
Main	IP Rating	IP65
	RF Card	<ul style="list-style-type: none">• XPE-PoE: 125kHz EM• XPM-PoE: 13.56MHz MIFARE, DESFire/EV1 (CSN)• XPH-PoE: 125kHz HID Prox
	Multi-Controller	Yes (RF)
Capacity	Max. User (1:1)	40,000
	Max. User (1:N)	40,000
	Max.Text Log	50,000
Interface	TCP/IP	Yes
	RS-485	1ch
	Wiegand	1ch In or Out (Selectable)
	TTL Input	2 Inputs
	Relay	1 Relay
Relay	Voltage	Max. 24VDC
	Current	Typ. 0.5A, Max. 1.0A
Hardware	CPU	533MHz DSP
	Memory	16MB RAM + 8MB Flash
	LED	Multi-Color
	Sound	16-bit Hi-Fi
	Operating Temp.	-20°C ~ 50°C
	Tamper	Yes
	Power	12VDC
	PoE	Optional
	Dimensions (W x H x D mm)	45 x 130 x 27
	Certification	CE, FCC, KC, RoHS

ANEXO Nº 3: DIAGRAMA DE CHAPA ELECTROMAGNÉTICA

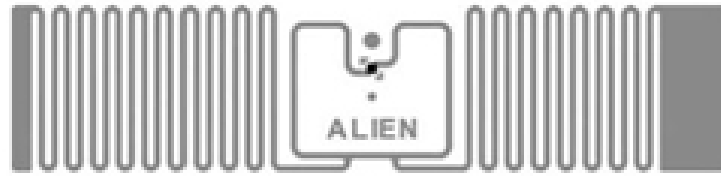


 Remark:

CONEXIÓN



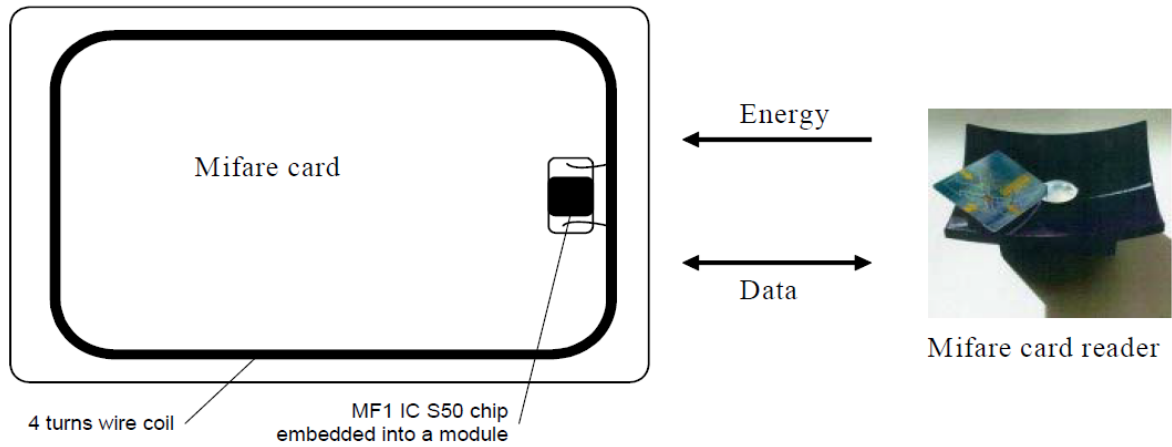
ANEXO Nº 4: CARACTERISTICAS TARJETA ADHESIVA UHF



Dry Inlay		Environmental	
Antenna Width	1.752" [44.5mm]	Shelf Life	Dry Inlays: 5 years at +77°F [+25°C] @ 40% RH Wet Inlays: 2 years at +77°F [+25°C] @ 40% RH
Antenna Length	0.409" [10.4mm]	Recommended Storage	+77°F [+25°C] @ 40% RH
Web Width	2.26" [57.5mm]	Storage Limits	-13°F to 122°F [-25°C to +50°C] 20% to 90% RH Non-condensing
Web Pitch	0.625" [15.875mm]	Operating Limits	-40°F to +158°F [-40°C to +70°C] 20% to 90% RH Non-condensing
Core Width	2.26" [57.5mm]	Bend Diameter	> 1.97" [50mm]
Core ID	6" [152.4mm]*	Pressure	< 5N/mm ²
Core Material	Fiberboard	Drop Resistance	Per ASTM D5276
Inlays per Roll	20,000 Nominal	Write Cycles	100,000 @ 25°C
Maximum Roll OD	< 12" [304.8mm]	RoHs	2002/95/EC, 2005/618/EC, 2011/65/EU Compliant
Roll Labeling Data	Roll #, Quantity	REACH	1907/2006/EC Compliant (SVHC and ECHA)
Wet Inlay		ESD Limit- HBM / CDM	5.0kV / 1.5kV
Inlay Width	1.87" [47.5mm]	RFID	
Inlay Length	0.528" [13.4mm]	Protocols Supported	ISO/IEC 18000-6C EPCglobal Class 1 Gen 2
Web Width	2.0" [50.8mm]	Integrated Circuit	Alien Higgs-4
Web Pitch	0.625" [15.875mm]	EPCglobal Certificate	950110126000001084
Core Width	2.0" [50.8mm]	Operating Frequency	840-960 MHz
Core ID	6" [152.4mm]*	EPC Size	128 Bits
Core Material	Fiberboard	User Memory	128 Bits
Inlays per Roll	20,000 Nominal	TID	32 Bits
Maximum Roll OD	< 16" [406.4mm]	Unique TID	64 Bits
Roll Labeling Data	Roll #, Quantity	Access Password	32 Bits
White	TT Printable White Film Only	Kill Password	32 Bits
Overlay Adhesive	General Purpose Permanent		
Inlay Adhesive	General Purpose Permanent		
Adhesive Application Temperature	> +25°F [-4°C]		
Adhesive Service Temperature	-40°F to +200°F [-40°C to +93.3°C]		
Release Liner	40# SCK		

Shipped with 6" to 3" plastic core adapter

ANEXO N° 5: DIAGRAMA TARJETA PASIVA MIFARE 1K



ESPECIFICACIONES

Product features	MIFARE Classic EV1 1k	MIFARE Classic EV1 4k
Memory		
EEPROM Size [byte]	1 K	4 K
Write Endurance [typical cycles]	200 000	
Data Retention [years]	10	
Organization	16 sectors with 4 blocks	32 sectors with 4 blocks 8 sectors with 16 blocks
RF Interface		
According to ISO 14443A	Yes - up to layer 3	
Frequency [MHz]	13.56	
Bit-rate [kbit /s]	106	
Anticollision	Bit-wise	
Security		
Unique Serial Number [byte]	4-byte NUID or 7-byte UID	
4-byte Random ID	yes (7 B UID versions only)	
Random Number Generator	Yes	
Access Keys	2 CRYPTO1 keys per sector	
Access Conditions	Per sector	
Cryptography	CRYPTO1	
Packaging		
Sawn Wafer - Au Bumps		
7-byte UID	(120 μ) MF1S5001XDUD/V1 (75 μ) MF1S5001XDUF/V1	(120 μ) MF1S7001XDUD/V1 (75 μ) MF1S7001XDUF/V1
4-byte NUID	(120 μ) MF1S5031XDUD/V1 (75 μ) MF1S5031XDUF/V1	(120 μ) MF1S7031XDUD/V1 (75 μ) MF1S7031XDUF/V1
MOA4 Module		
7-byte UID	MF1S5000XDA4/V1	MF1S7000XDA4/V1
4-byte NUID	MF1S5030XDA4/V1	MF1S7030XDA4/V1
MOA8 Module		
7-byte UID	MF1S5000XDA8/V1	MF1S7000XDA8/V1
4-byte NUID	MF1S5030XDA8/V1	MF1S7030XDA8/V1

ANEXO Nº 6: LECTOR UHF SL130



Frecuencia	920MHz~925MHz
Protocolo	ISO18000-6B/C
Etiqueta apoyo	ISO18000-6B/C, EPC Class1 Gen2 tags
Interfaz	RS232 / RS485 / RJ45 / Wiegand
Temperatura de funcionamiento	-10°C ~ +55°C
Distancia de la operación	Leer distancia de > 8m, escribir distancia > 1 m (depende de las etiquetas)
Potencia de salida	20~30dBm
Velocidad de lectura	32bits/6ms
Velocidad de escritura	32bits/50ms
Peso	6.4kg
Dimensión	600 × 480 × 110 mm

ANEXO Nº 7: ESCRITOR TAGS UHF RT400A



Frecuencia	840 ~ 960MHz (personalizada de acuerdo a los requerimientos del cliente)
Protocolo	ISO18000-6C/EPC C1 GEN2
Potencia de salida	+10 ~ +30dBm
interfaz de la antena	IPX
Antena Integrada	Yes
Distancia de la operación	0.1m ~ 1m (depende de RF de salida, la antena y etiquetas)
Interfaz	USB Virtual COM
Voltaje	3.6 ~ 5.5V
Dimensión	110 × 90 × 42 mm
El apoyo de la energía baja	Yes (modo de espera / modo Normal)
Temperatura de funcionamiento	-20 ~ +70°C
Temperatura de almacenamiento	-40 ~ +85°C

ANEXO Nº 8: ESCRITOR TARJETAS HF SL500A



Frecuencia	13.56MHz
Etiqueta apoyo	ISO14443A, ISO14443B, ISO15693
Interfaz	RS232/USB
Rango de temperatura	-20°C ~ +50°C
Voltaje	4.5 - 5.5 VDC
Dimensión	110 × 80 × 26 mm
Peso	100g
Sistema	Windows 98 2000 XP NT ME Vista

	SL500L - RS232	SL500L - USB	SL500A - RS232	SL500A - USB	SL500D - RS232	SL500D - USB	SL500F - RS232	SL500F - USB
Protocolo	ISO14443A		ISO14443A		ISO15693		ISO14443A ISO14443B ISO15693	
Tags apoyo	FM11RF08, MIFARE Ultralight®, NTAG203, Ultralight C, MIFARE Mini, MIFARE Classic® 1K, MIFARE Classic® 4K		FM11RF08, MIFARE Ultralight®, NTAG203, Ultralight C, MIFARE Mini, MIFARE Classic® 1K, MIFARE Classic® 4K, DESFire®, MIFARE ProX		I.CODE SLI, Tag_it HFI		FM11RF08, MIFARE Ultralight®, NTAG203, Ultralight C, MIFARE Mini, MIFARE Classic® 1K, MIFARE Classic® 4K, DESFire®, MIFARE ProX, AT88RF020, SR176, SR1X4K, I.CODE SLI, Tag_it HFI, T = CL con tarjeta inteligente	

ANEXO Nº 9: BOTÓN DE SALIDA ABK-800A



- Tamaño: 86x50x20 (mm).
- Energía soportada: 12V DC 3Amp.
- Accesorio opcional: ABK-800-M
- Temperatura de operación: -10°C~+55°C.
- Material: Aluminio.
- Estructura estandar: Aluminio y boton de metal.
- Contacto de salida: NO/NC/COM.
- Humedad: 0 - 95%.
- Peso: 0.18Kg.
- Modelo: ZABK-800A.
- Tamaño: ZABK-800A 86L*50W*20T (mm).
- Manejo de corriente: 3A@36VDC Máximo.
- Temperatura de operación: 10°C - 55°C.
- Humedad de operación: 0% - 95%.
- Peso: 0.16Kg.
- Estructura: Estructura de aluminio.
- Prueba de rendimiento: Probado 500.000 veces.
- Adecuado para puertas huecas.

ANEXO Nº 10: CABLE UTP BRAND REX CAT6



Estándares de cable

El cable cumple con:

- IISO/IEC 11801, EN50173-1 ,
ANSI/EIA/TIA Serie 568C,
ISO/IEC 61156-5, EN 50288-5-1

Características eléctricas a 20°C	Especificaciones	Funcionamiento normal
Resistencia bucle de conductor	Máx 19 Ω /100m	14 Ω /100m
Desequilibrio de la resistencia del conductor	Máx 2%	0,2%
Resistencia dieléctrica	1,0kV cc o 0,7kV ca para 1min	100% en proceso de prueba
Resistencia del aislamiento	>500 M Ω .km a 100-500V tensión de prueba	>5000 M Ω .km
Asimetría de capacidad a tierra	Máx 160 pF/100m	20 pF/100m
Inclinación	Máx 40 ns/100m a 100MHz	20 ns/100m a 100MHz
Promedio de impedancia característica	100 $\Omega \pm 5\Omega$ a 100 MHz	100 $\Omega \pm 3\Omega$ a 100 MHz
Impedancia de transferencia	Máx 100 m Ω /m a 10MHz	10 m Ω /m a 10MHz
Atenuación de acoplamiento hasta 1GHz	Mín 55dB	80dB

ANEXO Nº 11: CONFIGURACIÓN DE LOS SWITCHES

```
Switch>ENABLE
Switch#CONF T
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hos
Switch(config)#hostname SW-CENTRAL
SW-CENTRAL(config)#vlan 10
SW-CENTRAL(config-vlan)#name LAB-A
SW-CENTRAL(config-vlan)#exit
SW-CENTRAL(config)#vlan 20
SW-CENTRAL(config-vlan)#name LAB-B
SW-CENTRAL(config-vlan)#exit
SW-CENTRAL(config)#vlan 30
SW-CENTRAL(config-vlan)#name LAB-C
SW-CENTRAL(config-vlan)#exit
SW-CENTRAL(config)#vlan 40
SW-CENTRAL(config-vlan)#name LAB-D
SW-CENTRAL(config-vlan)#exit
SW-CENTRAL(config)#vlan 50
SW-CENTRAL(config-vlan)#name LAB-E
SW-CENTRAL(config-vlan)#exit
SW-CENTRAL(config)#vlan 60
SW-CENTRAL(config-vlan)#name LAB-F
SW-CENTRAL(config-vlan)#exit
SW-CENTRAL(config)#vlan 70
SW-CENTRAL(config-vlan)#name RFID-ACCESS
SW-CENTRAL(config-vlan)#exit
SW-CENTRAL(config)#vlan 80
```

```
Vlan      Vlan interface
SW-CENTRAL(config)#interface range fa0/1 - fa0/6
SW-CENTRAL(config-if-range)#swit
SW-CENTRAL(config-if-range)#switchport mode access
SW-CENTRAL(config-if-range)#swit
SW-CENTRAL(config-if-range)#switchport access vlan 90
SW-CENTRAL(config-if-range)#exit
SW-CENTRAL(config)#interface range fa0/7 - fa0/8
SW-CENTRAL(config-if-range)#switchport mode access
SW-CENTRAL(config-if-range)#switchport access vlan 10
SW-CENTRAL(config-if-range)#exit
SW-CENTRAL(config)#interface range fa0/9 - fa0/10
SW-CENTRAL(config-if-range)#switchport mode access
SW-CENTRAL(config-if-range)#switchport access vlan 20
SW-CENTRAL(config-if-range)#exit
SW-CENTRAL(config)#interface range fa0/11 - fa0/12
SW-CENTRAL(config-if-range)#switchport mode access
SW-CENTRAL(config-if-range)#switchport access vlan 30
SW-CENTRAL(config-if-range)#exit
SW-CENTRAL(config)#interface range fa0/13 - fa0/14
SW-CENTRAL(config-if-range)#switchport mode access
SW-CENTRAL(config-if-range)#switchport access vlan 40
SW-CENTRAL(config-if-range)#exit
SW-CENTRAL(config)#interface range fa0/15 - fa0/16
SW-CENTRAL(config-if-range)#switchport mode access
SW-CENTRAL(config-if-range)#switchport access vlan 50
SW-CENTRAL(config-if-range)#exit
SW-CENTRAL(config)#interface range fa0/17 - fa0/18
```

```
SW-CENTRAL(config)#interface range fa0/15 - fa0/16
SW-CENTRAL(config-if-range)#switchport mode access
SW-CENTRAL(config-if-range)#switchport access vlan 50
SW-CENTRAL(config-if-range)#exit
SW-CENTRAL(config)#interface range fa0/17 - fa0/18
SW-CENTRAL(config-if-range)#switchport mode access
SW-CENTRAL(config-if-range)#switchport access vlan 60
SW-CENTRAL(config-if-range)#exit
SW-CENTRAL(config)#interface range fa 0/19 - fa 0/20
SW-CENTRAL(config-if-range)#switchport mode access
SW-CENTRAL(config-if-range)#switchport access vlan 70
SW-CENTRAL(config-if-range)#exit
SW-CENTRAL(config)#interface range fa 0/21 - fa 0/22
SW-CENTRAL(config-if-range)#switchport mode access
SW-CENTRAL(config-if-range)#switchport access vlan 80
SW-CENTRAL(config-if-range)#exit
SW-CENTRAL(config)#interface gigabit0/1
SW-CENTRAL(config-if)#switch
SW-CENTRAL(config-if)#switchport mode
SW-CENTRAL(config-if)#switchport mode trunk
SW-CENTRAL(config-if)#switchport mode tru?
trunk
SW-CENTRAL(config-if)#switchport mode trunk
SW-CENTRAL(config-if)#exit
SW-CENTRAL(config)#
```

% Invalid input detected at '^' marker.

ANEXO N° 12: RELEVAMIENTO DE INFORMACIÓN DE LOS LABORATORIOS DE COMPUTACIÓN

CUESTIONARIO

1.- ¿Cuántos laboratorios de computación hay en la universidad?

Hay 8 laboratorios de computación A, B, C, D, E, F, Cisco y Microsoft.

2.- ¿Cuántos equipos hay en cada uno de los laboratorios?

A=36 B=20 C=17 D=20 E=17 F=25 Cisco=12 Microsoft=14

3.- ¿Cuáles son las carreras que más utilizan los laboratorios?

Ing. en sistemas e ing. En redes y telecomunicaciones.

4.- ¿Cada cuanto se realizan mantenimiento a los equipos en los laboratorios de computación?

Terminando el semestre.

5.- ¿En qué horarios se puede ingresar a los laboratorios?

En los horarios que se cursan materias

mañana de 7:30 a 10:45

medio día de 11:00 a 14:00

tarde de 15:00 a 18:15

noche de 19:00 a 22:00

6.- ¿se controla el ingreso y egreso de los laboratorios de computación?

Están cerrados con llave y los docentes son los encargados del control cuando se les provee de la llave de acceso.

7.- ¿Cuántas personas transitan los laboratorios de computación durante el día?

Entre 200 a 400 personas.

8.- ¿Son los laboratorios de computación de acceso libre?

No, es necesario un permiso del área de soporte técnico para el uso de los mismos.

9.- ¿Cuántas cámaras hay en cada laboratorio?

hay una cámara de video vigilancia por laboratorio de computación.

10.- ¿Quiénes administran los laboratorios de computación?

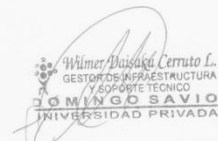
El área de soporte técnico se encarga de administrar los laboratorios de computación.

11.- ¿Se perdió alguna vez algún activo de los laboratorios de computación? Indique la frecuencia.

Si, en los últimos 3 años se han perdido componentes internos de los equipos de computación, se han perdido proyectores y cpu, con respecto a la frecuencia, en promedio se ha perdido un ejemplar de cada unidad por gestión

12.- ¿Cuáles son los laboratorios de computación más usados?

Los laboratorios de computación A, B y D


Walter Delgado Cerruto L.
GESTOR DE INFRAESTRUCTURA
Y SOPORTE TÉCNICO
DOMINGO SAVIO
UNIVERSIDAD PRIVADA