

UNIVERSIDAD TÉCNICA DE AMBATO



FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

DIRECCIÓN DE POSGRADO

MAESTRÍA EN REDES Y TELECOMUNICACIONES

TEMA:

**LA ESTRUCTURA DEL SISTEMA DE GESTIÓN DE RED PARA LA
COMUNICACIÓN DE LA SEGURIDAD, DE LA INFRAESTRUCTURA FÍSICA DE LA
UNIVERSIDAD TÉCNICA DE AMBATO**

Trabajo de Titulación

Previo a la obtención del Grado Académico de Magister en Redes y Telecomunicaciones.

AUTOR: Ing. Santiago Mauricio Altamirano Meléndez

DIRECTORA: Ing. Elsa Pilar Urrutia Urrutia, Mg.

Ambato – Ecuador

2014

Al Consejo de Posgrado de la Universidad Técnica de Ambato.

El Tribunal de Defensa del trabajo de titulación presidido por Ingeniero Edison Homero Álvarez Mayorga Magíster, Presidente del Tribunal e integrado por los señores Ingeniero Giovanni Danilo Brito Moncayo Magíster, Ingeniero Julio Enrique Cuji Rodríguez Magister, Ingeniero Mario Geovanny García Carrillo Magister, Miembros del Tribunal de Defensa, designados por el Consejo de Posgrado de la Universidad Técnica de Ambato, para receptar la defensa oral del trabajo de titulación con el tema: “LA ESTRUCTURA DEL SISTEMA DE GESTIÓN DE RED PARA LA COMUNICACIÓN DE LA SEGURIDAD, DE LA INFRAESTRUCTURA FÍSICA DE LA UNIVERSIDAD TÉCNICA DE AMBATO”, elaborado y presentado por el señor Ingeniero Santiago Mauricio Altamirano Meléndez, para optar por el Grado Académico de Magíster en Redes y Telecomunicaciones.

Una vez escuchada la defensa oral el Tribunal aprueba y remite el trabajo de titulación para uso y custodia en las bibliotecas de la UTA.

Ing. Edison Homero Álvarez Mayorga, Mg.
Presidente del Tribunal de Defensa

Ing. Giovanni Danilo Brito Moncayo, Mg.
Miembro del Tribunal

Ing. Julio Enrique Cuji Rodríguez, Mg.
Miembro del Tribunal

Ing. Mario Geovanny García Carrillo, Mg.
Miembro del Tribunal

AUTORÍA DE LA TESIS

La responsabilidad de las opiniones, comentarios y críticas emitidas en el trabajo de titulación con el tema: **“LA ESTRUCTURA DEL SISTEMA DE GESTIÓN DE RED PARA LA COMUNICACIÓN DE LA SEGURIDAD, DE LA INFRAESTRUCTURA FÍSICA DE LA UNIVERSIDAD TÉCNICA DE AMBATO”**, le corresponde exclusivamente a: Ingeniero Santiago Mauricio Altamirano Meléndez, Autor bajo la Dirección de Ingeniera Elsa Pilar Urrutia Urrutia Magíster, Directora del trabajo de titulación; y el patrimonio intelectual a la Universidad Técnica de Ambato.

Ing. Santiago Mauricio Altamirano Meléndez	Ing. Elsa Pilar Urrutia Urrutia, Mg.
Autor	Directora

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este trabajo de titulación como un documento disponible para su lectura, consulta y procesos de investigación.

Cedo los Derechos de mi trabajo de titulación, con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la Universidad.

Ing. Santiago Mauricio Altamirano Meléndez
c.c. 1802338838

DEDICATORIA

El presente trabajo investigativo dedico a las personas que más amo y representan en mi vida lo más valioso que tengo.

A mi hija Angelly Sarahi, quien a su corta edad me ha enseñado lo frágil que es la vida, pero que con constancia, amor y esfuerzo se pueden superar los retos y las adversidades más difíciles de la vida.

A mi esposa Ruth del Carmen, compañera inseparable de mis alegrías y penas, mujer, esposa, madre y amiga ejemplar, motor que me impulsa a vivir el día a día.

A mi padre Luis Antonio, quien con su ejemplo y constancia supo forjarme y hacer de mí un hombre de bien.

A mi madre Sara Gregoria, su ejemplo de vida y lucha siempre estará presente en mí, hoy desde el cielo sé que me protege y cuida para seguir adelante.

A mi hermano Luis Miguel, mis primos Daniel Alejandro y Marco Patricio, mis tíos Mélida Yolanda y Carlos Humberto, sus recuerdos siempre estarán conmigo.

Santiago Mauricio.

AGRACECIMIENTO

A la Universidad Técnica de Ambato, por acogerme en sus aulas y laboratorios para seguirme preparando académicamente.

A la Dirección de Sistemas Informáticos y Redes (DISIR) y personal de seguridad de la Universidad Técnica de Ambato por permitirme desarrollar el presente trabajo de investigación.

A la Ing. Mg. Pilar Urrutia, por toda la ayuda brindada para el presente trabajo investigativo.

Al personal docente y administrativo de la Maestría en Redes y Telecomunicaciones de la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la Universidad Técnica de Ambato y al Centro de Estudios de Posgrado.

Santiago Mauricio.

CONTENIDO

TEMA	i
Al Consejo de Posgrado de la Universidad Técnica de Ambato.	ii
AUTORÍA DE LA TESIS	iii
DERECHOS DE AUTOR.....	iv
DEDICATORIA	v
AGRACECIMIENTO	vi
ÍNDICE DE TABLAS	x
ÍNDICE DE GRÁFICOS	xiii
RESUMEN EJECUTIVO	xvi
INTRODUCCIÓN	1
CAPÍTULO I.....	2
PROBLEMA	2
1.1 TEMA:	2
1.2 PLANTEAMIENTO DEL PROBLEMA	2
1.2.1 CONTEXTUALIZACIÓN	2
1.2.2 ANÁLISIS CRÍTICO.....	5
1.2.3 PROGNOSIS.....	6
1.2.4 FORMULACIÓN DEL PROBLEMA.....	6
1.2.5 INTERROGANTES.....	7
1.2.6 DELIMITACIÓN DEL OBJETO DE LA INVESTIGACIÓN	7
1.3 JUSTIFICACIÓN	8
1.4 OBJETIVOS	9
1.4.1 OBJETIVO GENERAL	9
1.4.2 OBJETIVOS ESPECÍFICOS.....	9
CAPÍTULO II	10
MARCO TEÓRICO.....	10
2.1 ANTECEDENTES INVESTIGATIVOS.....	10
2.2 FUNDAMENTACIÓN FILOSÓFICA.....	12
2.3 FUNDAMENTACIÓN TECNOLÓGICA.....	12
2.4 FUNDAMENTACIÓN LEGAL	12
2.5 CATEGORÍAS FUNDAMENTALES	13
2.5.1 DEFINICIÓN DE LA VARIABLE INDEPENDIENTE	14
2.5.2 DEFINICIÓN DE LA VARIABLE DEPENDIENTE.....	15
2.5.3 SISTEMA.....	16
2.5.4 SISTEMA DE GESTIÓN	17
2.5.5 SISTEMA DE GESTIÓN DE RED	20
2.5.6 COMUNICACIÓN	31
2.5.7 SEGURIDAD.....	33
2.5.8 COMUNICACIÓN DE LA SEGURIDAD	39
2.6 HIPÓTESIS.....	41
2.7 SEÑALAMIENTO DE VARIABLES.....	42
CAPÍTULO III.....	43
METODOLOGÍA	43
3.1 ENFOQUE	43
3.2 MODALIDAD BÁSICA DE LA INVESTIGACIÓN.....	43

3.3 NIVEL O TIPO DE LA INVESTIGACIÓN	44
3.4 POBLACIÓN Y MUESTRA	45
3.5 OPERACIONALIZACIÓN DE LA VARIABLE INDEPENDIENTE: ESTRUCTURA DEL SISTEMA DE GESTIÓN DE RED	46
3.6 OPERACIONALIZACIÓN DE LA VARIABLE DEPENDIENTE: COMUNICACIÓN DE LA SEGURIDAD.	47
3.7 PLAN DE RECOLECCIÓN DE INFORMACIÓN	48
3.8 PLAN DE PROCESAMIENTO DE LA INFORMACIÓN.....	48
CAPÍTULO IV	49
ANÁLISIS E INTERPRETACIÓN DE RESULTADOS.....	49
4.1 ENCUESTA DIRIGIDA AL PERSONAL DEL DISIR – UTA.	49
4.2. ENCUESTA DIRIGIDA A LOS ADMINISTRADORES DE RED DE LA UNIVERSIDAD TÉCNICA DE AMBATO.	55
4.3. ENCUESTA DIRIGIDA AL PERSONAL DE SEGURIDAD DE LA UNIVERSIDAD TÉCNICA DE AMBATO	62
4.4 SITUACIÓN ACTUAL DE LOS PROCESOS DE COMUNICACIÓN DE LA UNIVERSIDAD TÉCNICA DE AMBATO.	72
4.5 VERIFICACIÓN DE HIPÓTESIS	74
4.5.1. PLANTEAMIENTO DE LA HIPÓTESIS	74
4.5.2. DESCRIPCIÓN DE LA POBLACIÓN	74
4.5.3. DECISIÓN FINAL	74
CAPÍTULO V	75
CONCLUSIONES Y RECOMENDACIONES.....	75
5.1. CONCLUSIONES	75
5.2. RECOMENDACIONES	76
CAPÍTULO VI.....	77
PROPUESTA.....	77
6.1. DATOS INFORMATIVOS	77
6.2. ANTECEDENTES DE LA PROPUESTA	77
6.3. JUSTIFICACIÓN	78
6.4. OBJETIVOS	79
6.4.1 OBJETIVO GENERAL	79
6.4.2. OBJETIVOS ESPECÍFICOS.....	79
6.5. ANÁLISIS DE FACTIBILIDAD	80
6.6. FUNDAMENTACIÓN	80
6.6.1. FUNDAMENTO TEÓRICO CONCEPTUAL	80
6.6.2. DISEÑO FÍSICO Y LÓGICO	92
6.6.3 SELECCIÓN DE EQUIPOS.....	106
6.7 PRESUPUESTO	124
6.8 CONCLUSIONES	125
6.9 RECOMENDACIONES	126
BIBLIOGRAFÍA.....	127
ANEXOS.....	130
ANEXO A.....	131
ANEXO 1A.....	131

ENCUESTA DIRIGIDA AL PERSONAL DEL DISIR – UTA.	131
ANEXO 2A.	133
ENCUESTA DIRIGIDA A LOS ADMINISTRADORES DE REDES DE LA UNIVERSIDAD TÉCNICA DE AMBATO.	133
ANEXO 3A.	135
ENCUESTA DIRIGIDA AL PERSONAL DE SEGURIDAD DE LA UNIVERSIDAD TÉCNICA DE AMBATO	135
ANEXO 4A.	138
ENTREVISTA REALIZADA AL INGENIERO FERNANDO GARCÉS, DIRECTOR DEL DISIR – UTA Y AL TECNÓLOGO RUBÉN MOREJÓN, JEFE DE GUARDIAS DE LA UTA.	138

ÍNDICE DE TABLAS

Tabla 3. 1: Población y Muestra Entrevista	45
Tabla 3. 2: Población y Muestra Encuesta	45
Tabla 3. 3: Operacionalización de la V. I.....	46
Tabla 3. 4: Operacionalización de la V. D.	47
Tabla 3. 5: Recolección de la información.....	48
Tabla 4. 1: ¿Cuenta la Universidad con un proceso de planificación para tomar acciones y conductas para monitorear un evento de seguridad?	50
Tabla 4. 2: ¿Existen elementos necesarios y suficientes para observar los procesos de seguridad en la Universidad?	51
Tabla 4. 3: ¿La institución posee recursos necesarios y suficientes para una administración sostenible del sistema de seguridad?	52
Tabla 4. 4 ¿El sistema de seguridad tiene una red adecuada y actualizada en los predios universitarios?	53
Tabla 4. 5: ¿Qué porcentaje de cobertura de seguridad tiene la infraestructura de la Universidad Técnica de Ambato?	54
Tabla 4. 6: ¿Cuenta la Facultad con un proceso de planificación para tomar acciones y conductas para monitorear un evento de seguridad? Porcentaje total.	55
Tabla 4. 7: ¿Cuenta la Facultad con un proceso de planificación para tomar acciones y conductas para monitorear un evento de seguridad? Referencia individual.....	55
Tabla 4. 8: ¿Existen elementos necesarios y suficientes para observar los procesos de seguridad en la Facultad? Porcentaje Total	56
Tabla 4. 9: ¿Existen elementos necesarios y suficientes para observar los procesos de seguridad en la Facultad? Referencia individual.....	57
Tabla 4. 10: ¿La unidad académica posee recursos necesarios y suficientes para una administración sostenible del sistema de seguridad? Porcentaje total.	57
Tabla 4. 11: ¿La unidad académica posee recursos necesarios y suficientes para una administración sostenible del sistema de seguridad? Referencia individual..	58

Tabla 4. 12: ¿El sistema de seguridad tiene una red adecuada y actualizada en los dominios de la facultad? Porcentaje total.....	59
Tabla 4. 13: ¿El sistema de seguridad tiene una red adecuada y actualizada en los dominios de la facultad? Referencia individual.	59
Tabla 4. 14: ¿Qué porcentaje de cobertura de seguridad tiene la infraestructura de la Facultad? Porcentaje total.	60
Tabla 4. 15: ¿Qué porcentaje de cobertura de seguridad tiene la infraestructura de la Facultad? Referencia individual.....	61
Tabla 4. 16: ¿Considera Usted que el sistema de comunicación interno es?.....	62
Tabla 4. 17: ¿En el caso de una emergencia, a su conocimiento el reporte le llega?	63
Tabla 4. 18: ¿Cuándo suena la alarma en una dependencia o edificio, el tiempo que se demora en encontrar donde está focalizado el problema es?	64
Tabla 4. 19: ¿Tienen algún sistema de requisas para los vehículos que ingresan o salen de la institución?	65
Tabla 4. 20: ¿Tienen alguna identificación, los vehículos de los docentes, alumnos o visitantes de la institución?	66
Tabla 4. 21: ¿En su turno, que tiempo se demora en volver a pasar por el mismo punto?	67
Tabla 4. 22: ¿Cree Usted, que el actual sistema de seguridad es satisfactorio?....	68
Tabla 4. 23: ¿Qué tan confiable es el sistema de seguridad actual?	69
Tabla 4. 24: ¿En caso de detectar alguna anomalía dentro de los predios universitarios, que procedimiento realiza?.....	70
Tabla 4. 25: ¿En caso de detectar alguna anomalía dentro de los predios universitarios, que procedimiento realiza?.....	71
Tabla 6. 1: FISEI 1	94
Tabla 6. 2: FISEI 2	94
Tabla 6. 3: FDAA.....	96
Tabla 6. 4: FCADM 1	97
Tabla 6. 5: FCADM 2	97
Tabla 6. 6: FCHE 1	98

Tabla 6. 7: FCHE 2	99
Tabla 6. 8: FCHE 3	99
Tabla 6. 9: FCIA	101
Tabla 6. 10; FCAUD 1	102
Tabla 6. 11: FCAUD 2	102
Tabla 6. 12: FICM 1.....	104
Tabla 6. 13: FICM 2.....	104
Tabla 6. 14: FJCS	105
Tabla 6. 15: DIBESAU	106
Tabla 6. 16: Especificaciones Central de Monitoreo	108
Tabla 6. 17: Características panel de control	114
Tabla 6. 18: Presupuesto	124

ÍNDICE DE GRÁFICOS

Gráfico 1. 1: Árbol de problemas.....	4
Gráfico 2. 1: Categorías fundamentales	13
Gráfico 2. 2: Constelación de categorías de la Variable. Independiente	14
Gráfico 2. 3: Constelación de categorías de la Variable. Dependiente	15
Gráfico 2. 4: Sistema de gestión	21
Gráfico 2. 5: Red autónoma	24
Gráfico 2. 6: Red heterogénea.....	25
Gráfico 2. 7: Arquitectura de Administración de Redes.....	27
Gráfico 2. 8: Funcionamiento de SNMP	28
Gráfico 2. 9: Protocolo SNMP	28
Gráfico 2. 10: Generación de Interrupciones	28
Gráfico 2. 11: Sistema RMON.....	29
Gráfico 4. 1: ¿Cuenta la Universidad con un proceso de planificación para tomar acciones y conductas para monitorear un evento de seguridad?.....	50
Gráfico 4. 2: ¿Existen elementos necesarios y suficientes para observar los procesos de seguridad en la Universidad?	51
Gráfico 4. 3: ¿La institución posee recursos necesarios y suficientes para2 una administración sostenible del sistema de seguridad?	52
Gráfico 4. 4:¿El sistema de seguridad tiene una red adecuada y actualizada en los predios universitarios?	53
Gráfico 4. 5: ¿Qué porcentaje de cobertura de seguridad tiene la infraestructura de la Universidad Técnica de Ambato?	54
Gráfico 4. 6: ¿Cuenta la Facultad con un proceso de planificación para tomar acciones y conductas para monitorear un evento de seguridad?.....	55
Gráfico 4. 7: ¿Existen elementos necesarios y suficientes para observar los procesos de seguridad en la Facultad?	56
Gráfico 4. 8: ¿La unidad académica posee recursos necesarios y suficientes para una administración sostenible del sistema de seguridad?	58

Gráfico 4. 9: ¿El sistema de seguridad tiene una red adecuada y actualizada en los dominios de la Facultad?.....	59
Gráfico 4. 10: ¿Qué porcentaje de cobertura de seguridad tiene la infraestructura de la Facultad?.....	60
Gráfico 4. 11: ¿Considera Usted que el sistema de comunicación interno es?	62
Gráfico 4. 12: ¿En el caso de una emergencia, a su conocimiento el reporte le llega?	63
Gráfico 4. 13: ¿Cuándo suena la alarma en una dependencia o edificio, el tiempo que se demora en encontrar donde está focalizado el problema es?	64
Gráfico 4. 14: ¿Tienen algún sistema de requisas para los vehículos que ingresan o salen de la institución?	65
Gráfico 4. 15: ¿Tienen alguna identificación, los vehículos de los docentes, alumnos o visitantes de la institución?.....	66
Gráfico 4. 16: ¿En su turno, que tiempo se demora en volver a pasar por el mismo punto?.....	67
Gráfico 4. 17: ¿Cree Usted, que el actual sistema de seguridad es satisfactorio?. 68	
Gráfico 4. 18: ¿Qué tan confiable es el sistema de seguridad actual?	69
Gráfico 4. 19: ¿En caso de detectar alguna anomalía dentro de los predios universitarios, que procedimiento realiza?.....	70
Gráfico 4. 20: ¿En caso de detectar alguna anomalía dentro de los predios universitarios, que procedimiento realiza?.....	71
 Gráfico 6. 1: Topología de central de monitoreo	83
Gráfico 6. 2: Esquema de red.....	91
Gráfico 6. 3: Red IP UTA	93
Gráfico 6. 4: Diagrama de red FISEI	95
Gráfico 6. 5: Diagrama de red de FDAA	96
Gráfico 6. 6: Diagrama de red FCADM.....	98
Gráfico 6. 7: Diagrama de red FCHE.....	100
Gráfico 6. 8: Diagrama de red de FCIA.....	101
Gráfico 6. 9: Diagrama de red de FCAUD	103
Gráfico 6. 10: Diagrama de red de FICM	104

Gráfico 6. 11: Diagrama de red de FJCS	105
Gráfico 6. 12: Diagrama de red de DIBESAU	106
Gráfico 6. 13: Central de monitoreo SG-SYSTEM II.....	109
Gráfico 6. 14: Modo seguidor de sirena.....	110
Gráfico 6. 15: Panel de cuatro zonas.....	110
Gráfico 6. 16: Panel de doce zonas	111
Gráfico 6. 17: Modo estándar.....	112
Gráfico 6. 18: Modo DVACS	112
Gráfico 6. 19: Grabador digital	120
Gráfico 6. 20: sirena Ss-101a	122
Gráfico 6. 21: Detector de movimiento LC 123 PIMSK	122
Gráfico 6. 22: Contacto magnético SM-205Q	123
Gráfico 6. 23: Estación manual de incendio FMM-325A	123

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL
DIRECCIÓN DE POSGRADO
MAESTRIA EN REDES Y TELECOMUNICACIONES

**TEMA: LA ESTRUCTURA DEL SISTEMA DE GESTIÓN DE RED PARA LA
COMUNICACIÓN DE LA SEGURIDAD, DE LA INFRAESTRUCTURA
FÍSICA DE LA UNIVERSIDAD TÉCNICA DE AMBATO.**

Autor: Ing. Santiago Mauricio Altamirano Meléndez

Tutor: Ing. Elsa Pilar Urrutia Urrutia, Mg.

Fecha: 26 de Noviembre del 2013

RESUMEN EJECUTIVO

La Universidad Técnica de Ambato se encuentra catalogada como una de las mejores universidades del Ecuador, pues se halla dentro de las mejores de la región central, y actualmente está obteniendo la certificación internacional. La Universidad Técnica de Ambato en este último tiempo se ha dedicado a invertir en la infraestructura física y de equipamiento de los laboratorios, esto hace que en la actualidad posea infraestructura moderna y equipamiento tecnológico de punta, de la misma manera su población y parque automotriz ha ido en aumento, por lo que se ha visto en la necesidad de actualizar y poder monitorear de una manera centralizada su sistema de seguridad interno, pues en la actualidad posee cada edificio alarmas y el control general son de manera independiente. En el presente trabajo investigativo se presenta un análisis de la prospectiva actual del campus Huachi, se indica así mismo el ancho de banda de la intranet del predio para conectar entre facultades, el diseño de un sistema de gestión de red optimizando los recursos existentes para la seguridad de la infraestructura de la Universidad Técnica de Ambato, a su vez se selecciona los equipos más adecuados para la instalación del sistema de seguridad con sus respectivos manuales de usuario, siendo el sistema de seguridad por medio de monitoreo con tecnología IP, en donde se consigue digitalizar, modernizar y aprovechar la infraestructura de la red, obteniendo un sistema de seguridad integrado en su totalidad, aprovechando la red existente y logrando que el tiempo de respuesta en casos de emergencia, sea efectivo y eficaz.

Descriptores: Ancho de banda, gestión, intranet, IP, manuales, monitoreo, prospectiva, red, seguridad, sistema.

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL
DIRECCIÓN DE POSGRADO
MAESTRIA EN REDES Y TELECOMUNICACIONES

**THEME: THE STRUCTURE MANAGEMENT SYSTEM FOR THE
COMMUNICATION NETWORK SECURITY, PHYSICAL
INFRASTRUCTURE TECHNICAL UNIVERSITY AMBATO.**

Author: Engineer Santiago Mauricio Altamirano Meléndez

Directed by: Engineer Mg. Elsa Pilar Urrutia Urrutia

Date: November 26, 2013

EXECUTIVE SUMMARY

The Technical University of Ambato is ranked as one of the best universities of Ecuador, it is within the best in the Midwest, and is currently obtaining international certification. The Technical University of Ambato in recent times has been dedicated to investing in physical and laboratory equipment infrastructure, this makes today possesses modern infrastructure and technology with the tip, the same way their people and cars has been increased, so has seen the need to update and monitor a centralized system of internal security as currently owns each building alarms and overall control are independently. An analysis of the current campus Huachi foresight is presented in this research work, the bandwidth of the intranet of the property is likewise indicated for connecting power, the design of a network management system optimizing existing resources for infrastructure Security Technical University of Ambato turn the most appropriate equipment for the installation of security system with their respective user manuals are selected, with the security system monitoring via IP technology, where gets scanned, modernize and leverage network infrastructure, obtaining an integrated security system in its entirety, using the existing network and making the response time in an emergency, to be effective and efficient.

Keywords: Bandwidth, management, intranet, IP, manuals, monitoring, prospective, network, security, system.

INTRODUCCIÓN

El proyecto de investigación “La estructura del sistema de gestión de red para la comunicación de la seguridad, de la infraestructura física de la Universidad Técnica de Ambato.”, trata sobre la centralización del sistema de seguridad, para tener un mejor servicio en el caso de una emergencia.

Está estructurado de la siguiente manera:

El CAPÍTULO I, denominado EL PROBLEMA, abarca la contextualización, análisis crítico, la prognosis, la formulación del problema, interrogantes de la investigación, delimitación del objeto de investigación, justificación, objetivo general y objetivos específicos.

El CAPÍTULO II, nombrado MARCO TEÓRICO, contiene los antecedentes investigativos, la fundamentación filosófica, la fundamentación tecnológica, la fundamentación legal, categorías fundamentales, la hipótesis y el señalamiento de las variables.

El CAPÍTULO III, llamado METODOLOGÍA, engloba la modalidad básica de la investigación, el nivel o tipo de investigación, la población y muestra, la Operacionalización de variables, el plan de recolección de la información y el plan de procesamiento de la información.

El CAPÍTULO IV, mencionado ANÁLISIS E INTERPRETACIÓN DE RESULTADOS, implica la tabulación y la representación gráfica de las encuestas y entrevistas con sus respectivos análisis e interpretaciones.

El CAPÍTULO V, citado CONCLUSIONES Y RECOMENDACIONES, abarca las conclusiones que se encontró al momento de realizar la investigación y las recomendaciones que se hacen para la propuesta.

El CAPÍTULO VI, denominado PROPUESTA, describe los datos informativos, antecedentes de la propuesta, justificación, objetivo general, objetivos específicos, análisis de factibilidad, la fundamentación y las conclusiones y recomendaciones.

Se concluye con la bibliografía y los anexos, en los que se incorporan los instrumentos que se aplicaron en la investigación.

CAPÍTULO I

PROBLEMA

1.1 TEMA:

“La estructura del sistema de gestión de red para la comunicación de la seguridad, de la infraestructura física de la Universidad Técnica de Ambato.”

1.2 PLANTEAMIENTO DEL PROBLEMA

1.2.1 CONTEXTUALIZACIÓN

En este **mundo globalizado** la tecnología de última generación se puede adquirir en cualquier parte del globo terráqueo, puesto que si algún instrumento tecnológico se desarrolla en Japón por ejemplo, con solo realizar un clic se lo puede adquirir en Ecuador de manera inmediata, claro está, tomando en cuenta el costo económico que esto implica, en la actualidad, las empresas compiten por dar un mejor servicio a nivel mundial, adquiriendo un sinnúmero de elementos costosos y de tecnología actualizada, por ende también crece la expectativa por una buena seguridad y cuidado de los mismos, teniendo que las empresas monitorear las veinte y cuatro horas del día sus equipos, para salvaguardar su inversión y evitar desagradables malestares.

Hoy en día, los centros de educación superior en el **Ecuador**, debido a las acreditaciones que se están realizando en la actualidad para el mejoramiento académico, se encuentran equipados con laboratorios de última tecnología, así como sus oficinas y aulas se hallan abastecidas de inmuebles y enseres nuevos, por lo que amerita hoy en día tener un sistemas de seguridad eficiente, eficaz,

inmediato, centralizado y normado, para que en cualquier eventualidad que suceda, el tiempo de respuesta de auxilio sea el más corto posible.

La **Universidad Técnica de Ambato**, con trabajo y esfuerzo, ha llegado a destacarse como Alma Mater pionera en el centro del país, tiene tres Campus de estudio (Huachi, Ingahurco y Querochaca), y un Campus en el centro de la ciudad que es el Centro Cultural, todos ellos constan con infraestructura moderna y equipos tecnológicos de vanguardia, todos sus edificios tienen sistemas de seguridad individuales, por tal motivo cuando se procede a violentar alguna puerta de ingreso, se activa la alarma de esa unidad académica o administrativa, procediendo a sonar la sirena, debiendo los guardias de seguridad guiarse por el sonido de la misma, ya que la Universidad no cuenta con un sistema de gestión de red ni con la comunicación de sus sistemas de seguridad. Es por eso que para la Dirección de Sistemas Informáticos y Redes de la Universidad Técnica de Ambato, es prioridad centralizar y automatizar el sistema de seguridad en los predios del Alma Mater, para poder evitar robos como los que se han dado de vehículos y de suministros de los laboratorios, además esto permitirá que no se desperdicien recursos humanos, físicos, tecnológicos ni económicos, y se pueda actuar de una manera rápida, eficaz y eficiente en los eventuales casos de emergencia o auxilio de seguridad que se presenten.

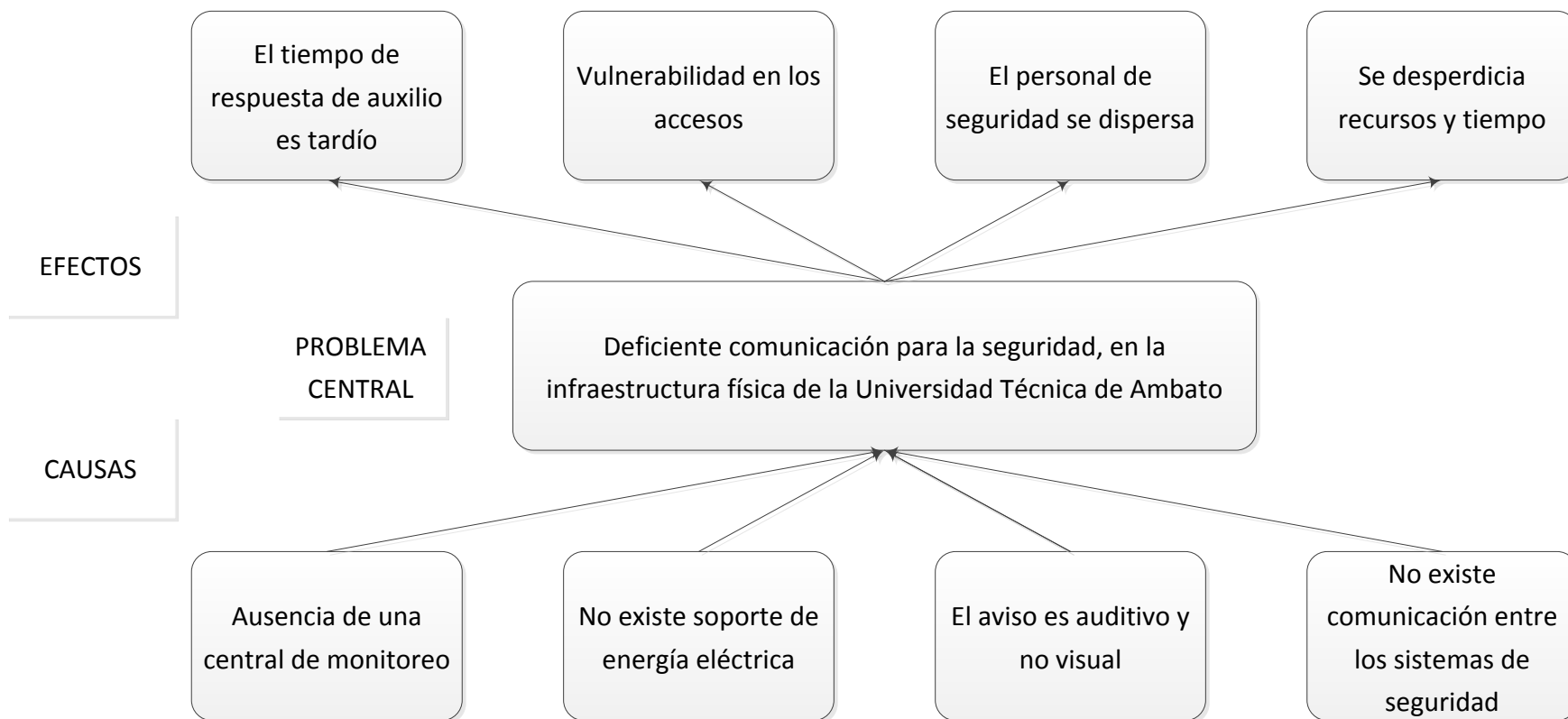


Gráfico 1. 1: Árbol de problemas
Elaborado por: El investigador

1.2.2 ANÁLISIS CRÍTICO

La ausencia de una central de monitoreo para poder controlar la seguridad dentro de los predios de la Universidad, ocasiona que el tiempo de respuesta de auxilio sea tardío, debido a que los señores guardias de la institución no pueden estar focalizados en un cien por ciento en un solo sitio, y deben realizar rondas para poder verificar cualquier evento que suceda en las unidades académicas o administrativas, esto hace que al momento de brindar su contingencia en una emergencia se demoren en llegar.

La no existencia de un respaldo de energía eléctrica o back up como plan de contingencia de emergencia, hace que los accesos sean vulnerables y desprotegidos ante un eventual suceso de robo, debido a que los sistemas de seguridad necesitan alimentación continuamente para funcionar de una manera óptima y correcta, en algún momento que se quede sin suministro de energía eléctrica en los predios de la universidad, prácticamente se estaría desconectando los servicios del sistema de seguridad.

Al ser el aviso de las alarmas de una manera auditiva y no visual, permite que el personal de seguridad se disperse de manera indiscriminada, puesto que el momento en que se activan cuando se haya violentado alguna de las seguridades en los edificios, suenan las sirenas respectivas de esa unidad académica, pero al no tener un aviso visual concreto, el personal de seguridad debe dispersarse para poder encontrar el edificio en problemas.

En los predios de la Universidad no existe comunicación entre los sistemas de seguridad de los edificios administrativos y unidades académicas, por lo que se desperdicia recursos y tiempo al requerir atención y respuesta independiente por parte de cada coordinador de seguridad.

Luego de analizar todos estos puntos podemos decir que existe una deficiente comunicación de la seguridad en la infraestructura física de la Universidad Técnica de Ambato.

1.2.3 PROGNOSIS

La omisión de una central de monitoreo para controlar la seguridad dentro de los predios de la universidad originara problemas para tener una respuesta eficaz y eficiente en caso de una emergencia.

De persistir la ausencia de un soporte o respaldo de energía eléctrica (back up) en las instalaciones del Alma Mater, serán blancos muy fáciles de incursión al realizar cortes en los cables de luz.

De permanecer el aviso solo auditivo y de la manera que está creciendo el sector universitario, se necesitara más personal de apoyo para poder controlar de mejor manera.

De seguir los sistemas de seguridad no comunicados o independientes, el personal que acuda en ayuda, demorara en llegar al punto de encuentro de auxilio para brindar la contingencia requerida y se seguirán desperdiciando recursos físicos y humanos.

1.2.4 FORMULACIÓN DEL PROBLEMA

Como influye la estructura del sistema de gestión de red en la comunicación de la seguridad, de la infraestructura física de la Universidad Técnica de Ambato.

1.2.5 INTERROGANTES

¿Cuál es el estado de la estructura del **sistema de gestión de red** para la optimización de la comunicación de **la seguridad en la infraestructura** física, de la Universidad Técnica de Ambato?

¿Cuáles son los **procesos de comunicación** de la seguridad en la infraestructura física, de la Universidad Técnica de Ambato?

¿Cómo es actualmente la **comunicación de la seguridad**, en la **infraestructura física**, de la Universidad Técnica de Ambato?

1.2.6 DELIMITACIÓN DEL OBJETO DE LA INVESTIGACIÓN

Delimitación del contenido

Área Académica: Hardware y Redes.

Línea de Investigación: Redes de comunicaciones.

Sublíneas de Investigación: Seguridad.

Delimitación Espacial

La investigación se desarrollara en los espacios físicos e infraestructura de la Universidad Técnica de Ambato – Campus Huachi.

Delimitación Temporal

El presente trabajo investigativo se desarrollara desde el mes de Mayo hasta el mes de Noviembre del año 2013.

1.3 JUSTIFICACIÓN

El presente estudio se origina debido al **interés** de centralizar y mejorar la seguridad existente en la Universidad Técnica de Ambato, tanto de su infraestructura como de los bien inmuebles existentes en la misma.

El presente estudio tiene la **importancia** del caso, porque existen equipos costosos de última tecnología y se necesita mejorar el tiempo de respuesta de auxilio en el caso que exista algún inconveniente o emergencia.

Existe **factibilidad** para realizar el presente trabajo investigativo, pues se cuenta con el apoyo necesario del DISIR (Dirección de Sistemas Informáticos y Redes) de la Universidad Técnica de Ambato, los conocimientos suficientes del investigador, bibliografía especializada y recursos tecnológicos y económicos necesarios.

La investigación tendrá una **utilidad teórica y práctica**, pues se contribuye con la teoría a mejorar el conocimiento científico con las temáticas relacionadas al problema de investigación, y en la práctica se lo demuestra con la presentación de una propuesta de solución al problema investigado.

La **originalidad** de este proyecto de investigación se basará en la aplicación de estudios actualizados, libros de consulta, apegados a las leyes vigentes y normativas en el país, además de un estudio minucioso de los problemas de seguridad que tiene el campus universitario y las correcciones que se deben hacer.

La investigación contribuirá con el cumplimiento de la **misión y visión** de la Universidad Técnica de Ambato, entre lo que se puede destacar como lo más importante el de formar profesionales líderes competentes, con pensamiento crítico a través de la investigación que apliquen, promuevan y difundan el conocimiento respondiendo a las necesidades del país.

Los **beneficiarios** de este proyecto serán la Universidad Técnica de Ambato, en lo relacionado a la seguridad de su infraestructura, e indirectamente docentes, administrativos, estudiantes y usuarios en general.

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL

Analizar la estructura del sistema de gestión de red y su influencia en la comunicación para la seguridad de la infraestructura física de la Universidad Técnica de Ambato.

1.4.2 OBJETIVOS ESPECÍFICOS

Realizar un estudio técnico de la estructura del sistema de gestión de red, actualmente aplicado en la Universidad Técnica de Ambato, con el fin de definir las fortalezas y debilidades de la seguridad en la infraestructura física del mismo.

Determinar los procesos de comunicación de la seguridad, en la infraestructura física de la Universidad Técnica de Ambato, con el fin de ubicar los nodos más vulnerables y sensibles.

Plantear una propuesta de diseño de un sistema de gestión de red alternativo, que optimice la comunicación para la seguridad, en la infraestructura física de la Universidad Técnica de Ambato.

CAPÍTULO II

MARCO TEÓRICO

2.1 ANTECEDENTES INVESTIGATIVOS

Una vez revisado el repositorio de las Bibliotecas General y de la Facultad de Ingeniería en Sistemas Electrónica e Industrial de la Universidad Técnica de Ambato, se encontró temas similares a la planteada en la presente investigación, de donde podemos detallar:

(Acuña Garcia & Caicedo Urresta, 2005) ***“GESTIÓN DE REDES DE UN CENTRO DE COMPUTO UTILIZANDO PROTOCOLO SNMP/RMON”***, en donde concluyen lo siguiente: *“Patrol DashBoard permite el manejo de perfiles de usuarios, lo que optimiza y centraliza la información requerida por cada usuario en forma confidencial. Permite a los usuarios medir el servicio que obtienen gracias a su interfaz basada en Web-Browser. Los eventos de red son trabajados en combinación con las alertas, estadísticas, reportes y tendencias que el mismo software los genera. Además recolecta y determina con exactitud la información generada y enviada por el equipo. Permite justificar la adquisición de nuevo hardware mediante la información histórica que proporciona Patrol DashBoard a través de los protocolos. Permite clasificar las alertas de acuerdo a las funciones o responsabilidades de cada perfil de usuario. No se puede olvidar, sin embargo, que la gestión de red, es un problema que nunca estará totalmente resuelto por las herramientas, ya que éstas, sin personal cualificado o procedimientos específicos, pierden su valor.”*. Extracto tomado del repositorio de la Facultad de Ingeniería en sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato.

(Hidalgo Gallo, 2012) **“SISTEMA CCTV (CIRCUITO CERRADO DE TELEVISIÓN) ENTRE EDIFICIOS, PARA LA SEGURIDAD Y VIGILANCIA EN EL AEROPUERTO INTERNACIONAL COTOPAXI”** concluye que: “El sistema CCTV (Circuito Cerrado de Televisión) es uno de los más completos, permite obtener una seguridad y vigilancia confiable; su principal característica de cámaras Pelco C10DN y PTZ IV Series es evitar cualquier situación y actos indebidos ocurridos en algún lugar o área específica, en este caso el Terminal aéreo, seguridad aeroportuaria, servicio de equipajes y counters (Venta de Ticket’s) son los más importantes y mayor influencia de personas. Para el diseño de comunicación del sistema CCTV fue de gran ayuda el conocimiento de la investigación como son los medios de transmisión, fibra óptica, ancho de banda, capacidad de almacenamiento de los DVR’s, distancias de ubicación de las cámaras, instalación del domo con tarjeta electrónica y contribuir con varias decisiones, obteniendo resultados favorables para el Aeropuerto. La labor de recopilación de información sobre el funcionamiento de los sistemas descritos en el presente proyecto, ha permitido obtener una visión más amplia respecto al diseño de comunicaciones por fibra óptica. Se puede concluir que para el correcto funcionamiento de la red se hace necesario el apoyo de otros sistemas adicionales como son: el sistema de respaldo de energía eléctrica UPS, en el momento de realizar cortes y el sistema de respaldo de información los Grabadores de video o DVR’s. El diseño implementado se realizó con tecnología, utilizando fibra óptica, contando con cámaras fijas y PTZ inteligentes con un control de TX y RX adecuado, que pueden ser adaptados a cualquier hora tanto el día como la noche, esto permite el manejo confiable y discreto del sistema. Además en el sistema se tiene una confiabilidad muy alta para todo el año en funcionamiento, lo que implica que no exista ninguna interrupción en la transmisión de datos.”. Extracto tomado del repositorio de la Facultad de Ingeniería en sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato.

2.2 FUNDAMENTACIÓN FILOSÓFICA

Los esquemas de la investigación filosófica, enmarcan aspectos importantes que nos ayudan a obtener información lógica y razonable ante las necesidades de los investigadores y sus proyectos con base en un análisis a fondo y sin temores de quedarse en un solo concepto, sino mucho más allá de lo conocido.

2.3 FUNDAMENTACIÓN TECNOLÓGICA

La tecnología es un baluarte para la mejora de los procesos y establecer un costo beneficio sobre proyectos que vayan en pos de la mejora de la seguridad y la comunicación en todo ámbito.

2.4 FUNDAMENTACIÓN LEGAL

La investigación se sustentara en una estructura legal contemplada en la Constitución de la República del Ecuador, las Normas internas de seguridad de la Universidad Técnica de Ambato y en las Leyes y Normativas de propiedad intelectual.

2.5 CATEGORÍAS FUNDAMENTALES

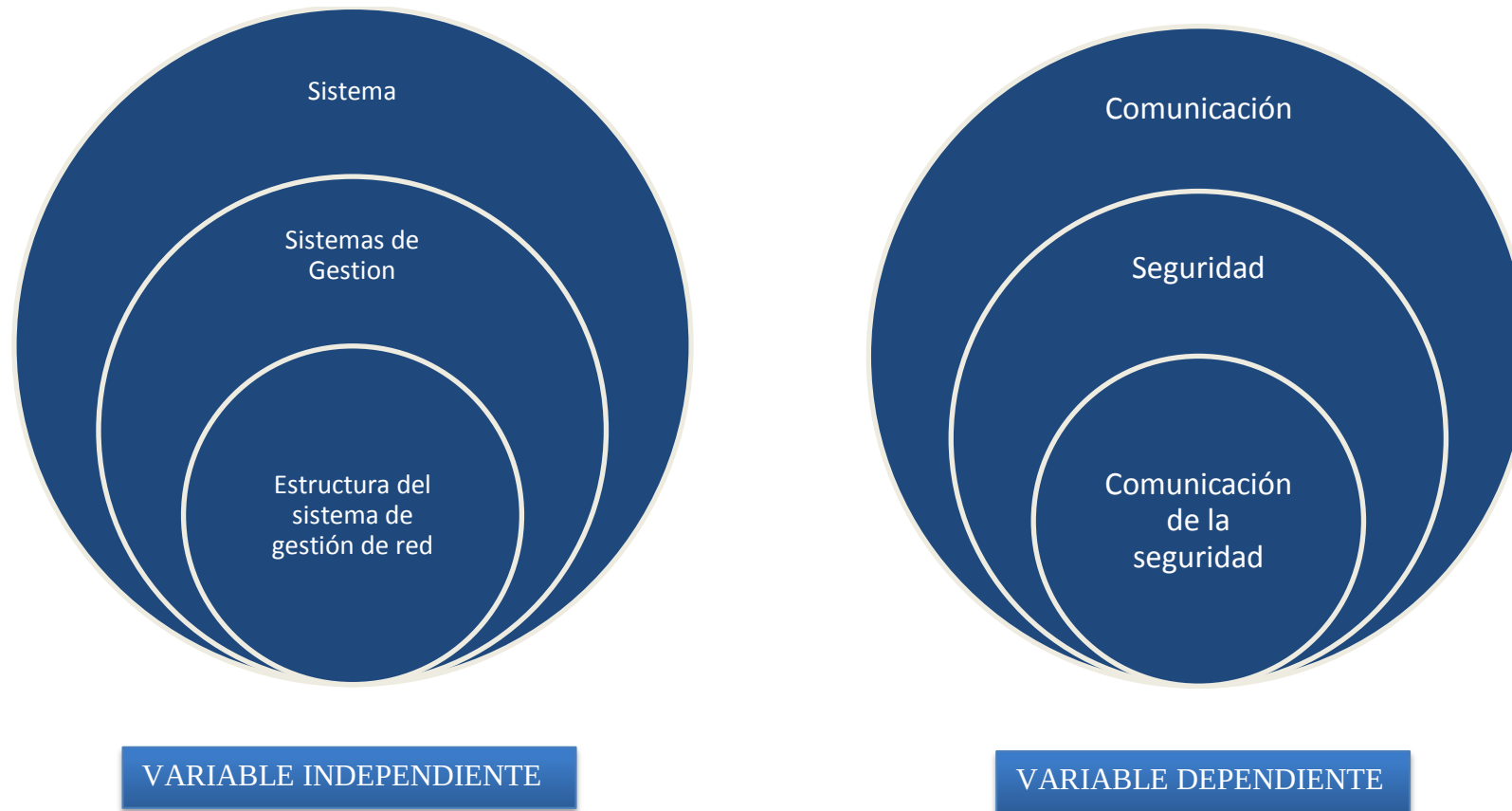


Gráfico 2. 1: Categorías fundamentales
Elaborado por: El investigador

2.5.1 DEFINICIÓN DE LA VARIABLE INDEPENDIENTE



Gráfico 2. 2: Constelación de categorías de la Variable. Independiente
Elaborado por: El investigador

2.5.2 DEFINICIÓN DE LA VARIABLE DEPENDIENTE

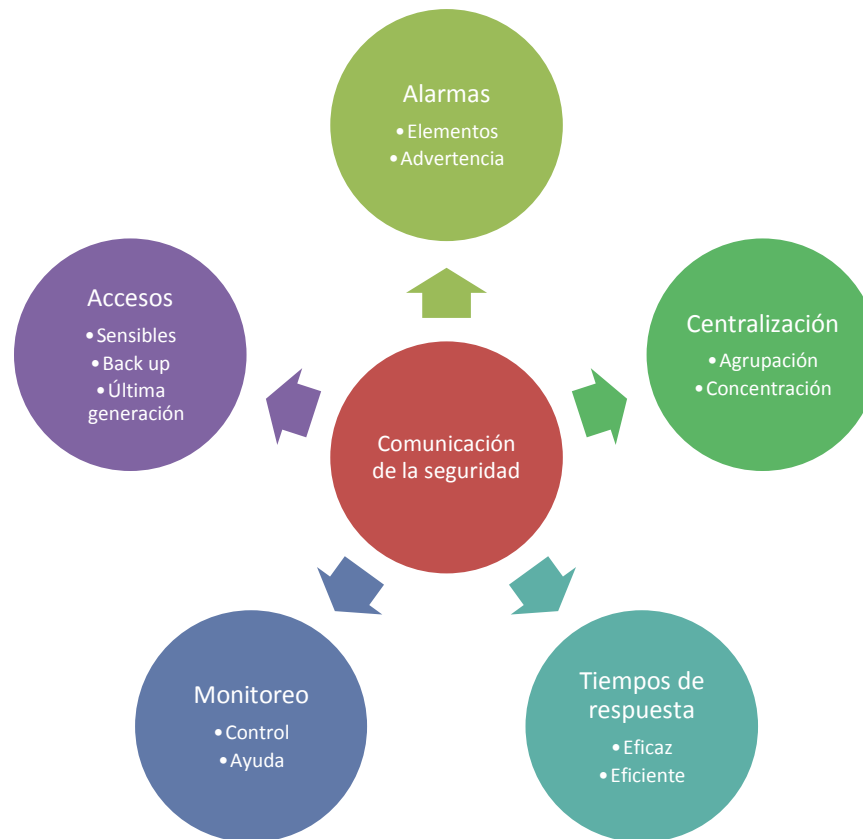


Gráfico 2. 3: Constelación de categorías de la Variable. Dependiente
Elaborado por: El investigador

2.5.3 SISTEMA

(Share, 2012) *Un sistema, de manera general proviene del latín *systema*, y del griego *σύστημα*, es un objeto complejo cuyos componentes se relacionan con al menos algún otro componente; este puede ser materias o conceptual. Todos los sistemas tienen composición, estructura y entorno, pero sólo los sistemas materiales tienen mecanismo, y sólo algunos sistemas materiales tienen forma. Según el Sistemismo, todos los objetos son sistemas o componentes de otro sistema.*

Entonces podemos decir que es módulo ordenado de elementos que se encuentran interrelacionados y que interactúan entre sí. El concepto se utiliza tanto para definir a un conjunto de conceptos como a objetos reales dotados de organización.

Un sistema conceptual o ideal es un conjunto organizado de definiciones, símbolos y otros instrumentos del pensamiento (como las matemáticas, la notación musical y la lógica formal).

Un sistema real, en cambio, es una entidad material formada por componentes organizados que interactúan de forma en que las propiedades del conjunto no pueden deducirse por completo de las propiedades de la partes (denominadas propiedades emergentes).

Los sistemas reales comprenden intercambios de energía, información o materia con su entorno. Las células y la biosfera son ejemplos de sistemas naturales. Existen tres tipos de sistemas reales: abiertos (recibe flujos de su ambiente, adaptando su comportamiento de acuerdo a esto), cerrados (sólo intercambia energía con su entorno) y aislados (no realiza ningún tipo de intercambio con su entorno).

Por ejemplo, un núcleo atómico es un sistema material físico compuesto de protones y neutrones relacionados por la interacción nuclear fuerte; una molécula es un sistema material químico compuesto de átomos relacionados por enlaces químicos; una célula es un sistema material biológico compuesto de orgánulos relacionados por enlaces químicos no-covalentes y rutas metabólicas;

una corteza cerebral es un sistema material psicológico (mental) compuesto de neuronas relacionadas por potenciales de acción y neurotransmisores; un ejército es un sistema material social y parcialmente artificial compuesto de personas y artefactos relacionados por el mando, el abastecimiento, la comunicación y la guerra; el anillo de los números enteros es un sistemas conceptual algebraico compuesto de números positivos, negativos y el cero, relacionados por la suma y la multiplicación; y una teoría científica es un sistema conceptual lógico compuesto de hipótesis, definiciones y teoremas relacionados por la correferencia y la deducción.

2.5.4 SISTEMA DE GESTIÓN

(ACCID, 2010) Actualmente las empresas e instituciones innovadoras se manejan por medio de sistemas de gestión, para poderse desarrollar de mejor manera, para poder enfrentar los retos que hoy en día se presentan, como son: rentabilidad, competitividad, globalización, velocidad de los cambios, capacidad de adaptación, crecimiento, tecnología, entre otros. Equilibrar estos requisitos, puede constituir un proceso difícil. Es aquí donde entran los sistemas de gestión, al permitir aprovechar y desarrollar el potencial existente en la organización. La implementación de un sistema de gestión eficaz puede ayudar a:

- *Gestionar los riesgos sociales, medioambientales y financieros.*
- *Mejorar la efectividad operativa.*
- *Reducir costos.*
- *Aumentar la satisfacción de clientes y partes interesadas.*
- *Proteger la marca y la reputación.*
- *Lograr mejoras continuas.*
- *Potenciar la innovación.*
- *Eliminar las barreras al comercio.*
- *Aportar claridad al mercado.*

El uso de un sistema de gestión probado permite renovar constantemente su objetivo, sus estrategias, sus operaciones y niveles de servicio.

Un sistema de gestión ayuda a lograr las metas y objetivos de una organización mediante una serie de estrategias, que incluyen la optimización de procesos, el enfoque centrado en la gestión y el pensamiento disciplinado. Por tanto es un conjunto de etapas unidas en un proceso continuo, que deja trabajar ordenadamente una idea hasta lograr mejoras y su continuidad.

Un sistema de gestión hace que las empresas funcionan como unidades completas con una visión compartida. Ello engloba la información compartida, evaluaciones comparativas, trabajo en equipo y un funcionamiento acorde con los más rigurosos principios de calidad y del medioambiente.

(IMPLEMENTACION SIG), *En un sistema de gestión “se establecen cuatro etapas en este proceso, que hacen de este sistema, un proceso circular virtuoso, pues en la medida que el ciclo se repita recurrente y recursivamente, se logrará, obtener una mejora, respecto al anterior ciclo, lo que se denomina la Mejora Continua de un Sistema de Gestión.*

En un sistema de gestión existen cuatro etapas a cumplir.

- *Etapas de Ideación.*
- *Etapas de Planeación.*
- *Etapas de Implementación.*
- *Etapas de Control”.*

Etapas de Ideación

Esta etapa consiste en trabajar en la idea que guiará los primeros pasos del proceso de creación que se logra con el sistema de gestión propuesto. Existen varias metodologías para lograr refinar la idea. Siendo la más conocida la conocida como lluvia de ideas o brainstorming, que consiste en generar el máximo de ideas para obtener un amplio espectro de posibilidades en dónde atacar. Este proceso consiste en que un grupo o una persona, durante un tiempo prudente se enfocan en generar o “lanzar” ideas sin restricciones, pero que tengan cercanía con el tema que se está tratando. Una vez que se tenga un listado adecuado, se procede a analizar

las ideas y a pulir su cercanía con lo que realmente se quiere. La idea central de este proceso es que aquí se debe definir claramente el objetivo perseguido, es decir se debe plantear la pregunta “¿Qué queremos lograr?”. Una vez definido, se procede al “¿Cómo lograrlo?” y se pasa a la siguiente etapa.

Etapas de Planificación

Este paso constituye una etapa fundamental y el punto de partida de la acción directiva, ya que supone el establecimiento de sub-objetivos y los cursos de acción para alcanzarlos. Es así que en esta etapa, se definen las estrategias que se utilizarán, la estructura organizacional que se requiere, el personal que se asignará, el tipo de tecnología que se necesita, los recursos que se van emplear y la clase de controles que se aplicaran en todo el proceso.

Etapas de Implementación

Esta etapa se entiende por gestión, es decir la acción y efecto de administrar. Pero, en un contexto empresarial, esto se refiere a la dirección que toman las decisiones y las acciones para alcanzar los objetivos trazados. Se debe destacar que las decisiones y acciones que se toman para llevar adelante un propósito, se sustentan en los mecanismos o instrumentos administrativos (estrategias, tácticas, procedimientos, presupuestos, etc.), que están sistémicamente relacionados y que se obtienen del proceso de planificación.

Etapas de Control

Esta etapa es una función administrativa, de carácter regulador, que permite verificar si la actividad, proceso, unidad, sistema, etc., está cumpliendo sus objetivos o alcanzando los resultados que se esperan. Por tanto se debe señalar que la finalidad del control es la detección de errores, fallas o diferencias, en relación a un planteamiento inicial, para su corrección y/o prevención. Por tanto, el control debe estar muy relacionado con los objetivos inicialmente definidos, por lo que

debería permitir la medición y cuantificación de los resultados, la detección de desviaciones y el establecimiento de medidas correctivas y preventivas, empezando desde ya a considerar que las medidas preventivas serán las más convenientes para la organización.

2.5.5 SISTEMA DE GESTIÓN DE RED

Hasta ahora hemos analizado un sistemas de gestión de manera general, en lo que a la investigación propiamente se refiere, vamos a proceder a analizar un sistemas de gestión de red, que después de analizar varios autores podemos decir que consiste en monitorizar y controlar los recursos de una red con el fin de evitar que esta llegue a funcionar incorrectamente degradando sus prestaciones.

La utilización de un sistema de gestión de red, la monitorización del tráfico y la calidad de servicio, nos permitirá evitar problemas, y a su vez dar una solución rápida y eficaz. Una red corporativa debe contar con un sistema de administración porque hay que asegurar a los usuarios.

(Correa & Agudelo, 2009) *“...Existen diferentes tipos de gestión de redes, como pueden ser redes pequeñas, medianas y grandes, pero que por lo general deben ser redes heterogéneas. La monitorización no puede hacerse de una forma manual, a medida que se hacen más heterogéneas se requieren herramientas automatizadas de gestión de fallos, de cuentas, de configuración y nombres, de prestaciones y de seguridad, basadas sobre estándares, que funcionen sobre la gran variedad de equipos de diferentes fabricantes, con interfaces de operador únicos, con un conjunto de órdenes que realicen todas las tareas de administración de la red, con un software incorporado en las estaciones de usuario y en los dispositivos de red con capacidad de recoger estadísticas del equipo en que se aloja responder a las órdenes del centro de control y enviar mensajes bajo condiciones establecidas, y con capacidad de generación de estadísticas, de informes.”*

Necesitamos herramientas automatizadas que permita la gestión de: Fallos, cuentas de configuración y nombres de prestaciones de seguridad.

La gestión de red tiene como propósito la utilización y coordinación de los recursos para redes de comunicaciones, para adaptarse a la calidad de servicio necesaria, a un determinado costo.

Los elementos de un sistema de gestión son:

- El gestor.
- El agente.
- El protocolo de gestión.
- La base de información de gestión (MIB, Management Information Base).

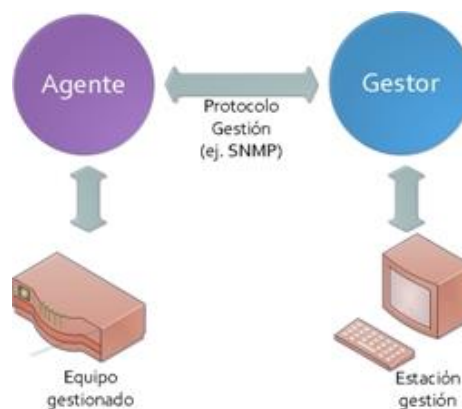


Gráfico 2. 4: Sistema de gestión

Tomado de: <http://www.aunclidelastic.com/wp-content/uploads/ModeloGestorAgenteSNMP.jpg>

El gestor.

Es la parte de la aplicación que emite las directivas de operaciones de gestión y recibe notificaciones y respuestas.

El agente.

Tiene la función de responder a las directivas enviadas por el gestor.

La MIB.

Es el conjunto de objetos gestionados que representan a los recursos de la red que permiten algún tipo de gestión en una forma abstracta.

El protocolo.

Es el conjunto de especificaciones y convenciones que gobiernan la interacción de procesos y elementos dentro de un sistema de gestión.

En la actualidad SNMP (Simple Network Management Protocol), forma parte del modelo de gestión de internet, y CMIP (Common Management Information protocol), es parte del modelo de gestión OSI, son los protocolos predominantes.

Dentro de las áreas funcionales de un sistema de gestión de red, podemos anotar las siguientes.

- Gestión de fallas.
- Gestión de configuración.
- Gestión de contabilidad.
- Gestión de desempeño.
- Gestión de seguridad.

Gestión de Fallas.

Establece la generación de notificaciones específicas de error (alarmas). Así como el registro de las notificaciones de error y la verificación de los recursos de red para trazar e identificar fallas.

Gestión de Configuración.

Se distribuye en actividades de inicialización, instalación, y abastecimiento. Esto permite tener información de configuración y estado en demanda, proporcionando

facilidades de inventario y además soporta el anuncio de cambios de configuración a través de notificaciones relevantes.

Gestión de Contabilidad.

Consiste en actividades de recolección de información de contabilidad y su procesamiento para propósitos de cobranza y facturación. Las actividades generalmente establecen un límite contable para que un conjunto de costos se combinen con recursos múltiples y se utilicen en un contexto de servicio.

Gestión de desempeño.

Proporciona información en forma ordenada, para determinar la carga del sistema y de la red, bajo condiciones naturales y artificiales. Además proporciona estadísticas y permite actividades de planeación de configuración.

Gestión de Seguridad.

La gestión de seguridad requiere la habilidad para supervisar y controlar la disponibilidad de facilidades de seguridad, y reportar amenazas y rupturas en la seguridad, así como se requiere la habilidad para autenticar usuarios y aplicaciones de gestión, con el fin de garantizar la confidencialidad e integridad de intercambios de operaciones de gestión y prevenir accesos no autorizados a la información.

Por lo tanto la gestión de red se define como el conjunto de actividades dedicadas al control y vigilancia de recursos de telecomunicación. Su principal objetivo es garantizar un nivel de servicio en los recursos gestionados con el mínimo costo.

Los métodos de gestión de red deben ser puestos en práctica mediante la organización de un Centro de Gestión de Red, que va a disponer de tres clases de recursos:

- Métodos de Gestión.
- Recursos humanos.
- Herramientas de apoyo.

Dentro de los métodos de gestión podemos señalar algunos tipos de gestión de red integrada, como:

- Gestión autónoma.
- Gestión heterogenia.

Gestión Autónoma.

Las primeras redes tenían pocos nodos y cada uno de ellos poseía su propio sistema de gestión local. Las decisiones que afectaban a más de un nodo, implicaban la comunicación con cada uno de los administradores de red.

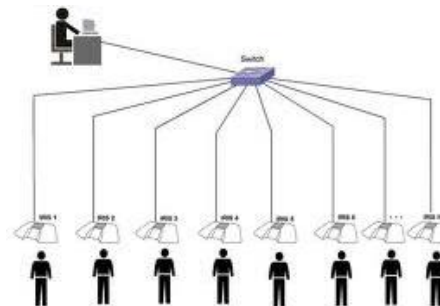


Gráfico 2. 5: Red autónoma
Tomado de: http://www.ebasis.es/slider/gestion_red.jpg

Gestión Heterogénea.

Las redes crecen y evolucionan a partir de la incorporación de una amplia variedad de tecnologías. Esta evolución de las redes ha traído consigo la necesidad de que coexistan sistemas de gestión de red de muy diversas naturaleza.



Gráfico 2. 6: Red heterogénea
Tomado de: http://www.ebasis.es/slider/gestion_red_1.jpg

(Correa & Agudelo, 2009) “Los organismos de normalización han definido tres modelos principales para la gestión de red integrada:

- *Arquitectura TMN (Telecommunications Management Network o Red de Gestión de las Telecomunicaciones).*
- *Gestión de red OSI (Open Systems Interconnection o Interconexión de Sistemas Abiertos).*
- *Gestión Internet (Definida por la ISOC para gestión de redes TCP/IP). ”*

Lo que tiene que ver con el modelo de Gestión en Internet, en los setenta el número de nodos de Internet era muy reducido, y se gestionaba Internet con las facilidades que ofrecía el protocolo ICMP, como el PING.

Cuando Internet avanzó en complejidad, multiplicando el número de nodos se empezó a trabajar en tres soluciones diferentes, que se definieron en 1987 de la siguiente manera:

- SGMP.
- HEMS.
- CMOT.

El Modelo de Gestión en Internet SGMP

Simple Gateway Monitoring Protocol, Protocolo Simple de Monitorización de Pasarelas. Fue un sencillo protocolo orientado fundamentalmente a la gestión de pasarelas IP. Posteriormente pasaría a llamarse SNMP (Simple Network Management Protocol), Protocolo Simple de Gestión de Red.

HEMS

High-Level Entity Management System, en español Sistema de Gestión de Entidades de Alto Nivel. Nunca llegó a tener aplicación práctica.

CMOT (CMIP).

Adopción de los estándares ISO como marco de gestión para Internet sobre una torre de protocolos TCP/IP.

En 1990 el SNMP se convirtió en el estándar de las redes TCP/IP y de Internet.

En 1992, se comenzó el trabajo para especificar una nueva versión de SNMP, la SNMPv2; hoy en día todavía continúan los trabajos de actualización para la SNMPV3.

Hasta el momento existen tres versiones del protocolo: SNMPv1 (versión 1), SNMPv2 (versión 2) SNMPv3 (versión 3). Las tres son muy parecidas, solo que SNMPv2 tiene algunas mejoras sobre la primera versión, y de la misma forma SNMPv3 tiene ciertas ventajas sobre la segunda versión.

Protocolo SNMPv1

Es un protocolo de la capa de aplicación diseñado para facilitar el intercambio de gestión de información entre los dispositivos de redes.

Arquitectura de Administración de Redes.

Incluye los siguientes elementos:

- Estación de Gestión (Manager).
- Agente Administrador (Agente).
- Base de Información de Administrada (MIB).
- Protocolo de Administración de Redes

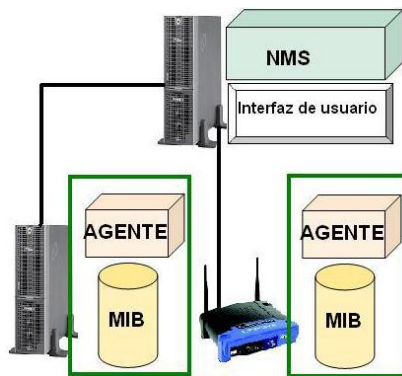


Gráfico 2. 7: Arquitectura de Administración de Redes

Tomado de: <http://velezconde.files.wordpress.com/2009/06/arquitectura-smnp.jpg?w=474&h=388>

Protocolo SNMPv1

El uso de SNMP requiere que todos los agentes, así como los managers, deben soportar una suite de protocolo, tal como UDP e IP. Esto limita la administración directa y excluye otros dispositivos, tales como puentes y módems, que no soportan cualquier parte de la suite del protocolo TCP/IP. Para acomodar dispositivos que no implementan SNMP, el concepto de proxy fue desarrollado. En este esquema un agente SNMP actúa como un proxy para uno o más dispositivos; esto es, el agente SNMP actúa en nombre de los dispositivos que se encuentran en el proxy. El SNMP es independiente del protocolo IP con USP y UDP, se implementa usando los puertos 161 y 162, el puerto 161 se usa para las transmisiones normales y el puerto 162 se utiliza para los mensajes de tipo Trap o interrupción.

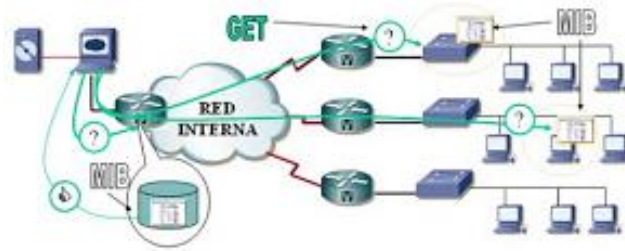


Gráfico 2. 8: Funcionamiento de SNMP

Tomado de: <http://image.slidesharecdn.com/gestionderedes-copia-090512200340-phpapp01/95/728.jpg>



Gráfico 2. 9: Protocolo SNMP

Tomado de: <http://image.slidesharecdn.com/gestionderedes-copia-090512200340-phpapp01/95/729.jpg>



Gráfico 2. 10: Generación de Interrupciones

Tomado de: <http://image.slidesharecdn.com/gestionderedes-copia-090512200340-phpapp01/95/730.jpg>

SNMP VERSION 2

De SNMPv1 se mejoró en reducir la carga de tráfico adicional para la monitorización (Get Bulk e Informs) y solucionar los problemas de monitorización remota o distribuida con (RMON).

SNMP VERSION 3

Mejoro en brindar mayor seguridad en las transmisiones (Cifrado y autenticación).

RMON

Remote Monitor o Monitoreo Remoto, brinda la capacidad para observar la red como un todo, aunque este distribuida. Se declara una MIB especial para guardar esta información. Pueden estar localizadas en cada segmento de la red y pueden introducirse en un Pc, Sw, Router.

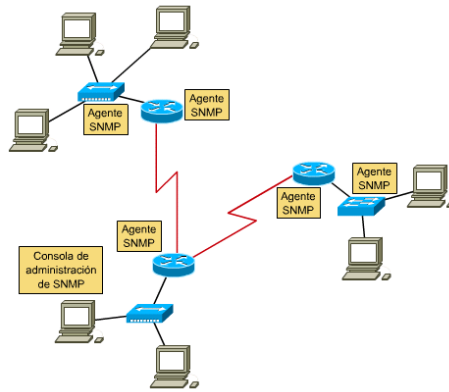


Gráfico 2. 11: Sistema RMON

Tomado de: <http://image.slidesharecdn.com/gestionderedes-copia-090512200340/slide731.jpg>

MRTG

Herramienta para monitorización del tráfico en las redes y sus enlaces tanto internos como externos.

- Genera paginas HTML con imágenes, que ofrecen visión en tiempo real del tráfico.
- Permite a través de un script Perl, leer atributos de los objetos (Routers, Switch).
- Guarda información por semanas, meses, y años.
- Monitorea la carga del sistema, sesiones establecidas, tráfico, errores, etc.
- Es de libre distribución.

Dependiendo del territorio que una red abarca, se puede clasificar en:

- LAN
- WAN
- MAN

LAN, Local Área Network

Una Red de Área Local está normalmente restringida a un área geográfica de tamaño limitado, como un edificio de oficinas y depende de un canal físico de comunicaciones con una velocidad media/alta y con una tasa de errores reducida.

WAN, Wide Area Network

Una Red de Área Extensa es una red que ofrece servicios de transporte de información entre zonas geográficamente distantes. Es el método más efectivo de transmisión de información entre edificios o departamentos distantes entre sí.

MAN, Metropolitan Area Network

Una red de área metropolitana es una red de alta velocidad (banda ancha) que dando cobertura en un área geográfica extensa, proporciona capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y vídeo, sobre medios de transmisión tales como fibra óptica y par trenzado de cobre a velocidades que van desde los 2 Mbps hasta 155 Mbps (Megabits por segundo).

El concepto de red de área metropolitana representa una evolución del concepto de red de área local a un ámbito más amplio, cubriendo áreas de una cobertura superior que en algunos casos no se limitan a un entorno metropolitano sino que pueden llegar a una cobertura regional e incluso nacional mediante la interconexión de diferentes redes de área metropolitana.

2.5.6 COMUNICACIÓN

Adicionalmente en el mundo globalizado que vivimos hoy en día, es importante tener una comunicación eficaz entre todos los entes relacionados dentro de las instituciones, para que la seguridad de los bienes y personas sea óptima y tangible, es decir esa sensación interior que nos hace sentir bien, confiados en nuestro entorno diario, de la cual abundan las definiciones según se trate de seguridad social, pública, privada, ciudadana, hemisférica, colectiva, entre otras; está cada vez emparentada con la temática de la comunicación, las nuevas tecnologías, los procesos de globalización y de cambio.

Cabe mencionar, que la Organización de las Naciones Unidas aporta la siguiente definición de seguridad, que amplía el concepto tradicional, incluyendo los temas económicos, políticos y sociales. La define como:

(ONU-2011) “En principio la seguridad es una condición en la que los Estados o los individuos consideran que están expuestos en pequeña medida al peligro de un ataque militar, a las penurias económicas, a la presión política o a la injusticia social”. A lo que puede sumarse el enfoque multidimensional de la seguridad emanado de la Declaración de Bridgetown - Organización de los Estados Americanos (OEA), en junio del 2002

Los procesos de aceleración histórica provocan constantes cambios y ellos llegan también a la esfera de la seguridad, he aquí el tema de la seguridad y las nuevas tecnologías adquieren otra dimensión.

En el devenir histórico, estamos ahora frente a un nuevo contexto, el del universo de la sociedad de las nuevas tecnologías, en un momento histórico de la vida del ser humano: la convivencia paralela y simultánea de dos sociedades. Por una parte una real y por otra la virtual; donde deberemos considerar las ventajas y las desventajas de las nuevas tecnologías de la información y la comunicación (NTIC) y la aplicación de las mismas a los temas de seguridad.

Podemos indicar que la *Seguridad Privada* es la seguridad de las personas en cuanto a su integridad física y sus bienes. Acción realizada por entidades u organismos cuyo objetivo es la protección de personas y bienes propios o dados en custodia, dentro del ambiente en que se desarrolla su quehacer conforme a la ley.

La palabra comunicación, viene del latín "communicare", que significa *poner en común*. Comunicar es: compartir, asociar y lleva implícita la idea de participación en interacción.

Se habla de comunicación como el intercambio de actitudes, sentimientos, entre otros, que se establecen entre los individuos. También como el proceso que pone en contacto dos polos: el comunicador (emite un mensaje) y el perceptor (recibe, analiza y responde al mensaje), mediante un canal, mensaje, de acuerdo con un código compartido por ambos, con un referente; en un contexto, inscripto en una formación social, bajo una forma interactiva (retroalimentación). En términos aristotélicos se puede decir que siempre que una persona desea comunicar algo a alguien, está presente la idea de la persuasión y que por lo tanto siempre que se "comunica" se lo hace con una intención.

Existen diferentes tipos de comunicación, aquí analizamos algunos de ellos.

Comunicación Social.

Es una forma de comunicación que intenta favorecer la convivencia humana, para mejorar la condición de vida material y espiritual de los individuos. Es lo opuesto a comunicación de masas aunque se valga de los mismos soportes para difundir sus mensajes.

Comunicación de Masas.

Es una comunicación dirigida a un público masivo, heterogéneo, anónimo y que se vale de los medios masivos de comunicación para propalar mensajes. Ellos tienen

como características ser niveladores hacia abajo, producen una comunicación impersonal, privatizan (aislamiento), narcotizan (dan una información tipo collage: se sabe poco de muchos temas y la información queda en la periferia) y provocan sincretismo (confusión entre realidad y fantasía) y presentan estereotipos. Es el puente de unión entre la sociedad de masas y la cultura de masas.

Comunicación Estratégica.

Es la coordinación de todos los recursos comunicacionales externos e internos de una empresa para diferenciarlos de la competencia y lograr un lugar en la mente de los públicos que nos interesan.

2.5.7 SEGURIDAD

El término seguridad proviene de la palabra en latín securitas. Cotidianamente se puede referir a la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien. Sin embargo, el término puede tomar diversos sentidos según el área o campo a la que haga referencia.

Según la pirámide de Maslow, “la seguridad en el hombre ocupa el segundo nivel dentro de las necesidades de déficit.”

Según la teoría de las necesidades de Bronisław Malinowski, “la seguridad es una de las siete necesidades básicas a satisfacer por el hombre.”

La seguridad se da, debido a que existe el riesgo, que es la proximidad o posibilidad de un daño o peligro de cada uno de los imprevistos o hechos desafortunados, que puede cubrir un seguro.

A la seguridad se lo puede definir como la cualidad o estado de seguro, de la garantía o conjunto de garantías que se da a alguien sobre el cumplimiento de algo.

A continuación podemos citar algunos ejemplos como el de Seguridad Social, que es el conjunto de organismos, medios, medidas, de la administración estatal para prevenir o remediar los posibles riesgos, problemas y necesidades de los trabajadores, como enfermedad, accidentes laborales, incapacidad, maternidad o jubilación; se financia con aportaciones del Estado, trabajadores y empresarios.

Se dice también de todos aquellos objetos, dispositivos, o medidas, que contribuyen a hacer más seguro el funcionamiento o el uso de una cosa: cierre de seguridad, cinturón de seguridad.

Con estos conceptos podemos hablar de la criminología, ya que se ha calificado hoy en día a los delitos mediante diferentes formas, como los físicos o los por medio de la computadora o sistemas de información.

A continuación citaremos consideraciones que se deben tener para elaborar la evaluación de la seguridad.

Uso del control de acceso

Se debe observar el uso adecuado del control de acceso de monitoreo y su software, que puede ser susceptible de uso ajeno y de copias de los programas que utiliza la institución para realizar copias de acceso directo o telefónico a bases de datos con fines fraudulentos.

Sistema de Acceso

Para evitar los fraudes tecnológicos se debe contemplar de forma clara los accesos a las computadoras de acuerdo al nivel de seguridad de acceso, al empleo de las claves de acceso, y a evaluar la seguridad contemplando la relación costo, ya que a mayor tecnología de acceso mayor costo.

Cantidad y Tipo de Información

El tipo y la cantidad de información que se introduce en las memorias de las computadoras deben considerarse como un factor de alto riesgo ya que podrían producir que la información esté en manos de algunas personas y la alta dependencia en caso de pérdida de datos.

Control de Programación

Se debe tener en cuenta que el delito más común está presente en el momento de la programación de los dispositivos de entrada, ya que puede ser cometido intencionalmente o no, para lo cual se debe controlar que los programas no contengan bombas lógicas y sus respectivas actualizaciones.

Personal

Se debe observar este punto con mucho cuidado, ya que hablamos de las personas que están ligadas al sistema de información de forma directa y se deberá contemplar principalmente la dependencia del sistema a nivel operativo y técnico, la evaluación del grado de capacitación operativa y técnica, el contemplar la cantidad de personas con acceso operativo y administrativo, conocer la capacitación del personal en situaciones de emergencia.

Medios de Control

Se debe contemplar la existencia de medios de control para conocer cuando se produce un cambio o un fraude en el sistema del acceso de entrada.

Rasgos del Personal

Se debe ver muy cuidadosamente el carácter del personal relacionado con el sistema de seguridad, ya que pueden surgir malos manejos de administración, malos manejos por negligencia o malos manejos por ataques deliberados.

Instalaciones

Es muy importante no olvidar las instalaciones físicas y de servicios, que significan un alto grado de riesgo. Para lo cual se debe verificar la continuidad del flujo eléctrico, los efectos del flujo eléctrico sobre el software y hardware, evaluar las conexiones con los sistemas eléctrico, telefónico, cable, etc., verificar si existen un diseño, especificación técnica, manual o algún tipo de documentación sobre las instalaciones.

Establecer las Áreas y Grados de Riesgo

Es muy importante el crear una conciencia en los usuarios sobre el riesgo que corre la información y hacerles comprender que la seguridad es parte de su trabajo. Se deben conocer los principales riesgos que acechan a la seguridad y los medios de prevención que se deben tener, para lo cual se debe establecer el Costo del Sistema de Seguridad (Análisis Costo vs Beneficio), este estudio se realiza considerando el costo que se presenta cuando se pierde la información vs el costo de un sistema de seguridad. Para lo cual se debe considerar:

- Clasificar la instalación en términos de riesgo (alto, mediano, pequeño).
- Identificar las aplicaciones que tengan alto riesgo.
- Cuantificar el impacto en el caso de suspensión del servicio aquellas aplicaciones con un alto riesgo.
- Formular las medidas de seguridad necesarias dependiendo del nivel de seguridad que se requiera.
- La justificación del costo de implantar las medidas de seguridad.

Sistema Integral de Seguridad

Un sistema integral debe contemplar las siguientes etapas:

- Definir elementos administrativos.
- Definir políticas de seguridad.
 - A nivel departamental.
 - A nivel institucional.
- Organizar y dividir las responsabilidades.
- Contemplar la seguridad física contra catástrofes (incendios, terremotos, inundaciones, etc.)
- Definir prácticas de seguridad para el personal.
- Plan de emergencia de evacuación, uso de recursos de emergencia como:
 - Extinguidores.
 - Números telefónicos de emergencia.
 - Pólizas de seguros.
 - Elementos técnicos de procedimientos.
- Definir las necesidades de sistemas de seguridad para:
 - Hardware y software.
 - Flujo de energía.
 - Cableados locales y externos.
- Aplicación de los sistemas de seguridad incluyendo datos y archivos.
- Planificación de los papeles de los auditores internos y externos.
- Planificación de programas de desastre y sus pruebas (simulación).
- Planificación de equipos de contingencia con carácter periódico.
- Control de desechos de los nodos importantes del sistema.
- Política de destrucción de basura copias, fotocopias.
- Consideración de las normas ISO 14000.

Etapas para Implementar un Sistema de Seguridad

Para dotar de medios necesarios para elaborar su sistema de seguridad se debe considerar los siguientes puntos:

- Sensibilizar a los ejecutivos de la organización en torno al tema de seguridad.
- Se debe realizar un diagnóstico de la situación de riesgo y seguridad de la información en la organización a nivel software, hardware, recursos humanos, y ambientales.
- Elaborar un plan para un programa de seguridad.

Consideraciones para con el Personal

Es de gran importancia la elaboración del plan considerando el personal, pues se debe llevar a una conciencia para obtener una autoevaluación de su comportamiento con respecto al sistema de seguridad, que lleve a la persona a:

- Asumir riesgos
- Cumplir promesas
- Innovar

Para apoyar estos objetivos se debe cumplir los siguientes pasos:

Motivar

Se debe desarrollar métodos de participación reflexionando sobre lo que significa la seguridad y el riesgo, así como su impacto a nivel empresarial, de cargo e individual.

Capacitación General

En un principio al personal con el fin de que conozcan y entiendan la relación entre seguridad, riesgo y la información, y su impacto en la institución. El objetivo de este punto es que se podrán detectar las debilidades y potencialidades de la organización frente al riesgo. Este proceso incluye como práctica necesaria la implantación la ejecución de planes de contingencia y la simulación de posibles delitos.

Capacitación de Técnicos

Se debe formar técnicos encargados de mantener la seguridad como parte de su trabajo y que esté capacitado para capacitar a otras personas en lo que es la ejecución de medidas preventivas y correctivas.

Ética y Cultura

Se debe establecer un método de educación estimulando el cultivo de elevados principios morales, que tengan repercusión a nivel personal e institucional. De ser posible realizar conferencias periódica sobre doctrina, familia, educación sexual, relaciones humanas, etc.

Beneficios de un Sistema de Seguridad

Los beneficios de un sistema de seguridad bien elaborado son inmediatos, ya que el la organización trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos:

- Aumento de la productividad.
- Aumento de la motivación del personal.
- Compromiso con la misión de la compañía.
- Mejora de las relaciones laborales.
- Ayuda a formar equipos competentes.
- Mejora de los climas laborales para los RR.HH.

2.5.8 COMUNICACIÓN DE LA SEGURIDAD

(Avogadro, 2012) “...Es una rama de la comunicación que se encarga de realizar el nexo de unión entre los ciudadanos, los organismos públicos y privados; empresas, entidades no gubernamentales; para generar lazos de unión y certezas, contribuir al bienestar de los individuos en el seno social y aportar alternativas de solución en temas de seguridad tanto pública como ciudadana y privada.”

En la actualidad vivimos en una sociedad interconectada a todo momento, donde las nuevas tecnologías de la información y la comunicación (NTIC), entre ellas el Internet, ofrecen varias posibilidades de transmisión y generación de información, traspasando barreras geográficas y culturales, recorriendo el mundo en tiempos antes impensados.

Conviviendo una sociedad real y una virtual, que se transforma en un nuevo escenario de ilícitos, producidos en el mundo virtual pero de absoluta incidencia en el mundo real, encontramos nuevos paradigmas sociales: de seguridad, de comunicación y de “modus operando” en el ámbito delictual.

En un proceso de comunicación interpersonal entran en juego dos factores: el racional y el emocional. En un mensaje 30% es percibido de “Lo que decimos” y el 70% de “Cómo lo decimos”, provocando diferentes estados emocionales en la persona que escucha que influyen en su nivel de escuchar.

Según estudios, dentro de las causas de accidentes en el trabajo o malas prácticas se han identificado algunos problemas de comunicación:

1. Entender mal o diferente una instrucción
2. Asumir que el otro está pensando lo mismo que nosotros.
3. Expresiones no verbales inadecuadas, es decir, no congruentes con lo que estoy comunicando de manera verbal.

Es importante saber que para que haya una escucha efectiva, debemos habituarnos a observar tanto nuestros estados emocionales cuando hablamos, como el estado emocional del receptor. Percibir lo verbal y lo no verbal, el lenguaje corporal, los gestos y las actitudes. También es posible escuchar las posturas del cuerpo y los movimientos en la medida que seamos capaces de atribuirles un sentido.

¿Cómo escuchamos? cuando una persona habla por lo general la escuchamos en alguno de los siguientes niveles:

- La ignoramos, nuestro cuerpo está presente pero nuestra mente no, damos señales como si estuviéramos escuchando, pero no estamos escuchando en absoluto.
- Competitiva, escuchamos a medias, mientras vamos ideando respuestas rápidas. Interrumpimos para dar nuestra opinión, no hay interés por escuchar sino por probar que somos competentes.
- Selectiva, oímos solo ciertas partes de la conversación, prestando atención al contenido dejando de lado los mensajes no verbales.
- Atenta, prestamos atención y centramos nuestra energía en las palabras que se pronuncian.
- Empática, escuchamos lo verbal y percibimos lo no verbal y las emociones.

De los niveles de escucha, solo ésta última se realiza desde el marco referencial de la otra persona, es decir, primero escuchamos y comprendemos.

Esta forma de escucha es un principio fundamental en el éxito de las relaciones interpersonales y supone un cambio de paradigmas ya que la mayor parte de las personas no escuchan para comprender, sino para contestar.

Escuchar es un arte que ha llegado a ser un asunto de vital importancia para asegurar una comunicación efectiva, el éxito personal y una buena convivencia tanto personal como organizacional.

En un mundo de acelerados cambios donde la seguridad cumple más que nunca un rol protagónico el líder de seguridad requiere desarrollar la habilidad de escuchar. Escuchar no es fácil, para hacerlo hay que abrir la mente, los ojos, los oídos y cerrar la boca.

2.6 HIPÓTESIS

La estructura del sistema de gestión de red de la Universidad Técnica de Ambato influye en los procesos de comunicación de la seguridad.

2.7 SEÑALAMIENTO DE VARIABLES

Variable Independiente: Estructura del sistema de gestión de red.

Variable Dependiente: Comunicación de la seguridad.

CAPÍTULO III

METODOLOGÍA

3.1 ENFOQUE

Predominante Cualitativo

La investigación fue cualitativa porque procedimos a realizar modalidad descriptiva, logrando evaluar los problemas existentes en el sistema de seguridad.

Predominante Cuantitativo

La investigación se hizo de forma cuantitativa porque se realizó exploración de campo, alcanzando cuantificar los tiempos de respuesta para mejorar los sistemas de gestión de red para la seguridad.

Paradigma

A de más se trabajó con el paradigma propositivo pues se propuso la mejor solución para la investigación que se realizó y el paradigma critico porque perpetrarnos críticas constructivas para la solución de esta investigación.

3.2 MODALIDAD BÁSICA DE LA INVESTIGACIÓN

Bibliografía – documental

La investigación fue en esta modalidad porque se acudió a fuentes de información secundaria en libros, revistas especializadas, publicaciones, módulos e internet. A

si mismo se utilizó fuentes primarias obtenidas a través de documentos válidos y confiables.

De Campo

Se trabajó con la modalidad de campo en cuanto a la observación, la inspección, la aplicación de entrevistas, cuestionarios, fotografías y todo tipo de evidencias necesarias, además se acudió al lugar en donde se producen los hechos interactuando y recabando toda la información necesaria.

De Intervención Social o Proyecto Factible

Además de las modalidades anteriores, el trabajo de grado asume la modalidad de proyectos factibles porque se planteó una propuesta de solución al problema investigado.

3.3 NIVEL O TIPO DE LA INVESTIGACIÓN

Exploratorio

Porque permite reconocer variables de interés investigativo, sondeando un interés desconocido en un contexto particular, y con la investigación necesaria para indagar sobre sistemas de seguridad y factores de contingencia de respuesta de auxilio inmediata.

Descriptivo

Porque permite comparar y clasificar fenómenos, elementos y estructuras que pudieran ser consideradas aisladamente y cuya descripción estará procesada de manera ordenada y sistemática.

Asociación de variables

Porque permite medir el grado de relación entre variables con los mismos sujetos de un contexto determinado.

3.4 POBLACIÓN Y MUESTRA

En la presente investigación se tomó en cuenta la siguiente población y muestra:

Para entrevista:

POBLACIÓN	MUESTRA
Director de la Dirección de Sistemas Informáticos y Redes de la Universidad Técnica de Ambato.	1
Jefe de Guardianía de la Universidad Técnica de Ambato.	1
TOTAL	2

Tabla 3. 1: Población y Muestra Entrevista
Elaborado por: El Investigador.

Para la encuesta:

POBLACIÓN	MUESTRA
Personal de la Dirección de Sistemas Informáticos y Redes de la Universidad Técnica de Ambato.	5
Personal de Guardianía de la Universidad Técnica de Ambato.	75
Administrador de redes de las facultades del predio Huachi	8
TOTAL	88

Tabla 3. 2: Población y Muestra Encuesta
Elaborado por: El Investigador.

- Por ser la población pequeña (menor a 100u), se trabajara con su totalidad.
- Para el análisis se toma en cuenta una población de 88 personas que son las encuestadas, las dos restantes son entrevistas personales.

3.5 OPERACIONALIZACIÓN DE LA VARIABLE INDEPENDIENTE: ESTRUCTURA DEL SISTEMA DE GESTIÓN DE RED

CONCEPTUALIZACIÓN	DIMENSIONES	INDICADORES	ÍTEMS BÁSICOS	TÉCNICAS E INSTRUMENTOS
Consiste en monitorizar y controlar los recursos de una red con el fin de evitar que esta llegue a funcionar incorrectamente degradando sus prestaciones.	Monitorizar	➤ Proceso ➤ Planificación ➤ Acciones ➤ Conductas	¿Cuenta la Universidad con un proceso de planificación para tomar las acciones y conductas necesarias para monitorear un evento?	Observación Inspección Check list Datos estadísticos
	Controlar	➤ Examinar ➤ Observar ➤ Fiscalizar ➤ Inspeccionar	¿Existen elementos para examinar, observar, fiscalizar e inspeccionar los procesos de seguridad?	
	Recursos	➤ Beneficio ➤ Competencia ➤ Sostenibilidad ➤ Administración	¿Posee recursos para una administración sostenible del sistema de seguridad competitiva para beneficio de la institución?	
	Red	➤ Medios ➤ Tecnologías ➤ Protocolos	¿Tiene una red adecuada con medios, tecnología y protocolo de vanguardia?	

Tabla 3. 3: Operacionalización de la V. I.
Elaborado por: El investigador

3.6 OPERACIONALIZACIÓN DE LA VARIABLE DEPENDIENTE: COMUNICACIÓN DE LA SEGURIDAD.

CONCEPTUALIZACIÓN	DIMENSIONES	INDICADORES	ÍTEMS BÁSICOS	TÉCNICAS E INSTRUMENTOS
Es una rama de la comunicación que se encarga de realizar el nexo de unión entre los ciudadanos, los organismos públicos y privados; empresas, entidades no gubernamentales, instituciones; para generar lazos de unión y certezas, contribuir al bienestar de los individuos en el seno social y aportar alternativas de solución en temas de seguridad tanto pública como ciudadana y privada.	Comunicación	➤ Emisor ➤ Mensaje ➤ Receptor ➤ Código ➤ Canal	¿Existe en la Universidad códigos de comunicación y canal de transmisión entre el emisor y receptor para enviar un mensaje de seguridad?	Entrevista Cuestionario Guía de entrevista Check list Datos estadísticos
	Institución	➤ Orden ➤ Normas ➤ Comportamiento	¿Tiene la institución normas o un orden establecido para el comportamiento de su población universitaria en caso de un contingente de seguridad?	
	Bienestar	➤ Calidad de vida ➤ Satisfacción ➤ Tranquilidad	¿Ofrece tranquilidad, calidad de vida y satisfacción al bienestar universitario el actual sistema de seguridad?	
	Seguridad	➤ Confianza ➤ Inmunidad ➤ Protección	¿Qué tan confiable e inmune es la protección del sistema de seguridad actual?	

Tabla 3. 4: Operacionalización de la V. D.
Elaborado por: El investigador

3.7 PLAN DE RECOLECCIÓN DE INFORMACIÓN

PREGUNTAS BASICAS	EXPLICACION
¿Para qué?	Para alcanzar los objetivos de la investigación
¿De qué personas u objetos?	Director del DISIR Personal del DISIR Jefe de guardianía Personal de guardianía de la Universidad
¿Sobre qué aspectos?	Indicadores
¿Quién, quienes?	El investigador
¿Cuándo?	Junio, Julio, Agosto y Septiembre 2013
¿Dónde?	Campus Huachi – UTA
¿Cuántas veces?	Lo necesario.
¿Qué técnicas de recolección?	Entrevista Cuestionario Observación
¿Con qué?	Guía de entrevista Cuestionario Inspecciones Check list
¿En qué situación?	Condiciones Circunstancias

Tabla 3. 5: Recolección de la información
Elaborado por: El investigador

3.8 PLAN DE PROCESAMIENTO DE LA INFORMACIÓN

Revisión crítica de la información recogida; procediendo a realizar la eliminación de información defectuosa, contradictoria, incompleta y no pertinente.

Tabulación según las variables de la hipótesis.

Revisión de cuadros tabulados con datos no influyentes indicados en el análisis.

Análisis de resultados, destacando relaciones fundamentales entre objetivos e hipótesis.

Interpretación de los resultados, con el apoyo del marco teórico y con un sustento aplicable de la propuesta dentro de lo posible para la Universidad.

Comprobación de la hipótesis y establecimiento de conclusiones y recomendaciones.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Análisis de los resultados estadísticos, destacando tendencias o relaciones fundamentales de acuerdo con los objetivos y preguntas directrices.

Interpretación de los resultados, con apoyo del marco teórico, en el aspecto pertinente.

Verificación de las preguntas directrices.

Establecimientos de conclusiones y recomendaciones.

Una vez realizado el proceso de observación de encuestas se procedió a realizar el análisis e interpretación de los resultados obtenidos. Este de datos se lo realizo de forma tabular y grafica obteniendo los siguientes resultados.

4.1 ENCUESTA DIRIGIDA AL PERSONAL DEL DISIR – UTA.

Para realizar la encuesta al personal del DISIR, se trabajó en su totalidad con el número de personas, es decir el 100%, puesto que la población es de 5 personas, por lo tanto se considera pequeña al ser menor a 100u.

1.- ¿Cuenta la Universidad con un proceso de planificación para tomar acciones y conductas para monitorear un evento de seguridad?

ALTERNATIVA	FRECUENCIA	PORCENTAJE
NO	0	0,00
SI	5	100,00
TOTAL	5	100,00

Tabla 4. 1: ¿Cuenta la Universidad con un proceso de planificación para tomar acciones y conductas para monitorear un evento de seguridad?
Elaborado por: El investigador



Gráfico 4. 1: ¿Cuenta la Universidad con un proceso de planificación para tomar acciones y conductas para monitorear un evento de seguridad?
Elaborado por: El investigador

ANÁLISIS E INTERPRETACIÓN

Los encuestados en su mayoría, 5 personas que corresponde al 100% manifiestan que si están de acuerdo con que cuenta la Universidad cuenta con un proceso de planificación para tomar acciones y conductas para monitorear un evento de seguridad.

De los resultados se establece que la Universidad cuenta con un proceso de planificación para tomar acciones y conductas para monitorear un evento de seguridad.

2.- ¿Existen elementos necesarios y suficientes para observar los procesos de seguridad en la Universidad?

ALTERNATIVA	FRECUENCIA	PORCENTAJE
NO	2	40,00
SI	3	60,00
TOTAL	5	100,00

Tabla 4. 2: ¿Existen elementos necesarios y suficientes para observar los procesos de seguridad en la Universidad?

Elaborado por: El investigador

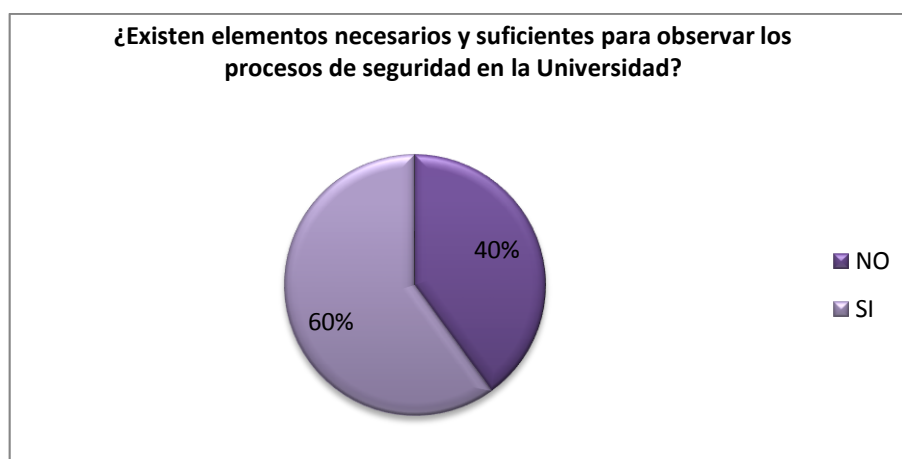


Gráfico 4. 2: ¿Existen elementos necesarios y suficientes para observar los procesos de seguridad en la Universidad?

Elaborado por: El investigador

ANÁLISIS E INTERPRETACIÓN

De los encuestados, 3 personas que corresponde el 60% manifiestan que si están de acuerdo con que existen elementos necesarios y suficientes para observar los procesos de seguridad en la Universidad; y 2 personas que corresponde al 40% dice que no.

De los resultados se establece que existen elementos necesarios y suficientes para observar los procesos de seguridad en la Universidad.

3.- ¿La institución posee recursos necesarios y suficientes para una administración sostenible del sistema de seguridad?

ALTERNATIVA	FRECUENCIA	PORCENTAJE
NO	2	40,00
SI	3	60,00
TOTAL	5	100,00

Tabla 4. 3: ¿La institución posee recursos necesarios y suficientes para una administración sostenible del sistema de seguridad?
Elaborado por: El investigador

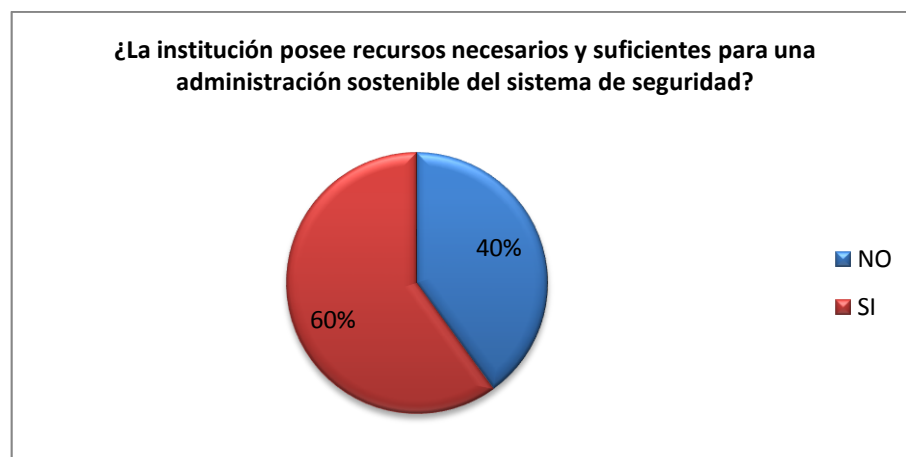


Gráfico 4. 3: ¿La institución posee recursos necesarios y suficientes para una administración sostenible del sistema de seguridad?
Elaborado por: El investigador

ANÁLISIS E INTERPRETACIÓN

Los encuestados en su mayoría, 3 personas que corresponde el 60% manifiestan que están de acuerdo con que la institución posee recursos necesarios y suficientes para una administración sostenible del sistema de seguridad; 2 encuestados a los que corresponde el 40% señala que desconoce.

De los resultados se establece que la institución posee recursos necesarios y suficientes para una administración sostenible del sistema de seguridad para poderlo aplicar.

4.- ¿El sistema de seguridad tiene una red adecuada y actualizada en los predios universitarios?

ALTERNATIVA	FRECUENCIA	PORCENTAJE
NO	3	60,00
SI	2	40,00
TOTAL	5	100,00

Tabla 4. 4 ¿El sistema de seguridad tiene una red adecuada y actualizada en los predios universitarios?
Elaborado por: El investigador

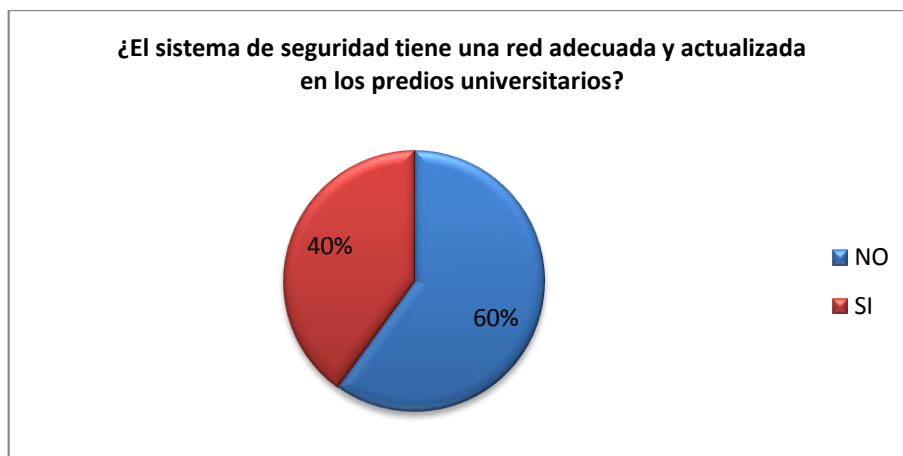


Gráfico 4. 4 ¿El sistema de seguridad tiene una red adecuada y actualizada en los predios universitarios?
Elaborado por: El investigador

ANÁLISIS E INTERPRETACIÓN

De los encuestados, 2 personas que corresponde el 40% manifiestan que si están de acuerdo con que el sistema de seguridad tiene una red adecuada y actualizada en los predios universitarios y 3 que corresponde al 60% dice que no.

De los resultados se establece que el sistema de seguridad no tiene una red adecuada y actualizada en los predios universitarios

5.- ¿Qué porcentaje de cobertura de seguridad tiene la infraestructura de la Universidad Técnica de Ambato?

ALTERNATIVA	FRECUENCIA	PORCENTAJE
MENOS DEL 20%	0	0,00
ENTRE EL 20% Y EL 40%	0	0,00
ENTRE EL 40% Y EL 60%	2	40,00
ENTRE EL 60% Y EL 80%	3	60,00
MÁS DEL 80%	0	0,00
TOTAL	5	100,00

Tabla 4. 5: ¿Qué porcentaje de cobertura de seguridad tiene la infraestructura de la Universidad Técnica de Ambato?
Elaborado por: El investigador

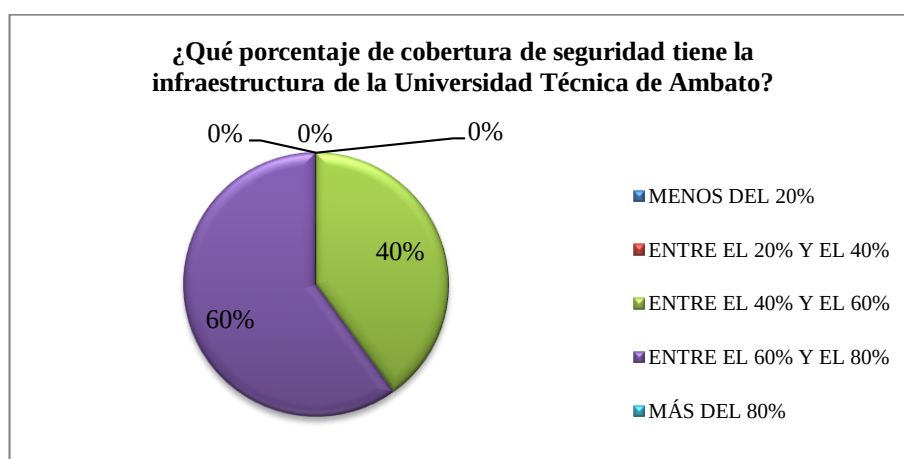


Gráfico 4. 5: ¿Qué porcentaje de cobertura de seguridad tiene la infraestructura de la Universidad Técnica de Ambato?
Elaborado por: El investigador

ANÁLISIS E INTERPRETACIÓN

Los encuestados en su mayoría, 3 personas que corresponde el 60% manifiestan que el porcentaje de cobertura de seguridad que tiene la infraestructura de la Universidad Técnica de Ambato está entre el 60% y 80% de su totalidad; 2 encuestados a los que corresponde el 40% señala que esta entre el 40% y 60%.

De los resultados se establece que debe aumentar la cobertura de seguridad que tiene la infraestructura de la Universidad Técnica de Ambato.

4.2. ENCUESTA DIRIGIDA A LOS ADMINISTRADORES DE RED DE LA UNIVERSIDAD TÉCNICA DE AMBATO.

Para realizar la encuesta a los señores administradores de red, se trabajó en su totalidad con el número de personas, es decir el 100%, puesto que la población es de 8 personas, por lo tanto se considera pequeña al ser menor a 100u.

1.- ¿Cuenta la Facultad con un proceso de planificación para tomar acciones y conductas para monitorear un evento de seguridad?

ALTERNATIVA	FRECUENCIA	PORCENTAJE
NO	0	0,00
SI	8	100,00
TOTAL	8	100,00

Tabla 4. 6: ¿Cuenta la Facultad con un proceso de planificación para tomar acciones y conductas para monitorear un evento de seguridad? Porcentaje total.

Elaborado por: El investigador

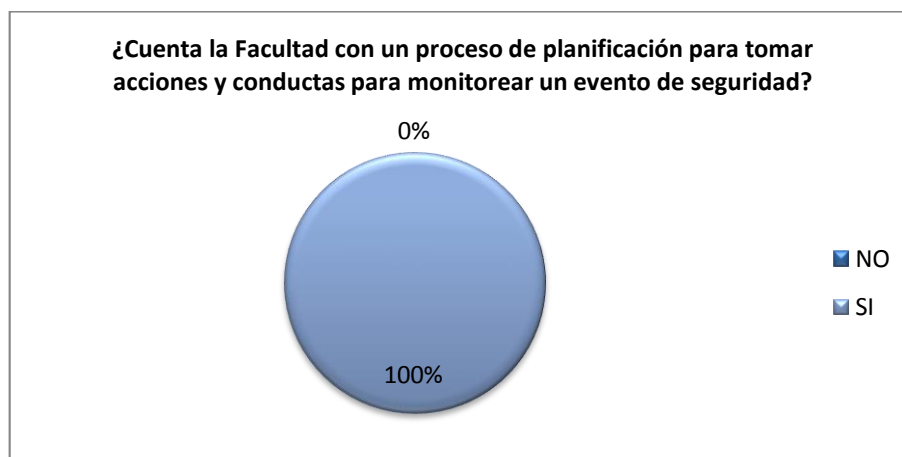


Gráfico 4. 6: ¿Cuenta la Facultad con un proceso de planificación para tomar acciones y conductas para monitorear un evento de seguridad?

Elaborado por: El investigador

FACULTAD	SI	NO
FISEI	X	
FDA A	X	
FCADM	X	
FCHE	X	
FCIA	X	
FCAUD	X	
FICM	X	
DIBESAU	X	

Tabla 4. 7: ¿Cuenta la Facultad con un proceso de planificación para tomar acciones y conductas para monitorear un evento de seguridad? Referencia individual.

Elaborado por: El investigador

ANÁLISIS E INTERPRETACIÓN

Los encuestados, que en su totalidad son 8 personas, correspondiente al 100% manifiestan que si están de acuerdo con que las Facultades cuentan con un proceso de planificación para tomar acciones y conductas para monitorear un evento de seguridad.

De los resultados se establece que en algunas facultades falta mejorar el proceso de planificación para tomar acciones y conductas para monitorear un evento de seguridad.

2.- ¿Existen elementos necesarios y suficientes para observar los procesos de seguridad en la Facultad?

ALTERNATIVA	FRECUENCIA	PORCENTAJE
NO	0	0,00
SI	8	100,00
TOTAL	8	100,00

Tabla 4. 8: ¿Existen elementos necesarios y suficientes para observar los procesos de seguridad en la Facultad? Porcentaje Total
Elaborado por: El investigador



Gráfico 4. 7: ¿Existen elementos necesarios y suficientes para observar los procesos de seguridad en la Facultad?
Elaborado por: El investigador

FACULTAD	SI	NO
FISEI	X	
FDAA	X	
FCADM	X	
FCHE	X	
FCIA	X	
FCAUD	X	
FICM	X	
DIBESAU	X	

Tabla 4. 9: ¿Existen elementos necesarios y suficientes para observar los procesos de seguridad en la Facultad? Referencia individual
Elaborado por: El investigador

ANÁLISIS E INTERPRETACIÓN

Los encuestados en su mayoría, 8 personas que corresponde el 100% manifiestan que si están de acuerdo con que existen elementos necesarios y suficientes para observar los procesos de seguridad en la Facultad.

De los resultados se establece que en las diferentes facultades existen elementos necesarios y suficientes para observar los procesos de seguridad en la Facultad más críticos, sin embargo se deben aumentar para poder tener un mejor control y abarcar todas las instalaciones.

3.- ¿La unidad académica posee recursos necesarios y suficientes para una administración sostenible del sistema de seguridad?

ALTERNATIVA	FRECUENCIA	PORCENTAJE
NO	2	25,00
SI	6	75,00
TOTAL	8	100,00

Tabla 4. 10: ¿La unidad académica posee recursos necesarios y suficientes para una administración sostenible del sistema de seguridad? Porcentaje total.
Elaborado por: El investigador

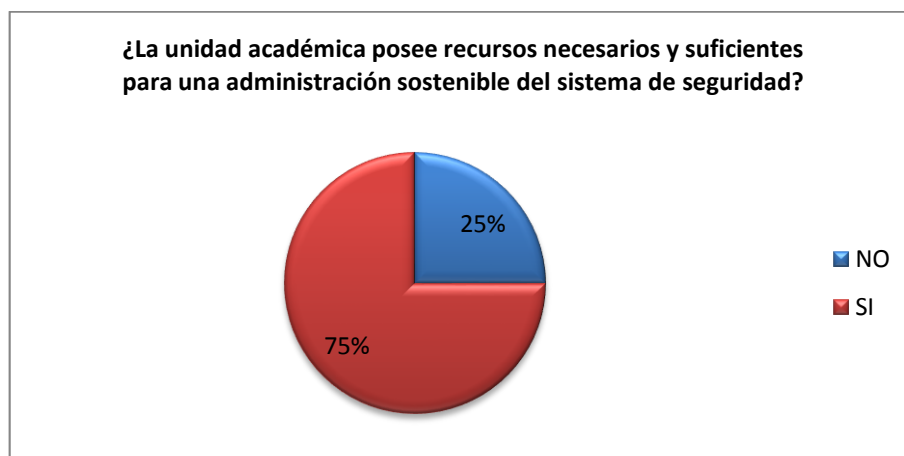


Gráfico 4. 8: ¿La unidad académica posee recursos necesarios y suficientes para una administración sostenible del sistema de seguridad?
Elaborado por: El investigador

FACULTAD	SI	NO
FISEI	X	
FDAA		X
FCADM	X	
FCHE	X	
FCIA	X	
FCAUD	X	
FICM	X	
DIBESAU		X

Tabla 4. 11: ¿La unidad académica posee recursos necesarios y suficientes para una administración sostenible del sistema de seguridad? Referencia individual.
Elaborado por: El investigador

ANÁLISIS E INTERPRETACIÓN

Los encuestados en su mayoría, 6 personas que corresponde el 75% manifiestan que si están de acuerdo con que la unidad académica posee recursos necesarios y suficientes para una administración sostenible del sistema de seguridad; y 2 encuestados que corresponde el 25% señala que no.

De los resultados se establece que la unidad académica de Diseño Arquitectura y Artes y el DIBESAU, no poseen en la actualidad recursos necesarios y suficientes para una administración sostenible del sistema de seguridad, puesto que se encuentran equipando los laboratorios, mientras que el resto de facultades poseen

los recursos y por tal motivo se está realizando su implementación de forma paulatina.

4.- ¿El sistema de seguridad tiene una red adecuada y actualizada en los dominios de la facultad?

ALTERNATIVA	FRECUENCIA	PORCENTAJE
NO	1	12,50
SI	7	87,50
TOTAL	8	100,00

Tabla 4. 12: ¿El sistema de seguridad tiene una red adecuada y actualizada en los dominios de la facultad? Porcentaje total.
Elaborado por: El investigador



Gráfico 4. 9: ¿El sistema de seguridad tiene una red adecuada y actualizada en los dominios de la Facultad?
Elaborado por: El investigador

FACULTAD	SI	NO
FISEI	X	
FDA A	X	
FCADM	X	
FCHE	X	
FCIA	X	
FCAUD	X	
FICM	X	
DIBESAU		X

Tabla 4. 13: ¿El sistema de seguridad tiene una red adecuada y actualizada en los dominios de la facultad? Referencia individual.
Elaborado por: El investigador

ANÁLISIS E INTERPRETACIÓN

Los encuestados en su mayoría, 7 personas que corresponde el 87,50% manifiestan que están de acuerdo con que el sistema de seguridad tiene una red adecuada y actualizada en los dominios de la facultad; 1 encuestado al que corresponde el 12.5% señala que no.

De los resultados se establece que en los edificios de las diferentes facultades el sistema de seguridad tiene medianamente una red adecuada, puesto que desde que fueron instalados no se ha incrementado dejándolo solo en los puntos más críticos y su actualización en algunos dominios de la facultad se lo ha ido haciendo según las necesidades.

5.- ¿Qué porcentaje de cobertura de seguridad tiene la infraestructura de la Facultad?

ALTERNATIVA	FRECUENCIA	PORCENTAJE
MENOS DEL 20%	0	0,00
ENTRE EL 20% Y EL 40%	0	0,00
ENTRE EL 40% Y EL 60%	2	25,00
ENTRE EL 60% Y EL 80%	4	50,00
MÁS DEL 80%	2	25,00
TOTAL	8	100,00

Tabla 4. 14: ¿Qué porcentaje de cobertura de seguridad tiene la infraestructura de la Facultad?
Porcentaje total.

Elaborado por: El investigador

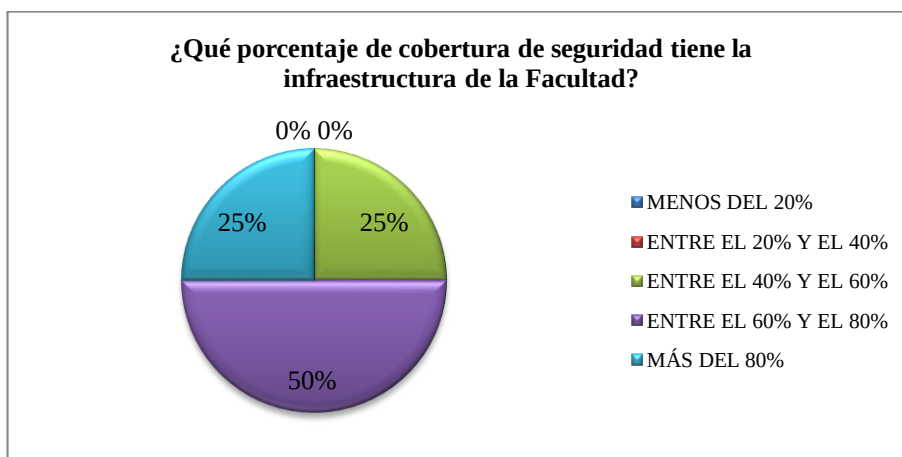


Gráfico 4. 10: ¿Qué porcentaje de cobertura de seguridad tiene la infraestructura de la Facultad?
Elaborado por: El investigador

FACULTAD	<20%	20-40%	40-60%	60-80%	>80%
FISEI				X	
FDAA			X		
FCADM					X
FCHE				X	
FCIA				X	
FCAUD					X
FICM				X	
DIBESAU			X		

Tabla 4. 15: ¿Qué porcentaje de cobertura de seguridad tiene la infraestructura de la Facultad?
Referencia individual.
Elaborado por: El investigador

ANÁLISIS E INTERPRETACIÓN

Los encuestados en su mayoría, 4 personas que corresponde el 50% manifiestan que el porcentaje de cobertura de seguridad que tiene la infraestructura de la Facultad está entre el 60% y 80%; 2 encuestados que corresponden el 25% señalan que está entre el 40% y 60% y 2 personas que es el 25% manifiesta que pasa el 80%.

De los resultados se establece que falta cubrir los espacios físicos de las diferentes facultades con el sistema de seguridad puesto que la facultad de Diseño Arquitectura y Artes y el edificio DIBESAU apenas tiene una cobertura de entre el 40 y 60%, las facultades de Ingeniería en Sistemas Electrónica e Industrial, Civil y Mecánica, Ingeniería en Alimentos y de Ciencias Humanas y de la Educación tiene una cobertura de entre el 60 y 80%, y las facultades de Ciencias Administrativas y de Contabilidad y Auditoría tiene una cobertura de más del 80% pero no llega a cubrir un cien por ciento.

4.3. ENCUESTA DIRIGIDA AL PERSONAL DE SEGURIDAD DE LA UNIVERSIDAD TÉCNICA DE AMBATO

Para realizar la encuesta al personal de seguridad, se trabajó en su totalidad con el número de personas, es decir el 100%, puesto que la población es de 75 personas, por lo tanto se considera pequeña al ser menor a 100u.

1.- ¿Considera Usted que el sistema de comunicación interno es?

ALTERNATIVA	FRECUENCIA	PORCENTAJE
MALO	0	0,00
REGULAR	0	0,00
BUENO	11	14,67
MUY BUENO	49	65,33
EXCELENTE	15	20,00
TOTAL	75	100,00

Tabla 4. 16: ¿Considera Usted que el sistema de comunicación interno es?
Elaborado por: El investigador

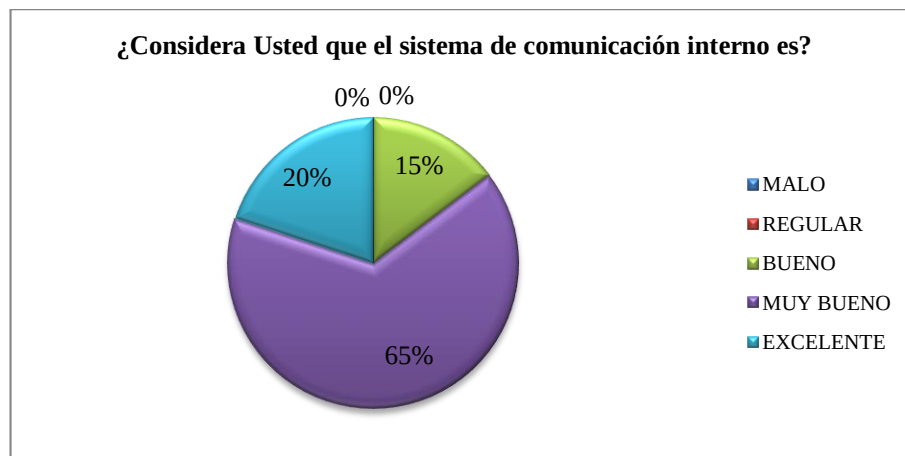


Gráfico 4. 11: ¿Considera Usted que el sistema de comunicación interno es?
Elaborado por: El investigador

ANÁLISIS E INTERPRETACIÓN

Los encuestados en su mayoría, 49 personas que corresponde el 65.33% manifiestan que el sistema de comunicación interno es muy bueno; 15 encuestados que corresponde el 20% señala que es malo y 11 personas que representa el 14.67% que es bueno.

De los resultados se establece que el sistema de comunicación interno es deficiente todavía.

2.- ¿En el caso de una emergencia, a su conocimiento el reporte le llega?

ALTERNATIVA	FRECUENCIA	PORCENTAJE
DE INMEDIATO	2	2,67
DENTRO DE LOS 5 MINUTOS	69	92,00
DENTRO DE LOS 15 MINUTOS	4	5,33
DENTRO DE LOS 60 MINUTOS	0	0,00
PASADO LOS 60 MINUTOS	0	0,00
TOTAL	75	100,00

Tabla 4. 17: ¿En el caso de una emergencia, a su conocimiento el reporte le llega?
Elaborado por: El investigador

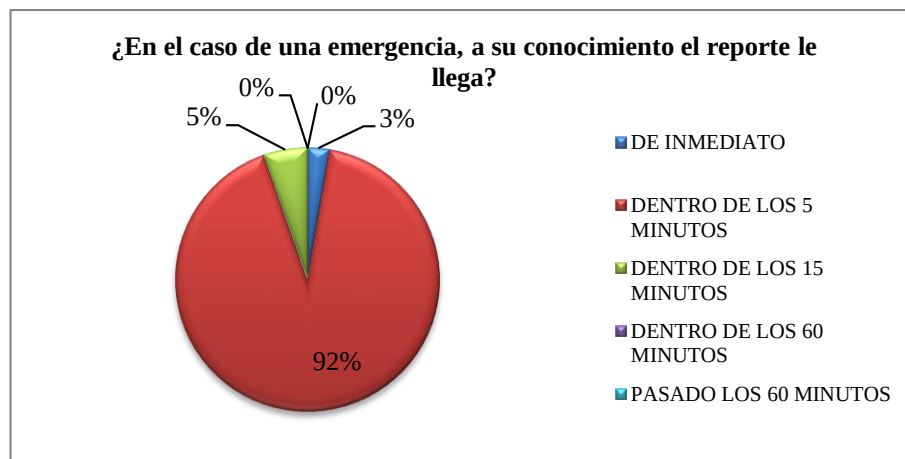


Gráfico 4. 12: ¿En el caso de una emergencia, a su conocimiento el reporte le llega?
Elaborado por: El investigador

ANÁLISIS E INTERPRETACIÓN

Los encuestados en su mayoría, 69 personas que corresponde el 92% manifiestan que en el caso de una emergencia, a su conocimiento el reporte le llega dentro de los cinco minutos; 4 encuestados que corresponde el 5.33% señala que dentro de los 15 minutos y 2 personas que representa el 2.67% que le llega el reporte de inmediato.

De los resultados se establece que en el caso de una emergencia, a su conocimiento el reporte no les llega en un tiempo óptimo.

3.- ¿Cuándo suena la alarma en una dependencia o edificio, el tiempo que se demora en encontrar donde está focalizado el problema es?

ALTERNATIVA	FRECUENCIA	PORCENTAJE
DE INMEDIATO	6	8,00
DENTRO DE LOS 5 MINUTOS	21	28,00
DENTRO DE LOS 15 MINUTOS	48	64,00
DENTRO DE LOS 60 MINUTOS	0	0,00
PASADO LOS 60 MINUTOS	0	0,00
TOTAL	75	100,00

Tabla 4. 18: ¿Cuándo suena la alarma en una dependencia o edificio, el tiempo que se demora en encontrar donde está focalizado el problema es?
Elaborado por: El investigador

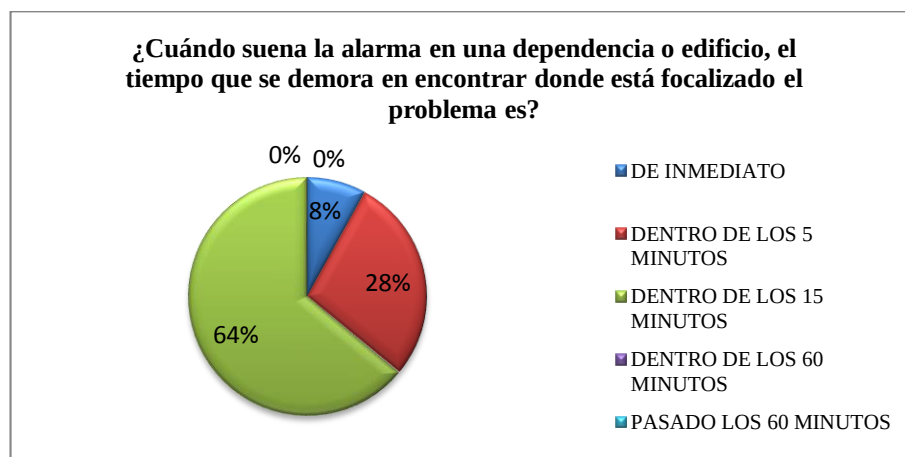


Gráfico 4. 13: ¿Cuándo suena la alarma en una dependencia o edificio, el tiempo que se demora en encontrar donde está focalizado el problema es?
Elaborado por: El investigador

ANÁLISIS E INTERPRETACIÓN

Los encuestados en su mayoría, 48 personas que corresponde el 64% manifiestan que cuándo suena la alarma en una dependencia o edificio, el tiempo que se demora en encontrar donde está focalizado el problema es dentro de los 15 minutos; 21 encuestados que corresponde el 28% señala que dentro de los 5 minutos y 6 personas que representa el 8% inmediato.

De los resultados se establece que cuando suena la alarma en una dependencia o edificio, el tiempo que se demora en encontrar donde está focalizado el problema es tardío y no eficaz.

4.- ¿Tienen algún sistema de requisas para los vehículos que ingresan o salen de la institución?

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI	0	0,00
NO	75	100,00
TOTAL	75	100,00

Tabla 4. 19: ¿Tienen algún sistema de requisas para los vehículos que ingresan o salen de la institución?

Elaborado por: El investigador



Gráfico 4. 14: ¿Tienen algún sistema de requisas para los vehículos que ingresan o salen de la institución?

Elaborado por: El investigador

ANÁLISIS E INTERPRETACIÓN

Los encuestados en su totalidad, 75 personas que corresponde el 100% manifiestan que no tienen algún sistema de requisas para los vehículos que ingresan o salen de la institución.

De los resultados se establece que no existe ningún sistema de requisas para los vehículos que ingresan o salen de la institución.

5.- ¿Tienen alguna identificación, los vehículos de los docentes, alumnos o visitantes de la institución?

ALTERNATIVA	FRECUENCIA	PORCENTAJE
NO	69	92,00
SI	6	8,00
TOTAL	75	100,00

Tabla 4. 20: ¿Tienen alguna identificación, los vehículos de los docentes, alumnos o visitantes de la institución?

Elaborado por: El investigador



Gráfico 4. 15: ¿Tienen alguna identificación, los vehículos de los docentes, alumnos o visitantes de la institución?

Elaborado por: El investigador

ANÁLISIS E INTERPRETACIÓN

Los encuestados en su mayoría, 69 personas que corresponde el 92% manifiestan que no tienen alguna identificación los vehículos de los docentes, alumnos o visitantes de la institución; 6 encuestados que corresponde el 8% señala que sí.

De los resultados se establece que es mínima la identificación de los vehículos de los docentes, alumnos o visitantes de la institución.

6.- ¿En su turno, que tiempo se demora en volver a pasar por el mismo punto?

ALTERNATIVA	FRECUENCIA	PORCENTAJE
MENOS DE 5 MINUTOS	22	29,33
ENTRE 5 Y 15 MINUTOS	12	16,00
ENTRE 15 Y 30 MINUTOS	41	54,67
ENTRE 30 Y 60 MINUTOS	0	0,00
MAS DE 60 MINUTOS	0	0,00
TOTAL	75	100,00

Tabla 4. 21: ¿En su turno, que tiempo se demora en volver a pasar por el mismo punto?
Elaborado por: El investigador

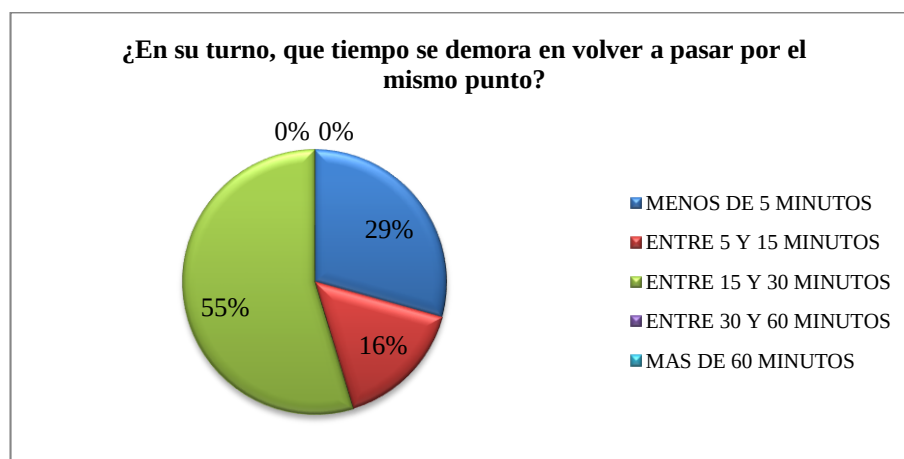


Gráfico 4. 16: ¿En su turno, que tiempo se demora en volver a pasar por el mismo punto?
Elaborado por: El investigador

ANÁLISIS E INTERPRETACIÓN

Los encuestados en su mayoría, 41 personas que corresponde el 54.67% manifiestan que en su turno, el tiempo que se demora en volver a pasar por el mismo punto está entre 15 y 30 minutos; 22 encuestados que corresponde el 29.33% señala que se encuentra en un punto fijo, y 12 personas que representa el 16% se demora entre 5 minutos y quince minutos.

De los resultados se establece que en su turno, el tiempo que se demora en volver a pasar por el mismo punto depende de la asignación que le den al señor guardia.

7.- ¿Cree Usted, que el actual sistema de seguridad es satisfactorio?

ALTERNATIVA	FRECUENCIA	PORCENTAJE
NO	29	38,67
SI	46	61,33
TOTAL	75	100,00

Tabla 4. 22: ¿Cree Usted, que el actual sistema de seguridad es satisfactorio?
Elaborado por: El investigador

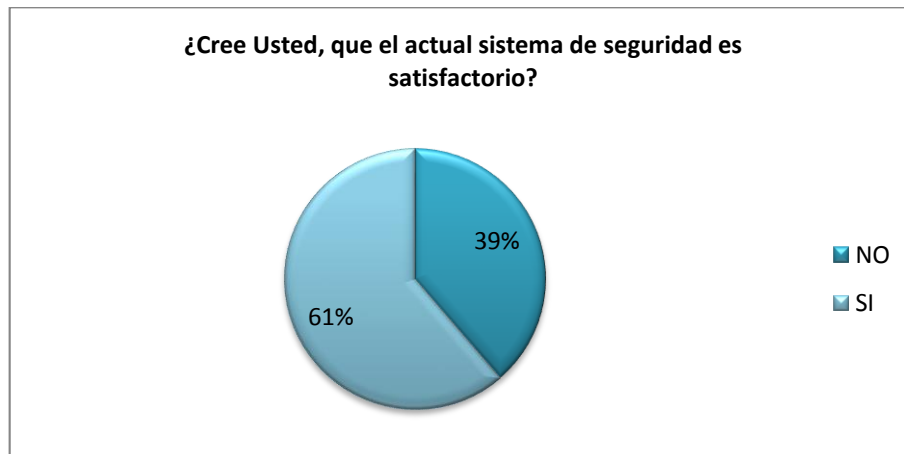


Gráfico 4. 17: ¿Cree Usted, que el actual sistema de seguridad es satisfactorio?
Elaborado por: El investigador

ANÁLISIS E INTERPRETACIÓN

Los encuestados en su mayoría, 46 personas que corresponde el 61.33% manifiestan que si están de acuerdo con que el actual sistema de seguridad es satisfactorio y 29 personas que representa el 38.67% manifiesta que no.

De los resultados se establece que el actual sistema de seguridad es medianamente satisfactorio.

8.- ¿Qué tan confiable es el sistema de seguridad actual?

ALTERNATIVA	FRECUENCIA	PORCENTAJE
MALO	0	0,00
REGULAR	0	0,00
BUENO	21	28,00
MUY BUENO	45	60,00
EXCELENTE	9	12,00
TOTAL	75	100,00

Tabla 4. 23: ¿Qué tan confiable es el sistema de seguridad actual?
Elaborado por: El investigador

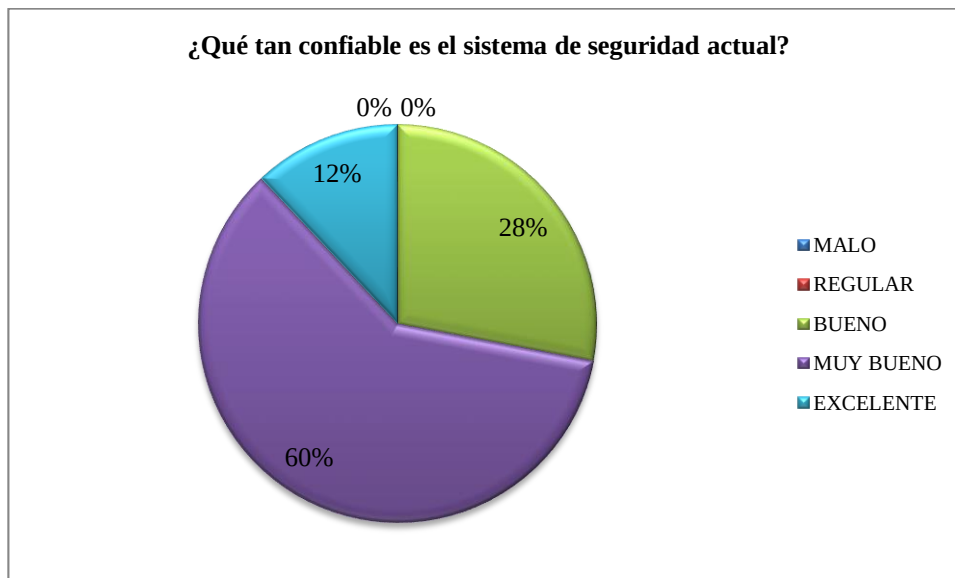


Gráfico 4. 18: ¿Qué tan confiable es el sistema de seguridad actual?
Elaborado por: El investigador

ANÁLISIS E INTERPRETACIÓN

Los encuestados en su mayoría, 45 personas que corresponde el 60% manifiestan que es muy bueno la confiabilidad del sistema de seguridad actual, 21 encuestados que es el 28% indica que es bueno, y 9 personas que representa el 12% manifiesta que es excelente.

De los resultados se establece que no es tan confiable el sistema de seguridad actual.

9.- ¿En caso de detectar alguna anomalía dentro de los predios universitarios, (Persona sospechosa, vidrio bajado de un auto, puerta abierta de un vehículo, persona con proyector o laptops en sus brazos, personas con bultos grandes, etc.) que procedimiento realiza? (Varias opciones)

En caso de personas:

ALTERNATIVA	FRECUENCIA	PORCENTAJE
LO INTERROGA	17	22,67
LO DETIENE	2	2,67
NOTIFICA A SU SUPERIOR	12	16,00
NINGUNO	31	41,33
OTRO	13	17,33
TOTAL	75	100,00

Tabla 4. 24: ¿En caso de detectar alguna anomalía dentro de los predios universitarios, que procedimiento realiza?

Elaborado por: El investigador

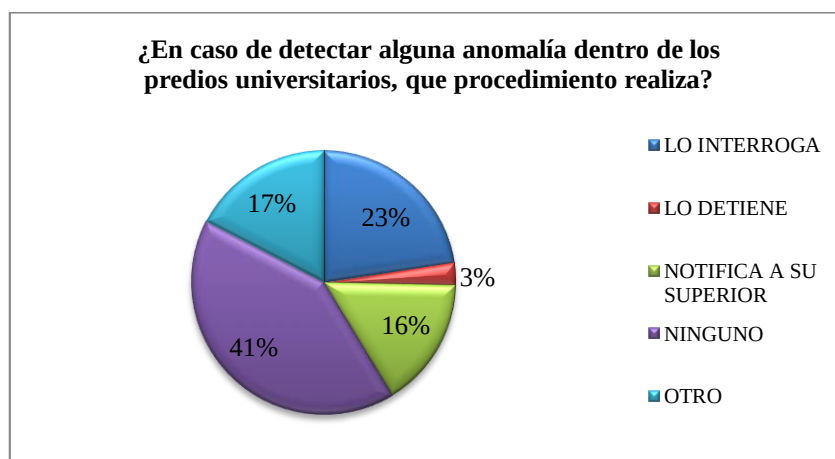


Gráfico 4. 19: ¿En caso de detectar alguna anomalía dentro de los predios universitarios, que procedimiento realiza?

Elaborado por: El investigador

ANÁLISIS E INTERPRETACIÓN

Los encuestados en su mayoría, 31 personas que corresponde el 41.3% manifiestan que, en caso de detectar alguna anomalía dentro de los predios universitarios, no realizan ningún procedimiento, 17 encuestados que es el 22.67% indica que lo interroga, 13 encuestados que es el 17.33% realiza otras actividades, 12 personas que es el 16% indica que notifica a su superior y 2 personas que representa el 2.67% manifiesta que lo detiene.

De los resultados se establece que en caso de detectar alguna anomalía dentro de los predios universitarios, no se tiene definido que procedimiento realizar en el caso de personas.

En caso de objetos:

ALTERNATIVA	FRECUENCIA	PORCENTAJE
NOTIFICA AL DUEÑO	33	44,00
BUSCA SOLUCIÓN	16	21,33
NOTIFICA A SU SUPERIOR	16	21,33
NINGUNO	0	0,00
OTRO	10	13,33
TOTAL	75	100,00

Tabla 4. 25: ¿En caso de detectar alguna anomalía dentro de los predios universitarios, que procedimiento realiza?

Elaborado por: El investigador

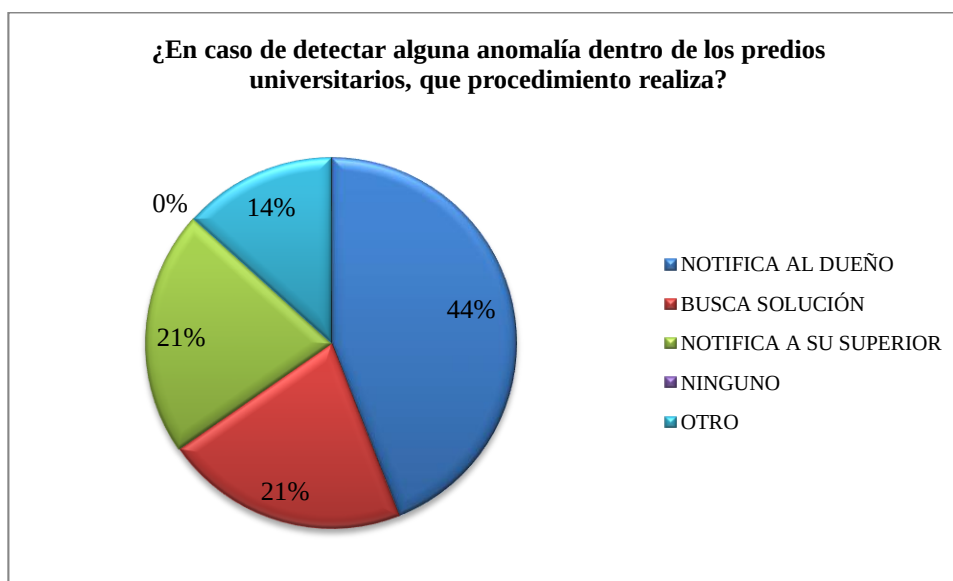


Gráfico 4. 20: ¿En caso de detectar alguna anomalía dentro de los predios universitarios, que procedimiento realiza?

Elaborado por: El investigador

ANÁLISIS E INTERPRETACIÓN

Los encuestados en su mayoría, 33 personas que corresponde el 44% manifiestan que, en caso de detectar alguna anomalía dentro de los predios universitarios, notifican al dueño, 16 encuestados que es el 21.33% indica que busca una solución, 16 encuestados que es el 21.33% notifica a su superior, y 10 personas que representa el 13.33% manifiesta que realiza otra actividad.

De los resultados se establece que en caso de detectar alguna anomalía dentro de los predios universitarios, no se tiene definido que procedimiento realizar en el caso de objetos.

4.4 SITUACIÓN ACTUAL DE LOS PROCESOS DE COMUNICACIÓN DE LA UNIVERSIDAD TÉCNICA DE AMBATO.

Actualmente el Campus Huachi de la Universidad Técnica de Ambato, tiene implementado moderadamente un sistema de seguridad, teniendo en cuenta equipos electrónicos y personal humano.

Por motivos de seguridad y confidencialidad no se va a realizar un análisis detallado del sistema de seguridad existente, pero se van a enunciar los elementos más relevantes del mismo.

A nivel general, el campus Huachi tiene instalado cámaras IP, colocadas estratégicamente en los puntos más altos de los edificios de la Facultad de Ingeniería Civil y Mecánica, en la Facultad de Contabilidad y Auditoría y en la Facultad de Administración, los cuales permiten tener una visión de los parqueaderos principales del campus, tomándolos como puntos estratégicos de vigilancia, aunque analizando de una manera global constituye solamente una parte del total de los parqueaderos existentes en todo el campus, pues debido al aumento del parque automotor y de la infraestructura física del mismo, no abastecen en su totalidad el enfoque completo del predio, por lo que se tiene en consideración aumentar el número de cámaras IP para video vigilancia; la central de monitoreo se encuentra ubicada en el edificio posterior de la Facultad de Ingeniería en Sistemas Electrónica e Industrial, desde donde se lleva un control visual de lo que sucede en el campus y de igual forma es el centro base de radio comunicación de los señores guardias de seguridad de la Universidad Técnica de Ambato. Adicionalmente se tiene el contingente de los señores guardias de seguridad, quienes en una cantidad total de 75 personas prestan su servicio a la Universidad Técnica de Ambato, se realizan por día 4 turnos de 13 señores guardias cada uno de manera rotativa y 12

guardias permanecen en puestos fijos, con este proceso se puede cubrir la extensión del Campus, controlando y dando apoyo a las diferentes facultades y parqueaderos, los señores guardias se comunican por medio de radios inalámbricos entre ellos. Debido a que es un trabajo que se realiza de manera externa y físicamente requiere mayor esfuerzo, se completa el pelotón de seguridad con 11 guardias más para poder cubrir de mejor manera los turnos en caso de días libres y vacaciones.

A nivel de facultades existen diferentes tipos de nivel de seguridad, tienen cámaras IP, sensores de movimiento, detectores de humo y de ingreso de personas, no todas las facultades tienen sus servicios completos, algunas facultades tienen las cámaras IP en los pasillos principales de los edificios y otras en los laboratorios y aulas, de igual forma no todos los equipos de computación y periféricos pertenecientes a las facultades tienen el dispositivo de seguridad o candado electrónico para poder detectar si algún artefacto está siendo sacado de los predios, también los sensores de movimiento están colocados en lugares estratégicos pero no cubre en su totalidad el espacio físico, por lo tanto ninguna facultad tiene una cobertura de un 100% de su infraestructura, los sistemas de seguridad son controlados y monitoreados desde la oficina de los señores administradores de red de cada facultad, pero debido a las diversas funciones que cumplen, no pueden prestar su atención fija en su totalidad a los paneles de control, ni tampoco existe una persona que se encargue de dicho control.

A nivel de comunicación entre las diferentes facultades y la central de monitoreo no existe ningún protocolo o elemento que permita su comunicación, por lo que cada administrador de red se encarga de solucionar los diferentes inconvenientes que pudieran presentarse en cada facultad, sin embargo, en la actualidad en el predio de Huachi, existe conectividad por medio de fibra óptica entre facultades, siendo la Facultad de Contabilidad y Auditoría el centro base, y de donde se despliega una red tipo estrella, con un ancho de banda de 1Gbps hacia cada facultad.

4.5 VERIFICACIÓN DE HIPÓTESIS

Para poder verificar la hipótesis, se tiene diferentes modelos para poder ser aplicado, para el presente trabajo investigativo, debido a que se tiene diferentes tipos de encuestas para poder cubrir su población, quienes tienen diferentes tipos de trabajo para cubrir el sistemas de seguridad, se analizara por medio de estadística descriptiva, basándome en las encuestas, en las gráficas de las mismas y en el análisis e interpretación de resultados, en donde nos permite obtener información suficiente para poder aceptar o rechazar la hipótesis.

4.5.1. PLANTEAMIENTO DE LA HIPÓTESIS

La estructura del sistema de gestión de red de la Universidad Técnica de Ambato influye en los procesos de comunicación de la seguridad.

4.5.2. DESCRIPCIÓN DE LA POBLACIÓN

Se trabajará con toda la muestra que es 88 personas, entre personal de guardianía, personal del DISIR y jefes del departamento de redes de la Universidad Técnica de Ambato”, a quienes se les aplicó la encuesta sobre la comunicación de la seguridad, en la infraestructura física de la Universidad Técnica de Ambato.

4.5.3. DECISIÓN FINAL

Una vez analizado las diferentes respuestas de las encuestas y el análisis e interpretación de resultados, se puede observar que debido a que no existe una comunicación rápida y oportuna entre los estamentos de seguridad, y que su comunicación es analógica y no digital, la comunicación del sistema de seguridad es tardía y no se puede abarcar en su totalidad el respectivo monitoreo, por lo que se acepta la hipótesis que dice: La estructura del sistema de gestión de red de la Universidad Técnica de Ambato influye en los procesos de comunicación de la seguridad.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

Del presente trabajo investigativo se puede concluir que el estado de la estructura del sistema de gestión de red para la optimización de la comunicación de la seguridad en la infraestructura física, de la Universidad Técnica de Ambato existente es aceptable si hablamos de una manera individual por facultad, ya que cada entidad posee sus propios elementos de seguridad.

Los procesos de comunicación de la seguridad en la infraestructura física de la Universidad Técnica de Ambato son de una forma analógica y manual, y la institución no cuenta con el suficiente contingente humano ni de monitoreo para poder cubrir en su totalidad los predios universitarios, pues eso genera recursos económicos elevados mensuales que la institución no posee, ya que al momento tiene otras prioridades como es la edificación de la infraestructura civil para las diferentes facultades.

La comunicación de la seguridad en la infraestructura física de la Universidad Técnica de Ambato es de forma manual y vía radio entre los señores guardias y la central de monitoreo, por lo que el nivel de vigilancia en su respuesta de tiempo no es muy eficaz ni efectivo, así como los recursos humanos y financieros son poco desperdiciados, así mismo al no poseer un sistema de respaldo de energía se dificulta el control.

5.2. RECOMENDACIONES

Del presente trabajo investigativo se recomienda, interconectar de forma global los sistemas de seguridad independientes de cada facultad, a su vez realizar mejoras, actualizaciones y aprovechar la infraestructura y tecnología existente, para poder brindar un sistema de seguridad de alta calidad y tranquilidad para la comunidad universitaria y sus visitantes.

Los procesos de comunicación de la seguridad en la infraestructura física de la Universidad Técnica de Ambato se debe digitalizar usando la infraestructura y tecnología existente en el campus, para poder optimizar los recursos y personal humano mejorando la calidad de comunicación.

La comunicación de la seguridad en la infraestructura física de la Universidad Técnica de Ambato se lo deba automatizar para poder complementar con la existente y así poder mejorar el nivel de vigilancia y que pueda ser eficaz y efectivo en su tiempo de respuesta, incluyendo un sistema de respaldo de energía como UPS o baterías alternas para que los sistemas de seguridad no dejen de funcionar.

CAPÍTULO VI

PROPUESTA

SISTEMA DE GESTIÓN DE RED ALTERNATIVO DE OPTIMIZACIÓN DE LA COMUNICACIÓN PARA LA SEGURIDAD, EN LA INFRAESTRUCTURA FÍSICA DE LA UNIVERSIDAD TÉCNICA DE AMBATO.

6.1. DATOS INFORMATIVOS

Nombre del Plantel:	Universidad Técnica de Ambato
Provincia:	Tungurahua
Cantón:	Ambato
Parroquia:	Huachi Chico
Dirección:	Av. Los Chasquis y Río Guayllabamba
Teléfono:	032521081
Jornada:	Matutina, Vespertina y Nocturna
Equipo técnico:	Investigador, Tutor, Docentes y Empleados
Beneficiarios:	Comunidad Universitaria
Responsable:	Ing. Santiago Mauricio Altamirano Meléndez

6.2. ANTECEDENTES DE LA PROPUESTA

La Universidad Técnica de Ambato, durante muchos años ha sufrido el embate de los “amigos de lo ajeno” en sus diferentes formas, tanto en las diferentes facultades, así como en los patios y estacionamientos del campus Huachi.

Siendo lo más habitual la sustracción de laptops y proyector de imágenes de los diferentes laboratorios, así como accesorios vehiculares de los estacionamientos, pero sin dejar de lado cosas más pequeñas que se demoran mucho tiempo en poderse dar cuenta de su desaparición o como la sustracción del vehículo en sí.

A todo esto podemos decir la falta de control más específico y riguroso en las puertas de ingreso y salida del predio, a los transeúntes y vehículos particulares o de servicio público, tanto por la falta de personal que no se daría abasto como por el tiempo e inversión que eso demandaría al realizarlo de manera manual.

6.3. JUSTIFICACIÓN

El interés de mejorar la seguridad existente en la Universidad Técnica de Ambato, al centralizar su control y monitoreo tanto de su infraestructura como de los bienes inmuebles existentes en la misma.

La propuesta tiene importancia porque existen equipos de última tecnología dentro de los laboratorios de las diferentes facultades y se necesita mejorar el tiempo de respuesta de auxilio en el caso que exista algún inconveniente o emergencia.

Se cuenta con el apoyo necesario del DISIR (Dirección de Sistemas Informáticos y Redes) y del personal de seguridad de la Universidad Técnica de Ambato, para poder encaminar de una mejor manera la presente propuesta.

La propuesta tiene su financiamiento en lo que corresponde al autor de esta investigación quien correrá a cargo del aspecto económico y tecnológico, ya que la finalidad es desarrollar un plan estratégico e innovador para que las autoridades tengan los suficientes argumentos para tomar la mejor decisión para el mejoramiento de la seguridad.

Es útil, pues se contribuye con la teoría a mejorar el conocimiento científico con las temáticas relacionadas en la propuesta.

La propuesta se basa en la aplicación de estudios actualizados, además de un estudio minucioso de los problemas de seguridad que tiene el campus universitario y las correcciones que se deben hacer.

Los beneficiarios de este proyecto serán la Universidad Técnica de Ambato, en lo relacionado a la seguridad de su infraestructura, e indirectamente docentes, administrativos, estudiantes, personal de seguridad y usuarios en general que ingresen a los predios universitarios, sabiendo que lo pueden hacer sin ningún inconveniente.

6.4. OBJETIVOS

6.4.1 OBJETIVO GENERAL

Diseñar un sistema de gestión de red alternativo, que optimice la comunicación para la seguridad, en la infraestructura física de la Universidad Técnica de Ambato.

6.4.2. OBJETIVOS ESPECÍFICOS

Definir la tecnología más adecuada para la optimización de recursos y personal para el mejoramiento de la comunicación para la seguridad de la infraestructura.

Diseñar la red para el sistema de gestión de seguridad en la infraestructura de la Universidad Técnica de Ambato.

Establecer los procesos de comunicación de la seguridad, en la infraestructura física de la Universidad Técnica de Ambato, con el fin de ubicar los nodos más vulnerables y sensibles.

Realizar un presupuesto de la implementación de la red IP de seguridad del Campus Huachi de la Universidad Técnica de Ambato.

6.5. ANÁLISIS DE FACTIBILIDAD

La propuesta planteada es factible de ejecutarla ya que se ha considerado todos los aspectos que tienen relación con el problema, con la finalidad de dar una solución eficaz y que pueda ser aplicada en la realidad en que se desempeña la institución motivo de estudio.

6.6. FUNDAMENTACIÓN

6.6.1. FUNDAMENTO TEÓRICO CONCEPTUAL

Hoy en día se debe utilizar toda la tecnología que se encuentre a nuestro alcance, ya que es una fortaleza para mejorar procesos y establecer un costo beneficio sobre proyectos que vayan en pos de la mejora de la seguridad y la comunicación en todo ámbito.

A continuación explicare como un sistema de gestión de red puede notificar que ha ocurrido un evento dentro de alguno de los edificios del predio Huachi de la Universidad Técnica de Ambato. Y a su vez veremos algunos conceptos básicos obtenidos de (Herrera, 2013) sobre los sistemas de alarma para ayudar a comprender de mejor forma la propuesta.

Panel de Alarma

Es la tarjeta electrónica en la que se conectan los dispositivos de entrada que por lo general son sensores y los dispositivos de salida que por lo general puede ser línea telefónica, radios, módulos de transmisión, celular GPRS y teclado. La capacidad del panel puede medirse por la cantidad de zonas que acepta. Se alimenta de corriente alterna y de una batería de respaldo que, en caso de falla de energía eléctrica, le proporciona autonomía de entre 12 horas y 4 días. Están colocados por lo general en la primera oficina de ingreso de las facultades.

Teclado

Es el elemento más fácil de identificar del sistema; este dispositivo se utiliza para configurar, activar o desactivar el sistema. A veces pueden tener botones con funciones especiales como: Emergencia Médica, Intrusión, Fuego, etc. Dependiendo del tipo de sistema de seguridad que se desee implementar.

Transformador de Corriente

Dispositivo conectado a la corriente alterna para proporcionar la energía eléctrica para el panel de alarma y cargar la batería.

Batería de Respaldo

Es la encargada de mantener al sistema funcionando en caso de fallas de energía eléctrica.

Sensores y Detectores

Estos son los dispositivos utilizados para supervisar las distintas áreas de los edificios por donde pueden ingresar los intrusos. Existen varios tipos especializados para aplicaciones específicas. En las facultades se encuentran solo en las puertas de ingreso.

Sirenas, Bocinas y Estrobos

Proporcionan señales audiovisuales advirtiendo de una posible intrusión.

Comunicador a la Central

Esta tarjeta o módulo tiene la importante función de enviar la señal de auxilio a la central de monitoreo, a través de distintos medios como: línea telefónica, radio, celular o internet.

Cableado

Los detectores son conectados al panel usando alambres que se conectan a los terminales del detector. La integridad del cableado es supervisada usando resistencias de fin de línea. Cada uno de los detectores se conecta a una zona física del panel. Una variante de este tipo de instalación, es el cableado en bus, en el cual, los detectores se conectan a un cableado común, que se conecta a terminales específicos del panel para el bus de detectores o a los terminales del bus de datos del sistema. Esta comunicación es muy útil para reducir los costos del cableado.

Inalámbrico

Se usa la tecnología de radio frecuencia para enviar los eventos de alarma y sabotaje a la central de alarmas.

Tipos de Monitoreo

Luego de ocurrir un evento en el sistema de alarma, el panel tiene la opción de notificar del evento al usuario final o a la empresa de monitoreo. Hay diferentes medios de enviar una notificación, por línea telefónica tradicional, radio, internet, celular convencional (canal GSM), celular GPRS, existe otro método de notificación, que es local; esto quiere decir, que la alarma no enviará la notificación por los medios de comunicación anteriormente mencionados, sino que solamente generará el sonido de las sirenas, bocinas y estrobos para la notificación.

Topología de la central de monitoreo

Luego de ocurrir un evento en el sistema de alarma, el panel tiene la opción de notificar del evento a la central de monitoreo o a los señores guardias. Hay diferentes medios de enviar una notificación, a continuación se presenta una topología general:

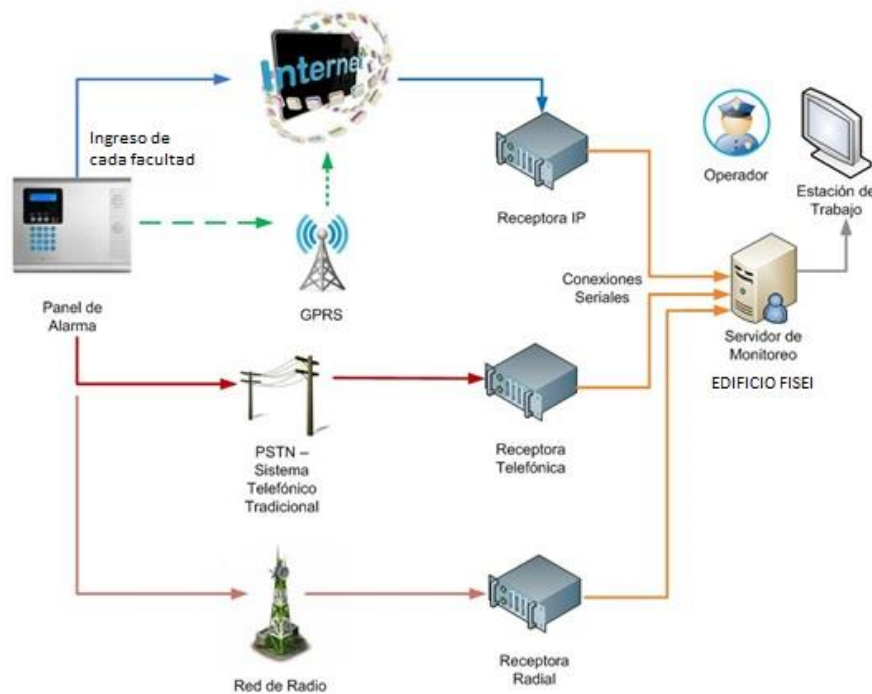


Gráfico 6. 1: Topología de central de monitoreo
Elaborado por: El investigador

Módulos de Comunicación

Se refiere a los módulos electrónicos conectados al panel para poder utilizar los diferentes medios de comunicación. Estos módulos adaptan la información para que pueda “viajar” por los medios de comunicación de manera rápida y eficiente:

Comunicador IP

Módulo que convierte la información suministrada por el panel en paquetes TCP/IP para ser enviados por medio de las redes de datos IP o Ethernet.

Comunicador GSM/GPRS

Módulo que contiene un transmisor celular, similar al utilizado en los teléfonos celulares, que envía la información del panel a la red celular.

Comunicador vía Radio

Módulo que envía la información a una red de radio, normalmente privada, usando canales de muy alta frecuencia (VHF) o ultra alta frecuencia (UHF).

Medio de Comunicación

Es el medio utilizado por los módulos de comunicación para enviar la información desde el panel de cada facultad a la central de monitoreo que se encuentra ubicada en el edificio nuevo de la facultad de Ingeniería en Sistemas Electrónica e Industrial.

Redes Ethernet o IP

Es uno de los medios de comunicación más modernos y flexibles con los que se cuenta actualmente en los predios universitarios. La rápida difusión del Internet y las redes de comunicación, han hecho que los fabricantes de sistemas de alarmas hayan desarrollado módulos de comunicación capaces de utilizar esta tecnología y proveer beneficios importantes a las empresas de monitoreo y a los usuarios.

Canal de Voz GSM

Es el que usamos cuando hacemos llamadas desde un teléfono móvil a otro. Este medio fue el primero en ser usado para monitorear alarmas vía celular, pero su alto costo rápidamente lo sacó del mercado. Sin embargo, en algunas aplicaciones se sigue usando como respaldo de la línea telefónica.

Canal de datos o GPRS

Es el mismo canal que se usa para hacer navegación o para enviar correos desde un celular. Para el monitoreo, se utiliza un dato encapsulado en una trama GPRS con destino la dirección IP de la central de monitoreo o del proveedor del servicio de monitoreo por GPRS. Este medio reemplazó rápidamente al GSM para el respaldo de comunicación de línea telefónica, debido a que el costo de los planes de datos es significativamente menor al de los planes de Voz. Sin embargo, tradicionalmente, el valor de los módulos comenzó siendo un poco costoso, pero a medida que ha pasado el tiempo, han comenzado a volverse más económicos. Mediante este módulo, el panel envía información a la receptora IP por medio del INTERNET.

Receptora IP

Esta receptora cumple prácticamente la misma función que la receptora telefónica. La diferencia es que esta receptora no está conectada a una línea telefónica sino a un puerto de red. Esta comunicación de red, permite recibir eventos provenientes desde un panel conectado a la red local o a un panel conectado a Internet. Al ser estas redes un medio “no seguro”, los módulos de comunicación encriptan la información con algoritmos propietarios de cada empresa fabricante de alarmas, y la receptora se encarga de desencriptar la información para adquirir el evento enviado y transmitirlo al software de gestión de alarmas. Este punto de red debe ser identificado por medio de una dirección IP, que puede estar direccionada por medio de un enrutador a Internet o funcionar como una dirección local, en caso de que se haga un monitoreo interno de los paneles. Normalmente, estas receptoras son capaces de recibir los eventos provenientes de paneles con módulos IP y/o GPRS Y también envían su señal, por un puerto serial al servidor en el que se ejecuta el software de monitoreo. Las receptoras IP pueden ser concebidas como un equipo físico o como un software.

Software de Gestión de Alarmas

Es el encargado de traducir los códigos del protocolo de comunicación, entregados por las receptoras, a información entendible para el operador de la central de monitoreo. Son software muy robustos, con una gran capacidad de almacenamiento de información, habitualmente utilizan motores de bases de datos de alta capacidad para dar manejo a la información. Es en este software donde finaliza el proceso electrónico de una señal o evento. En este software, el operador recibe el evento, lo procesa y almacena para posteriormente poder hacer reportes y trazabilidad de eventos. Así mismo el operador de acuerdo a la información entregada por el software, realizará las acciones pertinentes para atender, el evento (Ejemplo: Una llamada al usuario, un despacho de la reacción, una llamada a organismos de apoyo como cuerpo de bomberos, etc.).

Ahora para el presente trabajo investigativo se propone trabajar con tecnología IP, debido a que la Universidad tiene esta tecnología ya instalada en los predios para poderse comunicar y entonces podemos aprovechar esos recursos ya existentes para mejorar el sistema de gestión de red de la seguridad en la infraestructura de la Universidad Técnica de Ambato en sus predios de Huachi, por lo que a continuación veremos los beneficios que aporta la vigilancia IP a los sistemas de seguridad:

Accesibilidad remota.

Rentabilidad de la inversión.

Flexibilidad.

Escalabilidad.

Integración y funcionalidad actualizable.

La vigilancia IP cumple los requisitos de un sistema económico y de alta calidad, y ha demostrado ser un medio eficaz de reducir la delincuencia y la violencia en zonas conflictivas, por tal motivo se escoge esta tecnología para implementar en los predios universitarios.

Las soluciones de vigilancia IP se usan para supervisar la seguridad y para el seguimiento a distancia de patios, pasillos, pabellones y aulas de las diferentes facultades, haciendo de los predios más seguros. Las soluciones de vigilancia IP aprovechan la red informática ya existente en los predios universitarios, simplificando la instalación y reduciendo el costo, por lo que constituyen una opción viable para la propuesta.

Sistema de Monitoreo con comunicaciones IP y GPRS/GSM

Se basa en la provisión, implementación y soporte de una estación de monitoreo de alarmas en la central de monitoreo que se ubica en el edificio nuevo de la Facultad de Ingeniería en Sistemas Electrónica e Industrial, integrando la tecnología de paneles de alarma, comunicadores IP y GPRS, receptores y software de monitoreo de alarma recibidos por distintas vías.

Router

Un router, también conocido como ruter, enrutador, ruteador o encaminador de paquetes, es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un enrutador mediante bridges, y que por tanto tienen prefijos de red distintos.

Switch

Un conmutador o switch es un dispositivo digital lógico de interconexión de redes de computadoras que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las redes de área local.

Fibra óptica

La fibra óptica es un medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir. El haz de luz queda completamente confinado y se propaga por el interior de la fibra con un ángulo de reflexión por encima del ángulo límite de reflexión total, en función de la ley de Snell. La fuente de luz puede ser láser o un LED.

Las fibras se utilizan ampliamente en telecomunicaciones, ya que permiten enviar gran cantidad de datos a una gran distancia, con velocidades similares a las de radio y superiores a las de cable convencional. Son el medio de transmisión por excelencia al ser inmune a las interferencias electromagnéticas, también se utilizan para redes locales, en donde se necesite aprovechar las ventajas de la fibra óptica sobre otros medios de transmisión.

El grosor del filamento es comparable al grosor de un cabello humano, es decir, aproximadamente de 0,1mm. En cada filamento de fibra óptica podemos apreciar 3 componentes, la fuente de luz: LED o laser, el medio transmisor: fibra óptica y el detector de luz: fotodiodo, además un cable de fibra óptica está compuesto por: Núcleo, recubrimiento, tensores y chaqueta.

Convencionalmente, un pulso de luz indica un bit 1 y la ausencia de luz indica un bit 0. El detector genera un pulso eléctrico cuando la luz incide en él. Éste sistema de transmisión tendría fugas de luz y sería inútil en la práctica excepto por un principio interesante de la física. Cuando un rayo de luz pasa de un medio a otro, el rayo se refracta (se dobla) entre las fronteras de los medios.

Cable UTP

UTP, viene de las siglas Unshielded Twisted Pair (Par trenzado no blindado). Es una clase de cable que no se encuentra blindado y que suele emplearse en las telecomunicaciones.

El cable de par trenzado son dos conductores eléctricos aislados entrelazados para anular las interferencias de fuentes externas y diafonía de los cables opuestos.

Dirección IP

Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz de un dispositivo dentro de una red que utilice el protocolo IP, que corresponde al nivel de red del Modelo OSI. Dicho número no se ha de confundir con la dirección MAC, que es un identificador de 48 bits para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizado ni de la red. La dirección IP puede cambiar muy a menudo por cambios en la red o porque el dispositivo encargado dentro de la red de asignar las direcciones IP decida asignar otra IP (por ejemplo, con el protocolo DHCP). A esta forma de asignación de dirección IP se denomina también dirección IP dinámica.

Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados generalmente tienen una dirección IP fija. Esta no cambia con el tiempo. Los servidores de correo, DNS, FTP públicos y servidores de páginas web necesariamente deben contar con una dirección IP fija o estática, ya que de esta forma se permite su localización en la red.

Los ordenadores se conectan entre sí mediante sus respectivas direcciones IP. Sin embargo, es más cómodo utilizar otra notación más fácil de recordar, como los nombres de dominio; la traducción entre unos y otros se resuelve mediante los servidores de nombres de dominio DNS, que a su vez facilita el trabajo en caso de cambio de dirección IP, ya que basta con actualizar la información en el servidor DNS y el resto de las personas no se enterarán, ya que seguirán accediendo por el nombre de dominio.

Protocolo de Internet

Internet Protocol ('Protocolo de Internet') o IP es un protocolo de comunicación de datos digitales clasificado funcionalmente en la Capa de Red según el modelo internacional OSI.

Su función principal es el uso bidireccional en origen o destino de comunicación para transmitir datos mediante un protocolo no orientado a conexión que transfiere paquetes conmutados a través de distintas redes físicas previamente enlazadas según la norma OSI de enlace de datos.

Descripción del Sistema

Se trata de una solución para el monitoreo de paneles de alarma de diferentes tipos, tanto existentes como por instalar, que deben enlazarse con la Estación de Monitoreo, como indicamos anteriormente cada unidad académica tiene por su cuenta un sistema de seguridad diferente y se debe aprovechar para no generar gastos en vano.

Permitiendo implementar una solución tecnológica en la modalidad “llave en mano”, combinando equipos, servicios técnicos y software, que brinde un alto nivel de independencia al personal de seguridad.

Y priorizando en el diseño una modalidad de trabajo que facilite la acción inmediata ante problemas técnicos y evite gastos operativos innecesarios.

Como funciones principales del sistema podemos decir que debe tener:

Conexión rápida y confiable desde cada panel remoto a la Estación de Monitoreo.

Administración de toda la información desde la Estación de Monitoreo.

Posibilidad de reportes vía SMS a responsables locales (eventos relevantes).

Aprovechamiento de la inversión actual en paneles.

Distintos canales de comunicación para los paneles.

Administración remota de los sistemas instalados.

Plataforma expandible, que acompañe el crecimiento del cliente.

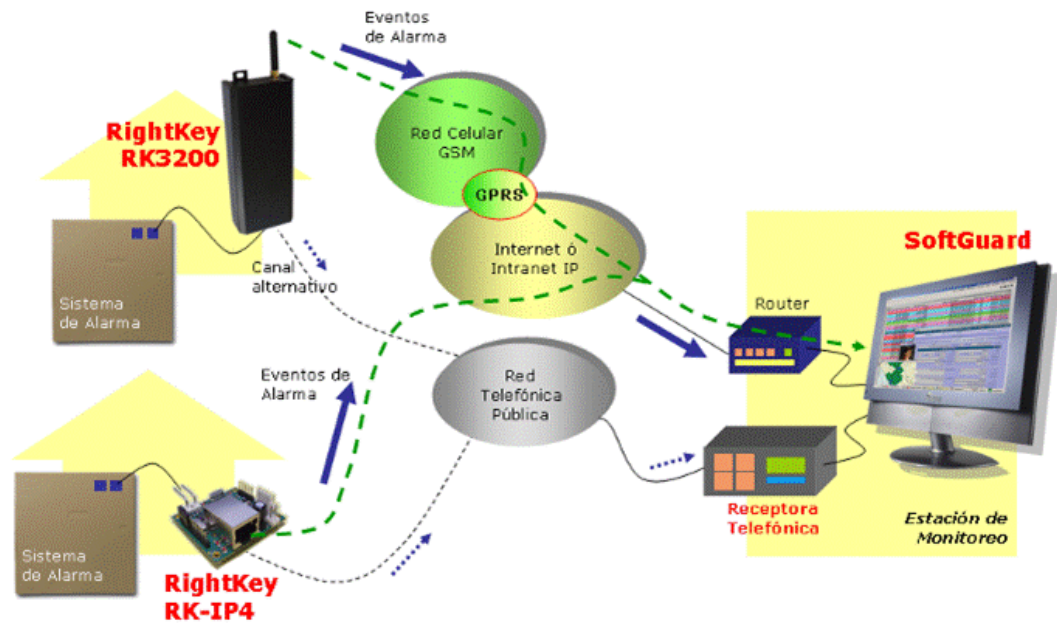


Gráfico 6. 2: Esquema de red
Elaborado por: El investigador

En este esquema vemos la secuencia de generación, transmisión y procesamiento de eventos de alarma, desde paneles nuevos o preexistentes, utilizando las distintas alternativas de comunicación propuestas: GPRS e IP, con back up por línea telefónica.

Se considera la provisión de tecnología de hardware y software de última tecnología, para que resulte eficiente la puesta en marcha de la estación de monitoreo, generando servicios que sean de calidad y competitivos, y al mismo tiempo tenga posibilidad de crecer.

6.6.2. DISEÑO FÍSICO Y LÓGICO

La Universidad Técnica de Ambato consta de cuatro predios universitarios como lo hemos anotado al inicio de la presente investigación, de los cuales se ha centrado el desarrollo de la propuesta en el Campus Huachi, ubicado en la Avenida Los Chasquis y Río Guayllabamba, en este predio universitario se encuentran funcionando actualmente ocho facultades y algunas dependencias universitarias que están en proceso de cambio. De manera general se tomó en cuenta un panel de control por cada edificio, dos detectores de movimiento por cada puerta de ingreso, un contacto magnético por cada puerta de ingreso o acceso, una sirena blindada por cada unidad académica, una estación manual de incendios por cada ingreso y una sirena interna con luz estroboscópica por cada puerta de ingreso.

La Universidad Técnica de Ambato tiene actualmente a su disposición un Ancho de Banda para internet de 400 Mbps, para ser distribuidos a todos sus estamentos según lo requieran, la conexión entre facultades tiene un ancho de banda de 1Gbps por medio de fibra óptica, para la utilización del sistema de seguridad que se analiza en la propuesta no se requiere más allá de 10 Kbps para enviar información sobre acontecimientos que puedan ocurrir, por lo que no es necesario que se aumente el ancho de banda, pues la afectación es mínima.

El diagrama de red IP implementado en los predios de la Universidad Técnica de Ambato, se detalla en el gráfico 6.3, con sus respectivos puertos y direccionamientos para cada unidad académica y administrativa:

Una vez analizada la red y realizada la visita a las distintas unidades académicas del predio mencionado, se determinó las necesidades que tiene cada una para ser implementadas con su respectiva red.

UNIVERSIDAD TÉCNICA DE AMBATO Direccionamiento

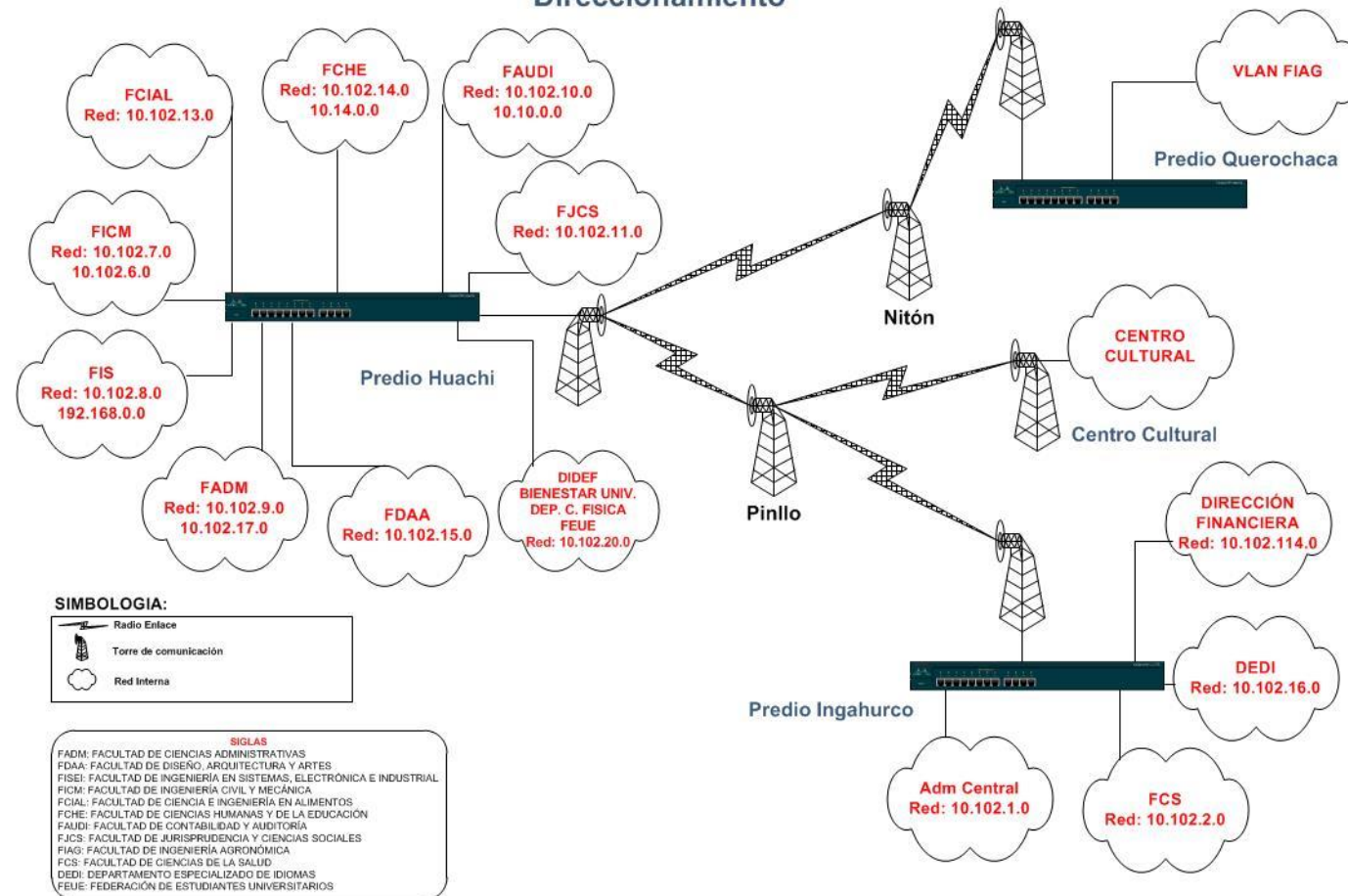


Gráfico 6. 3: Red IP UTA
Tomado de: DISIR

A continuación se detalla los requerimientos de cada facultad desde la tabla 6.1 hasta la tabla 6.15.

Facultad de Ingeniería en Sistemas, Electrónica e Industrial

Consta de dos edificios, en el bloque uno se encuentran dos entradas de ingreso, su edificación es de tres pisos y tiene los ductos adecuados para proceder a la implantación de una nueva red.

Red: 10.102.8.0
192.168.0.2

FISEI 1	
CANTIDAD	EQUIPOS
1	Panel de control
1	Sirena blindada
4	Detectores de movimiento
2	Contactos magnéticos
2	Estaciones manuales de incendio
2	Sirena interna con luz estroboscópica

Tabla 6. 1: FISEI 1
Elaborado por: El investigador

En el bloque dos se encuentran tres entradas de ingreso, su edificación es de tres pisos y tiene los ductos adecuados para proceder a la implantación de una nueva red. Además aquí se encuentra la central de monitoreo del predio Huachi.

FISEI 2	
CANTIDAD	EQUIPOS
1	Panel de control
1	Sirena blindada
6	Detectores de movimiento
3	Contactos magnéticos
3	Estaciones manuales de incendio
3	Sirena interna con luz estroboscópica

Tabla 6. 2: FISEI 2
Elaborado por: El investigador

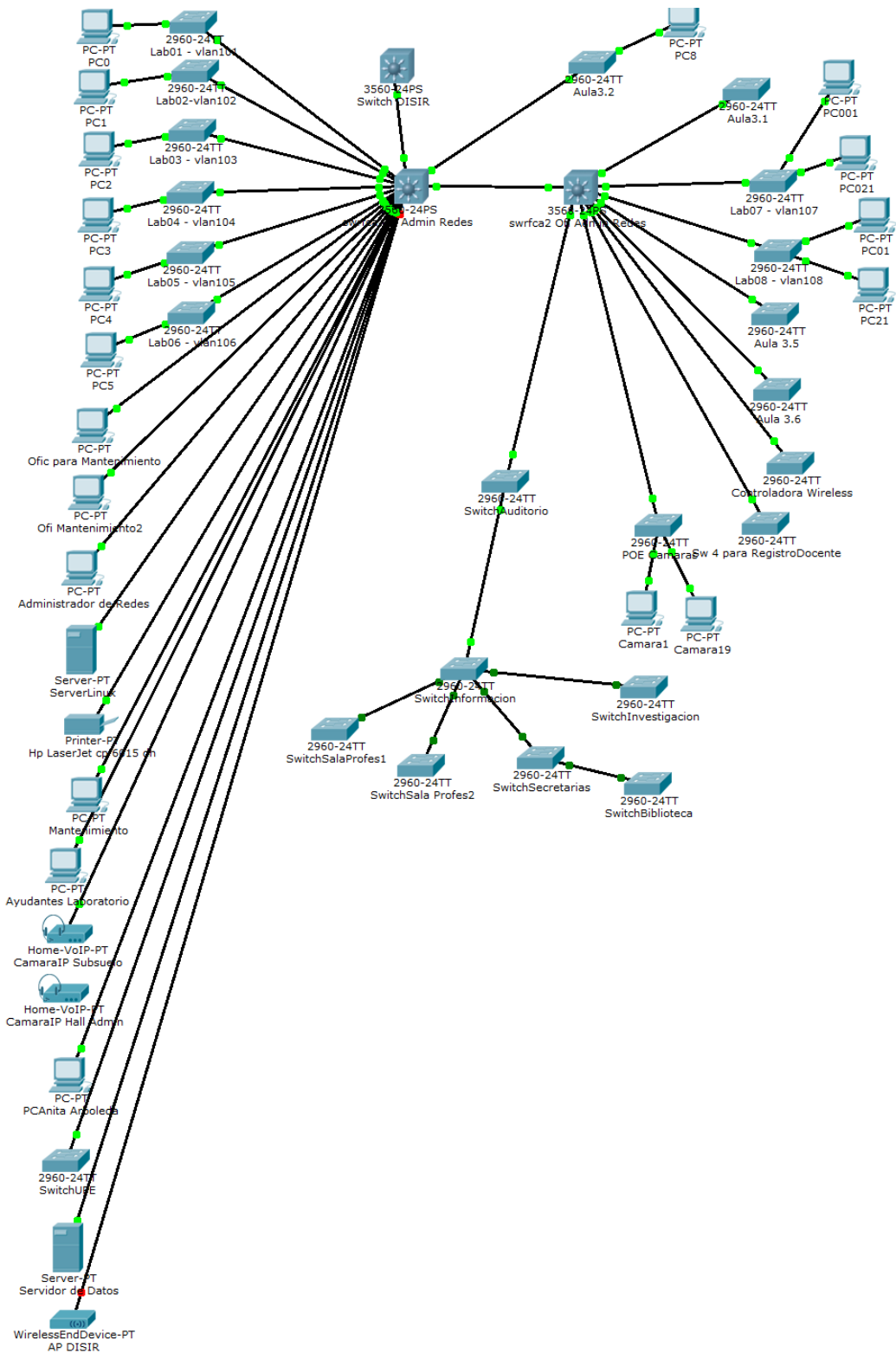


Gráfico 6. 4: Diagrama de red FISEI
 Elaborado por: El investigador

Facultad de Diseño, Arquitectura y Artes.

Consta de un edificio, con una entrada de ingreso, es de cuatro pisos y tiene los ductos adecuados para proceder a la implantación de una nueva red.

Red: 10.102.15.0

FDAA	
CANTIDAD	EQUIPOS
1	Panel de control
1	Sirena blindada
2	Detectores de movimiento
1	Contactos magnéticos
1	Estaciones manuales de incendio
1	Sirena interna con luz estroboscópica

Tabla 6. 3: FDAA
Elaborado por: El investigador

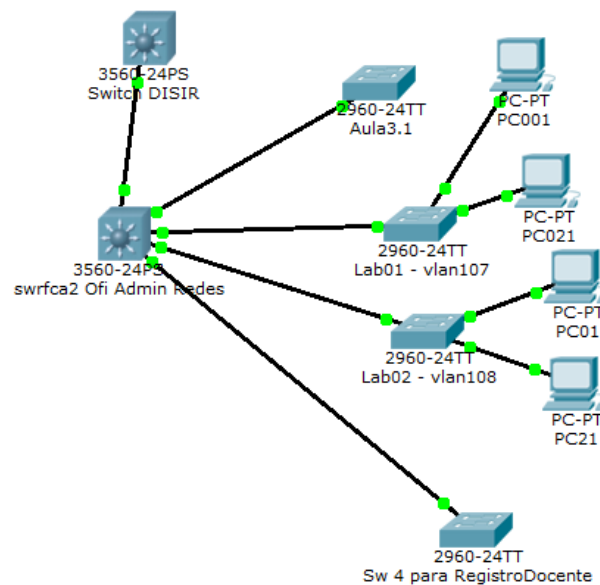


Gráfico 6. 5: Diagrama de red de FDAA
Elaborado por: El investigador

Facultad de Ciencias Administrativas

Consta de dos edificios, en el bloque uno tiene una entrada de ingreso, su edificación es de tres pisos y tiene los ductos adecuados para proceder a la implantación de una nueva red.

Red: 10.102.9.0
10.102.17.0

FCADM 1	
CANTIDAD	EQUIPOS
1	Panel de control
1	Sirena blindada
2	Detectores de movimiento
1	Contactos magnéticos
1	Estaciones manuales de incendio
1	Sirena interna con luz estroboscópica

Tabla 6. 4: FCADM 1
Elaborado por: El investigador

En el bloque dos tiene una entrada de ingreso, su edificación es de tres pisos y tiene los ductos adecuados para proceder a la implantación de una nueva red.

FCADM 2	
CANTIDAD	EQUIPOS
1	Panel de control
1	Sirena blindada
2	Detectores de movimiento
1	Contactos magnéticos
1	Estaciones manuales de incendio
1	Sirena interna con luz estroboscópica

Tabla 6. 5: FCADM 2
Elaborado por: El investigador

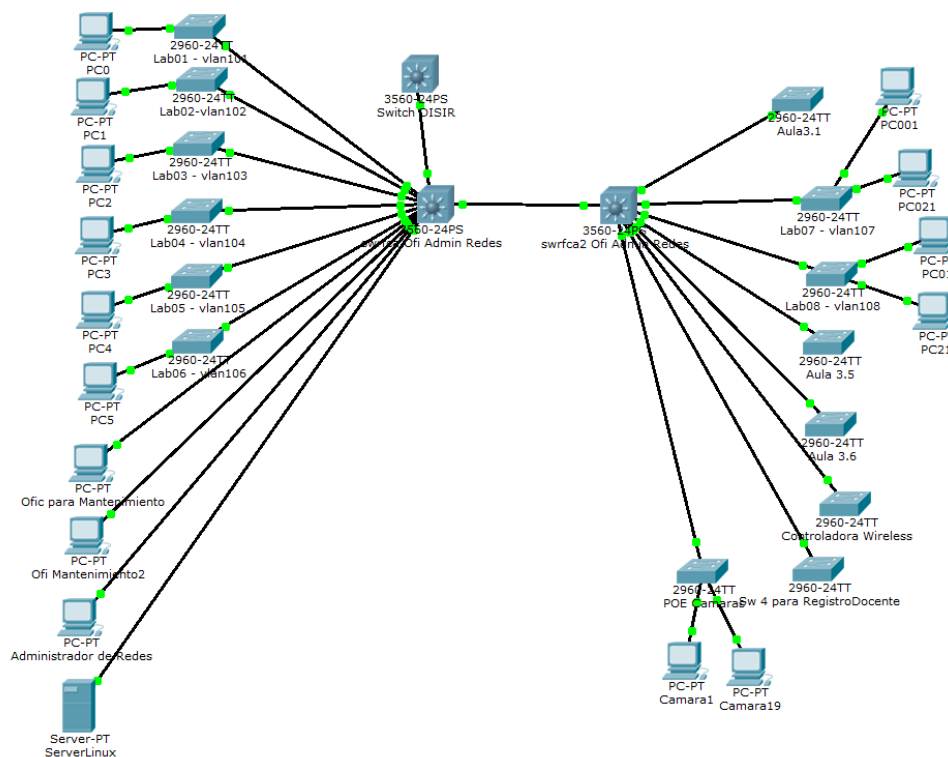


Gráfico 6. 6: Diagrama de red FCADM
Elaborado por: El investigador

Facultad de Ciencias Humanas y de la Educación

Consta de tres edificios, en el bloque uno tiene tres entradas de ingreso, su edificación es de cuatro pisos y tiene los ductos adecuados para proceder a la implantación de una nueva red.

Red: 10.102.14.0

10.14.0.0

FCHE 1	
CANTIDAD	EQUIPOS
1	Panel de control
1	Sirena blindada
6	Detectores de movimiento
3	Contactos magnéticos
3	Estaciones manuales de incendio
3	Sirena interna con luz estroboscópica

Tabla 6. 6: FCHE 1
Elaborado por: El investigador

En el bloque dos tiene dos entradas de ingreso, su edificación es de tres pisos y tiene los ductos adecuados para proceder a la implantación de una nueva red.

FCHE 2	
CANTIDAD	EQUIPOS
1	Panel de control
1	Sirena blindada
4	Detectores de movimiento
2	Contactos magnéticos
2	Estaciones manuales de incendio
2	Sirena interna con luz estroboscópica

Tabla 6. 7: FCHE 2
Elaborado por: El investigador

En el bloque tres tiene dos entradas de ingreso, su edificación es de cuatro pisos y tiene los ductos adecuados para proceder a la implantación de una nueva red.

FCHE 3	
CANTIDAD	EQUIPOS
1	Panel de control
1	Sirena blindada
4	Detectores de movimiento
2	Contactos magnéticos
2	Estaciones manuales de incendio
2	Sirena interna con luz estroboscópica

Tabla 6. 8: FCHE 3
Elaborado por: El investigador

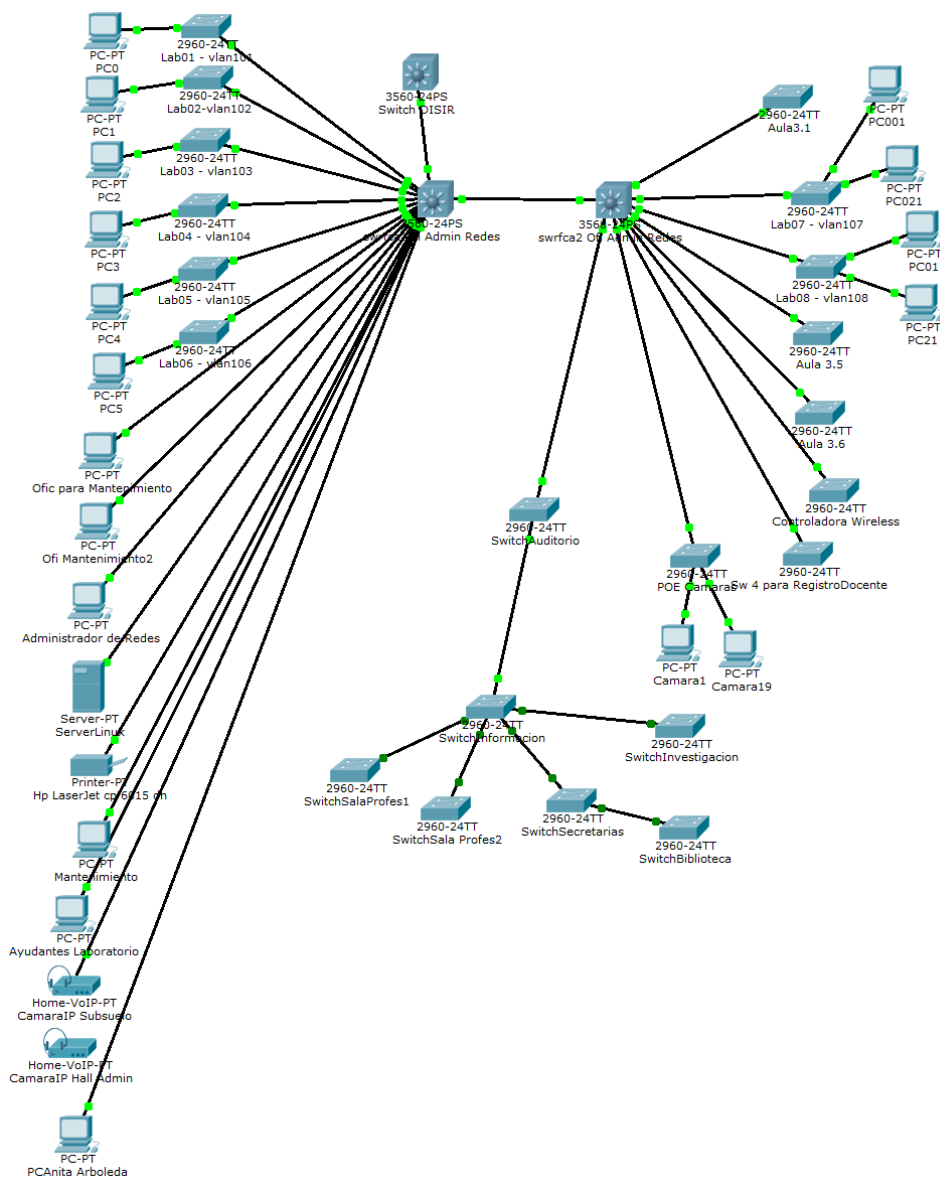


Gráfico 6. 7: Diagrama de red FCHE
Elaborado por: El investigador

Facultad de Ciencia e Ingeniería en Alimentos

Consta de un edificio, tiene dos entradas de ingreso, su edificación es de tres pisos y tiene los ductos adecuados para proceder a la implantación de una nueva red.

Red: 10.102.13.0

FCIA	
CANTIDAD	EQUIPOS
1	Panel de control
1	Sirena blindada
4	Detectores de movimiento
2	Contactos magnéticos
2	Estaciones manuales de incendio
2	Sirena interna con luz estroboscópica

Tabla 6. 9: FCIA
Elaborado por: El investigador

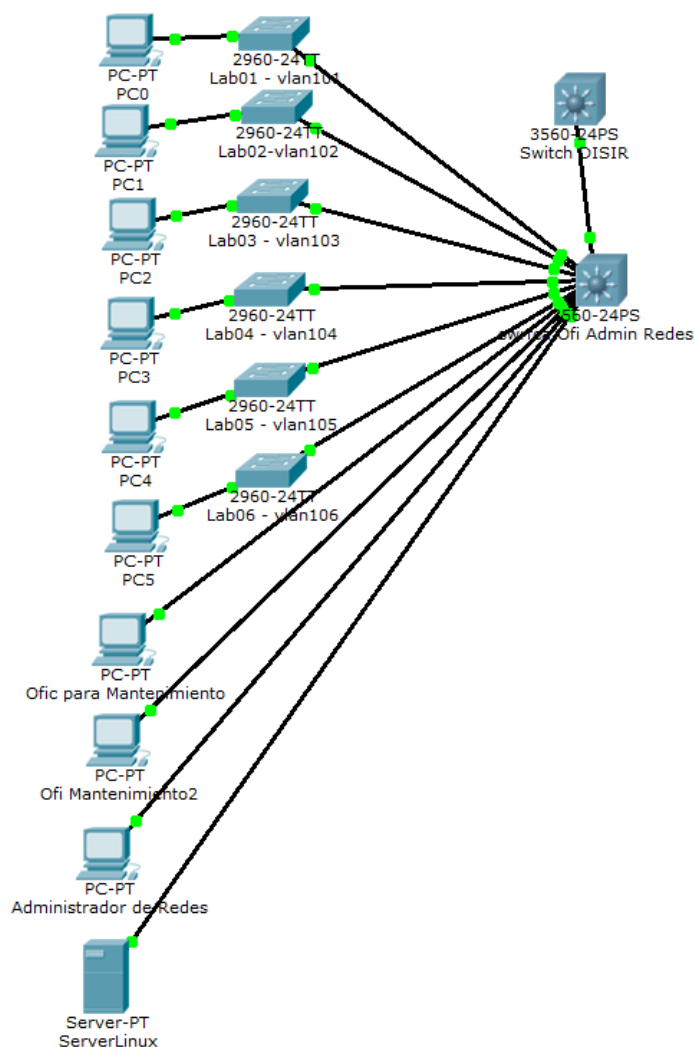


Gráfico 6. 8: Diagrama de red de FCIA
Elaborado por: El investigador

Facultad de Contabilidad y Auditoria

Consta de dos edificios, en el bloque uno tiene una entrada de ingreso, su edificación es de tres pisos y tiene los ductos adecuados para proceder a la implantación de una nueva red.

Red: 10.102.10.0

10.10.0.0

FCAUD 1	
CANTIDAD	EQUIPOS
1	Panel de control
1	Sirena blindada
2	Detectores de movimiento
1	Contactos magnéticos
1	Estaciones manuales de incendio
1	Sirena interna con luz estroboscópica

Tabla 6. 10; FCAUD 1
Elaborado por: El investigador

En el bloque dos tiene una entrada de ingreso, su edificación es de tres pisos y tiene los ductos adecuados para proceder a la implantación de una nueva red.

FCAUD 2	
CANTIDAD	EQUIPOS
1	Panel de control
1	Sirena blindada
2	Detectores de movimiento
1	Contactos magnéticos
1	Estaciones manuales de incendio
1	Sirena interna con luz estroboscópica

Tabla 6. 11: FCAUD 2
Elaborado por: El investigador

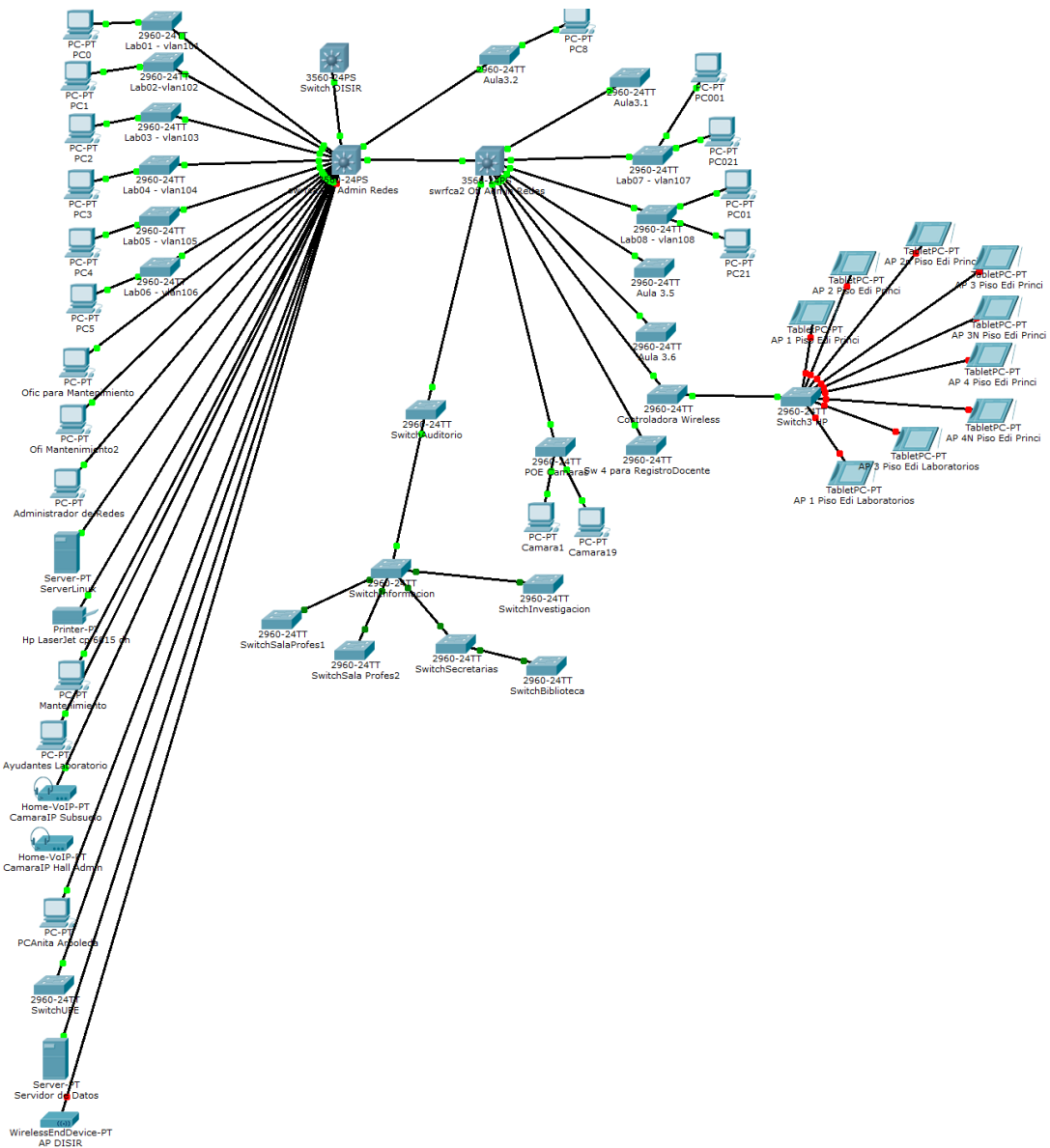


Gráfico 6. 9: Diagrama de red de FCAUD
Elaborado por: El investigador

Facultad de Ingeniería Civil y Mecánica

Consta de dos edificios, en el bloque uno tiene una entrada de ingreso, su edificación es de tres pisos y tiene los ductos adecuados para proceder a la implantación de una nueva red.

Red: 10.102.7.0
10.102.6.0

FICM 1	
CANTIDAD	EQUIPOS
1	Panel de control
1	Sirena blindada
2	Detectores de movimiento
1	Contactos magnéticos
1	Estaciones manuales de incendio
1	Sirena interna con luz estroboscópica

Tabla 6. 12: FICM 1
Elaborado por: El investigador

En el bloque dos tiene una entrada de ingreso, su edificación es de tres pisos y tiene los ductos adecuados para proceder a la implantación de una nueva red.

FICM 2	
CANTIDAD	EQUIPOS
1	Panel de control
1	Sirena blindada
2	Detectores de movimiento
1	Contactos magnéticos
1	Estaciones manuales de incendio
1	Sirena interna con luz estroboscópica

Tabla 6. 13: FICM 2
Elaborado por: El investigador

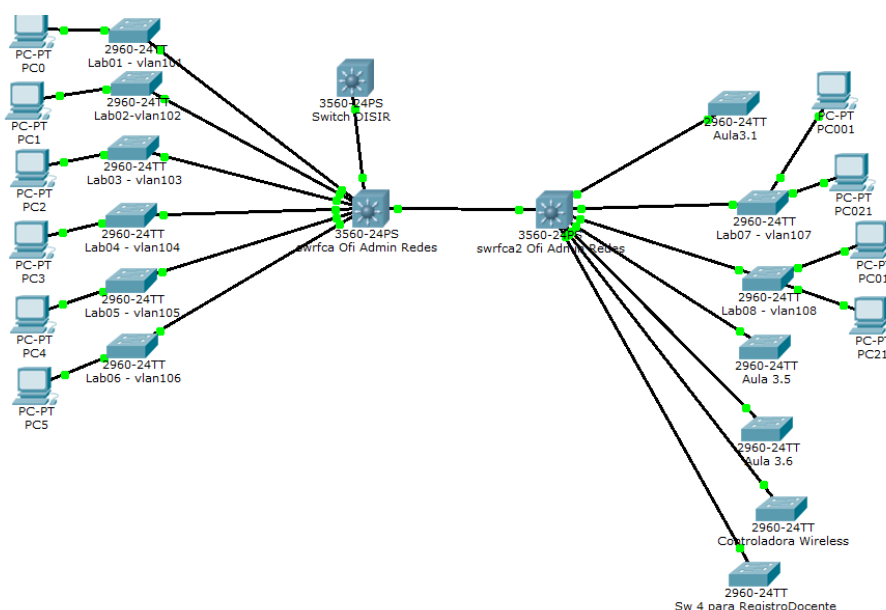


Gráfico 6. 10: Diagrama de red de FICM
Elaborado por: El investigador

Facultad de Jurisprudencia y Ciencias Sociales

Consta de dos edificios pero representan un solo bloque, en donde sus entradas de ingreso son abiertas, su edificación es de tres pisos y tiene los ductos adecuados para proceder a la implantación de una nueva red.

Red: 10.102.11.0

FJCS	
CANTIDAD	EQUIPOS
1	Panel de control
1	Sirena blindada
8	Detectores de movimiento
3	Contactos magnéticos
2	Estaciones manuales de incendio
2	Sirena interna con luz estroboscópica

Tabla 6. 14: FJCS
Elaborado por: El investigador

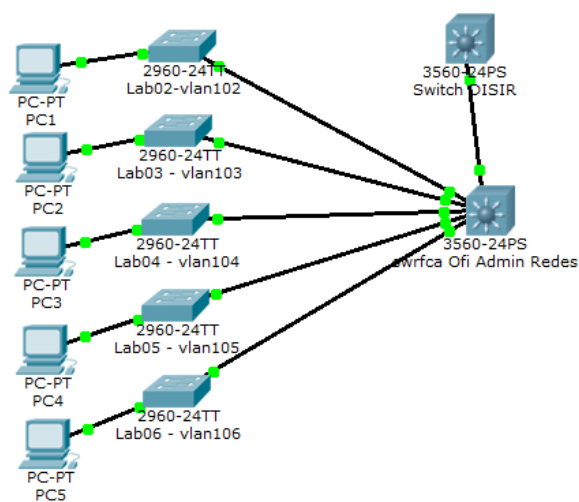


Gráfico 6. 11: Diagrama de red de FJCS
Elaborado por: El investigador

Dirección de Bienestar Universitario

Consta de un edificio, tiene una entrada de ingreso, su edificación es de tres pisos y tiene los ductos adecuados para proceder a la implantación de una nueva red.

Red: 10.102.20.0

DIBESAU	
CANTIDAD	EQUIPOS
1	Panel de control
1	Sirena blindada
2	Detectores de movimiento
1	Contactos magnéticos
1	Estaciones manuales de incendio
1	Sirena interna con luz estroboscópica

Tabla 6. 15: DIBESAU
Elaborado por: El investigador

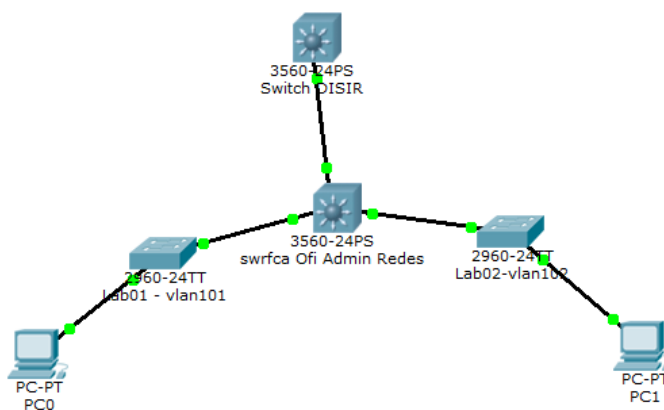


Gráfico 6. 12: Diagrama de red de DIBESAU
Elaborado por: El investigador

6.6.3 SELECCIÓN DE EQUIPOS

Una vez analizados los requisitos que se necesita para poder proponer el diseño de un sistema de gestión de red alternativo, que optimice la comunicación para la seguridad, en la infraestructura física de la Universidad Técnica de Ambato, por costo beneficio se llegó a determinar los siguientes equipos:

Central de monitoreo

Se tomó la central de monitoreo “Single-Line IP Receiver SG-SYSTEM II” debido a que es compacto, eficiente y rentable.

Las características que marcan la diferencia con respecto a otro tipo de centrales son:

- Monitorización remota para la solución ideal para las aplicaciones.
- Sistema II soporta hasta 1536 IP comunicadores (DSC celular o Ethernet) en las cuentas, 512 pueden ser supervisados
- Adicional 1536 (512 Supervisado) comunicadores IP disponibles utilizando clave de licencia opcional.
- Escritorio o montaje en rack con el uso de un kit de rack
- TCP / IP, USB o salidas serie para software de automatización
- Basado en menús y 40 caracteres, 2 líneas Pantalla LCD con retroiluminación azul proporciona instrucción cuando en modo manual
- 4 botones para la programación manual y el reconocimiento de la alarma señales durante el modo manual.
- Fuente de alimentación universal compatible con 110/220 V CA, 50 Hz/60 Hz
- Memoria flash a bordo y DSP para futuras actualizaciones de software y mejoras
- CE enumerado
- UL, ULC, CSFM, NIST, CE, y CNC aprobado

Además proporciona IP remota, seguimiento de Fuego y sistemas de allanamientos. Basándose en el linaje de monitoreo Sur-Gard dando confianza a los receptores de la estación, el Sistema II receptor IP de una sola línea se ha diseñado para aplicaciones propietarias, tales como los campus de la universidad.

Todos los datos de alarma que se recibe antes de transmitirla a la automatización a través TCP / IP, USB o salidas en serie. Los datos de alarma también se pueden transmitir directamente a una impresora utilizando el puerto paralelo de la impresora y se puede ver en la pantalla LCD en la parte frontal del receptor.

Es programable vía PC basado en el Software de la consola SG-Systems o manualmente mediante los botones de desplazamiento y la pantalla LCD, el receptor puede configurarse para revisar desde el escritorio la operación para montaje en el rack.

Es fácil de usar, la programación es rápida y la actualización es sencilla, el sistema II se puede programar localmente usando el menú de la unidad accionada, la pantalla se lo puede configurar en línea o de forma remota a través de una red Ethernet, cuya conexión se lo hace utilizando SG-Systems software de la consola.

El software también se puede utilizar para actualizar la memoria flash de la unidad con el nuevo software operativo sin el manejo de hardware o tirando de los chips. El sistema II cuenta con medidas de seguridad líderes tales como 128 - bit AES de cifrado y un diseño anti hack que aísla las comunicaciones internas de las transmisiones de datos externos, El sistema II proporciona la supervisión continua de software de automatización.

Las especificaciones de la central de monitoreo son:

Dimensiones	30,4 cm x 31 cm x 4,3 cm, estándar rack 19 "
Peso	8,5 libras (3,8 kg)
Voltaje de entrada	110-230 VAC, 50-60 Hz
Consumo de energía	25 W
Salidas	24 VDC
Respaldo de batería	UPS externo
Condiciones de trabajo	32 ° a 122 ° F / (0 ° a 50 ° C)
Humedad Relativa	90 % , sin condensación

Tabla 6. 16: Especificaciones Central de Monitoreo
Elaborado por: El investigador



Gráfico 6. 13: Central de monitoreo SG-SYSTEM II
Tomado de: Manual de usuario de SG-SYSTEM II

Tarjeta IP

Se seleccionó la tarjeta T-LINK TL-250, debido a sus bondades prestadas.

Los módulos T-Link TL250 son comunicadores de red en la Internet que envían información del sistema de alarma a un receptor en la estación central. El módulo es previamente programado con las configuraciones utilizadas más comúnmente para la instalación rápida. Las opciones estándar pueden programarse de forma personalizada utilizando el software T-Link Console, en su caso.

Existen cinco modos de operación de la tarjeta IP TL-250, a continuación describimos cada una.

Modo 1: Bell Follower (Seguidor de sirena)

En el modo 1, el T-Link TL250 monitorea la sirena de un panel de control. El sistema identifica la cadencia de la sirena y transmite el código de informe de alarma de incendio o robo correspondiente para la estación central.

No se debe utilizar el modo 1 para instalaciones listadas UL ó ULC.

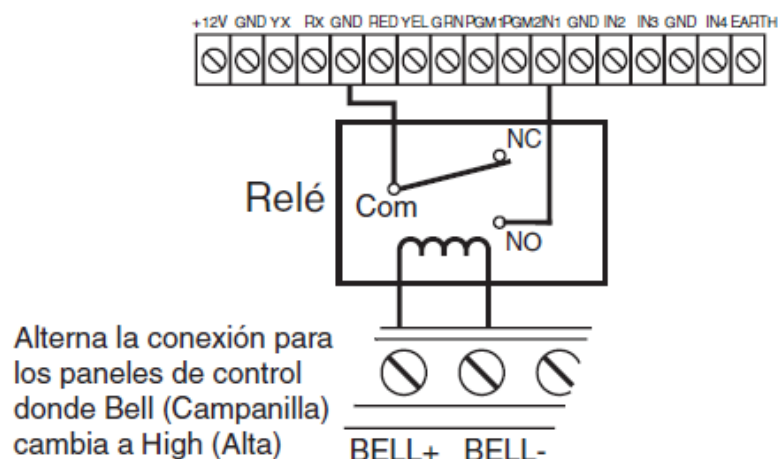


Gráfico 6. 14: Modo seguidor de sirena
Tomado de: Manual de usuario de T-LINK TL-250

Modo 2: Panel de cuatro zonas

En el modo 2, el sistema es configurado para operación autónoma en cuatro zonas.

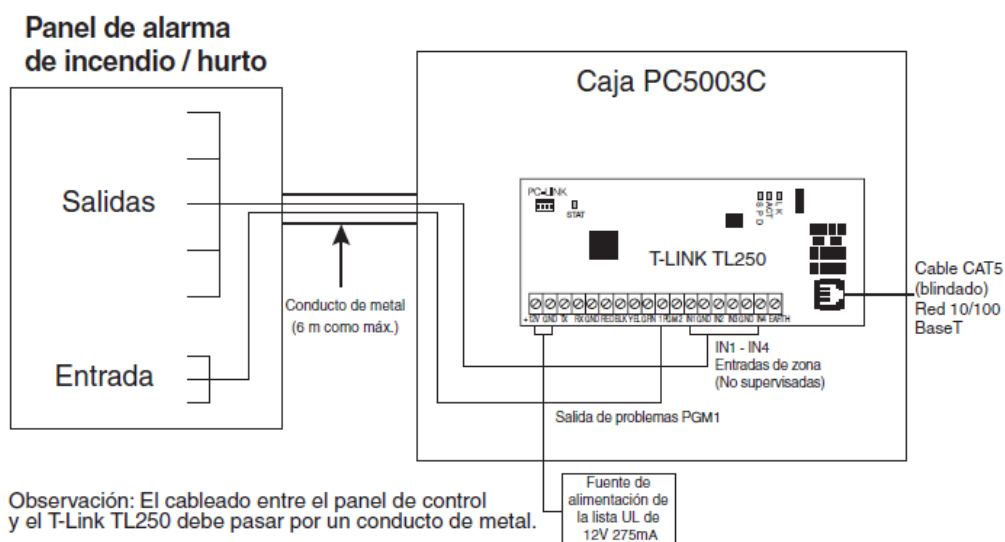


Gráfico 6. 15: Panel de cuatro zonas.
Tomado de: Manual de usuario de T-LINK TL-250

Modo 3: Panel de 12 zonas

Si el T-Link TL250 detecta una tarjeta de expansión PC5108 en la iniciación del sistema, el T-Link configurará automáticamente la operación autónoma con 12 zonas con circuitos normalmente abiertos.

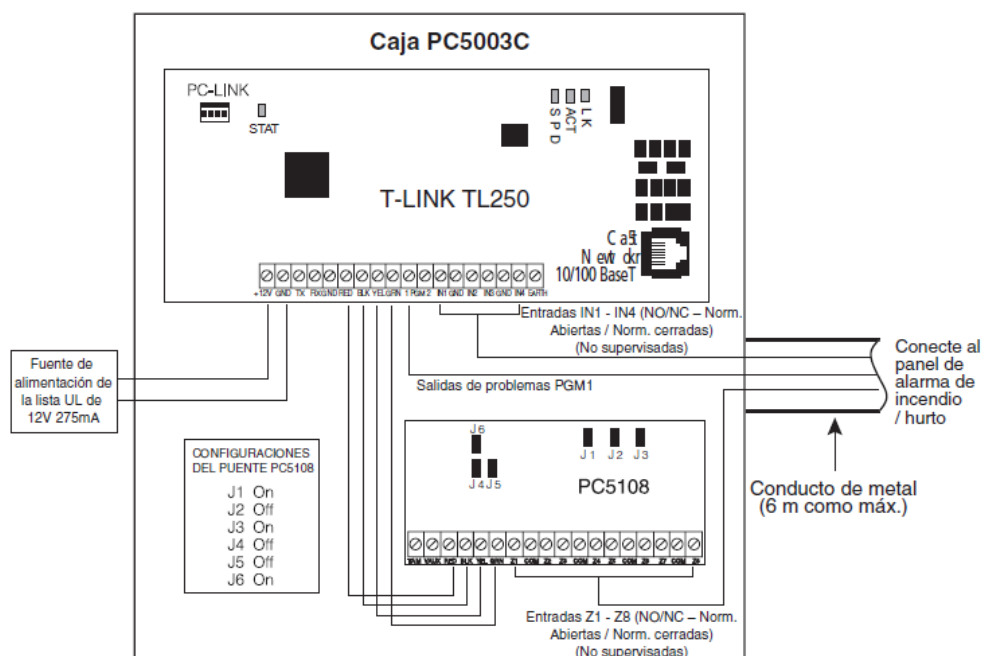


Gráfico 6. 16: Panel de doce zonas
Tomado de: Manual de usuario de T-LINK TL-250

En los modos 2 y 3, las conexiones entre las entradas de la PC5108 o del T-Link TL250 y las salidas de la unidad de control de alarma (contactos de relé) deberán hacerse en conductos metálicos, dentro de 7m. La operación autónoma también requerirá que las entradas sean programadas con los tipos de alarma deseados.

Modo 4: Modo estándar

En el modo estándar, el sistema está configurado como un comunicador con un panel de alarma compatible con DSC: Modelos PC4020, PC4020CF, PC5020 ó PC5020CF.

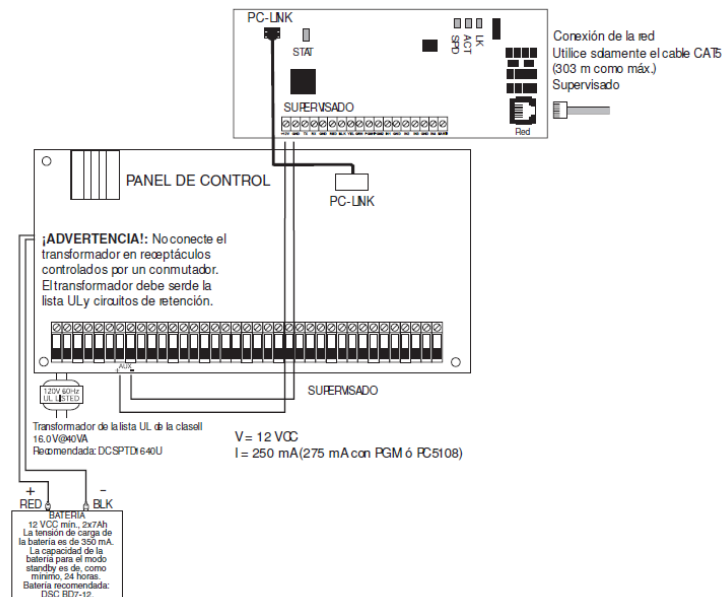


Gráfico 6. 17: Modo estándar.
Tomado de: Manual de usuario de T-LINK TL-250

Modo 5: Modo DVACS

En el modo DVACS, el sistema es configurado como un comunicador con un panel de alarma compatible con DVACS:

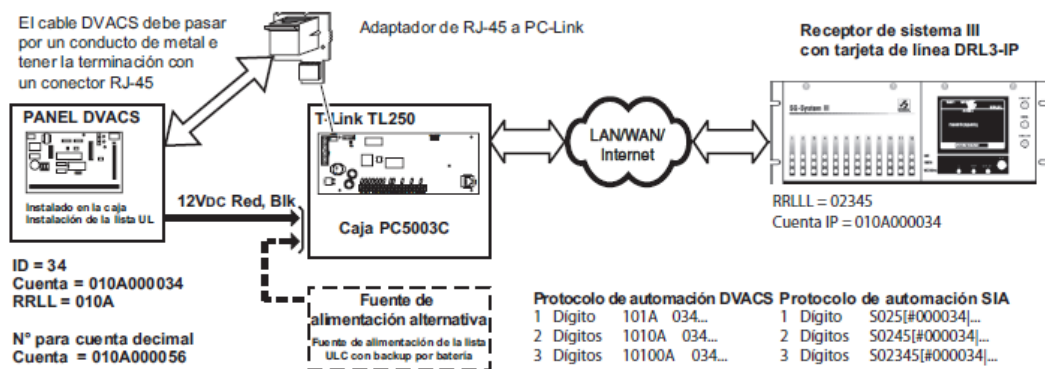


Gráfico 6. 18: Modo DVACS
Tomado de: Manual de usuario de T-LINK TL-250

Los eventos de la zona del T-Link TL250 son transmitidos a través de un protocolo T-Link SIA estándar. Los eventos generados por el DVACS son transmitidos a través del protocolo DVACS.

El modo 5 del DVACS es utilizado en instalaciones listadas UL.

Especificaciones y Requisitos

- El consumo de corriente máximo permitido de un panel compatible con DSC en la salida de terminación Aux es de 500 mA 12VCC.
- El consumo de corriente operativa del T-Link TL250 es de 250 mA.
- El módulo T-Link TL250 tiene dos salidas programables negativas conmutables (50 mA 12 VCC).
- Tensión de entrada: 12 VCC
- Corriente de entrada: Consumo de corriente máximo del T-LINK TL250: 275mA Consumo de corriente máximo del T-LINK TL300: 360 mA Dimensiones: 8,3 cm x 13,3 cm Temperatura operativa: 0° a 49°C
- Protocolos de salida: UDP/IP 10/100 BaseT semidúplex, TCP/IP para comunicaciones del console y DLS
- Protocolos de entrada: PC-Link (formato SIA), DVACS (V1.10 y superior), protocolo de identificación de contacto.
- Entradas digitales: cuatro entradas digitales (pueden aumentarse a 12 con el PC5108) Conectores: recolector de cuatro pernos para el PC-Link y RJ-45 para Ethernet, adaptador DVACS (solamente kit DVACS)
- Programación: teclado del panel, console en el RS232 o console T-Link remota. Red: Ethernet LAN/WAN 10 BaseT ó 10/100 BaseT
- E-mail: envía mensajes de alarma para en el máximo dos direcciones de e-mail (NO disponible para instalaciones DVACS)
- Soporte a download para paneles DSC:software DLS-3 y/o System Administrator (Administrador del sistema)
- Varias estaciones centrales: principal y de back up por vía línea telefónica* (NO disponible para instalaciones DVACS).
- Opciones de orientación de llamadas: comunicador principal o de back up que utiliza la orientación de llamadas del panel.

Panel de control

Se tomó el panel de control “PowerSeries v4.5” de marca DSC por las características que ofrece.

Tiene varias ventajas, entre las cuales se detalla la programación de plantillas, la descarga puede ser de forma local y remota, audio de 2 vías, bloqueo de teclado, características programables para reducción de falsas alarmas incluida la demora de salida acústica y fallo, salida rápida, armado/desarmado automático temporizador programable de aviso.

Especificaciones

- Rango de temperatura 0°C-49°C
- Humedad (Máx.) Humedad relativa de 93%
- Alimentación: 16,5 VCA/40 VA a 60 Hz
- Consumo de corriente (Panel).110 mA (nominal)
- Salida Aux+ 11,1-12,6 V CC/700 mA
- Salida de la campanilla 11,1-12,6 V CC/700 mA

CARACTERÍSTICAS	PC1616	PC1832	PC1864
Zonas en la tarjeta	6	8	8
Zonas con hilo	16 (1xPC5108)	32(3xPC5108)	64 (7xPC5108)
Zonas inalámbricas	32	32	32
Soporte para zonas de teclado	✓	✓	✓
Salidas PGM en la tarjeta	PGM 1 – 50 mA PGM 2 – 300 mA	PGM 1 – 50 mA PGM 2 – 300 mA	PGM 1, 3, 4 – 50 mA PGM 2 – 300 mA
Expansión PGM	8x50 mA (PC5208) 4x500 mA (PC5204)	8x50 mA (PC5208) 4x500 mA (PC5204)	8x50 mA (PC5208) 4x500 mA (PC5204)
Teclados	8	8	8
Particiones	2	4	8
Códigos de usuario	47 + Código maestro	71 + Código maestro	94 + Código maestro
Memoria de eventos	500 eventos	500 eventos	500 eventos
Transformador necesario	16,5 VCA/40 VA	16,5 VCA/40 VA	16,5 VCA/40 VA
Batería necesaria	4 Ah/7 Ah/14 AHr	4 Ah/7 Ah/14 AHr	4 Ah/7 Ah/14 AHr
Salida de campanilla	12 V/700 mA (cont.)	12 V/700 mA (cont.)	12 V/700 mA (cont.)

Tabla 6. 17: Características panel de control
Tomado de: Manual de usuario de PowerSeries v4.5

Conexión del barramiento

El barramiento de 4 hilos (rojo, negro, amarillo y verde) es la conexión de comunicación entre el panel de control y todos los módulos.

Los 4 terminales KEYBUS en todos los módulos deben estar conectados en los 4 terminales KEYBUS del panel de control principal.

Para poder conectar el barramiento se debe tener en cuenta que el cable de 22 AWG debe ser mínimo o máximo 18 AWG (2 cables trenzados preferentemente), no utilizar cable blindado, los módulos pueden conectarse todos directamente al panel de control principal, conectados en serie o pueden ser derivados en T, considerándose que la distancia máxima del panel de control hasta cualquier módulo no deba exceder 305 m y no se deben utilizar más que 915 m de cable total.

Conexión de zonas

Las zonas pueden conectarse a contactos Normalmente Abiertos o Normalmente Cerrados, con resistencias Fin de línea Simple (SEOL) o Fin de línea Doble (DEOL).

Para instalaciones con certificación UL solamente utilice SEOL o DEOL, cable de 22 AWG como mínimo, 18 AWG como máximo, no cable blindado, la resistencia de la extensión del cableado no debe exceder 100Ω.

Expansores de zonas

Los expansores de zonas agregan zonas en grupos de ocho al sistema de alarma. Los puentes de módulo J1, J2, J3 son necesarios para atribuir zonas a esos módulos.

El PC5108v1.0 soporta solamente las primeras 32 zonas, el PC5700 está registrado como dos módulos, hay que tener en cuenta que no se debe utilizar el PC5108v1 y v2 en el mismo panel.

Conexión de alimentación Auxiliar

El panel de control puede proveer un máximo de 700mA de corriente para módulos, detectores alimentados, relés, Leds, etc. Si la corriente total necesaria excede 700mA, es necesaria una fuente de alimentación adicional (por ejemplo, PC5200, PC5204).

Las tensiones máximas y mínimas de operación para los dispositivos, sensores y módulos son de 9,5 VCC - 14 VCC

Conexión de línea telefónica

Se debe conectar terminales de teléfono (TIP, Ring, T-1, R-1) a un conector RJ-31x, según lo indicado en el manual. Por lo general se utiliza un hilo de 26 AWG, como mínimo, para la conexión. Para la conexión de múltiples dispositivos a la línea telefónica, hay que llamar en la secuencia indicada en el manual.

Grabador digital de 500 GB FW5071

El grabador digital FW-5071 de 8 canales con disco duro incluido de 500 Gb puede grabar las cámaras de red IP de diferentes marcas como son: Flexwatch, Axis, Panasonic, Mobotix, Arecont, IQinvision, Vivotek, entre otras. Esta característica le da una gran flexibilidad al momento de su configuración en los sistemas de vigilancia.

Características destacadas:

- Solución profesional 100% intuitiva.
- Nueva interfaz mejorada.
- Grabación de imágenes y audio.

- Conversión fácil de grabaciones a formato .AVI.
- Servicio de enlace de IP dinámica.
- Visualización en dispositivos móviles PDA.
- Log (registro del sistema).
- Gestión y actualización completa del sistema a través de Internet.
- Sistemas totalmente ampliables.
- Conexión 100% segura.

El grabador digital unifica la capacidad del protocolo de comunicación, que permite todas las funcionalidades tales como visión en tiempo real, reproducción y configuración a través de un puerto HTTP.

Puede grabar el video en los formatos H.264, MPEG-4, o MJPEG. Cada canal de vídeo permite configuración individual, que significa que cada canal puede funcionar con diferentes velocidades de fotogramas por segundo, compresión, y resolución. Esto da a los usuarios la máxima flexibilidad en el modo multi-streaming.

FW-5071 puede grabar hasta 120 secuencias por segundo en la resolución D1. La visualización en directo, grabación digital, reproducción, y función back up pueden funcionar simultáneamente. En modo de reproducción, los ocho canales de vídeo se pueden ver al mismo tiempo. El vídeo, el audio y los datos se pueden grabar juntos. En modo de visionado a través de internet en tiempo real, los ocho canales de vídeo, el audio, y los datos se pueden ver simultáneamente.

Grabador digital FW-5071 permite asignar diferentes niveles de permiso de acceso individual a cada canal de video de modo que la accesibilidad se puede controlar por separado. El permiso de niveles múltiples se puede aplicar para el visionado en tiempo real, PTZ, DI/DO, y control de audio respectivamente.

Cuenta con un interfaz de red de Ethernet 10/100/100BASE-T así que puede ser utilizado en cualquier ambiente de red de alta velocidad, y lo utiliza para transferencias de 120 fps en modo D1 de streaming de vídeo en multi-formato.

El grabador de cámaras IP permite la mayor parte de los usos del CMS de las marcas principales en la industria de la vigilancia, así que puede ser incorporado flexiblemente en cualquier tipo de sistema de vigilancia con éxito. Su compatibilidad cubre varios protocolos de red incluyendo HTTP, RTP/RTSP, transmisión de Unicast /Multicast, y así sucesivamente.

El protocolo incorporado en el dispositivo PTZ (movimiento y zoom) permite más de 30 marcas, que incluye Pelco, Kalatel, Sony, Panasonic, Canon, Honeywell, etc. Esta característica se aplica a todos los canales respectivamente.

Ficha técnica:

Sistema de Hardware: 32bit RISC CPU / Linux embebido / 128Mb SDRAM / 8Mb Flash.

Visualización en red: Visionado de imágenes en directo, control de PTZ y búsquedas de grabaciones, directamente a través del navegador Internet Explorer. [Requisitos mínimos: Windows XP, 2000, Vista / IE 6.x o sup.]

Cámaras IP compatibles: FlexWATCH, Axis, Arecont, Panasonic, Vivotek, Mobotix, IQinVision.

Canales de vídeo: 1~8 cámaras IP

Soporte de grabación: 1 Disco duro SATA incluido. Soporta hasta 1500Gb. Anti vibración y ventilación por aire.

Gestión de HDD:

Notificación de disco lleno por e-mail.

Notificación periódica de estado de disco por e-mail.

Notificación de error por e-mail.

Notificación sonora de error (sólo localmente).

Sistema de grabación: MJPEG/MPEG-4/H.264. Máx. 100fps en resolución D1 (704x576); G.723 (4bit, 8KHz), ADPM IMA; POS, ATM, Vídeo Analytics, Controles de acceso y diferentes dispositivos serie.

Condiciones de grabación: Basadas en múltiples combinaciones de fecha, hora, detección de movimiento y alarma de entrada digital, utilizando las condiciones "AND" & "OR".

Tasa de frames de grabación: 2 modos de tasa de frames (rápido por evento / lento en modo de grabación continua) Hasta 100pfs en formato D1 (23kb).

Búsqueda de grabaciones: Basada en múltiples combinaciones de fecha, hora, evento, utilizando las condiciones "AND" & "OR".

Reproducción de grabaciones: Play, avance y retroceso rápido, avance y retroceso paso a paso, pausa y stop.

Reproducción sincronizada: El vídeo grabado de las 8 cámaras IP puede ser reproducido simultáneamente.

Ancho de banda gestionable: Control de tasa de frames / Control de ancho de banda.

PTZ support: Compatible con más de 30 protocolos: Pelco, Vicon, Kalatel, Sony, Panasonic, Canon, Honeywell, etc...

Seguridad: Sistema basado en REGISTRO DE USUARIOS con permisos o restricciones para visionado en tiempo real, control PTZ, salida de alarma y audio.

Función de seguridad: Acceso al servidor protegido por contraseña.

Conexiones: 1 puerto LAN (10/100/1000-Base-T Ethernet Interface), 1 puerto COM.

Protocolos compatibles: HTTP, TCP/IP, ARP, ICMP, Telnet, FTP, PPPoE, SMTP, DHCP, NTP, uPNP.

Alimentación: SMPS 12V (5A) AC100-240V, 50/60Hz.

Consumo: Normal: 1.0 / Peak: 1.8.

Temperatura de trabajo: Desde 5 ° hasta 50° C.

Humedad de trabajo: Desde 20% hasta 80 %.

Dimensiones: 224 mm (largo) x 140 mm (ancho) x 44 mm (grosor), 950 gramos sin alimentador.



Gráfico 6. 19: Grabador digital
Tomado de: Manual de usuario de FW5071

Sirena blindada

Se determinó recomendar la sirena “Ss-101a” de la marca DSC puesto que ofrece protección a la intemperie y por su tamaño se lo puede colocar estratégicamente.

A continuación detallamos sus características.

- Ruido: 128db
- Frecuencia: 1850hz
- Tono de la sirena: yelp
- Rango de frecuencia: 1300-2400hz
- Linterna: Lámpara 12vdc/5w
- Suministro de energía de voltaje: 13.8-14.2vdc
- Carga límite de corriente: 250ma
- Consumo de corriente(altavoz y la luz estroboscópica): Modo de espera: 8ma, Alarma en 1600ma 13.8 vdc
- Máxima potencia: 30w
- Nivel de disparo: Gatillo low=max. Vdc 1, Gatillo high=min. Vdc 9
- Sirena de alarma período: F. T- seguir gatillo, Tmr-3 min
- Impedancia de entrada(alarma/flash/gatillo): ohm 1k
- Interruptor de sabotaje: N. C 28 vdc corriente máxima 0.1a- abierta cuando la cubierta se quita.
- Batería de copia de seguridad: Recargable de plomo ácido de la batería 12 vdc hasta 1.3ah
- Nivel de batería baja: 8vdc+/- 0.3 vdc
- Dimensiones de la unidad: L=270mm*w=193mm*h=100mm
- Peso(sin batería): 1.85kg
- Rango de temperatura: A-30 +60& deg; c
- Nivel de protección: resistente a salpicaduras de agua, plástico con protección uv.



Gráfico 6. 20: sirena Ss-101a
Tomado de: Manual de usuario de Ss 101a

Detectores de movimiento

Se recomienda el detector “DSC LC-123-PIMSK” debido a sus múltiples beneficios ofrecidos.

Sus características principales son que utiliza una lente óptica especialmente diseñado junto con un sensor PIR especial Quad (de cuatro elementos) y un nuevo circuito integrado de aplicación específica (ASIC) optimizado para eliminar las falsas alarmas provocadas por pequeños animales y mascotas. Además proporciona un grado de inmunidad sin precedente contra la luz visible.



Gráfico 6. 21: Detector de movimiento LC 123 PIMSK
Tomado de: Manual de usuario de LC 123 PIMSK

Contactos magnéticos

Se ha considerado el modelo “SM-205Q”.

Dentro de las características principales puedo indicar:

Contacto magnético autoadhesivo montado sobre superficies con guías que salen de un lado, para circuitos de lazo cerrado, con cables 15" (38cm) los plomos extienden de extremo del contacto, SM-204M -- Imanes solamente para SM-204, SM-205Q, abertura: 1" (25mm).



Gráfico 6. 22: Contacto magnético SM-205Q
Tomado de: Manual de usuario de SM-205Q

Estaciones manuales de incendio

Se procedió a escoger la estación "FMM-325A" que es una estaciones manual Analógica de la compañía BOSH.

Dentro de sus principales características tenemos que es compatible con el protocolo de comunicación digital avanzada, comunicación de datos digitales y alimentación proporcionada a través de un circuito de dos cables, asignación de direcciones EEPROM en la unidad de módulo, carcasa inyectada resistente y construcción resistente a la corrosión.



Gráfico 6. 23: Estación manual de incendio FMM-325A
Tomado de: Manual de usuario de FMM 325A

Sirena interna con luz estroboscópica

Debido a sus excelentes características se tomó la sirena PC1616 de la empresa DSC.

Dentro de las características más importantes podemos anotar que el rango de temperatura de 0°C a 49°C, una humedad relativa de 93%, consume de corriente de 110mA.

6.7 PRESUPUESTO

Analizando algunos proveedores de equipos con tecnologías IP y observando los requerimientos necesarios, se obtiene el siguiente presupuesto para el sistema de gestión de red alternativo, que optimice la comunicación para la seguridad, en la infraestructura física de la Universidad Técnica de Ambato.

CAN T	DETALLE	PRECI O	TOTAL
15	PANEL DE CONTROL POWER 1832 INTEGRAL DSC INCLUYE COMUNICADOR IPTECLADO, BATERIA Y TRANSFORMADOR	\$ 550,00	\$ 8.250,00
52	DETECTORES DE MOVIMIENTO	\$ 28,00	\$ 1.456,00
25	CONTACTOS MAGNETICOS	\$ 12,00	\$ 300,00
15	SIRENA BLINDADA 30 W	\$ 48,00	\$ 720,00
24	ESTACIONES MANUALES DE INCENDIO	\$ 45,00	\$ 1.080,00
24	SIRENA INTERNA CON LUZ ESTREBOSCOPICA	\$ 55,00	\$ 1.320,00
1	CENTRAL DE MONITOREO DE ALARMAS CON 2 LINEAS TELEFONICAS Y COMUNICADOR IP	\$ 8.800,00	\$ 8.800,00
SUBTOTAL			\$ 21.926,00
I.V.A. 12%			\$ 2.631,12
TOTAL:			\$ 24.557,12

Tabla 6. 18: Presupuesto
Elaborado por: El investigador

6.8 CONCLUSIONES

De la propuesta se concluye que la tecnología más adecuada para la optimización de recursos y personal para el mejoramiento de la comunicación de la seguridad de la infraestructura es el monitoreo utilizando tecnología IP, ya que se aprovecha la red existente y su interconexión es factible con los diversos equipos instalados.

La red IP existente en el campus Huachi se encuentra en buenas condiciones, por lo que es factible utilizar la misma para el sistema de seguridad y así poder optimizar recursos, esta a su vez permite interconectar con la red que se plantea en las diferentes facultades y así poder tener el control absoluto de toda la infraestructura.

La parte más vulnerable se localiza en la falta de un sistema alternativo de energía eléctrica o back up, ya que no existe respaldo al momento de ausencia de energía eléctrica, dejando desamparado los sistemas de seguridad; otro punto vulnerable es que no existe control sobre los insumos tecnológicos cuando son sacados de los laboratorios.

En la propuesta se tiene un presupuesto estimativo para la implementación de la red IP de seguridad del Campus Huachi de la Universidad Técnica de Ambato, de acuerdo al tiempo en que se realizó la investigación, tomando en cuenta que pueden variar las características y precios de acuerdo al avance tecnológico.

6.9 RECOMENDACIONES

Se recomienda realizar la centralización del sistema de seguridad según la propuesta planteada en la presente investigación, pues esto ayudara a mejorar significativamente a controlar el hurto dentro de los predios universitarios y optimizara los recursos económicos y humanos.

Ocupar como base del proyecto la red IP existente en la Universidad Técnica de Ambato para implementar el sistema de seguridad, manteniendo los números IP asignados a las diferentes facultades.

Implementar un sistema de respaldo de energía eléctrica, para que el sistema de seguridad funcione cien por ciento operativo durante las veinte y cuatro horas del día.

Adquirir los equipos y materiales lo antes posible, para no tener problemas de compatibilidad de equipos y cambio en el presupuesto.

BIBLIOGRAFÍA

- ACCID. (2010). *MANUAL DE CONTROL DE GESTION*. Barcelona, España: Profit Editorial.
- Acuña Garcia, E., & Caicedo Urresta, V. (2005). “*GESTIÓN DE REDES DE UN CENTRO DE COMPUTO UTILIZANDO PROTOCOLO SNMP/RMON*”. Ambato: UTA.
- Alonso Revenga, J. (2008). *FLUJO EN REDES Y GESTION DE PROYECTOS*. La Coruña, España: Netbiblo.
- Alonso, J. M. (2004). *SISTEMAS DE SEGURIDAD Y CONFORTABILIDAD*. mADRID: Paraninfo.
- Antonio Jesús, L. (2004). *AUXILIARES DE SEGURIDAD DE LA JUNTA DE ANDALUCIA*. Sevilla, España: Mad S. L.
- Avogadro, M. (2012). *COMUNICACION Y SEGURIDAD*. Recuperado el 4 de Mayo de 2013, de RAZON Y PALABRA: http://www.razonypalabra.org.mx/comunicarte/2011/feb_comunicacionysseguridad.html
- Barba Martí, A. (2009). *Gestión de red*. Barcelona: Edicions upc.
- Caballero, J. (2008). *REDES DE BANDA ANCHA*. Barcelona, España: Marcombo S.A.
- Cespedes Alvarez, M. (15 de Abril de 2013). *LA IMPORTANCIA DE LA COMUNICACION PARA LA SEGURIDAD*. Recuperado el 6 de Mayo de 2013, de REVISTA MAXIMA SEGURIDAD: <http://www.maximaseguridad.co/index.php/seguridad/salud-ocupacional/item/247-la-importancia-de-la-comunicacion-para-la-seguridad>
- Correa, D., & Agudelo, W. (7 de Septiembre de 2009). *GESTION DE RED EN SOFT PERFECT NETWORK SCANNER*. Recuperado el 5 de Junio de 2013, de <http://www.slideshare.net/diegoc88/tutorial-soft-perfect-network-scanner>
- De Pablos Heredero, C., Lopez Hermoso, J., Martin-Romo Romero, S., & Medina Salgado, S. (2011). *ORGANIZACION Y TRANSFORMACION DE LOS*

- SISTEMAS DE INFORMACION EN LA EMPRESA* (Primera ed.). Madrid, España: ESIC Editorial.
- Diccionario. (s.f.). *Definicion*. Obtenido de <http://definicion.de/guia/>
- edificación, C. d. (2008). *SEGURIDAD INDUSTRIAL* (Segunda ed.). Liteam.
- GESTION DE RED*. (s.f.). Recuperado el 15 de Abril de 2013, de WIKIPEDIA: http://es.wikipedia.org/wiki/Gesti%C3%B3n_de_red
- Gormaz Gonzales, I. (2007). *TECNICAS Y PROCESOS EN LAS INSTALACIONES SINGULARES EN LOS EDIFICIOS* (Segunda ed.). Madrid: Paraninfo.
- GROUP, B. (s.f.). *bsi*. Recuperado el 16 de Mayo de 2013, de <http://www.bsigroup.com.mx/es-mx/Auditoria-y-Certificacion/Sistemas-de-Gestion/De-un-vistazo/Que-son-los-sistemas-de-gestion/>
- Herrera, H. (11 de Enero de 2013). Estructura de una Central de Monitoreo de Alarmas: Topología y tendencias. *Magazin Digital*, 6.
- Hidalgo Gallo, E. (2012). “*SISTEMA CCTV (CIRCUITO CERRADO DE TELEVISIÓN) ENTRE EDIFICIOS, PARA LA SEGURIDAD Y VIGILANCIA EN EL AEROPUERTO INTERNACIONAL COTOPAXI*”. Ambato: UTA.
- IMPLEMENTACION SIG*. (s.f.). Recuperado el 18 de Mayo de 2013, de <http://www.implementacionsig.com/index.php/23-noticiac/28-que-es-un-sistema-de-gestion>
- Mora, H. (2012). *MANUAL DEL VIGILANTE DE SEGURIDAD* (Tercera ed., Vol. 1). Alicante, España: Club Universitario.
- Moreno Leon, J., & Ruiz Padilla, R. (Mayo de 2012). *PLANIFICACION Y ADMINISTRACION DE REDES SNMP*. Recuperado el 30 de Abril de 2013, de Slide Share: <http://www.slideshare.net/jmorenol/snmp-12911648>
- Ogalla Segura, F. (2005). *SISTEMA DE GESTION UNA GUIA PRACTICA*. Ediciones Diaz de Santos.
- Pérez Fernandez de Velasco, J. A. (Julio 2012). *GESTION POR PROCESOS* (Quinta ed.). Madrid, España: ESIC Editorial.
- Rodriguez Fernandez, J. (2012). *INSTALACIONES DOMOTICAS* (Primera ed.). Madrid, España: Paraninfo.

- Rodriguez Penin, A. (2012). *SISTEMAS SCADA* (Tercera ed.). Barcelona, España: MARCOMBO.
- Ros Marin, J., & Barrera Doblado, O. (2011). *SISTEMAS ELECTRICOS Y DE SEGURIDAD Y CONFORTABILIDAD*. Madrid: Parafino S.A.
- Saavedra Silveira, R. (2009). *AUTOMATIZACION DE VIVIENDAS Y EDIFICIOS*. Barcelona: Ceac.
- Share, S. (2012). *SLIDESHARE*. Recuperado el 19 de Mayo de 2013, de <http://www.slideshare.net/ing.adolfo/gestion-de-redes>
- Stallings, W. (2004). *FUNDAMENTOS DE SEGURIDAD EN REDES APLICACIONES Y ESTANDARES* (Segunda ed.). Madrid, España: Pearson Educacion S. A.
- Verón Piquero, J. (2009). *PRACTICA DE REDES*.
- Zimmermann, A. (2004). *LA GESTION DE REDES, CAMINOS Y HERRAMIENTAS*. Quito: Abya - Yala.

ANEXOS

ANEXO A

ANEXO 1A.

Encuesta 1.

ENCUESTA DIRIGIDA AL PERSONAL DEL DISIR – UTA.

Sr/Srta. Ingeniero/a.

Buenos días, como parte de mi tesis de maestría en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, estoy realizando una investigación acerca de la estructura del sistema de gestión de red para la comunicación de la seguridad, de la infraestructura física de la Universidad Técnica de Ambato. La información brindada en esta encuesta es de carácter confidencial, solo será utilizada para los propósitos de la investigación. Agradezco su colaboración.

Objetivo: La presente encuesta tiene por objeto, recopilar información para ver el grado de seguridad, control y el tiempo de respuesta que tiene la Universidad Técnica de Ambato.

DATOS GENERALES

Fecha de la encuesta:

Instructivo:

- Seleccione una sola respuesta en cada pregunta, marcando con en  el espacio correspondiente.
- Sea lo más sincero y objetivo posible

1.- ¿Cuenta la Universidad con un proceso de planificación para tomar acciones y conductas para monitorear un evento de seguridad?

- ☐ Totalmente de acuerdo
- ☐ De acuerdo
- ☐ Ni de acuerdo, ni en desacuerdo
- ☐ En desacuerdo
- ☐ Totalmente en desacuerdo

2.- ¿Existen elementos necesarios y suficientes para observar los procesos de seguridad en la Universidad?

Totalmente de acuerdo

De acuerdo

Ni de acuerdo, ni en desacuerdo

En desacuerdo

Totalmente en desacuerdo

3.- ¿La institución posee recursos necesarios y suficientes para una administración sostenible del sistema de seguridad?

☐ Totalmente de acuerdo

☐ De acuerdo

☐ Ni de acuerdo, ni en desacuerdo

☐ En desacuerdo

☐ Totalmente en desacuerdo

4.- ¿El sistema de seguridad tiene una red adecuada y actualizada en los predios universitarios?

☐ Totalmente de acuerdo

☐ De acuerdo

☐ Ni de acuerdo, ni en desacuerdo

☐ En desacuerdo

☐ Totalmente en desacuerdo

5.¿Qué porcentaje de cobertura de seguridad tiene la infraestructura de la Universidad Técnica de Ambato?

☐ Menos del 20%

☐ Entre el 20% y 40%

☐ Entre el 40% y 60%

☐ Entre el 60% y 80%

☐ Más del 80%

¡GACIAS POR SU COLABORACION Y TIEMPO!

ANEXO 2A.

Encuesta 2.

ENCUESTA DIRIGIDA A LOS ADMINISTRADORES DE REDES DE LA UNIVERSIDAD TÉCNICA DE AMBATO.

Sr/Srta. Administrador/a

Buenos días, como parte de mi tesis de maestría en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, estoy realizando una investigación acerca de la estructura del sistema de gestión de red para la comunicación de la seguridad, de la infraestructura física de la Universidad Técnica de Ambato. La información brindada en esta encuesta es de carácter confidencial, solo será utilizada para los propósitos de la investigación. Agradezco su colaboración.

Objetivo: La presente encuesta tiene por objeto, recopilar información para ver el grado de seguridad, control y el tiempo de respuesta que tiene la Universidad Técnica de Ambato.

DATOS GENERALES

Facultad:

Fecha de la encuesta:

Instructivo:

- Seleccione una sola respuesta en cada pregunta, marcando con en ☒ el espacio correspondiente.
- Sea lo más sincero y objetivo posible

1.- ¿Cuenta la Facultad con un proceso de planificación para tomar acciones y conductas para monitorear un evento de seguridad?

- ☐ Totalmente de acuerdo
- ☐ De acuerdo
- ☐ Ni de acuerdo, ni en desacuerdo
- ☐ En desacuerdo
- ☐ Totalmente en desacuerdo

2.- ¿Existen elementos necesarios y suficientes para observar los procesos de seguridad en la Facultad?

- ☐ Totalmente de acuerdo
- ☐ De acuerdo
- ☐ Ni de acuerdo, ni en desacuerdo
- ☐ En desacuerdo
- ☐ Totalmente en desacuerdo

3.- ¿La unidad académica posee recursos necesarios y suficientes para una administración sostenible del sistema de seguridad?

- ☐ Totalmente de acuerdo
- ☐ De acuerdo
- ☐ Ni de acuerdo, ni en desacuerdo
- ☐ En desacuerdo
- ☐ Totalmente en desacuerdo

4.- ¿El sistema de seguridad tiene una red adecuada y actualizada en los dominios de la facultad?

- ☐ Totalmente de acuerdo
- ☐ De acuerdo
- ☐ Ni de acuerdo, ni en desacuerdo
- ☐ En desacuerdo
- ☐ Totalmente en desacuerdo

5.¿Qué porcentaje de cobertura de seguridad tiene la infraestructura de la Facultad?

- ☐ Menos del 20%
- ☐ Entre el 20% y 40%
- ☐ Entre el 40% y 60%
- ☐ Entre el 60% y 80%
- ☐ Más del 80%

¡GACIAS POR SU COLABORACION Y TIEMPO!

ANEXO 3A.

Encuesta 3.

ENCUESTA DIRIGIDA AL PERSONAL DE SEGURIDAD DE LA UNIVERSIDAD TÉCNICA DE AMBATO

Señores guardias.

Buenos días, como parte de mi tesis de maestría en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, estoy realizando una investigación acerca de la estructura del sistema de gestión de red para la comunicación de la seguridad, de la infraestructura física de la Universidad Técnica de Ambato. La información brindada en esta encuesta es de carácter confidencial, solo será utilizada para los propósitos de la investigación. Agradezco su colaboración.

Objetivo: La presente encuesta tiene por objetivo recopilar información para ver el grado de seguridad, control y el tiempo de respuesta, según la ubicación del Señor guardia en el caso de un evento de emergencia.

DATOS GENERALES:

Cargo:

Fecha de la encuesta:

Instructivo:

- Seleccione una sola respuesta en cada pregunta, marcando con un ☒ en el espacio correspondiente.
- Sea lo más sincero y objetivo posible.

1.- ¿Considera Usted que el sistema de comunicación interno es?

- ☐ Excelente
- ☐ Muy Bueno
- ☐ Bueno
- ☐ Regular
- ☐ Malo

2.- ¿En el caso de una emergencia, a su conocimiento el reporte le llega?

- ☐ De inmediato.
- ☐ Dentro de los 5 primeros minutos.
- ☐ Dentro de los 15 minutos.
- ☐ Dentro de 1 hora.
- ☐ Después de 1 hora.

3.- ¿Cuándo suena la alarma en una dependencia o edificio, el tiempo que se demora en encontrar donde está focalizado el problema es?

- ☐ De inmediato
- ☐ Dentro de los 5 minutos.
- ☐ Dentro de los 15 minutos.
- ☐ Dentro de 1 hora.
- ☐ Después de 1 hora.

4.- ¿Tienen algún sistema de requisas para los vehículos que ingresan o salen de la institución?

- ☐ Si
- ☐ No

5.- ¿Tienen alguna identificación, los vehículos de los docentes, alumnos o visitantes de la institución?

- ☐ Totalmente de acuerdo
- ☐ De acuerdo
- ☐ Ni de acuerdo, ni en desacuerdo
- ☐ En desacuerdo
- ☐ Totalmente en desacuerdo

6.- ¿En su turno, que tiempo se demora en volver a pasar por el mismo punto?

- ☐ Antes de 5 minutos
- ☐ Entre 5 y 15 minutos
- ☐ Entre 15 y 30 minutos
- ☐ Entre 30 y 60 minutos
- ☐ Después de 1 hora

7.- ¿Cree Usted, que el actual sistema de seguridad es satisfactorio?

- ☐ Totalmente de acuerdo
- ☐ De acuerdo
- ☐ Ni de acuerdo, ni en desacuerdo
- ☐ En desacuerdo
- ☐ Totalmente en desacuerdo

8.- ¿Qué tan confiable es el sistema de seguridad actual?

- ☐ Excelente
- ☐ Muy Bueno
- ☐ Bueno
- ☐ Regular
- ☐ Malo

9.- ¿En caso de detectar alguna anomalía dentro de los predios universitarios, (Persona sospechosa, vidrio bajado de un auto, puerta abierta de un vehículo, persona con proyector o laptops en sus brazos, personas con bultos grandes, etc.) que procedimiento realiza? (Varias opciones)

9.1.- En caso de personas:

- ☐ Lo interroga
- ☐ Lo detiene
- ☐ Notifica a su superior
- ☐ Ninguno
- ☐ Otros.....

9.2.- En caso de objetos:

- ☐ Notifica al dueño.
- ☐ Busca solución
- ☐ Notifica a su superior.
- ☐ Ninguno
- ☐ Otros.....

¡GARCIAS POR SU COLABORACION Y TIEMPO!

ANEXO 4A.

Entrevista 1.

ENTREVISTA REALIZADA AL INGENIERO FERNANDO GARCÉS, DIRECTOR DEL DISIR – UTA Y AL TECNÓLOGO RUBÉN MOREJÓN, JEFE DE GUARDIAS DE LA UTA.

Señor director.

Buenos días, como parte de mi tesis de maestría en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, estoy realizando una investigación acerca de la estructura del sistema de gestión de red para la comunicación de la seguridad, de la infraestructura física de la Universidad Técnica de Ambato. La información brindada en esta encuesta es de carácter confidencial, solo será utilizada para los propósitos de la investigación. Agradezco su colaboración.

Objetivo: La presente entrevista tiene por objeto, recopilar información para ver el grado de seguridad, control y el tiempo de respuesta que tiene la Universidad Técnica de Ambato.

DATOS GENERALES:

Nombre:

Cargo:

Fecha de la entrevista:

1.- ¿Ingeniero, en estos momentos, tiene la Universidad un proceso de planificación para tomar acciones y conductas para monitorear un evento de seguridad?

2.- ¿Actualmente, existen elementos necesarios y suficientes para observar los procesos de seguridad?

3.- ¿La institución posee recursos necesarios y suficientes para una administración sostenible del sistema de seguridad?

4.- ¿El sistema de seguridad tiene una red adecuada y actualizada?

5.- ¿Qué porcentaje de cobertura de seguridad tiene la infraestructura de la Universidad Técnica de Ambato?

6.- ¿Cómo considera Usted que en la actualidad se encuentra el sistema de comunicación interno?

7.- ¿En el caso de que suceda una emergencia, en que tiempo se lo hace conocer?

8.- ¿Al momento tienen algún sistema de requisas para los vehículos que ingresan o salen de la institución?

9.- ¿Se ha pensado en poner alguna identificación para los vehículos de los docentes, alumnos o visitantes de la institución? Sea en el vehículo o en el predio.

10.- ¿Cree Usted, que el actual sistema de seguridad que se maneja en la Universidad, es satisfactorio?

11.- ¿Qué tan confiable es el sistema de seguridad actual, tienen un buen control?

12.- ¿En caso de detectar alguna anomalía dentro de los predios universitarios, (Persona sospechosa, vidrio bajado de un auto, puerta abierta de un vehículo, persona con proyector o laptops en sus brazos, personas con bultos grandes, etc.) que procedimiento o protocolo se realiza en la institución?

¡GACIAS POR SU COLABORACION Y TIEMPO!