UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

"AUDITORÍA DE SEGURIDAD INFORMÁTICA EN LA RED INTERNA DE LA UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI, BASADA EN LA NORMA ISO/IEC 27001 Y LA METODOLOGÍA OSSTMMv3"

AUTOR: ANDERSON HUMBERTO AZA MIMALCHI

DIRECTOR DE TESIS: ING. EDGAR ALBERTO MAYA OLALLA, MSc.

IBARRA-ECUADOR

2019

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

IDENTIFICACIÓN DE LA OBRA

La UNIVERSIDAD TÉCNICA DEL NORTE dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO		
Cédula de identidad:	0401873096	
Apellidos Y Nombres:	Aza Mimalchi Anderson Humberto	
Dirección:	Barrio Jardín del Norte, Calle las Palmas y Ensueños	
E-mail:	ahaza@utn.edu.ec	
Teléfono:	Fijo: 290522	Móvil**:** 0967117986
DATOS DE LA OBRA		
Título	**“AUDITORÍA DE SEGURIDAD INFORMÁTICA EN LA RED INTERNA DE LA UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI, BASADA EN LA NORMA ISO/IEC 27001 Y LA METODOLOGÍA OSSTMMv3”**	
Autora:	Aza Mimalchi Anderson Humberto	
Fecha:	2019/03/22	
Título por el que opta:	Ingeniería en Electrónica y Redes en Comunicación	
Director	Ing. Edgar Maya, MSc.	

AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Anderson Humberto Aza Mimalchi, con cédula de identidad Nro. 0401873096, en calidad de autora y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en formato digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión; en concordancia con la Ley de Educación Superior Artículo 144.

CONSTANCIAS

La autora manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es las titulares de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

En la ciudad de Ibarra,

.....

El Autor:

Anderson Humberto Aza Mimalchi
C.I. 040187309-6

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, Anderson Humberto Aza Mimalchi, con cédula de ciudadanía Nro. 040187309-6, expreso mi voluntad a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de propiedad intelectual del Ecuador, Artículo 4, 5 y 6 en calidad de autores de la obra o trabajo de grado denominado: **"AUDITORÍA DE SEGURIDAD INFORMÁTICA EN LA RED INTERNA DE LA UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI, BASADA EN LA NORMA ISO/IEC 27001 Y LA METODOLOGÍA OSSTMMv3",** que ha sido desarrollada para optar el Título de Ingeniería en Electrónica y Redes de Comunicación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En mi condición de autor me reservo los derechos morales de la obra antes citada, aclarando que el trabajo aquí descrito es de mi autoría y que no ha sido previamente presentado para una calificación profesional.

En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

.....

Firma
Anderson Humberto Aza Mimalchi
C.I. 040187309-6
Ibarra, Marzo 2019

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DECLARACIÓN

Yo, Anderson Humberto Aza Mimalchi, con cédula de ciudadanía nro. 040187309-6, estudiante de la carrera de Ingeniería en Electrónica y Redes de Comunicación, libre y voluntariamente declaro bajo juramento que el trabajo aquí descrito es de mi autoría; y que este no ha sido previamente presentado para ningún grado o calificación profesional, para efectos académicos y legales será de mi responsabilidad.

A través de la presente declaración cedo los derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Técnica del Norte, según lo establecido por las leyes de propiedad intelectual, del reglamento y normativa vigente de la Universidad Técnica del Norte.

.....

Anderson Humberto Aza Mimalchi

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

Certifico que el presente trabajo de titulación **"AUDITORÍA DE SEGURIDAD INFORMÁTICA EN LA RED INTERNA DE LA UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI, BASADA EN LA NORMA ISO/IEC 27001 Y LA METODOLOGÍA OSSTMMv3"** ha sido realizada en su totalidad por el señor: Anderson Humberto Aza Mimalchi portador de la cédula de identidad con número: 040187309-6 bajo mi supervisión.

Es todo en cuanto puedo certificar en honor a la verdad.

.....

Ing. Edgar Maya, MSc

DEDICATORIA

La presente investigación está dirigida a mis padres: Segundo Humberto Aza Vallejo y Beatriz del Carmen Mimalchi Canchala, a mis hermanos y hermanas, quienes supieron apoyarme en cada instante para culminar esta etapa, de manera especial este trabajo lo dedico a Janneth Benavides mi compañera de vida quien se ha convertido en mi soporte en este largo camino, y a mi hijo Jayden Sebastián Aza Benavides, desde que llego a formar parte de mi vida se convirtió en mi mayor razón para poder terminar esta meta, a todos ellos por su paciencia y comprensión.

Con gratitud

Anderson H. Aza

AGRADECIMIENTO

Agradezco a Dios por haberme dado vida y salud para poder culminar una etapa más de mi formación profesional. A la universidad Técnica del Norte por haberme abierto las puertas para seguir instruyéndome en la carrera de Ingeniería en Electrónica y Redes de Comunicación.

A mis padres, hermanos y hermanas por haber sido mi sustento económico y mi apoyo incondicional durante este periodo, gracias por la confianza que depositaron en mí en todo momento.

A las autoridades del Centro de TIC's de la UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI por dar acceso a las instalaciones y sea factible realizar el estudio, a ellos mis más sinceros agradecimientos.

Al Magister Edgar Maya, por haberme orientado y despejado en los momentos de confusión y dudas, quien con su tiempo, paciencia, constancia, conocimientos, esfuerzo y recomendaciones supo ayudarme y guiarme de manera desinteresada para que se lleve a cabo esta investigación.

A todos los docentes quienes formaron parte de mi vida estudiantil universitaria, ellos que supieron compartir sus conocimientos dentro y fuera del aula, haciendo de mí un profesional con ética y moral. Gracias infinitas al MSc. Luis Suarez y al MSc. Fabián Cuzme por aportar con sus consejos y conocimientos para terminar este proyecto.

Anderson H. Aza

ÍNDICE DE CONTENIDOS

ÍNDICE DE IMÁGENES

ÍNDICE DE TABLAS

ÍNDICE DE ECUACIONES

ÍNDICE DE DIAGRAMAS DE FLUJO

RESUMEN

La seguridad informática es muy importante para garantizar la confiabilidad, disponibilidad e integridad de la información. Sin embargo en la actualidad la posibilidad de sufrir un ataque cibernético es cada vez mayor, es por esto que en la Universidad Politécnica Estatal del Carchi es necesario la aplicación de una auditoria de seguridad informática, pues se han evidenciado algunas vulnerabilidades en su red interna lo cual puede comprometer la información que se maneja en la institución, además de no poseer políticas de seguridad informática que ayuden a proteger los activos e información de la universidad en caso de amenaza o ataque.

El objetivo del estudio fue realizar una auditoría de seguridad informática en la red interna de la Universidad Politécnica estatal del Carchi, con base en la norma ISO/IEC 27001 y la metodología OSSTMMv3 para mejorar la seguridad que posee la red interna de la institución. La auditoría se aplicó a los 5 canales que especifica la metodología, el canal Humano, Físico, Inalámbrico, Telecomunicaciones y Redes de Datos; los cuales se abordaron siguiendo las recomendaciones de OSSTMMv3. Para cada canal se evaluó la seguridad operacional, los controles y limitaciones, mediante la observación, persuasión, encuestas, entrevistas, y el software necesario para obtener los resultados que se representaran de forma numérica para luego ser ingresados en la calculadora RAV de OSSTMMv3 y obtener el valor de la seguridad actual de la institución.

Los resultados obtenidos de la calculadora se detallan en el informe STAR en el cual se incluyen los valores finales y las evidencias de los procedimientos realizados para el análisis de cada canal. Con los resultados se procedió a realizar un informe final que fue entregado al Director del Departamento de TIC'S, además se establecieron políticas de seguridad, que fueron socializadas con el personal del departamento de TIC's, aplicando algunas de ellas para verificar su cumplimiento y aceptación por parte del personal interno de la institución.

ABSTRACT

Computer security is very important to guarantee reliability, availability and integrity of information. Currently, the possibility of a cyber-attack has increased, for this reason in Politecnica Estatal de Carchi University is necessary to apply a computer security audit, as its internal network some vulnerabilities have been evidenced, compromising the information handled at the institution, in addition to not having IT security policies to protect assets and information.

The objective of this research was to perform a computer security audit on the internal network of Politecnica Estatal de Carchi University, based on ISO/IEC 27001 standard and OSSTMMv3 methodology to improve the security of the institution. The audit was applied to the five channels which are considered by the methodology, the Human, Physical, Wireless, Telecommunication and Data Network channels; following recommendations provided by OSSTMMv3. For each channel, safety, controls and limitations were evaluated, through observation, persuasion, surveys, interviews and the necessary software to obtain the results that will be represented in numerical form to be later entered into the RAV calculator of OSSTMMv3 to obtain the value of the current security level of the institution.

The results obtained from the calculator are detailed in the STAR report, which includes the final values and the evidences of the procedures performed for the analysis of each channel. With the results the final report was made and delivered to the ICTs Department Director, and also were established security policies, which were socialized with the ICTs department staff, some of them were applied to verify their compliance and the institution's internal staff acceptance

Victor Rodriguez

CENTRO DE IDIOMAS
UEMPRENDE E.P.
IBARRA - ECUADOR
SECRETARIA

CAPÍTULO I

1. Antecedentes

El presente capítulo presenta de manera breve el por qué es necesario realizar una auditoría de seguridad informática en la red interna de la Universidad Politécnica Estatal del Carchi, con el objetivo de mejorar la seguridad de la red, reconocer los principales problemas y brindar una solución detallada mediante la implementación de políticas de seguridad.

1.1 Tema

Auditoría de seguridad informática en la red interna de la Universidad Politécnica Estatal del Carchi, basada en la norma ISO/IEC 27001 y la metodología OSSTMMv3.

1.2 Problema

La Universidad Politécnica Estatal del Carchi es una institución de educación superior pública y acreditada, que cuenta con una red interna relativamente nueva, la cual es de uso de estudiantes, docentes, personal administrativo y técnico, para realizar las actividades universitarias tales como uso del aula virtual, registro de asistencia, registro de notas, acceso a la página web, entre otras.

En el centro de TIC’s se han reportado problemas de seguridad, pues, se han registrado varios ataques, como la denegación de servicios, específicamente la página WEB y el portafolio estudiantil afectando la confidencialidad, disponibilidad e integridad de estos sistemas. La infraestructura de la red de la Universidad Politécnica Estatal del Carchi cuenta con un firewall Cisco AZA 5220; sin embargo, no cuenta con políticas de seguridad que garanticen la seguridad de la información de ataques internos. Por otra parte, no se ha realizado una auditoría enfocada en seguridad informática, por tal motivo no se tiene

conocimiento de cuáles son las falencias de la red y por ende son propensos a sufrir ataques tales como espionaje, fraude, entre otros.

Se plantea realizar una auditoría de seguridad informática, en la red de la Universidad Politécnica Estatal del Carchi, basada en la norma ISO/IEC 27001 y la metodología OSSTMMv3, la cual cubre, pruebas y análisis de seguridad, indicadores de seguridad operacional, análisis de confianza, métricas operacionales y las tácticas necesarias para definir y construir una buena seguridad en cuanto la protección de los activos ubicados dentro de la red interna de la "Universidad Politécnica Estatal del Carchi".

En resumen, se propone la auditoría, debido a los ataques a los cuales ha sido propensa la universidad, además no cuenta con políticas de seguridad que brinden un buen nivel de confidencialidad, disponibilidad e integridad a sus servicios; por lo que mediante el presente proyecto se podrán identificar las vulnerabilidades de la red interna de la Universidad y se desarrollará las políticas de seguridad necesarias para brindar mayor confiabilidad a la red interna.

1.3 Objetivos

1.3.1 Objetivo General

Realizar una auditoría de seguridad informática en la red interna de la Universidad Politécnica estatal del Carchi, con base en la norma ISO/IEC 27001 y la metodología OSSTMMv3 para mejorar la seguridad que posee la red interna de la institución.

1.3.2 Objetivos Específicos:

Efectuar la fundamentación bibliográfica necesaria, acerca de la metodología OSSTMMv3 y la norma ISO/IEC 27001, las cuales serán usadas en el desarrollo del proyecto.

Detallar la situación actual de la infraestructura de la red interna, la cual consta de todos los activos y su ubicación en la red.

Aplicar la metodología OSSTMMv3 en la infraestructura de la red interna, detallando las pruebas de seguridad, las limitaciones que se tiene y un reporte con los resultados luego de culminar con las etapas de la metodología

Implementar las políticas de seguridad basadas en la norma ISO/IEC 27001, para solucionar las vulnerabilidades encontradas en la red.

1.4 Alcance

El presente proyecto iniciara con la revisión de la metodología, la cual permitirá se desarrolle de manera estructurada y ordenada la auditoría de seguridad informática, se ha escogido la metodología OSSTMMv3 (Open Source Security Testing Methodology Manual).

Se pedirán los respectivos permisos para tener acceso a la información de la Universidad y los activos que se encuentran dentro de la infraestructura de la red interna.

Como primera etapa se empezará con la recolección de la información acerca de los activos de la red, es decir todo lo que se encuentra dentro de la red interna de la Universidad Politécnica Estatal del Carchi. Además, se debe conocer la ubicación exacta de todos estos recursos para determinar en qué parte de la red se encuentran.

La segunda etapa es identificar que software y que hardware son necesarios para la ejecución de cada prueba, teniendo en cuenta que se utilizara herramientas de software libre, además, se debe analizar por separado los 5 canales que estipula en la metodología: Humanos, en los cuales las pruebas se realizaran con la interacción física o psicológica haciendo uso de ingeniería social; Físicos, para abordar este cana las pruebas de seguridad comprenden el elemento tangible de la seguridad donde la interacción requiere esfuerzo físico; Inalámbricos, estas pruebas dependen de los elementos con los cuales cuenta la universidad; Telecomunicaciones, estas pruebas están sujetas a las redes con las que cuenta la universidad, ya sean analógicas o digitales; y Redes de Datos, donde la interacción se lleva a cabo a través de un cable establecido y líneas de la red cableadas. La forma de abordar el análisis de estos canales está estipulada en la metodología que será utilizada en la elaboración de este proyecto. Se establecerán las pautas para llevar a cabo un proceso ordenado durante el tiempo que tome en finalizar la auditoría como tal, para ello se dictan varias pautas a seguir dependiendo del canal que se vaya a probar.

Luego de haber culminado con la etapa anterior, se procederá a la elaboración de un reporte con los resultados obtenidos, detallando las vulnerabilidades encontradas, y la manera de cómo mejorar estas debilidades de la red. Adicional a este reporte se realizarán y se implementarán las políticas de seguridad basadas en la norma ISO/IEC 27001, con las que debe contar la empresa para garantizar la confiabilidad, disponibilidad e integridad de la red interna.

Finalmente se realizará una capitación al personal del departamento de redes con el fin de impartir estas políticas de seguridad para darles un buen uso como mecanismo de defensa en contra de posibles atacantes.

1.5 Justificación

La Universidad Politécnica Estatal del Carchi posee servicios tales como página WEB, portafolio Estudiantil y de docentes, en los cuales se maneja información como trabajos, evaluaciones y notas de los estudiantes, además alberga la información de personal administrativo, docente y estudiantil; por tal motivo es muy importante saber cuáles son las vulnerabilidades que presenta la red y como mejorarlas, logrando así que los servicios, tanto de hardware como de software sean más confiables, tengan un buen desempeño y sobre todo un buen nivel de seguridad garantizando la integridad de la información que manejan.

La auditoría contribuirá a mejorar la seguridad informática, ya que se ejecuta siguiendo la metodología OSSTMMv3 la cual consiste en realizar pruebas de seguridad a 5 canales: Humanos, Físicos, Inalámbricos, Telecomunicaciones y Redes de Datos; y de esta manera descubrir sus vulnerabilidades, además se desarrollaran políticas de seguridad en base a la norma ISO/IEC 27001, la cual verifica independientemente que los riesgos de la organización estén correctamente identificados, evaluados y gestionados.

El personal del área de redes debe estar capacitado, para de esta manera poder aplicar un mecanismo de defensa en contra de intrusos o posibles hackers, contrarrestando los ataques que pudieran suscitarse y tener un plan de contingencia en caso de sufrir un ataque que vulnere la seguridad de la red universitaria.

Con el presente proyecto se busca garantizar la seguridad, confidencialidad e integridad de la información dentro de la red interna de la Universidad Politécnica Estatal del Carchi, por otra parte, al identificar las vulnerabilidades se protegerá a la institución de posibles ataques a su red interna.

CAPÍTULO II

2. Fundamentación Teórica

En este capítulo se desarrolla el fundamento teórico que es necesario para la elaboración del proyecto de titulación. Se analizan los conceptos básicos de una red interna, de la seguridad de datos y de las herramientas necesarias para la realización de la auditoría de seguridad informática. Todo esto mediante el uso de la norma ISO/IEC 27001 y la metodología OSSTMMv3.

2.1 Red Informática

Este término es usado para hacer referencia al conjunto de dispositivos interconectados entre sí a través de diferentes medios de transmisión, para que se realice intercambio de información entre varios usuarios, en el cual existen dos roles bien definidos, el emisor y el receptor. “Las redes informáticas deben ser lo suficientemente efectivas para poder compartir todo tipo de información y recursos que estén disponibles en los dispositivos terminales a los que el usuario accede, proveyendo de herramientas para centralizar o distribuir, según se requiera, las diferentes necesidades informáticas que se pueda tener.”(Katz, 2013)

2.1.1 Componentes de una red

Los principales componentes que forman parte de una red son:

- Estaciones de Trabajo
- Medio de transmisión
- Dispositivos de Red
- Servidores

2.1.1.1 Estaciones de trabajo

Realizan funciones independientes y se contactan con los servidores cuando es necesario, para acceder a los recursos compartidos con los cuales es necesario trabajar. En algunas ocasiones es necesario instalar software específico para acceder a determinados servidores.

2.1.1.2 Medio de transmisión

Mediante este componente se transmite la información, es la conexión física entre los demás componentes de la red. Generalmente se usan medios de transmisión de cobre como el cable UTP, sin embargo, en los últimos tiempos la fibra óptica ha tenido un gran crecimiento en este campo. Adicionalmente a estos medios de transmisión tangibles, se cuenta con la tecnología inalámbrica con la cual se puede interconectar dispositivos utilizando el aire como medio de transmisión.

2.1.1.3 Dispositivos de red

Permiten la conexión de las estaciones de trabajo y los demás componentes de red; dependiendo de la red se utilizan distintos tipos de protocolos y de igual manera se utilizan diferentes dispositivos de red los cuales pueden ser: tarjeta de red, hub, switch, router, modem, etc.

2.1.1.4 Servidores

Este componente tiene como función primordial la gestión de los recursos e información compartida, y pueden ser servidores físicos o software. Además, provee de servicios como página WEB, aplicaciones entre otros.

2.2 Seguridad Informática

A menudo se piensa que seguridad de la información y seguridad informática son lo mismo, sin embargo, son conceptos diferentes pues la seguridad de la información son una serie de medidas y procedimientos, ya sea humanos o técnicos, con el fin de proteger la integridad, confidencialidad y disponibilidad de la información.

Por otra parte, la seguridad informática es una rama de la seguridad de la información que tiene como objetivo proteger la información que haga uso de una infraestructura informática y de telecomunicaciones, ya sea para almacenarla o transmitirla. Según Escrivá, Romero, Ramada, & Onrabia, en su libro "Seguridad Informática" se puede distinguir los siguientes tipos:

- En función de lo que se quiere proteger:

2.2.1 Seguridad Física

Se relaciona a la protección física del sistema ante amenazas tales como desastres naturales, robos, etc.

2.2.2 Seguridad Lógica

Se enfoca a la protección de la parte lógica del sistema informático la cual engloba datos, aplicaciones, sistemas operativos, entre otros.

- En función del momento en el cual se da lugar la protección:

2.2.3 Seguridad Activa

Son medidas preventivas las cuales consisten en detectar y evitar diferentes tipos de incidentes en el sistema con el fin de salvaguardad la información.

2.2.4 Seguridad Pasiva

Son medidas correctivas utilizadas para minimizar las consecuencias de incidentes de seguridad tales como ataques a los servidores.

2.2.5 Conceptos básicos de Seguridad

Para adentrarse en la seguridad informática se maneja terminología específica que se explica a continuación.

2.2.5.1 Activos

Son recursos necesarios para que una empresa u organización alcance sus objetivos, es decir todos los elementos que tengan valor y por ende deban ser protegidos. Por consiguiente, se considera como activos a trabajadores, software, hardware, datos, etc.

La seguridad informática tiene la finalidad de proteger los activos, por tal motivo es imprescindible identificarlos, para de esta manera poder establecer medidas de seguridad de acuerdo a su relevancia para la organización.

Escrivá, Romero, Ramada, & Onrabia, en su libro "Seguridad Informática", define a los activos de una empresa de la siguiente manera:

- **Información**

Se refiere a cualquier elemento que contenga datos almacenados como documentos, libros datos de empleados, manuales, etc.

- **Software**

Son las aplicaciones o programas que son indispensables para el funcionamiento de la empresa, para automatizar los procesos que se llevan a cabo en la misma.

- **Físicos**

Este activo se refiere a la infraestructura tecnológica que posee la empresa, es utilizada para almacenar, gestionar, procesar o transmitir la información que se necesita para que la organización tenga un buen funcionamiento.

- **Personal de la empresa**

Son los empleados que utilizan los recursos tecnológicos y de comunicación para manejar de forma adecuada la información de la empresa.

2.2.5.2 Vulnerabilidades

Una vulnerabilidad se refiere a cualquier debilidad de un activo que pueda afectar el correcto funcionamiento de la red. Estas debilidades pueden estar asociadas a errores en la configuración de los sistemas, descuidos en la utilización de los mismos, mal implementación de aplicaciones, entre otros.

"Las vulnerabilidades de algunas aplicaciones pueden permitir una escalada de privilegios, con lo que un atacante podría conseguir más privilegios de los previstos. Esto podría implicar que en algunos casos llegaran a tener los mismos que los administradores, pudiendo controlar el sistema." (Escrivá Gascó, Romero Serrano, & Ramada, 2013)

Por problemas como el ya mencionado es de vital importancia detectar y corregir las vulnerabilidades, porque constituyen un gran peligro para la seguridad de la red en general.

2.2.5.3 Amenazas

Se considera como amenaza a cualquier situación en la cual se atente contra el buen funcionamiento de un sistema informático. Dependiendo de las acciones realizadas por parte del atacante se puede clasificar a las amenazas como activas y pasivas.

- **Amenazas Pasivas**

Este tipo de amenazas tienen como objetivo obtener información, sin realizar ninguna alteración en el sistema.

- **Amenazas Activas**

Son aquellas que tratan de realizar cambios no autorizados en el sistema, por lo cual son más peligrosas que las anteriores.

Por otra parte, MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) presenta una clasificación diferente:

- Desastres naturales
- Desastres industriales
- Errores y fallos no intencionados
- Ataques deliberados

2.2.5.4 Riesgos

Es la probabilidad de que una amenaza sea materializada, aprovechando las vulnerabilidades con el fin de causar daños en el sistema. Según Escrivá, Romero, Ramada, & Onrabia, en su libro "Seguridad Informática", "existen diferentes niveles de riesgo a los que puede estar expuesto un activo. El nivel dependerá de la probabilidad de que se materialice una amenaza y al grado de impacto producido." Por ejemplo:

Tabla 1: Niveles de riesgo

NIVEL	TIPO DE RIESGO
Alto	Robo de información Robo de hardware
Medio	Accesos no autorizados
Bajo	Inundaciones

Fuente: Escrivá Gascó, Romero Serrano, & Ramada, 2013, pág. 12

2.2.5.5 Ataques

"Un ataque es una acción que trata de aprovechar una vulnerabilidad de un sistema informático para provocar un impacto sobre él e incluso tomar el control del mismo. Se trata de acciones tanto intencionadas como fortuitas que pueden llegar a poner en riesgo un sistema. Un ataque pasa pos las siguientes etapas:" (Escrivá Gascó et al., 2013)

- **Reconocimiento**

En esta etapa se obtiene la información que sea necesaria de la víctima, ya sea una persona o una institución.

- **Exploración**

En este punto se obtiene toda la información que sea posible sobre el sistema, por ejemplo, direcciones IP, nombres de host, datos de autenticación, etc.

- **Obtención de acceso**

Con la información obtenida en la fase previa, se procede a explorar las vulnerabilidades que la víctima posea, para de esta manera llevar a cabo el ataque.

- **Mantener el acceso**

Cuando ya se tenga acceso al sistema, se trata de instalar y esconder herramientas que permitan tener acceso al sistema en futuras ocasiones.

- **Borrar las huellas**

Con fase final, se borran todas las huellas que hayan podido dejar durante la intrusión, con el fin de evitar ser detectado.

2.2.5.6 Impacto

Cuando una institución se ve afectada por situaciones que atentan contra su funcionamiento normal, las consecuencias de estas acciones se conocen como impacto. En

otras palabras, un impacto es el alcance o daño producido cuando las amenazas se materializan.

2.2.5.7 Desastres

Según ISO 27001, un desastre es cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización. Por ejemplo, la caída de un servidor como consecuencia de una subida de tensión o un ataque.

2.2.6 Principios de la Seguridad Informática

Para poder considerar a un sistema razonablemente seguro de debe garantizar el cumplimiento de los principios básicos de la seguridad informática. (Escrivá Gascó et al., 2013) define estos principios de la siguiente manera:

2.2.6.1 Integridad

Consiste en garantizar que la información solo pueda ser modificada por personal autorizado, estos cambios pueden ser intencionados o no.

La vulneración de la integridad tiene distinto significado dependiendo de donde se produzca:

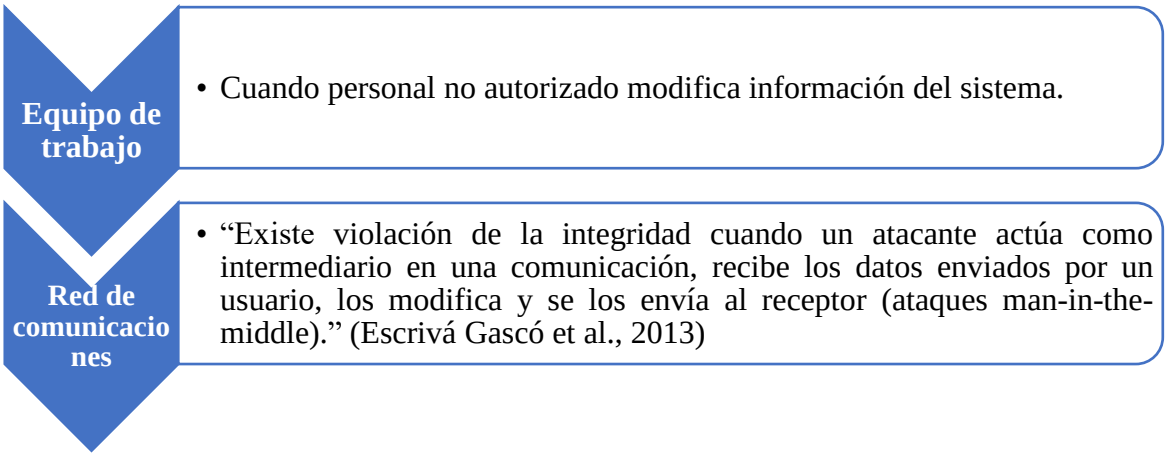


Imagen 1: Ejemplo de vulneración de la Integridad

Fuente: Escrivá Gascó et al., 2013

2.2.6.2 Confidencialidad

Garantiza que la información solo es accesible e interpretada por personas o sistemas autorizados.

La vulneración de la confidencialidad tiene distinto significado dependiendo de donde se produzca:

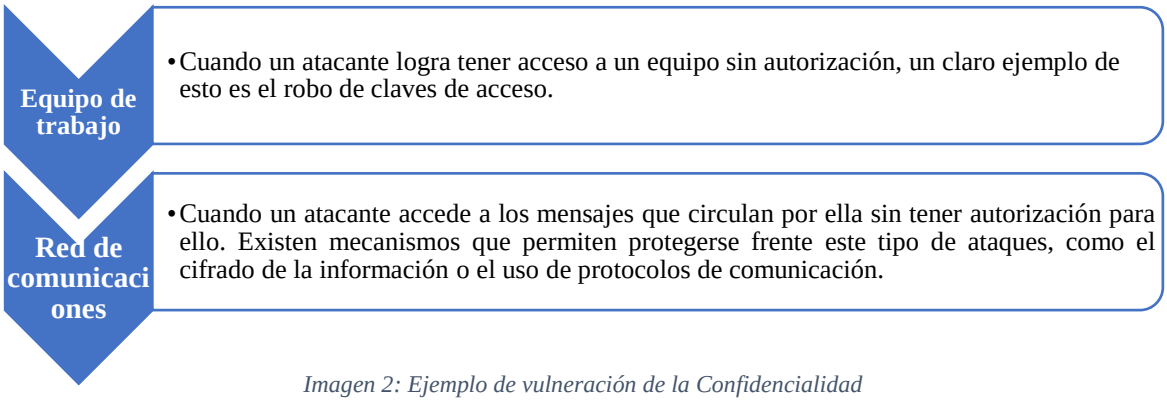


Imagen 2: Ejemplo de vulneración de la Confidencialidad

Fuente: Escrivá Gascó et al., 2013

2.2.6.3 Disponibilidad

Este es el tercer pilar básico es la disponibilidad, lo cual implica asegurar que la información será accesible en cualquier momento para el personal autorizado.

De igual manera la violación de la disponibilidad tiene distinto significado dependiendo de donde se produzca:

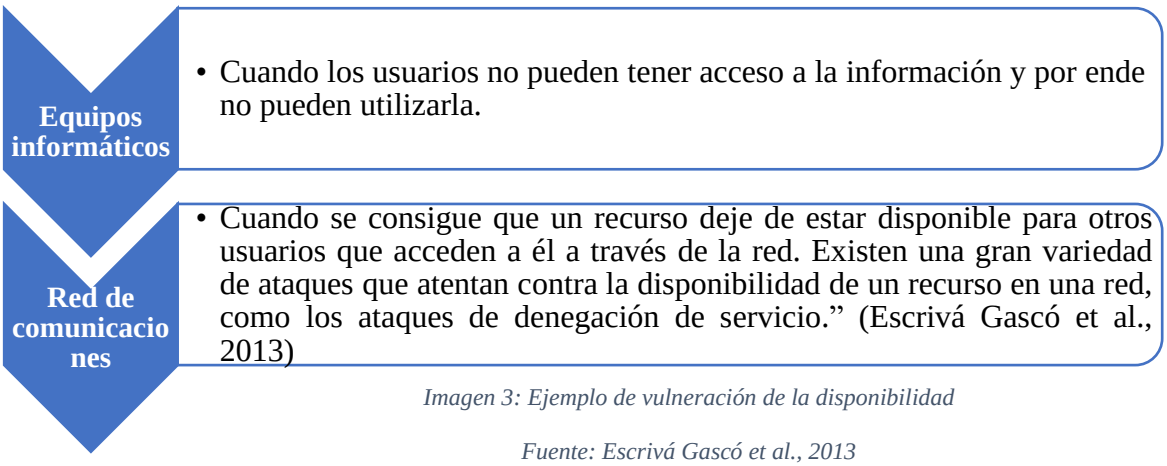


Imagen 3: Ejemplo de vulneración de la disponibilidad

Fuente: Escrivá Gascó et al., 2013

2.2.6.4 Otras características de un sistema seguro

Adicional a los principios ya mencionados, existen principios de seguridad que se consideran como deseables en todo sistema informático. Estos principios son los siguientes:

- **No repudio**

Consiste en comprobar la participación de las dos partes en una comunicación, por ejemplo, cuando se entrega la declaración de la renta telemáticamente, se firma con un certificado digital que solo puede poseer la persona que la presenta. La firma digital es una prueba irrefutable, de forma que impide que el ciudadano pueda negar o repudiar el trámite realizado. (Escrivá Gascó et al., 2013)

Este principio está estandarizado en la ISO-7498-2. Existen dos clases:

- **No repudio de origen**

Protege al destinatario del envío, ya que este recibe una prueba de que el emisor es quien dice ser.

- **No repudio de destino**

Protege al emisor del envío, ya que el destinatario no puede negar haber recibido el mensaje del emisor.

- **Autenticación**

“Permite comprobar la identidad de los participantes en una comunicación y garantizar que son quienes dicen ser. Esta característica asegura el origen de la información. Existen ataques que atentan contra este principio, como la suplantación de la identidad o los de robos de contraseñas.” (Escrivá Gascó et al., 2013)

2.3 Modelos de Seguridad Informática

2.3.1 Seguridad por oscuridad

Es el primer modelo de seguridad aplicado, se basa principalmente en desconocer u ocultar lo que se desea proteger. Para que este modelo sea efectivo se debe mantener en secreto esta información, por lo cual puede funcionar por un tiempo limitado, sin embargo, tarde o temprano se descubrirá la información oculta y será vulnerable.

2.3.2 Defensa en profundidad

La defensa en profundidad implementa varias líneas de protección debido a que divide la red en varias capas de tecnología de seguridad variada y estas se manejan de manera independiente, además de colaborar mutuamente para brindar la máxima seguridad.

El hecho de aplicar diferentes líneas de protección significa un costo, por lo cual es necesario evaluar si el valor de la información justifica las líneas de protección aplicadas.

2.3.3 Perímetro de defensa

Este es un modelo tradicional de seguridad, se basa en obtener la seguridad separando la red interna hacia fuera. “Protege todos los puntos de acceso a la red, lo que es correcto y en la actualidad se mantiene; sin embargo, únicamente como parte de un modelo de seguridad más completo, en el que se analiza además la seguridad en equipos, recursos locales y todos los puntos intermedios de conexión.” (Sánchez, 2011)

Este modelo presenta algunos problemas entre los cuales se encuentra el no brindar seguridad frente a ataques que se realicen desde la red interna, además no presenta un nivel de protección diferente cuando un ataque rompe la barrera de seguridad perimetral.

2.4 Tipos de Pruebas

Existen diferentes tipos de pruebas y estas se detallan a continuación:

2.4.1 Blindaje

Consiste en advertir a los administradores de red de la institución, más no en brindar ninguna información al Pentester. Esta estrategia requiere profundos conocimientos sobre los métodos usados por crackers además de una investigación extensa, lo cual aumenta su coste económico.

2.4.2 Doble Blindaje

En esta prueba no se advierte a los administradores de red, con el fin de probar la capacidad de respuesta del personal ante la detección de un ataque.

2.4.3 Caja Gris

El personal de la institución está informado de la auditoria, además se le brinda cierta información al Pentester.

2.4.4 Doble Caja Gris

Es similar a la prueba de caja gris, con la diferencia de que se informan fechas de las pruebas y se realiza bajo supervisión del personal de la institución.

2.4.5 Secuencial

El Pentester trabaja conjuntamente con el personal de la institución, el cual proporciona toda la información que se requiera.

2.4.6 Inversa

Aunque no se informa al personal de la institución, el Pentester tiene la información que él requiera sobre el sistema.

2.5 Auditoría de Seguridad Informática

2.5.1 Introducción

La palabra auditoría se define como un examen crítico y sistemático que normalmente realiza un grupo de expertos que son totalmente ajenos a la entidad auditada. Se debe realizar utilizando métodos de investigación o verificación que sean aceptados por el área sobre la cual se realiza la auditoría de modo que se haga una evaluación profunda de la manera en la cual se están realizando las actividades en el área que se está auditando.

Específicamente una auditoría informática es un conjunto de procedimientos y técnicas las cuales permiten evaluar completa o parcialmente el nivel en el cual se cumplen los niveles internos asociados al sistema informática de una empresa. Además, permite determinar el grado de protección de los activos y comprobar si las actividades se realizan de manera eficiente y segura.

2.5.2 Objetivo de la auditoría informática

El objetivo principal de una auditoria de seguridad informática es mejorar la seguridad, rentabilidad y eficacia del sistema informático, explorando las debilidades de la empresa, las cuales se encuentra en el proceso de la auditoria para luego especificar los planes correctivos para mejorar las falencias encontradas.

2.5.3 Importancia de una auditoría informática

Debido a que el progreso de la tecnología está mejorando cada día, los problemas de seguridad también aumentan y más aún los errores que se puedan suscitar. Es por esta razón que la auditoria de seguridad informática es de gran importancia, para revisar e inspeccionar lar vulnerabilidades y riesgos a los cuales está sometida la empresa.

2.5.4 Características de la auditoría informática

La auditoría de seguridad informática debe ser completamente independiente y ajena a la entidad auditada, pues las autoevaluaciones no son tan objetivas como se desea.

Debe ser sistemática es decir que los resultados que se obtengan son obtenidos luego de realizar un análisis minucioso y planificado por el auditor, esto otorga un alto nivel de confiabilidad.

Analiza la situación actual de la entidad auditada, con el objetivo de brindar soluciones a futuro, sin la necesidad de encontrar culpables a las falencias del sistema informático de la empresa.

2.5.5 Etapas de la auditoría informática

(Baca Urbina, 2016) en su libro Introducción a la Seguridad Informática dice que las etapas más comunes de una auditoría son las siguientes:

2.5.4.1 Planeación de la auditoría

Como primera etapa se debe recabar información de la entidad auditada, por ejemplo, políticas de seguridad, firewall, topologías de red, etc. Además, se debe constatar que estos elementos se encuentren funcionando correctamente y cumplan la función para la cual se encuentra en el sistema informático de la empresa.

2.5.4.2 Realización de la auditoría

Para la realización de esta etapa se requiere la colaboración de todo el personal de la entidad auditada. Durante los trabajos de auditoria el auditor entrevista al personal de la empresa, aplicando encuestas o cuestionarios realizados con anterioridad.

También se evalúan otros campos diferentes como auditar las conexiones inalámbricas, la red de datos y todo lo que se encuentre dentro del sistema informático de la empresa con la finalidad de encontrar las debilidades y vulnerabilidades del sistema.

2.5.4.3 Análisis de los datos recabados y de las condiciones observadas

Luego de concluir con la etapa anterior de manera exhaustiva, se analizan todos los datos obtenidos y se compara los resultados con estándares, para esto generalmente se hace uso de herramientas graficas como diagramas de flujo e incluso de mapas conceptuales. El análisis del auditor debe estar perfectamente sustentado para de esta manera poder realizar la siguiente etapa.

2.5.4.4 Elaboración de un informe escrito y emisión de una opinión

Esta etapa puede estar orientada en 4 sentidos:

Opinión limpia o sin calificación, significa que no se encontraron anomalías de gran importancia durante la auditoria, por lo cual se asume que todo está funcionando de la manera adecuada.

Opinión negativa o con calificación, implica que se encontraron vulnerabilidades importantes las cuales deben ser corregidas de inmediato pues significan un riesgo para la entidad auditada.

Opinión adversa, significa que además de las debilidades anteriores, se encontraron debilidades físicas.

Sin opinión, implica que el auditor no pudo cumplir con la auditoria al 100 %, debido a la falta de colaboración del personal de la entidad auditada, por este motivo el auditor se abstiene de dar una opinión pues no cuenta con las pruebas suficientes para esto.

2.5.6 Tipos de auditoría informática

"Una auditoria se puede clasificar en diferentes tipos, ya sea por los objetivos o por el lugar en el cual se realiza la auditoria; en este sentido se puede realizar la siguiente clasificación:" (Escrivá Gascó et al., 2013)

2.5.5.1 Auditoría se seguridad perimetral y DMZ

"Esta auditoria se realiza desde internet es decir fuera del perímetro de la seguridad de la empresa, su objetivo principal es evaluar el grado de protección del sistema informático frente a ataques externos. Se evalúa la red interna y la DMZ, utilizando diferentes tipos de ataques contra la red para de esta manera comprobar si esta es vulnerable." (Escrivá Gascó et al., 2013)

2.5.5.2 Auditoría de red interna

"Se realiza un análisis de riesgos, amenazas, vulnerabilidades e impactos dentro de la organización, sin tomar en cuenta las amenazas y riesgos desde internet. Este tipo de auditoria hace notar el nivel de seguridad y privacidad de las redes LAN y corporativas de carácter interno." (Escrivá Gascó et al., 2013)

2.5.5.3 Test de intrusión

"Este método consiste en intentar acceder a los sistemas de la entidad auditada con el fin de comprobar la resistencia a una intrusión no deseada. Para llevar a cabo este tipo de auditoria s utiliza una base de datos de las vulnerabilidades ya conocidas para de esta manera automatizar el análisis y realizar un informe con las nuevas vulnerabilidades encontradas. Es un gran complemento de la auditoría perimetral." (Escrivá Gascó et al., 2013)

2.5.5.4 Auditoría de aplicaciones

"En este tipo de auditoria se analizan y evalúan las aplicaciones que posee la empresa, sin tomar en cuenta servidores, dispositivos de red o sistemas operativos. Se realizan pruebas tales como escalada de directorios entre otros." (Escrivá Gascó et al., 2013)

2.5.5.5 Análisis forense

"El análisis forense se realiza luego de un incidente de seguridad, su objetivo es reconstruir la manera de como se ha penetrado el sistema, y también se valora los daños ocasionados." (Escrivá Gascó et al., 2013)

2.6 Metodología OSSTMM Versión 3

2.6.1 Introducción

Es una metodología que permite poner a prueba la seguridad operacional de lugares físicos, interacciones humanas y las diferentes formas de comunicación ya sean inalámbricas, cableadas, analógicas y digitales. Esta metodología es desarrollada por el Instituto de Seguridad y Metodologías Abiertas (Institute for Security and Open Methodologies) (ISECOM), y se encuentra completamente libre de influencias comerciales y políticas.

OSSTMM por sus siglas en ingles "Open Source Security Testing Methodology Manual" o "Manual de la Metodología Abierta del Testeo de Seguridad" creado por Pete Herzog y gracias al esfuerzo de más de 150 colaboradores directos, se ha convertido en un estándar profesional en cuanto al testeo de seguridad en cualquier entorno.

Desde sus inicios en el año 2000 creció rápidamente y actualmente abarca 5 canales de seguridad: humanos, físicos, medios inalámbricos, telecomunicaciones, redes de datos. "Esto también lo hace perfectamente adecuado para pruebas de computación en nube,

infraestructuras virtuales, middleware de mensajería, infraestructuras de comunicaciones móviles, lugares de alta seguridad, recursos humanos, computación confiable, y cualquier proceso lógico que cubra todos los múltiples canales y que requieran un tipo diferente de prueba de seguridad.” (Herzog, 2010)

2.6.2 Propósito de la metodología

El principal propósito que tiene OSSTMM es proporcionar una metodología científica para la caracterización de la seguridad operacional (OpSec) a través del examen y la correlación de los resultados de las pruebas. Este manual es adaptable a diferentes tipos de auditorías incluyendo pruebas de penetración, hacking ético, pruebas de seguridad, pruebas de vulnerabilidad, cajas de color rojo, cajas de color azul, etc.

Como segundo propósito tiene el brindar directrices que permiten realizar una auditoría de certificación OSSTMM. En el manual se especifica que las directrices sirven para asegurar lo siguiente:

- La prueba se llevó a cabo a fondo.
- La prueba incluyó a todos los canales necesarios.
- La postura de la prueba en cumplimiento con la ley.
- Los resultados son medibles de forma cuantificable.
- Los resultados son consistentes y repetibles.
- Los resultados sólo contienen hechos que se derivaron de las propias pruebas.

2.6.3 Contenido de OSSTMM

2.6.3.1 Capítulo 1: Lo que necesitas saber

En este capítulo se especifica todo lo que es necesario para poder llevar a cabo la auditoria, especialmente los términos usados debido a que el manual utiliza su propia nomenclatura para manejar los términos de seguridad informática. Algunos ejemplos de estos términos son: RAV, vector, porosidad, controles, seguridad operacional, etc.

2.6.3.2 Capítulo 2: Lo que usted necesita hacer

En este apartado se dan las pautas necesarias para realizar una prueba de seguridad y la mejor manera de abordar los problemas y errores que se presenten durante este proceso. (Herzog, 2010) detalla los siguientes 7 pasos para iniciar una prueba de seguridad de la mejor manera:

1. Definir lo que se desea proteger, los activos. Los mecanismos de protección de los activos son los **Controles** que se probaran para identificar las **Limitaciones.**
2. Identificar el área alrededor de los activos, que incluye los mecanismos de protección y los procesos o servicios construidos en torno a los activos. Esta es la **zona de enfrentamiento** donde la interacción se llevará a cabo.
3. Definir todo fuera de la zona de enfrentamiento que sea necesario para mantener a los activos operativos. Esto puede incluir cosas que pueden no ser capaz de influir directamente como la electricidad, alimentos, agua, aire, suelo estable, información, legislación, reglamentos y las cosas con las que se puede ser capaz de trabajar tales como sequedad, calidez, frescura, claridad, los contratistas, los colegas, la marca, asociaciones, y así sucesivamente. También contar lo que mantiene la infraestructura

de los procesos operativos como, protocolos y recursos continuos. Este es el **alcance** de la prueba.

4. Definir cómo el alcance interactúa dentro de sí y con el exterior. Lógicamente fraccionar los activos dentro del alcance a través de la dirección de las interacciones, como del interior al exterior, exterior al interior, en el interior para el interior, etc. Estos son los **vectores**. Cada vector debería idealmente ser una prueba separada para mantener una duración corta de cada prueba fraccionada antes de que puedan ocurrir muchos cambios en el medio ambiente.
5. Identificar qué equipos serán necesarios para cada prueba. Dentro de cada vector, las interacciones pueden ocurrir en varios niveles. Estos niveles pueden clasificarse de muchas maneras, sin embargo, aquí se han clasificado según su función como cinco **canales**. Los canales son Humano, Físico, Comunicaciones inalámbricas, Telecomunicaciones y Redes de Datos. Cada canal debe ser probado por separado para cada vector.
6. Determinar qué información se desea descubrir de la prueba. El tipo de **prueba** debe ser definido de forma individual para cada prueba, sin embargo, hay seis tipos comunes identificados aquí como Blindaje o Hacking Ético, Doble Blindaje (auditoría de Caja Negra o Pruebas de Penetración), Caja Gris, Doble Caja Gris, Test Tándem o Secuencial e Inverso.
7. Asegurar que la prueba de seguridad que se ha definido cumpla con las **normas judiciales**, con el fin de certificar el proceso para una prueba de seguridad adecuada sin crear malentendidos, confusiones, o falsas expectativas.

2.6.3.3 Capítulo 3: Análisis de Seguridad

Este apartado menciona que el auditor tome las pautas que la metodología recomienda para de esta manera poder llevar a cabo un buen análisis de seguridad, además, se profundiza acerca de OpSec (Seguridad Operacional) y la manera adecuada de realizar un informe de la auditoría usando como herramienta principal el análisis de confianza.

2.6.3.4 Capítulo 4: Métricas de Seguridad Operacional

En este capítulo se aprende a manejar las métricas de seguridad (RAV), que es la medida que la metodología utiliza para asignar valores a las métricas utilizadas para calcular la seguridad actual del canal probado.

2.6.3.5 Capítulo 5: Análisis de Confianza

Se trata de la manera en la cual el auditor en vez de usar el análisis de riesgos, use el análisis de confianza, valiéndosete de 10 propiedades: tamaño, simetría, visibilidad, subyugación, consistencia, integridad, compensación, valor, componentes y porosidad. Adicionalmente muestra algunas reglas para aplicar estas propiedades de la mejor manera.

2.6.3.6 Capítulo 6: Flujo de Trabajo

El flujo de trabajo hace referencia a los pasos que se debe seguir para tener un proceso ordenado durante el tiempo que tarde en finalizar la auditoria, para conseguir esto se dan varias pautas, dependiendo del canal que se esté evaluando.

2.6.3.7 Capítulo 7: Pruebas de Seguridad Humana

Tal como su nombre lo indica, en este capítulo se especifican las pruebas que se debe aplicar al personal de la institución auditada. Este canal es de vital importancia pues

actualmente se aplican técnicas de la conocida ingeniería social lo cual hace que el personal sea vulnerable y genere riesgos en la compañía.

2.6.3.8 Capítulo 8: Pruebas de Seguridad Física

En este apartado se detallan las pruebas a las cuales se debe someter todo lo tangible dentro de la empresa, en si el espacio físico donde se realizan las interacciones informáticas, tales como estaciones de trabajo, puertas de acceso, etc.

2.6.3.9 Capítulo 9: Pruebas de Seguridad Inalámbrica

En este capítulo se especifican las pruebas que se deben realizar para auditar las conexiones inalámbricas que se utilicen dentro de la institución, tales como la red Wi-Fi para de esta manera constatar que sea segura y se utilicen los equipos adecuados dependiendo de la actividad de la empresa.

2.6.3.10 Capítulo 10: Pruebas de Seguridad de las telecomunicaciones

En este canal se realizan pruebas para manipular los equipos de la red telefónica, ya sea analógica o digital, todo con la finalidad de constatar la comunicación entre el personal de la empresa por medio de este tipo de elementos.

2.6.3.11 Capítulo 11: Pruebas de seguridad para redes de datos

En este capítulo se aborda las pruebas de penetración al sistema informático, especialmente a los equipos que proveen la conexión a la red, para conseguir esto se utilizan varias herramientas con sniffers, capturadores de paquetes, etc.

2.6.3.12 Capítulo 12: Cumplimiento Normativo

Se especifica la existencia de 3 tipos de cumplimientos: legislativo, contractual y basado en estándares. Esto se realiza con el objetivo de realizar la auditoria bajo una normativa y conocer las regulaciones de la empresa y la región donde esta se desarrolla.

2.6.3.13 Capítulo 13: Presentación de informes con THE STAR

Los informes se presentan con STAR (Security Test Auditing Report) o informe de auditoría de pruebas de seguridad. OSSTMM brinda una plantilla con los datos que son necesarios incluir en el informe luego de haber realizado la auditoría.

2.6.3.14 Capítulo 14: Que Obtienes

Se detallan los beneficios de utilizar OSSTMM en una auditoria de seguridad informática, además, se dan recomendaciones en caso de aplicar la metodología en un proceso de auditoría futura.

2.6.3.15 Capítulo 15: Metodología de licencias abiertas

Se especifican 12 apartados en los cuales se explica en que consiste utilizar una metodología de código abierto.

2.6.4 Canales de la metodología

En este manual se organizan como medios reconocibles de comunicación e interacción. Esta organización está diseñada para facilitar el proceso de prueba mientras se minimiza los gastos generales ineficientes que a menudo se asocia con las metodologías estrictas.(Herzog, 2010)

2.6.4.1 Humanos

Comprende el elemento humano de la comunicación donde la interacción es tanto física o psicológica.

2.6.4.2 Físicos

Pruebas de seguridad física donde el canal es de naturaleza tanto física como no electrónica. Comprende el elemento tangible de la seguridad donde la interacción requiere esfuerzo físico o un transmisor de energía para manipular.

2.6.4.3 Inalámbricos

Comprende todas las comunicaciones electrónicas, señales y emanaciones que tienen lugar sobre el espectro electromagnético EM. Esto incluye ELSEC como las comunicaciones electrónicas, SIGSEC como señales y EMSEC que son emanaciones sin enlaces por cables.

2.6.4.4 Telecomunicaciones

Comprende todas las redes de telecomunicación, digitales o analógicas, donde la interacción se lleva a cabo a través de un teléfono determinado o similar a las líneas de la red telefónica.

2.6.4.5 Redes de Datos

Comprende todos los sistemas electrónicos y redes de datos donde la interacción se lleva a cabo a través de un cable establecido y líneas de la red cableadas.

2.6.5 Métricas Operacionales

Las métricas operacionales que se establecen en la auditoria se detallan en la tabla 2, en donde se puede apreciar como las limitaciones afectan a la seguridad operacional y a los controles.

Tabla 2: Controles, Seguridad Operacional y Limitaciones de la Auditoría

Categoría		OpSec	Limitaciones
Operaciones		Visibilidad (P_V)	Exposición
		Acceso (P_A)	Vulnerabilidad
		Confianza (P_T)	
Controles	Clase A – de Interacción	Autenticación (LC_{Au})	Debilidad
		Indemnización (LC_{Id})	
		Resistencia (LC_{Re})	
		Subyugación (LC_{Su})	
		Continuidad (LC_{Ct})	
	Clase B – de Proceso	No repudio (LC_{NR})	Preocupación
		Confidencialidad (LC_{Cf})	
		Privacidad (LC_{Pr})	
		Integridad (LC_{It})	
		Alarma (LC_{Al})	
			Anomalías

Fuente: Herzog, P. (2010). OSSTMM 3. Manual de la Metodología Abierta de Testeo de Seguridad. In. New York: ISECOM.

Para la seguridad operacional, los controles y limitaciones, existen fórmulas para ser calculados, estas se detallan a continuación.

- **Seguridad Operacional**

La seguridad operacional se identifica como **$OpSec_{Sum}$** y se calcula sumando la visibilidad, el acceso y la confianza.

$$\boldsymbol{OpSec_{Sum} = P_V + P_A + P_T}$$

Ecuación 1: Seguridad Operacional
Fuente: Herzog, P. (2010). OSSTMM 3. Manual de la Metodología Abierta de Testeo de Seguridad. In. New York: ISECOM.

- **Controles**

Los controles se identifican como LC_{sum}, para obtener este valor se deben sumar los 10 controles que se encuentran divididos en controles de Interacción y de Proceso. Es por esto que la suma de los controles está dada por la ecuación 2.

$$\boldsymbol{LC_{sum} = LC_{Au} + LC_{Id} + LC_{Re} + LC_{Su} + LC_{Ct} + LC_{NR} + LC_{Cf} + LC_{Pr} + LC_{It} + LC_{Al}}$$

Ecuación 2: Sumatoria de los controles
Fuente: Herzog, P. (2010). OSSTMM 3. Manual de la Metodología Abierta de Testeo de Seguridad. In. New York: ISECOM.

- **Controles Ausentes**

Los controles ausentes se identifican como MC_{sum}, y son necesarios para evaluar el valor de las restricciones de seguridad. Hay que tener en cuenta que este valor no puede ser menor que cero y está dado por la ecuación 3.

$$\boldsymbol{MC_{sum} = MC_{Au} + MC_{Id} + MC_{Re} + MC_{Su} + MC_{Ct} + MC_{NR} + MC_{Cf} + MC_{Pr} + MC_{It} + MC_{Al}}$$

Ecuación 3: Sumatoria de los controles Perdidos
Fuente: Herzog, P. (2010). OSSTMM 3. Manual de la Metodología Abierta de Testeo de Seguridad. In. New York: ISECOM.

Para determinar MC_{Au} se debe seguir el siguiente proceso:

$$\text{Si } OpSec_{sum} - LC \leq 0$$

$$\text{Entonces } MC_{Au} = 0$$

$$\text{Sino } MC_{Au} = OpSec_{sum} - LC_{Au}$$

Este proceso se debe realizar para todos los controles.

- **Limitaciones**

Como último punto se tiene que calcular el valor numérico para las limitaciones, las cuales se calculan de manera individual teniendo en cuenta la tabla 2 en la cual se puede apreciar si se encuentran ligadas a la seguridad operacional o a los controles.

- **Vulnerabilidad**

El símbolo de esta limitación es **Lv** y el valor numérico se obtiene contabilizando las fallas detalladas para cada canal.

- **Debilidad**

Por su parte esta debilidad se calcula sumando los errores encontrados en los controles de clase A. Su símbolo es **Lw** y se calcula con la ecuación 4.

$$L_W = FC_{Au} + FC_{Id} + FC_{Re} + FC_{Su} + FC_{Ct}$$

Ecuación 4: Debilidad
Fuente: Herzog, P. (2010). OSSTMM 3. Manual de la Metodología Abierta de Testeo de Seguridad. In. New York: ISECOM.

- **Preocupación**

La preocupación se calcula sumando los errores encontrados en los controles clase B, su símbolo es **L_C** y para obtener el valor numérico esta la ecuación 5.

$$L_C = FC_{NR} + FC_{Cf} + FC_{Pr} + FC_{It} + FC_{Al}$$

Ecuación 5: Preocupación
Fuente: Herzog, P. (2010). OSSTMM 3. Manual de la Metodología Abierta de Testeo de Seguridad. In. New York: ISECOM.

- **Exposición**

Para encontrar el valor numérico de esta limitación solo basta con contabilizar los ítems que se establecen para cada canal y su símbolo es **L_E.**

- **Anomalía**

Finalmente la anomalía tiene el símbolo **L_A** y se calcula teniendo en cuenta los puntos especificados para cada canal.

2.6.5.1 RAV

"El rav es una medición a escala de la superficie de ataque, la cantidad de interacciones no controladas con un objetivo, que se calcula por el equilibrio cuantitativo entre las operaciones, limitaciones y controles. En esta escala, 100 rav (también muestra como 100% rav por la sencillez de entendimiento, aunque no precisamente en porcentaje) es un equilibrio perfecto, también pocos controles y, por tanto, una superficie de ataque mayor. Más de 100 rav muestra que más controles son necesarios y que a su vez puede ser un problema, ya que los controles a menudo añaden interacciones dentro de un ámbito, así como cuestiones de complejidad y mantenimiento."(Herzog, 2010)

2.6.5.2 Calculadora RAV

La metodología tiene una hoja de Excel en la cual se ingresan los valores obtenidos en la seguridad operacional, los controles y limitaciones para posteriormente mostrar automáticamente diferentes valores para finalmente obtener la seguridad Δ, la protección verdadera y la seguridad actual de la institución auditada, la misma que tiene la unidad de rav. El formato de esta calculadora se muestra en la imagen 4.

OPSEC				ISECOM
Visibilidad	0			
Acceso	0			
Confianza	0			OPSEC 0,00
Total (Porosidad)	0			
CONTROLES				Controles Verdaderos 0,00
Clase A		Ausentes		
Autenticación	0	0		Controles Totales 0,00
Indemnización	0	0		
Resistencia	0	0		
Subyugación	0	0		Cobertura Verdadera A 0,00%
Continuidad	0	0		
Total Clase A	0	0		
Clase B		Ausentes		Cobertura Verdadera B 0,00%
No-Repudio	0	0		
Confidencialidad	0	0		
Privacidad	0	0		Cobertura Verdadera Total 0,00%
Integridad	0	0		
Alarma	0	0		
Total Clase B	0	0		
		Ausentes Verdaderos		
Total todos los Controles	0	0		
Cobertura Total	0,00%	0,00%		
LIMITATIONS		Item Value	Total Value	Limitaciones 0,000000
Vulnerabilidades	0	0,00	0,00	
Debilidades	0	0,00	0,00	
Preocupaciones	0	0,00	0,00	Seguridad Δ 0,00
Exposiciones	0	0,00	0,00	
Anomalías	0	0,00	0,00	
Total # Limitaciones	0		0,00	Proteccion Verdadera 100,00
Seguridad Actual:			**100,00**	**ravs**

Imagen 4: CALCULADORA RAV
Fuente: Herzog, P. (2010). OSSTMM 3. Manual de la Metodología Abierta de Testeo de Seguridad. In. New York: ISECOM

2.6.5.3 Presentación de informes con The STAR

The STAR es el Informe de Auditoria de Pruebas de Seguridad. Tiene como objetivo brindar un resumen indicado los resultados numéricos de las pruebas efectuadas, además de especificar datos informativos sobre el auditor y las fechas de las pruebas efectuadas. El formato para llenar este informe se puede encontrar en la página web de ISECOM y se muestra en la imagen 5.

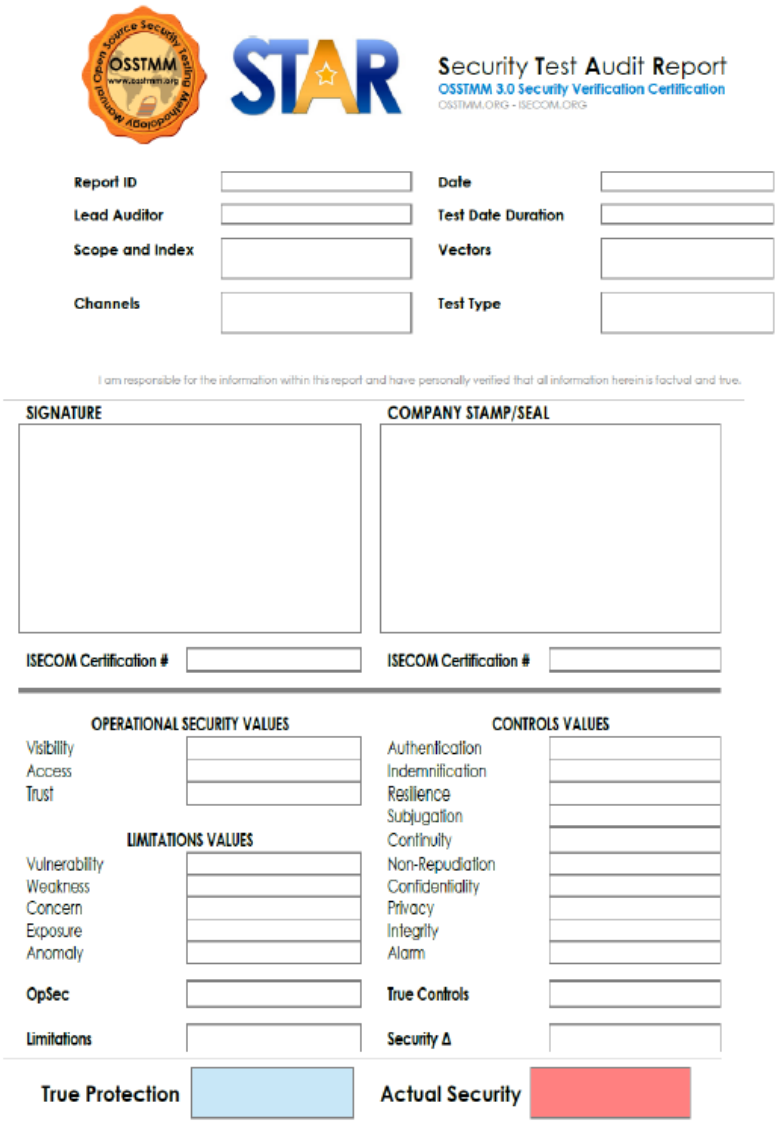


Imagen 5: INFORME STAR
Fuente: Herzog, P. (2010). OSSTMM 3. Manual de la Metodología Abierta de Testeo de Seguridad. In. New York: ISECOM

2.6.6 Ventajas de la metodología

Existen varias metodologías utilizadas para la auditoria de seguridad informática, entre ellas se encuentran OCTAVE, NIST 800-115, MAGERIT, MSAT, OSSTMM, entre otras; a continuación, se presenta un cuadro comparativo en el cual se puede evidenciar que OSSTMM es una de las más completas:

Tabla 3: Comparación entre varias metodologías

	OSSTMM	OCTAVE	NIST 800-115	MAGERIT	MSAT
Ámbito Físico	X			X	
Ámbito Digital	X	X	X	X	X
Ámbito Social	X	X	X		
Métricas	X			X	
Guía Técnica		X		X	X
Informes	X		X		X
Gestión de Proyecto					

Fuente: Elaboración Propia

Como se puede observar OSSTMM cubre más ámbitos que las demás metodologías, teniendo en cuenta que es una de las pocas que cubre el ámbito físico, lo cual es una gran ventaja pues, este campo es muy importante para la seguridad de las empresas auditadas.

Cuando se procede a realizar las pruebas es de vital importancia utilizar una métrica, para poder asignarle una nota al estado de seguridad de la entidad auditada, y solo OSSTMM es la metodología que cuenta con estas métricas.

Una vez terminada la auditoría es igual de importante la presentación del informe, debido a que documentar la auditoría es crucial para transmitir de manera adecuada la información al cliente o empresa auditada. OSSTMM es una de las metodologías que mejor explica la manera de realizar los informes finales.

Adicionalmente al realizar la auditoría con la metodología OSSTMM asegura que:

- Las pruebas han sido realizadas de forma exhaustiva.

- Las pruebas incluyen los ámbitos necesarios para asegurar la seguridad de la empresa.
- Se pueden medir de forma cuantitativa los resultados y estos son consistentes.

2.7 La ISO (International Organization For Standarization)

La ISO (International Organization for Standarization) es una federación integrada por diferentes organismos de estandarización de más de 153 países. Fue establecida en 1947 y su misión es promover el desarrollo de la estandarización.

Las normas de la ISO tienen como finalidad proporcionar herramientas para trabajar en el mundo real en campos tales como la medicina y la seguridad. Estas normas aseguran que tanto productos como servicios sean de buena calidad; dentro de una institución ayudan a mejorar la productividad y aumentar el desarrollo de la misma.

2.7.1 Norma ISO/IEC 27001

Es una norma internacional emitida por la ISO, y su función es describir cómo gestionar la seguridad de la información en una determinada institución. La version mas actual fue publicada en 2013 por lo cual su nombre completo es ISO/IEC 27001:2013 “Norma de Sistema de Gestión de Seguridad de la Información (SGSI)”

Esta norma tiene la ventaja de que puede ser implementada en cualquier organización ya sea pública, privada, con o sin fines de lucro. Fue redactada por especialistas en el tema de seguridad de la información y es de gran ayuda para implementar la gestión de seguridad de información de una organización.

La estructura de esta norma tiene dos etapas que sirven para la elaboración y la implementación de las políticas de seguridad de la empresa. Además, hace énfasis en que el SGSI debe proteger la CIA: confidencialidad, integridad y disponibilidad de la información.

A continuación, se muestra una tabla de la norma ISO/IEC 27001:

Tabla 4: Norma ISO/IEC 27001

	CLÁUSULAS	APARTADOS
0	Introducción	
1	Alcance	
2	Referencias Normativas	
3	Términos y definiciones	
4	Contexto de la Organización	4.1 Compresión de la organización y su contexto. 4.2 Comprensión de las necesidades y expectativas de las partes interesadas. 4.3 Determinación del alcance del sistema de gestión de continuidad de negocios. 4.4 Sistema de Gestión de Continuidad de Negocios
5	Liderazgo	5.1 Liderazgo y compromiso 5.2 Compromiso gerencial 5.3 Política 5.4 Roles, responsabilidades y autoridades de la organización.
6	Planificación	6.1 Acciones para atender los riesgos y las oportunidades. 6.2 Objetivos de continuidad de negocios y planes para lograrlos.
7	Soporte	7.1 Recursos 7.2 Competencia 7.3 Concientización 7.4 Comunicación 7.5 Información a documentar
8	Operación	8.1 Planificación y control operacional. 8.2 Análisis de impactos en los negocios y valuación de riesgos. 8.3 Estrategia de continuidad de negocios y planes para lograrlos. 8.4 Establecimiento e implementación de los procedimientos de continuidad de negocios. 8.5 Ejercicios y pruebas.
9	Evaluación de desempeño	9.1 Monitoreo, medición, análisis y evaluación 9.2 Auditoría Interna. 9.3 Revisión gerencial.
10	Mejoramiento	10.1 No conformidades y acciones correctivas. 10.2 Mejoramiento continuo

Fuente: Norma ISO/IEC 27001

2.7.1.1 Implementación de la Norma ISO/IEC 27001

Existen 6 fases o pasos para implementar la ISO/IEC 27001:

Paso 1: Definición del alcance (scope) y los límites de SGSI

El ámbito de aplicación aclara y establece en qué campos aplica el Sistema de Gestión de Seguridad de la Información.

Paso 2: Definición de la política de la seguridad de la información

Determinación de la política de seguridad de la información para el ámbito de aplicación definido.

Paso 3: Identificación de los activos de la empresa (assets) y sus riesgos asociados. ¿Dónde están las debilidades? ¿Qué amenazas hay que tener en cuenta?

- Identificación de activos y evaluación.
- Identificación de las debilidades.
- Identificación de las amenazas.
- Valor de las consecuencias.

Paso 4: Control de riesgos

En este paso se hacen las siguientes preguntas: ¿Qué riesgos se corren? ¿Son asumibles?

Paso 5: Fijación de controles y objetivos de control

En este paso se fijan los objetivos de control que se debe tener para garantizar la seguridad de la empresa.

Paso 6: Definición de la Declaración de Aplicabilidad, la conocida SOA (Statement of Applicability), de la norma ISO/IEC 27001

Consiste en un resumen de las decisiones tomadas en relación al tratamiento del riesgo.

2.7.2 Sistema de gestión de la seguridad de la información

La gestión de la seguridad de la información debe realizarse siguiendo un proceso sistematizado, documentado y debe ser conocido por toda la institución. Este proceso constituye un SGSI, el cual se puede considerar como sistema de calidad para la seguridad de la información.

A continuación, se detallarán algunos conceptos de SGSI según la norma ISO/IEC 27001:

2.7.2.1 Que es un SGSI

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

2.7.2.2 Para que sirve un SGSI

Un SGSI ayuda a establecer las políticas y procedimientos con relación a los objetivos de la institución, y su principal objetivo es tener un nivel de exposición menor al nivel de riesgo asumido por la misma institución.

Con un SGSI ls institución conoce todos los riesgos a los cuales está sometida su información, con lo cual los asume, minimiza y controla mediante un proceso sistemático conocido por todos y debidamente documentado.

2.7.2.3 Que incluye un SGSI

Un SGSI incluye documentos de 4 niveles diferentes:

Documentos de nivel 1

En estos documentos está el **manual de seguridad** que dirige a todo el sistema informático y determina las intenciones, objetivos, responsabilidades, políticas y directrices principales del SGSI.

Documentos de nivel 2

Aquí se encuentran los **procedimientos**, que son documentos de nivel operativo y aseguran que la planificación se realice de forma eficiente así mismo controla los procesos de seguridad de la información.

Documentos de nivel 3

En este nivel se encuentran las **instrucciones, checklists y formularios** que describen la manera de realizar las actividades relacionadas con la seguridad de la información.

Documentos de nivel 4

Finalmente se encuentran los **registros** que proporciona evidencia del cumplimiento de los requisitos de un SGSI.

2.7.2.4 Implementación de un SGSI

Para implementar el SGSI se utiliza el ciclo continuo PDCA, tradicional en sistemas de gestión de calidad.

- **Plan (planificar):** establecer el SGSI.
- **Do (hacer):** implementar y utilizar el SGSI.
- **Check (verificar):** monitorizar y revisar el SGSI.
- **Act (actuar):** mantener y mejorar el SGSI.

2.8 Legislación del Ecuador con Respecto a los Delitos Informáticos

Existen varias leyes relacionadas con delitos informáticos en el Ecuador, estas leyes y sanciones se detallan a continuación:

2.8.1 Constitución del Ecuador

La constitución de la República del Ecuador fue publicada en el registro oficial No. 449 el 22 de octubre del 2008, es la norma suprema que está sobre cualquier otra norma jurídica, misma que proporciona los lineamientos para la organización del Estado, la existencia del Ecuador y quienes han de gobernar. (Asamblea Nacional del Ecuador, 2008)

En ella se estipula los principios por los cuales han sido creadas todas las leyes incluyendo las mencionadas a continuación:

2.8.2 Ley de Propiedad Intelectual

"Art 1 El Estado reconoce, regula y garantiza la propiedad intelectual adquirida de conformidad con la ley, las Decisiones de la Comisión de la Comunidad Andina y los convenios internacionales vigentes en el Ecuador."(Congreso Nacional del Ecuador, 28 de 12 de 2006)

"La propiedad intelectual comprende:

1. Los derechos de autor y derechos conexos.

2. La propiedad industrial, que abarca, entre otros elementos, los siguientes:

   a. Las invenciones;
   b. Los dibujos y modelos industriales;
   c. Los esquemas de trazado (topografías) de circuitos integrados;
   d. La información no divulgada y los secretos comerciales e industriales;
   e. Las marcas de fábrica, de comercio, de servicios y los lemas comerciales;
   f. Las apariencias distintivas de los negocios y establecimientos de comercio;
   g. Los nombres comerciales;
   h. Las indicaciones geográficas;
   i. Cualquier otra creación intelectual que se destine a un uso agrícola, industrial o comercial.

3. Las obtenciones vegetales." (Congreso Nacional del Ecuador, 28 de 12 de 2006)

"Art. 2. Los derechos conferidos por esta Ley se aplican por igual a nacionales y extranjeros, domiciliados o no en el Ecuador." (Congreso Nacional del Ecuador, 28 de 12 de 2006)

"Art. 3. El Instituto Ecuatoriano de la Propiedad Intelectual (IEPI), es el Organismo Administrativo Competente para propiciar, promover, fomentar, prevenir, proteger y defender a nombre del Estado Ecuatoriano, los derechos de propiedad intelectual reconocidos en la presente Ley y en los tratados y convenios internacionales, sin perjuicio de las acciones civiles y penales que sobre esta materia deberán conocerse por la Función Judicial." (Congreso Nacional del Ecuador, 28 de 12 de 2006)

Esta ley tiene como objetivo hacer cumplir los derechos de propiedad intelectual por lo cual toda infracción es sancionada penalmente, tanto para extranjeros como para nacionales sin ningún tipo de excepción.

2.8.3 Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

La ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos fue publicada en el Registro Oficial Suplemento No. 577 de 17 de abril de 2002. El objetivo fundamental de esta ley es regular la información que circula por medio de las redes de telecomunicaciones, incluyendo el comercio electrónico y protección a los usuarios.

"Art. 1.- Objeto de la Ley.- Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas." (Congreso Nacional del Ecuador, 17 de 04 del 2002)

“Art. 2.- Reconocimiento jurídico de los mensajes de datos.- Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta Ley y su reglamento.” (Congreso Nacional del Ecuador, 17 de 04 del 2002)

“Art. 3.- Incorporación por remisión.- Se reconoce validez jurídica a la información no contenida directamente en un mensaje de datos, siempre que figure en el mismo, en forma de remisión o de anexo accesible mediante un enlace electrónico directo y su contenido sea conocido y aceptado expresamente por las partes.” (Congreso Nacional del Ecuador, 17 de 04 del 2002)

“Art. 4.- Propiedad Intelectual.- Los mensajes de datos estarán sometidos a las leyes, reglamentos y acuerdos internacionales relativos a la propiedad intelectual.” (Congreso Nacional del Ecuador, 17 de 04 del 2002)

“Art. 5.- Confidencialidad y reserva.- Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia.” (Congreso Nacional del Ecuador, 17 de 04 del 2002)

“Art. 6.- Información escrita.- Cuando la Ley requiera u obligue que la información conste por escrito, este requisito quedará cumplido con un mensaje de datos, siempre que la información que éste contenga sea accesible para su posterior consulta.” (Congreso Nacional del Ecuador, 17 de 04 del 2002)

“Art. 7.- Información original.- Cuando la Ley requiera u obligue que la información sea presentada o conservada en su forma original, este requisito quedará cumplido con un mensaje de datos, si siendo requerido conforme a la Ley, puede comprobarse que ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos.” (Congreso Nacional del Ecuador, 17 de 04 del 2002)

Al igual que la anterior ley, el incumplimiento conlleva a ser procesado penalmente sin importar la nacionalidad, pues los delitos son realizados en el país y se deben juzgar con forme a las leyes de este.

2.8.4 Ley Orgánica de Transparencia y Acceso a la Información Pública

“Art. 1.- Principio de Publicidad de la Información Pública:

El acceso a la información pública es un derecho de las personas que garantiza el Estado.

Toda la información que emane o que esté en poder de las instituciones, organismos y entidades, personas jurídicas de derecho público o privado que, para el tema materia de la información tengan participación del Estado o sean concesionarios de éste, en cualquiera de sus modalidades, conforme lo dispone la Ley Orgánica de la Contraloría General del Estado; las organizaciones de trabajadores y servidores de las instituciones del Estado, instituciones de educación superior que perciban rentas del Estado, las denominadas organizaciones no gubernamentales (ONG's), están sometidas al principio de publicidad; por lo tanto, toda información que posean es pública, salvo las excepciones establecidas en esta Ley.” (Congreso Nacional del Ecuador, 18 de 05 del 2004)

“Art. 5.- Información Pública:

Se considera información pública, todo documento en cualquier formato, que se encuentre en poder de las instituciones públicas y de las personas jurídicas a las que se refiere esta Ley, contenidos, creados u obtenidos por ellas, que se encuentren bajo su responsabilidad o se hayan producido con recursos del Estado.”(Congreso Nacional del Ecuador, 18 de 05 del 2004)

“Art. 6.- Información Confidencial.-

Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República.

El uso ilegal que se haga de la información personal o su divulgación, dará lugar a las acciones legales pertinentes.”(Congreso Nacional del Ecuador, 18 de 05 del 2004)

A pesar de que las instituciones públicas deben brindar acceso a la información pública, existen datos que son tomados como privados con el fin de resguardar la integridad de la institución pues poseen datos que no deben ser conocidos por ejemplo una universidad, los datos personales de los estudiantes.

2.8.5 Contraloría General del Estado

Art. 14.- “Auditoría Interna.- Las instituciones del Estado, contarán con una Unidad de Auditoría Interna, cuando se justifique, que dependerá técnica y administrativamente de la Contraloría General del Estado, que para su creación o supresión emitirá informe previo. El personal auditor, será nombrado, removido o trasladado por el Contralor General del Estado

y las remuneraciones y gastos para el funcionamiento de las unidades de auditoría interna serán cubiertos por las propias instituciones del Estado a las que ellas sirven y controlan."

Art. 15.- "Independencia.- Los auditores de esta unidad actuarán individual o colectivamente, con criterio independiente respecto a la operación o actividad auditada y no intervendrán en la autorización o aprobación de los procesos financieros, administrativos, operativos y ambientales."

2.8.6 Código Orgánico Integral Penal

"Artículo 1.- Finalidad. - Este Código tiene como finalidad normar el poder punitivo del Estado, tipificar las infracciones penales, establecer el procedimiento para el juzgamiento de las personas con estricta observancia del debido proceso, promover la rehabilitación social de las personas sentenciadas y la reparación integral de las víctimas."(Asamblea Nacional de la República del Ecuador, 10 de 02 del 2014)

"Artículo 178.- Violación a la intimidad. - La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y video, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años".(Asamblea Nacional de la República del Ecuador, 10 de 02 del 2014)

"Artículo 190.- Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de

bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años".(Asamblea Nacional de la República del Ecuador, 10 de 02 del 2014)

"Artículo 212.- Suplantación de identidad. - La persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa libertad de uno a tres años".(Asamblea Nacional de la República del Ecuador, 10 de 02 del 2014)

"Artículo 229.- Revelación ilegal de base de datos. - La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, base de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años".(Asamblea Nacional de la República del Ecuador, 10 de 02 del 2014)

"Artículo 232.- Ataque a la integridad de sistemas informáticos. - La persona que destruya, dañe borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años".(Asamblea Nacional de la República del Ecuador, 10 de 02 del 2014)

“Artículo 234.- Acceso no consentido a un sistema informático, telemático, o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o re direccionar el tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años”.(Asamblea Nacional de la República del Ecuador, 10 de 02 del 2014)

En el COIP se estipulan varios artículos los cuales se detallan las penas privativas de la libertad de acuerdo al delito que se cometa. En este código se detallan los diferentes tipos de delitos y la gravedad de cada uno de ellos y se han detallado algunos de los concernientes con delitos informáticos.

CAPÍTULO III

3. Aplicación de la Metodología

En el presente capitulo se procederá a aplicar la metodología OSSTMM versión 3, la cual consiste en analizar los cinco canales: humano, físico, inalámbrico, telecomunicaciones y redes de datos. Para la correcta aplicación de la metodología se debe revisar la legislación que se aplica en la región en cuanto a la seguridad informática, esta revisión ya se encuentra considerada en el capítulo II, por lo cual se procede con la aplicación de la auditoria.

3.1 Diagrama de la metodología

En el diagrama 1 se muestra la estructura de la metodología OSSTMMv3, la cual brinda una guia para el desarrollo de la auditoria de seguridad informática.

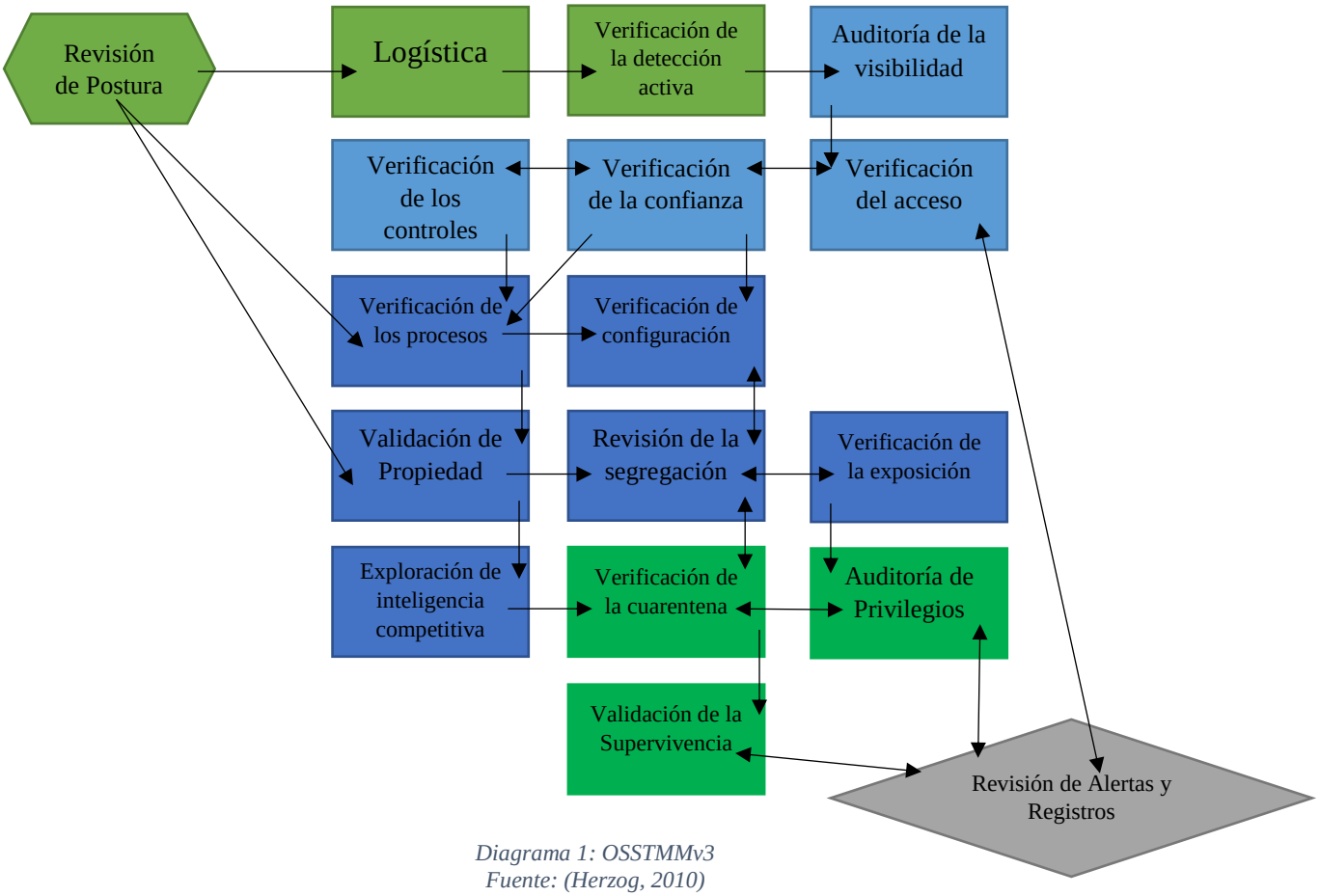


Diagrama 1: OSSTMMv3
Fuente: (Herzog, 2010)

3.2 Análisis de la Situación Actual de la Institución

3.2.1 Descripción general

Para este punto se detallaran los datos más importantes de la Universidad Politécnica Estatal del Carchi, tales como la infraestructura de la red, equipos informáticos. Toda esta información tendrá como base los datos proporcionados por el encargado del área de redes del Departamento de Tics de la Universidad y las visitas realizadas a las diferentes áreas de la institución.

3.2.2 Ubicación física de la institución

La Universidad Politécnica Estatal del Carchi (UPEC) está ubicada en la ciudad de Tulcán, en la parroquia urbana que lleva el mismo nombre, Tulcán. La institución se encuentra en la calle Antisana y Av. Universitaria, como se indica en la imagen 6. Las instalaciones de la UPEC son relativamente nuevas debido a que fue fundada en el año 2006.

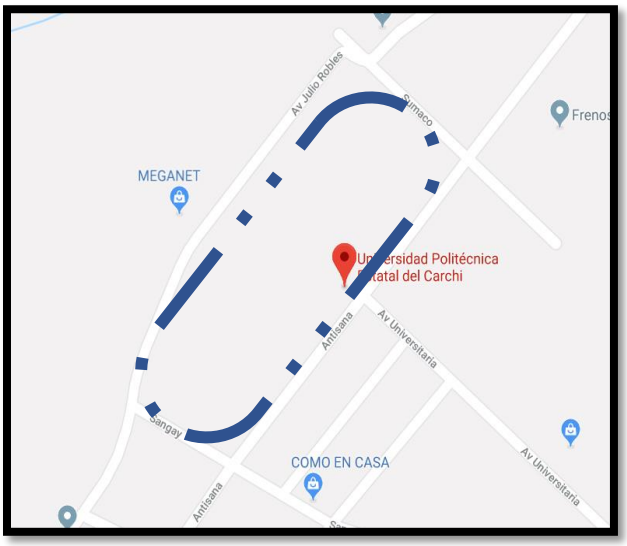


Imagen 6: Ubicación UPEC
Fuente: Google MAPS

3.2.3 Estructura del Campus

El campus consta de 8 edificaciones los cuales son: Edificio Central, Edificio Aulas 1, Edificio Aulas 2, Edificio Aulas 3, Edificio Aulas 4, Edificio Laboratorios, Centro de Educación Infantil y el coliseo de la institución. En los diferentes edificios se encuentran las aulas, el personal administrativo, y específicamente el Data Center en la planta 1 del edificio central, desde donde se distribuyen los recursos de la red a toda la institución.

Imagen 7: Estructura del Campus
Fuente: Universidad Politécnica Estatal del Carchi

3.2.4 Misión

"La Universidad Politécnica Estatal del Carchi es una institución de educación superior pública y acreditada, que satisface las demandas sociales a través de la formación de grado y posgrado, la investigación, la vinculación con la sociedad y la gestión, generando conocimientos que contribuyen al desarrollo económico, social, científico-tecnológico, cultural y ambiental de la región."(Universidad Politécnica Estatal del Carchi, 2005)

3.2.5 Visión

"Ser una universidad sin fronteras geográficas, acreditada, líder en la formación integral y reconocida por su excelencia, calidad, transparencia y compromiso con el desarrollo de la región y del país".(Universidad Politécnica Estatal del Carchi, 2005)

3.2.6 Medios de transmisión

Los medios de transmisión en los edificios son por medio de cable UTP cat 6, por su parte el medio de transmisión para interconectar el Data Center con los diferentes edificios es fibra óptica multimodo, evitando de esta manera que se generen cuellos de botella.

3.2.7 Topología Física de la red interna

La red interna de la UPEC, es una red tipo cascada como se muestra en la imagen 8, cuenta con un firewall, varios servidores y las estaciones de trabajo en los diferentes edificios. Su cableado es relativamente nuevo por lo que brinda estabilidad en el ancho de banda. El direccionamiento ip se encuentra segmentado, dependiendo de las carreras u oficinas, de tal manera que se posee varios dominios de broadcast.

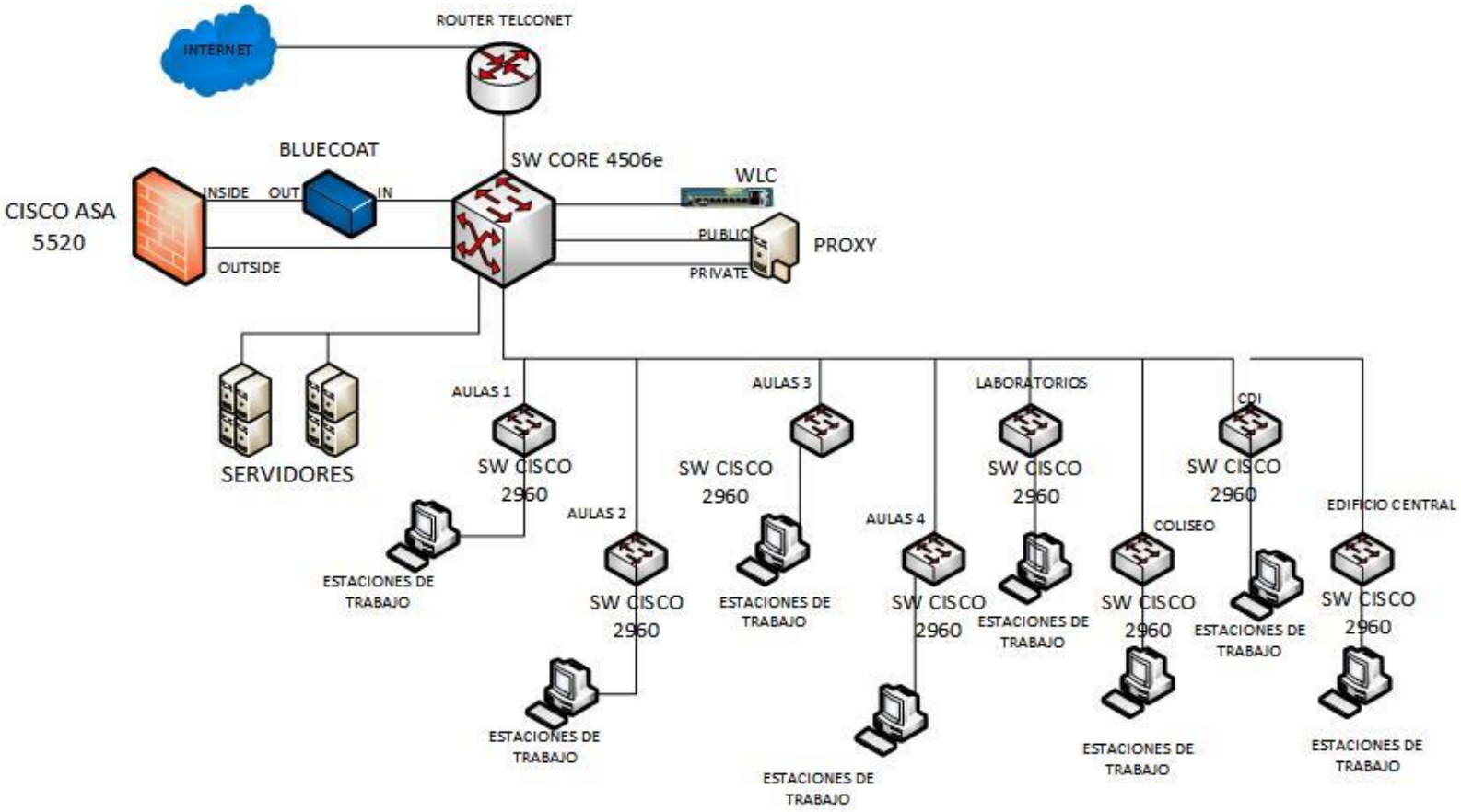


Imagen 8: Topología física de la red interna UPEC
Fuente: Elaboración Propia

3.2.8 Topología Lógica de la red interna

La topología lógica de la red interna de la UPEC se muestra en la imagen 9:

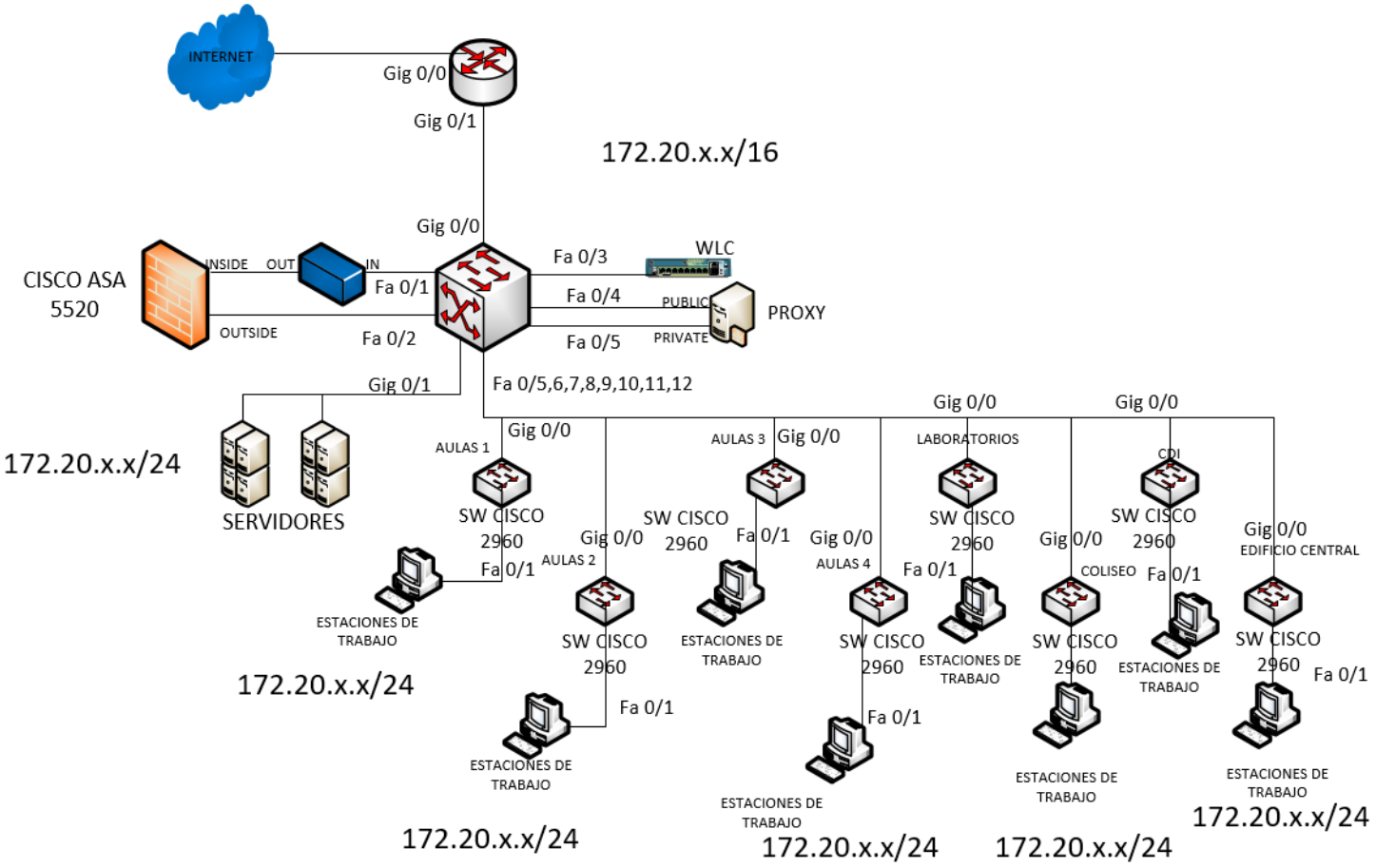


Imagen 9: Topología Lógica de la UPEC

Fuente: Elaboración Propia

3.2.9 Organigrama de la institución

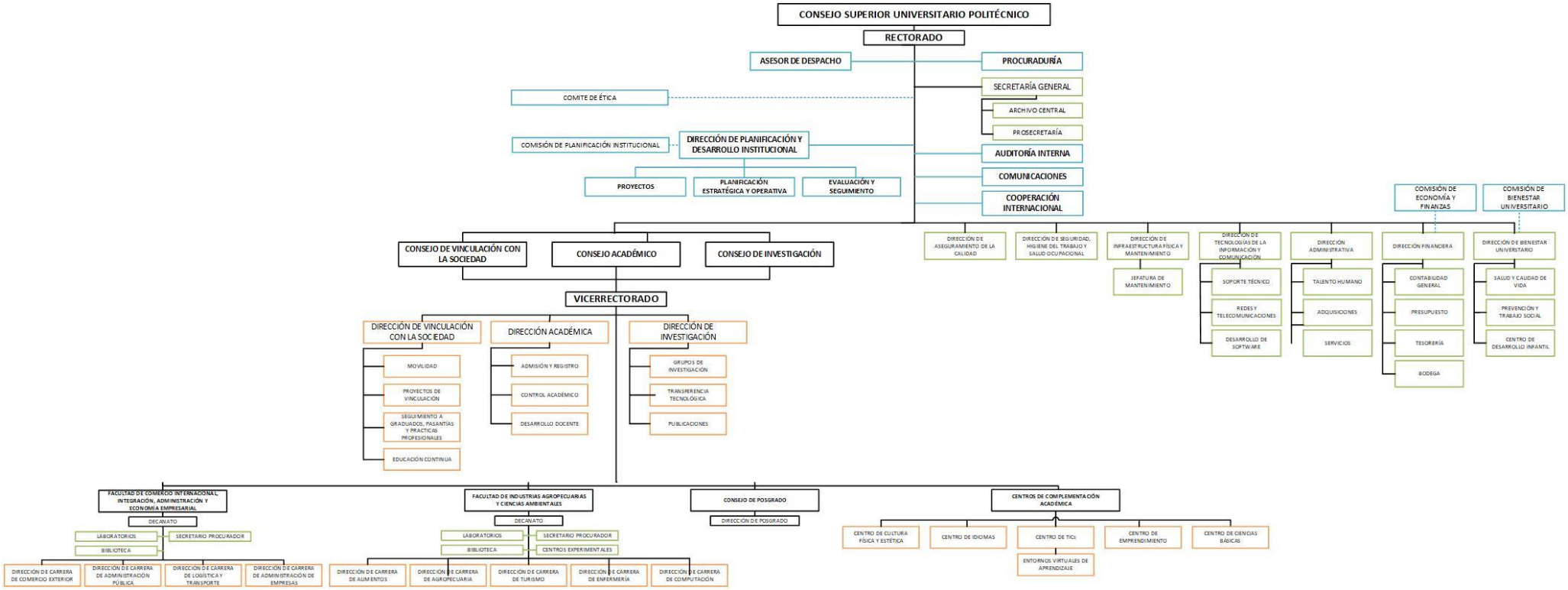


Imagen 10: Organigrama de la Universidad Politécnica Estatal del Carchi
Fuente: Universidad Politécnica Estatal del Carchi. (2017).

3.2.10 Data Center

El Data Center está ubicado en el edificio central en la planta 1, específicamente en la oficina de Redes y Telecomunicaciones, en este se encuentran 3 racks cerrados en los cuales se ubican el router del proveedor de internet, el firewall, el switch de Core, y los servidores. Para el acceso al cuarto de telecomunicaciones se posee una cerradura magnética que se abre mediante una tarjeta y el código de acceso como se muestra en la imagen 11:

Imagen 11: Entrada del Data Center UPEC
Fuente: Elaboración Propia

Este cuarto de telecomunicaciones, es de tipo TIER 1, pues no cuenta con el respectivo respaldo de la información, no posee aire acondicionado y tampoco sistema contra incendios, en cuanto a UPS solo dan el tiempo suficiente para apagar los equipos. En cuanto

a seguridad adicional a la cerradura magnética se cuenta con una cámara de video vigilancia en el interior del data center. En la imagen 12 se muestra el cuarto de telecomunicaciones:

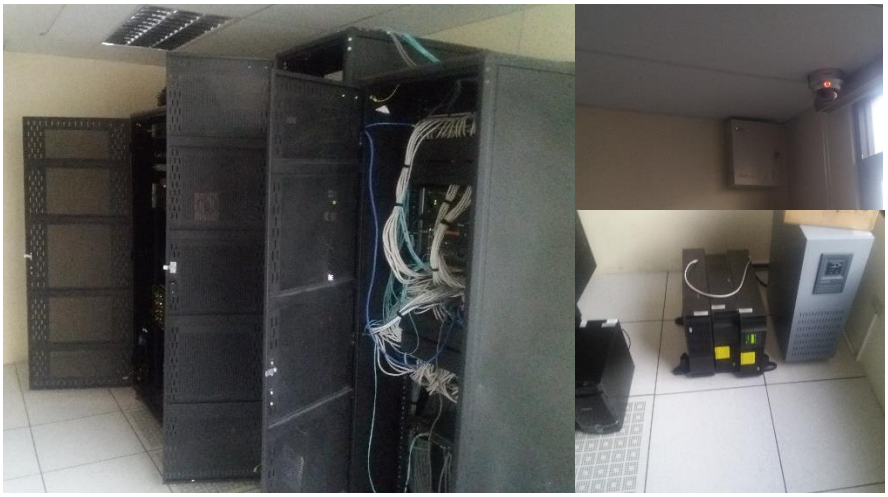


Imagen 12: Data Center UPEC
Fuente: Elaboración Propia

3.2.11 Racks en los edificios de la UPEC

En cuanto a los rack en los diferentes edificios de la institución están ubicados en bodegas, salas de reuniones y son pocos los que tienen dedicado un espacio específico para estos equipos. En todos los racks se encuentran switch cisco 2960, que son los que brindan conectividad al campus universitario.

A pesar de que estos equipos son importantes para la institución, en muchos casos el acceso es muy fácil, pues las puertas se encuentran abiertas y no son vigilados de ninguna manera como se aprecia en la imagen 13.

Imagen 13: Fácil acceso a los racks
Fuente: Elaboración Propia

3.2.12 Estaciones de trabajo

Las estaciones de trabajo son diferentes para el personal administrativo y para los estudiantes, pues el personal administrativo cuanta con oficinas en las cuales desarrollan sus labores como se muestra en la imagen 14, mientras que los estudiantes poseen estaciones de trabajo en los laboratorios y la biblioteca como se puede apreciar en la imagen 15.

3.2.13 Red inalámbrica

La red inalámbrica está conformada por AP CISCO, TP-Link y D-Link, en los cuales están configuradas la red eduroam para estudiantes, una red diferente para cada departamento, la red WUPEC para docente y la red WUPEC_EVENTOS para los

invitados. Estas redes funcionan las 24 horas del día, los 7 días de la semana, por lo cual son usadas constantemente por todo el personal de la institución.

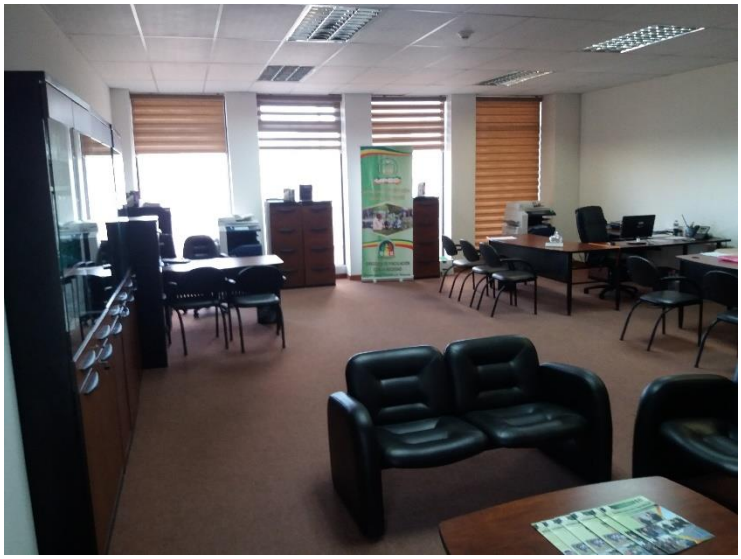


Imagen 14: Estaciones de Trabajo Personal Administrativo
Fuente: Elaboración Propia

Imagen 15: Estaciones de Trabajo Estudiantes
Fuente: Elaboración Propia

3.3 Desarrollo de Pruebas

OSSTMM versión 3, sugiere seis tipos de pruebas: Blindaje, Doble Blindaje, Caja Gris, Doble Caja Gris, Secuencial e Inversa. Para el desarrollo de la auditoria se eligió la **Caja Gris**, en vista de que el objetivo "Departamento de TIC's" ya conoce de la auditoria y el auditor tiene conocimientos limitados de las defensas y activos que posee la institución. A menudo esta prueba se conoce como **prueba de Vulnerabilidad**, y esto es lo que se pretende con la aplicación de la auditoría, encontrar las vulnerabilidades que tenga la red interna de la UPEC.

Para empezar con el proceso se comunicó al encargado del área de redes, para contar con el permiso para realizar las pruebas que sean necesarias, el cual fue solicitado por medio de un oficio, ANEXO 24, en el cual se propone un cronograma para la realización de la auditoría.

Los resultados de cada ítem se muestran en una tabla en la cual están marcados por una viñeta los puntos que serán tomados en cuenta para asignar el valor numérico de cada prueba.

3.4 Pruebas de Seguridad Humana

"Seguridad Humana (HUMSEC) es una subsección de PHYSSEC e incluye las operaciones psicológicas (PSYOPS). La aprobación de este canal requiere la interacción con las personas en posiciones de guardián de activos."(Herzog, 2010)

3.4.1 Seguridad Operacional

3.4.1.1 Visibilidad (Pv)

"Enumeración y verificación de pruebas para la visibilidad del personal con el que la interacción es posible a través de todos los canales."(Herzog, 2010)

Enumeración de Personal

- "Enumerar el número de personal dentro del ámbito de acceso tanto a los autorizados y a los no autorizados a los procesos dentro del campo de aplicación, sin importar el tiempo o el canal de acceso, y el método para la obtención de esos datos." (Herzog, 2010)

Los resultados se muestran en la tabla 5:

Tabla 5: Resultados Visibilidad Canal Humano

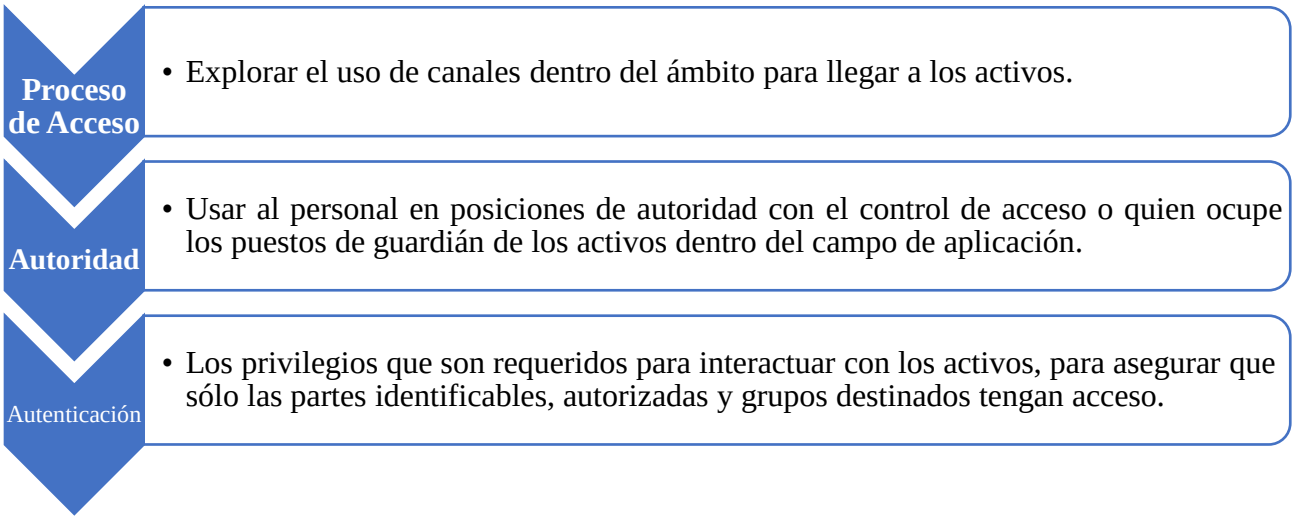
Visibilidad		
Personal autorizado	Objetivo: Data Center	❖ Rectorado ❖ Vicerrectorado ❖ Dirección de TICs
	Objetivo: Racks de comunicación	❖ Dirección de TICs
	Objetivo: Estaciones de trabajo	❖ Todo el personal puede acceder
Personal no autorizado	Objetivo: Data Center Objetivo: Racks de comunicación	Departamentos académicos Direcciones administrativas Centros de complementación académica
	Objetivo: Estaciones de trabajo	Personas ajenas a la institución.

Fuente: Elaboración Propia

Para la visibilidad se obtiene un valor de **P_V=5**; debido al personal que tiene acceso a los procesos dentro del campo de aplicación.

3.4.1.2 Acceso (P_A)

"Una persona que responde a una consulta cuenta como un acceso con todo tipo de consultas (todas las diferentes preguntas que usted pueda pedir o declaraciones hechas cuentan como el mismo tipo de respuesta en el mismo canal)."(Herzog, 2010)



Los resultados se muestran en la tabla 6:

Tabla 6: Resultados Acceso Canal Humano

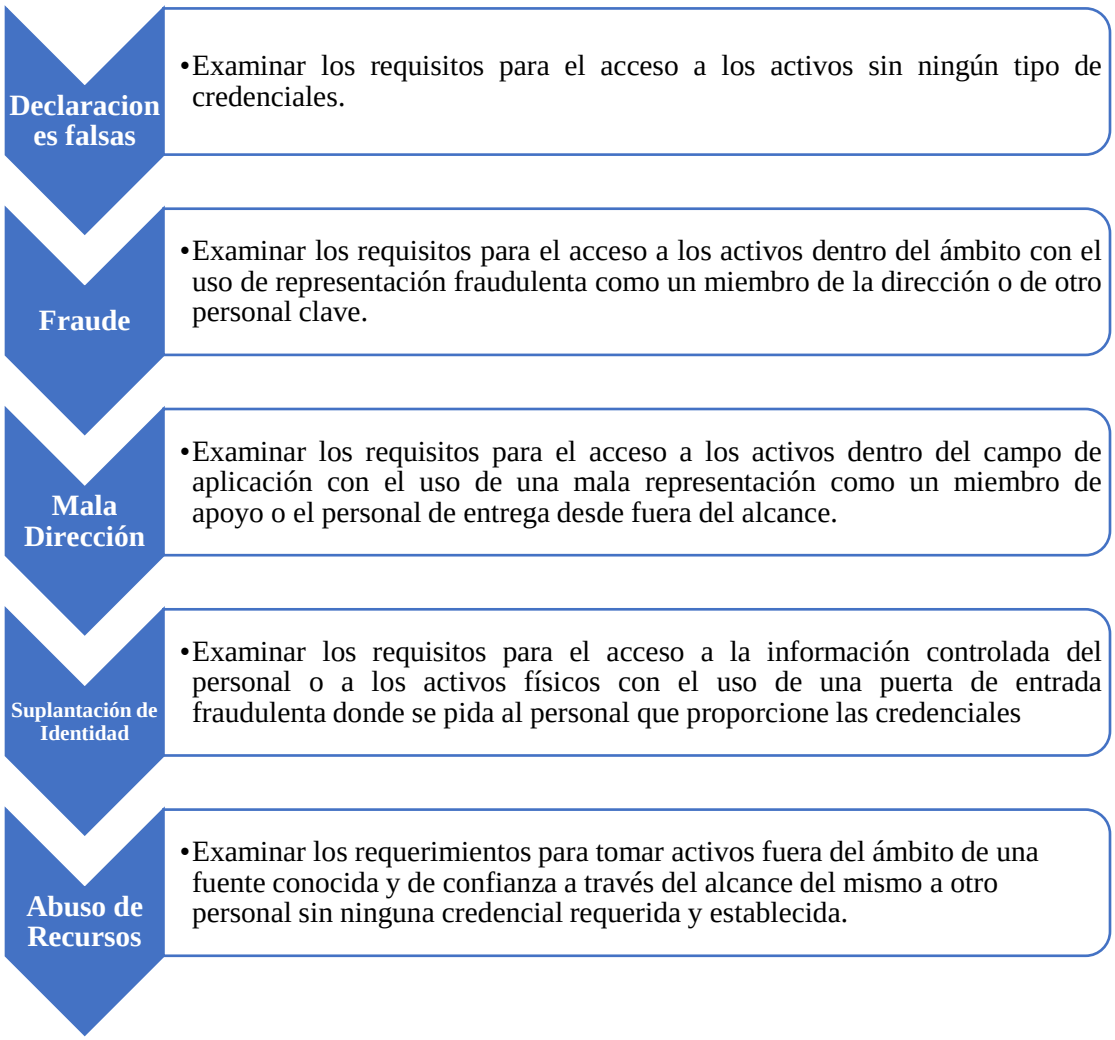
Acceso		
Proceso de acceso	Red Interna	❖ Laptops ❖ Celulares ❖ Estaciones de trabajo
Autoridad	Guardia	Seguridad privada Encargado de TIC's
Autenticación	❖ En la mayoría de los casos no se requiere autorización.	

Fuente: Elaboración Propia

Para el acceso se obtuvo un valor de **P_A = 4**; esto debido a las falencias que se tiene.

3.4.1.3 Confianza (P_T)

"Las pruebas de confianzas entre el personal dentro del ámbito donde la confianza se refiere al acceso a la información o los activos físicos de otros objetivos dentro del campo de aplicación."(Herzog, 2010)



Los resultados se muestran en la tabla 7:

Tabla 7: Resultados Confianza Canal Humano

Confianza	
Declaraciones falsas	Sin Requisitos: ❖ Estaciones de trabajo de estudiantes ❖ Racks
Fraude	No se tiene acceso
Mala Dirección	❖ Si se tiene acceso
Suplantación de Identidad	No se tiene acceso
Abuso de Recursos	No se pueden tomar los activos

Fuente: Elaboración Propia

Para la confianza se obtuvo un valor numérico de $\mathbf{P_T = 3}$, esto debido a los activos que se tiene acceso mediante declaraciones falsas y la mala dirección.

Con los valores de los puntos que plantea la seguridad operacional, se procede con el cálculo del valor de $\mathbf{OpSec_{sum}}$ o la **porosidad** del canal humano, aplicando la ecuación 1:

$$\mathbf{OpSec_{sum} = P_V + P_A + P_T}$$

$$\mathbf{OpSec_{sum} = 7 + 4 + 3}$$

$$\underline{\mathbf{OpSec_{sum} = 14}}$$

3.4.2 Controles

3.4.2.1 Autenticación ($\mathbf{LC_{Au}}$)

"Enumerar y examinar las deficiencias del personal de control del campo de aplicación y los privilegios que son requeridos para interactuar con ellos para asegurar que sólo las partes identificables, autorizadas y grupos destinados tengan acceso."(Herzog, 2010)

Los resultados para este control se muestran en la tabla 8:

Tabla 8: Resultados Autenticación Canal Humano

Autenticación	
Privilegios requeridos	❖ Identificación ❖ Claves de acceso ❖ Oficios de petición ❖ Biométrico ❖ Tarjeta RFID

Fuente: Elaboración Propia

Como se puede apreciar los privilegios requeridos para acceder a las diferentes instancias de la institución, dan un valor numérico para la autenticación de **$LC_{Au} = 5$**.

3.4.2.2 Indemnización (LC_{Id})

"Enumerar el abuso o burla de la política de empleo, el seguro, no divulgación, no competencia, contratos de responsabilidad, o el uso / renuncias de usuarios con todo el acceso al personal dentro del alcance sobre todos los canales."(Herzog, 2010)

Tabla 9: Resultados Indemnización Canal Humano

Indemnización	
Documentos que aseguran los objetivos	❖ Contrato en el cual se especifica el acuerdo de confidencialidad.

Fuente: Elaboración Propia

En vista de que los activos no se encuentran asegurados por compañías privadas y solo existen las normas estipuladas en el contrato de los empleados, el valor numérico de la indemnización es de **$LC_{Id} = 1$**.

3.4.2.3 Subyugación (LC_{Su})

"Enumerar las insuficiencias de los activos comunicados a través de canales en los que los controles no son necesarios, pueden ser eludidos o ignorados, como el correo electrónico inseguro o sobre una línea telefónica pública."(Herzog, 2010)

Debido a que en todos los canales son necesarios los controles, se asigna un valor numérico para la subyugación de **$LC_{Su} = 0$.**

3.4.2.4 Continuidad (LC_{Ct})

"Enumerar y poner a prueba las insuficiencias de todo el personal con respecto a los retrasos de acceso y el tiempo de respuesta del servicio a través del personal de apoyo o medios automatizados para el acceso a la puerta del campo de acción alternativa."(Herzog, 2010)

En caso de presentarse problemas con el personal, no se generan conflictos que atenten contra la seguridad de los activos de la institución, por tal motivo el valor numérico para la continuidad es de **$LC_{Ct} = 0$.**

3.4.2.5 Resistencia (LC_{Re})

"Enumerar y poner a prueba las insuficiencias en todos los canales del personal dentro del campo de acción mediante la eliminación o tranquilizar al personal de puerta, permitirá el acceso directo a los activos."(Herzog, 2010)

Los resultados para la resistencia se muestran en la tabla 10:

Tabla 10: Resultados Resistencia Canal Humano

Resistencia	
Activos a los que se tiene acceso	❖ Racks ❖ Estaciones de trabajo ❖ Equipos inalámbricos

Fuente: Elaboración Propia

En vista de que mediante la eliminación del personal de puerta se puede tener acceso a diferentes activos, para la resistencia se tiene un valor de **$LC_{Re} = 3$.**

3.4.2.6 No-repudio (LC_{NR})

"Enumerar y examinar para su uso o insuficiencias de personal de guardia para identificar correctamente y registrar el acceso o interacciones con los activos de evidencias específicas para desafiar el repudio."(Herzog, 2010)

Los resultados para este control se muestran en la tabla 11:

Tabla 11: Resultados No-Repudio Canal Humano

No-Repudio	
Áreas con registro de acceso	❖ Garaje ❖ Biblioteca ❖ Laboratorios

Fuente: Elaboración Propia

Para el No-Repudio se asigna un valor numérico de **LC_{NR} = 3**, pues son 3 las instancias en las cuales se lleva un registro.

3.4.2.7 Confidencialidad (LC_{Cf})

"Enumerar y examinar para su uso o insuficiencias de todos los segmentos de comunicación con el personal dentro del ámbito a través de un canal o propiedades transportadas por un canal usando líneas seguras, encriptación, interacciones personales "cercanas" o "calladas" para proteger la confidencialidad de la los activos de información que sólo conocen los que tienen la debida autorización de seguridad de ese activo."(Herzog, 2010)

Los resultados de la confidencialidad se muestran en la tabla 12:

Tabla 12: Resultados Confidencialidad Canal Humano

Confidencialidad	
Comunicaciones seguras	❖ Correo Electrónico ❖ Telefonía IP ❖ Encriptación ❖ Portafolios

Fuente: Elaboración Propia

Las confidencialidad obtiene un valor numérico de **LC_{Cf} = 4.** Pues los medios de comunicación usados son seguros.

3.4.2.8 Privacidad (LC_{Pr})

"Enumerar y examinar para el uso o insuficiencias de todos los segmentos de comunicación con el personal dentro del ámbito a través de un canal o propiedades transportados utilizando firmas individuales específicos, identificación personal, interacciones personales "calladas" o "a puerta cerrada" para proteger la privacidad de la interacción y el proceso de proporcionar activos sólo a aquellos dentro de la acreditación de seguridad adecuada para ese proceso, la información o los activos físicos."(Herzog, 2010)

El resultado para el control de la privacidad está en la tabla 13.

Tabla 13: Resultados Privacidad Canal Humano

Privacidad	
Procesos eficientes	❖ Interacciones personales ❖ Identificación personal

Fuente: Elaboración Propia

Los proceso eficientes nos dan un valor numérico para la privacidad de **$LC_{Pr} = 2$**.

3.4.2.9 Integridad (LC_{It})

"Enumerar y examinar las insuficiencias de todos los segmentos de la comunicación con el personal dentro del ámbito donde los activos son transportados por un canal mediante un proceso documentado, firmado, cifrado, encriptado, o con marcas para proteger y asegurar que la información de los activos físicos no puedan ser cambiados, conmutados, re-dirigidos o invertidos sin ser conocido por las partes involucradas."(Herzog, 2010)

El resultado para la integridad está en la tabla 14.

Tabla 14: Resultados Integridad Canal Humano

Integridad	
Procesos eficientes	❖ Firmas ❖ Marcas

Fuente: Elaboración Propia

El valor numérico para la integridad es **LC_{It} = 2.**

3.4.2.10 Alarma (LC_{Al})

"Verificar e indicar la utilización de un sistema de alerta localizado o el sistema de alarma en todo el alcance, registro, o un mensaje de cada puerta de enlace de acceso sobre cada canal cuando una situación sospechosa es observada por el personal al sospechar un intento de evasión, ingeniería social, o una actividad fraudulenta."(Herzog, 2010)

Los resultados para este control se muestran en la tabla 15.

Tabla 15: Resultados Alarma Canal Humano

Alarma	
Sistemas utilizados	❖ Sistema de video vigilancia ❖ Antivirus ❖ Guardias

Fuente: Elaboración Propia

Gracias a los sistemas utilizados, se obtiene un valor numérico para la alarma de **LC_{Al} = 3.**

Con los valores de los 10 controles que estipula la auditoria, se procede a calcular el valor total de la Suma de Controles, aplicando la ecuación 2:

$$LC_{sum} = LC_{Au} + LC_{Id} + LC_{Re} + LC_{Su} + LC_{Ct} + LC_{NR} + LC_{Cf} + LC_{Pr} + LC_{It} + LC_{Al}$$

$$LC_{sum} = 5 + 1 + 3 + 0 + 0 + 3 + 4 + 2 + 2 + 3$$

$$LC_{sum} = 23$$

3.4.3 Limitaciones

3.4.3.1 Vulnerabilidad (Lv)

"En HUMSEC, una vulnerabilidad puede ser un prejuicio cultural que no permite que un empleado pregunte a otros que miran fuera de lugar o una falta de formación que deja un nuevo secretario para dar a conocer la información comercial clasificada para uso interno." (Herzog, 2010)

Los resultados para esta limitación se muestran en la tabla 16.

Tabla 16: Resultados Vulnerabilidad Canal Humano

Vulnerabilidad
❖ Nuevo personal puede divulgar información clasificada.

Fuente: Elaboración Propia

En cuanto a esta limitación, el valor numérico para la vulnerabilidad es de **L_V = 1.**

3.4.3.2 Debilidad (L_W)

"En HUMSEC, una debilidad puede ser un proceso fallido de un segundo guardia al tomar el mando de guardia que se ejecuta después de un intruso o un clima cultural dentro de una empresa para permitir a los amigos en espacios publicados como restringidos."(Herzog, 2010)

Para la autenticación no se presentan fallas pues no se pueden vulnerar los controles existentes.

- En cuanto a la indemnización **no se puede comprobar al 100% que los empleados eludan el contrato firmado**.

Para los demás controles no se encontraron errores que puedan vulnerar la seguridad de la institución. En consecuencia el valor para la Debilidad es de:

$$L_W = FC_{Au} + FC_{Id} + FC_{Re} + FC_{Su} + FC_{Ct}$$

$$L_W = 0 + 1 + 0 + 0 + 0$$

$$L_W = 1$$

3.4.3.3 Preocupación (L_C)

"En HUMSEC, una preocupación puede ser un fallo de proceso de un guardia que mantiene el mismo horario y una rutina o un clima cultural dentro de una empresa que permite

a los empleados el uso de salas de reuniones públicas para los negocios internos.”(Herzog, 2010)

La preocupación también obtiene un valor numérico de **L_C = 0,** pues los guardias mantienen turnos rotativos.

3.4.3.4 Exposición (L_E)

“En HUMSEC, una exposición puede ser un guardia que permite a todos los visitantes ver la lista de nombres en la hoja de registro o un operador de empresa que informa a las personas que llaman que una persona está enferma o de vacaciones.”(Herzog, 2010)

Los guardias no tienen hoja de registro, y no pueden brindar información sin previa autorización. Por lo tanto la exposición tiene un valor numérico de **L_E = 0.**

3.4.3.5 Anomalía (L_A)

“En HUMSEC, una anomalía pueden ser inquietudes que un guardia le preguntan las que pueden parecer irrelevantes para el trabajo, ya sea una pequeña charla o estándar.”(Herzog, 2010)

Los guardias no poseen información crítica para la institución, es por esto que la anomalía tiene un valor numérico de **L_A = 0.**

3.4.4 Calculadora RAV

Los resultados obtenidos para el canal humano se muestran a continuación:

Métricas de Seguridad Humana

OSSTMM version 3.0

Rellene en los campos en blanco los valores numéricos para OPSEC, Controles y Limitaciones con los resultados de la prueba de seguridad. Consulte OSSTMM 3 (www.osstmm.org) para obtener más información.

OPSEC			
Visibilidad	5		
Acceso	4		
Confianza	3		
Total (Porosidad)	12		

CONTROLES			
Clase A		Ausentes	
Autenticación	5	7	
Indemnización	1	11	
Resistencia	3	9	
Subyugación	0	12	
Continuidad	0	12	
Total Clase A	9	51	
Clase B		Ausentes	
No-Repudio	3	9	
Confidencialidad	4	8	
Privacidad	2	10	
Integridad	2	10	
Alarma	3	9	
Total Clase B	14	46	
		Ausentes Verdaderos	
Total todos los Controles	23	97	
Cobertura Total	19,17%	80,83%	

LIMITATIONS		Item Value	Total Value
Vulnerabilidades	1	9,08	9,08
Debilidades	1	5,25	5,25
Preocupaciones	0	4,83	0,00
Exposiciones	0	0,77	0,00
Anomalías	0	0,37	0,00
Total # Limitaciones	2		14,33

OPSEC	9,48
Controles Verdaderos	5,59
Controles Totales	5,59
Cobertura Verdadera A	15,00%
Cobertura Verdadera B	23,33%
Cobertura Verdadera Total	19,17%
Limitaciones	9,964440
Seguridad Δ	-13,86
Proteccion Verdadera	86,14

Seguridad Actual: 86,00 ravs

Luego de ingresar los valores obtenidos en la calculadora RAV, se obtienen que la Seguridad Actual de la UPEC en el canal Humano es de **85,53 RAVS**, lo que se interpreta en que se posee una deficiencia de aproximadamente el 15%, lo cual no significa que la institución vaya a ser atacada, sino que muestra la vulnerabilidad de la institución en caso de un ataque. Los motivos principales para tener una deficiencia que supere el 10% es que los controles para la indemnización, subyugación y continuidad son prácticamente nulos, por lo cual deben ser los controles que se aborden con mayor prioridad.

Por otra parte la **Seguridad Δ,** toma un valor negativo de **-14,35,** este valor es interpretado como la insuficiencia de controles que posee la institución en cuanto al talento humano, además muestra que los controles que se encuentran aplicados tienen falencias por lo cual necesitan ser mejorados para que estos se adecúen a las necesidades de seguridad que la universidad requiere.

3.5 Pruebas de Seguridad Física

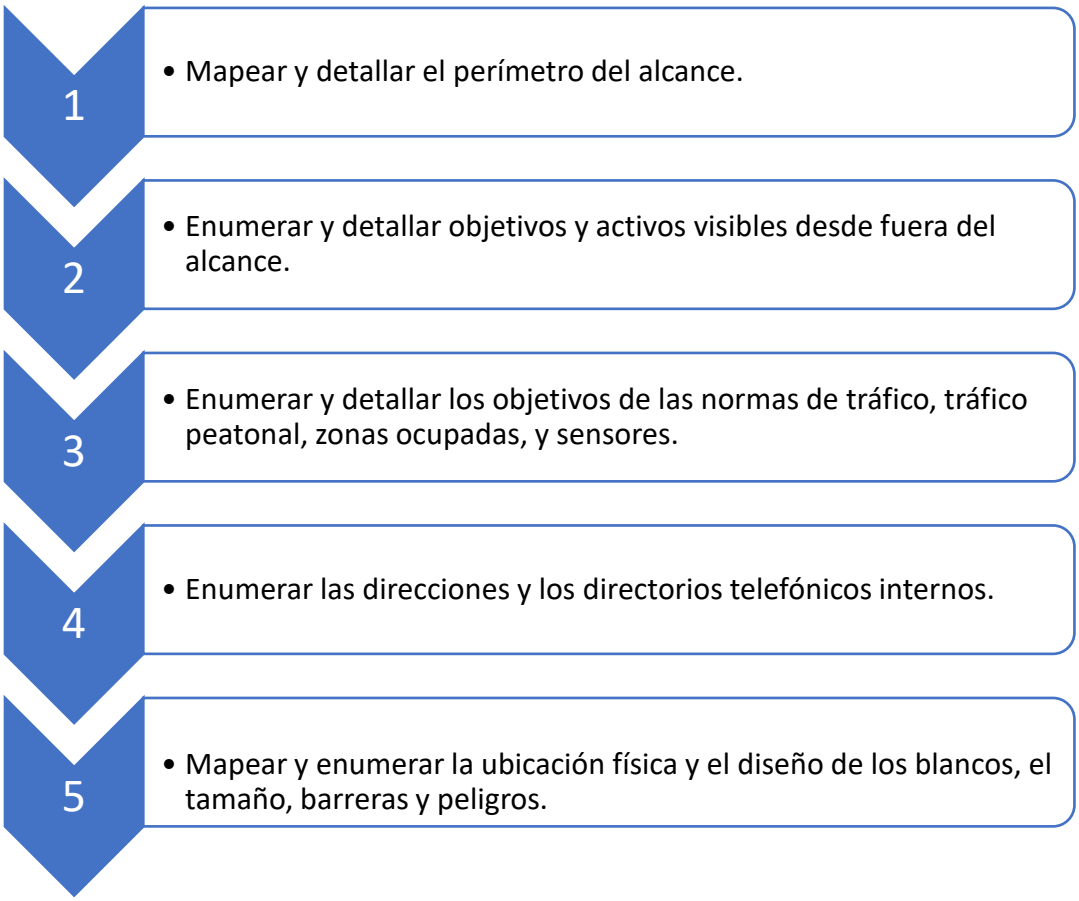
"PHYSSEC (Seguridad Física), para probar este canal se requiere una interacción no-comunicativa con las barreras y las personas encargadas de la seguridad de los activos. Aunque muchas veces es considerada como "allanamiento de morada" el verdadero objetivo es valorar la barrera física y lógica, además medir la brecha que existe con el estándar de seguridad requerida."(Herzog, 2010)

3.5.1 Seguridad Operacional

Para este punto se requiere las mediciones de visibilidad, confianza y acceso, es decir obtener los valores cuantitativos.

3.5.1.1 Visibilidad (Pv)

La visibilidad se evalúa siguiendo el siguiente proceso:



Los resultados de este proceso se muestran en la tabla 17:

Tabla 17: Resultados de visibilidad del Canal Físico

Visibilidad	
Perímetro del alcance	❖ Al ser una universidad, todo el campus es de acceso público.
Objetivos y activos fuera del alcance	❖ Centro de educación infantil
Normas de Tráfico	❖ Si se cuenta con normas de trafico ❖ La UPEC si cuenta con normas de tráfico peatonal
Direcciones y directorios telefónicos	❖ Al ser una institución pública, las direcciones, directorios telefónicos son accesibles al público.
Ubicación del objetivo	❖ Racks de comunicación de los edificios ❖ Estaciones de trabajo

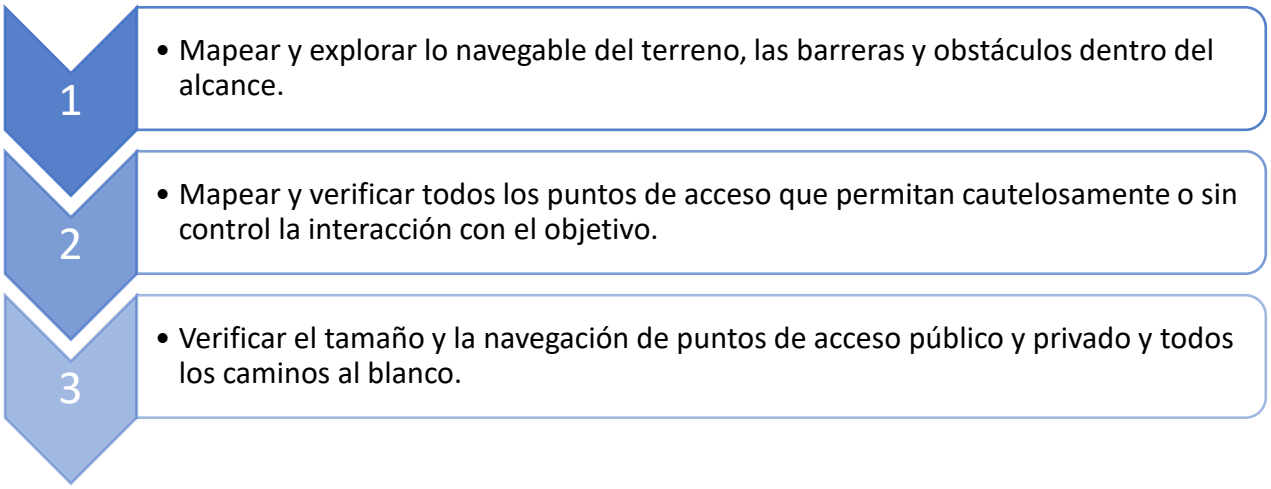
Fuente: Elaboración Propia

Para la **Visibilidad** se obtuvo un valor de: **$P_V = 7$**, este resultado se obtiene contabilizando los puntos enumerados en la tabla de resultados, en vista de que son objetivos y activos físicos visibles para cualquier persona debido a que es una institución educativa pública.

3.5.1.2 Acceso (P_A)

Para realizar estas pruebas se debe tomar en cuenta lo siguiente:

Enumeración:



Localización:

1. Mapear la distancia desde el perímetro del campo de aplicación a los blancos visibles y los activos de fuera del alcance.

Penetración:

1. Determinar cuáles barreras y obstáculos en el alcance proporcionan acceso remoto para cambiar, interrumpir, destruir, u obtener activos.
2. Determinar la efectividad de las barreras y obstáculos para soportar las condiciones definidas en Posture Review.
3. Determinar y evaluar la eficacia de las barreras y obstáculos para resistir incendios, explosiones, y las fuerzas de concusión generales.
4. Determinar y evaluar la eficacia de las barreras y obstáculos para reducir ingresos de: niveles de ruido críticos, calor, frío, humo, humedad, olores perjudiciales o cáusticos, campos magnéticos intensos, luz dañina, y contaminantes.
5. Determinar y evaluar la eficacia de las barreras y obstáculos para reducir: sonidos, olores, vibraciones, las condiciones para la aclimatación, el humo, los campos magnéticos, los residuos, y los contaminantes.

Los resultados se muestran en la tabla 18:

Tabla 18: Resultados de acceso del Canal Físico

Acceso		
Enumeración	Objetivo: Racks de Comunicación	❖ Guardias de seguridad pasan 2 veces por día ❖ 1 vía de acceso
	Objetivo: Estaciones de Trabajo	❖ Sistema de video-vigilancia.
Localización	Centro de educación infantil	❖ A 10 metros de la UPEC
Penetración	Barreras y Obstáculos	❖ Ruido ❖ Calor ❖ Frio

		❖ Humedad ❖ Humo ❖ Olores perjudiciales ❖ Luz dañina

Fuente: Elaboración Propia

Luego de evaluar este punto se obtiene que el valor numérico para el **Acceso** es de: **P_A = 11,** este valor fue obtenido contabilizando los valores con la viñeta, los cuales corresponde a las barreas físicas para proteger el objetivo de diferentes factores que estipula la metodología.

3.5.1.3 Confianza (P_T)

Pruebas de confianzas entre los procesos dentro del alcance donde la confianza se refiere al acceso a los activos sin la necesidad de identificación o autenticación.

Los resultados se muestran en la tabla 19:

Tabla 19: Resultados de confianza del Canal Físico

Confianza	
Identificación y autenticación	❖ Cualquier persona puede tener acceso a los activos de la Institución, sin necesidad de una identificación o autenticación.

Fuente: Elaboración Propia

La **Confianza** tomo el valor numérico de: **P_T = 1**, en vista de que al ser una institución educativa pública, cualquier persona tiene acceso a los activos de la institución, a excepción de los que se encuentran en el data center.

Con los valores de los 3 puntos que plantea la seguridad operacional, se procede con el cálculo del valor de **$OpSec_{sum}$** o la **porosidad** del canal físico, aplicando la ecuación 1:

$$\mathbf{OpSec_{sum} = P_V + P_A + P_T}$$

$$\mathbf{OpSec_{sum} = 7 + 11 + 1}$$

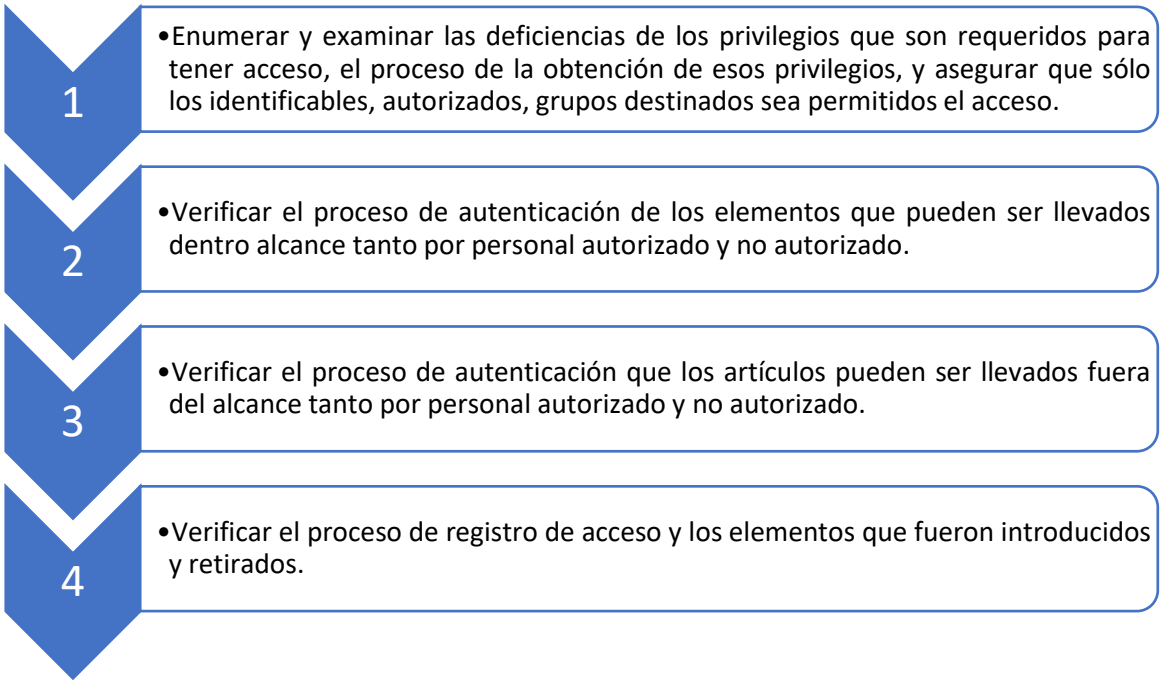
$$\underline{\mathbf{OpSec_{sum} = 19}}$$

3.5.2 Controles

Se realizan pruebas para enumerar los tipos de controles que se utilizan para proteger el valor de los activos.

3.5.2.1 Autenticación (LC_{Au})

Para evaluar este control se realiza el siguiente procedimiento:



Los resultados de este control se muestran en la tabla 20, para lo cual se tomó en cuenta todo el proceso sugerido por la metodología:

Tabla 20: Resultados del control Autenticación del Canal Físico

Autenticación		
Privilegios que son requeridos para tener acceso	Objetivo: Data Center	❖ Se requiere autorización del encargado del departamento de Redes y Telecomunicaciones.
	Objetivo: Racks de Comunicación	En vista de que no se encuentran bajo llave,

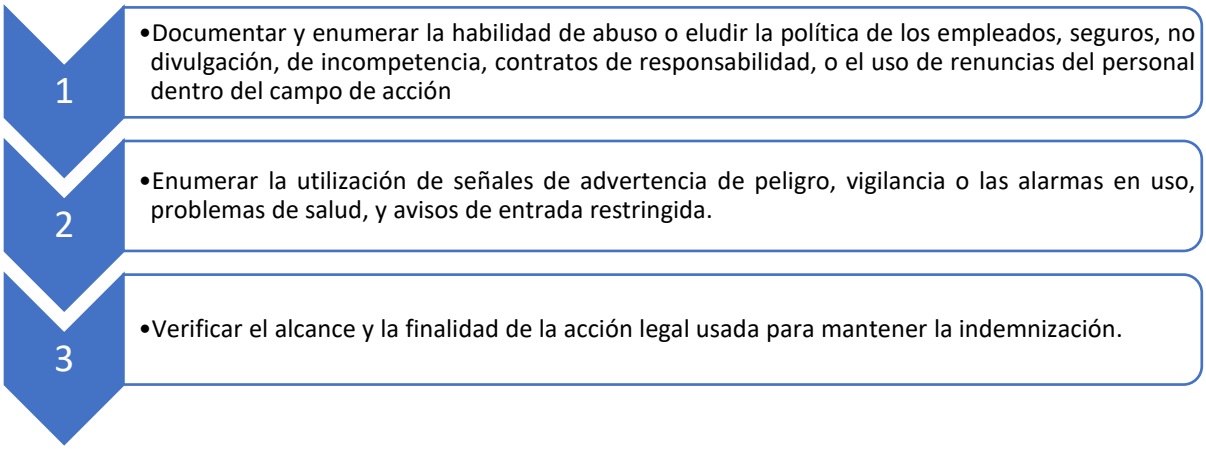
		cualquier persona puede tener acceso.
	Objetivo: Estaciones de Trabajo	Se tiene acceso a las estaciones de trabajo de los estudiantes, por cualquier persona.
Elementos que pueden ser llevados dentro alcance	Se puede llevar cualquier elemento dentro del alcance, debido a que es una institución de educación pública, entre los elementos que se puede llevar están, laptops, celulares, dispositivos de almacenamiento, incluso puntos de acceso básicos.	
Artículos pueden ser llevados fuera del alcance	❖ Los activos de la universidad no pueden ser llevados fuera del alcance, sin embargo no se puede controlar esto al 100%.	
Registro de acceso de elementos introducidos y retirados	No se lleva registro de los artículos que son introducidos y retirados de la universidad.	

Fuente: Elaboración Propia

Con los resultados obtenidos se asigna el valor numérico de la **Autenticación**: $LC_{Au} = 2$, en vista de que para acceder al objetivo solo se necesita la autorización del encargado del departamento de Redes y Telecomunicaciones, además no se puede llevar los activos de la universidad fuera del alcance, y esto es controlado por los guardias de seguridad y el sistema de video-vigilancia.

3.5.2.2 Indemnización (LC_{Id})

Para analizar este control se debe cumplir con los siguientes ítems:



El análisis correspondiente a este control se detalla en la tabla 21:

Tabla 21: Resultados del control Indemnización del Canal Físico

Indemnización		
Personal dentro del alcance	Política de los empleados Seguros Acuerdo de no divulgación Acuerdo de incompetencia Contratos de responsabilidad Renuncias del personal	❖ Se puede eludir No se puede eludir ❖ Se puede eludir No se puede eludir No se puede eludir No se puede eludir
Señalización dentro del alcance	Señales de advertencia de peligro Vigilancia o las alarmas Problemas de salud Avisos de entrada restringida.	❖ Si se utiliza ❖ Si se utiliza ❖ Si se utiliza ❖ Si se utiliza
Acción legal	❖ Los empleados al firmar el contrato, se comprometen a salvaguardar los activos de la UPEC, y en caso de infringir esta cláusula se procede con la acción legal para indemnizar a la institución.	

Fuente: Elaboración Propia

El valor numérico para la **Indemnización** es **LC_{Id} = 7**, sumando los ítems marcados con la viñeta, en los cuales están las políticas que pueden ser eludidas, las señales usadas dentro del campus y la acción legal en caso de dañar los activos de la institución.

3.5.2.3 Subyugación (LC_{Su})

"Para evaluar este control se debe enumerar y poner a prueba las deficiencias en el acceso a los bienes no controlados por la fuente que proporcione el acceso (es decir, números PIN, fotos de identificación, etc. seleccionado por el actor, insignias con números de identificación escritos por el actor, etc.)."(Herzog, 2010)

Los resultados para la subyugación se muestran en la tabla 22:

Tabla 22: Resultados del control Subyugación del Canal Físico

Subyugación:	
Deficiencias en el acceso a los bienes	❖ Para acceder a los diferentes servicios que posee la UPEC se hace

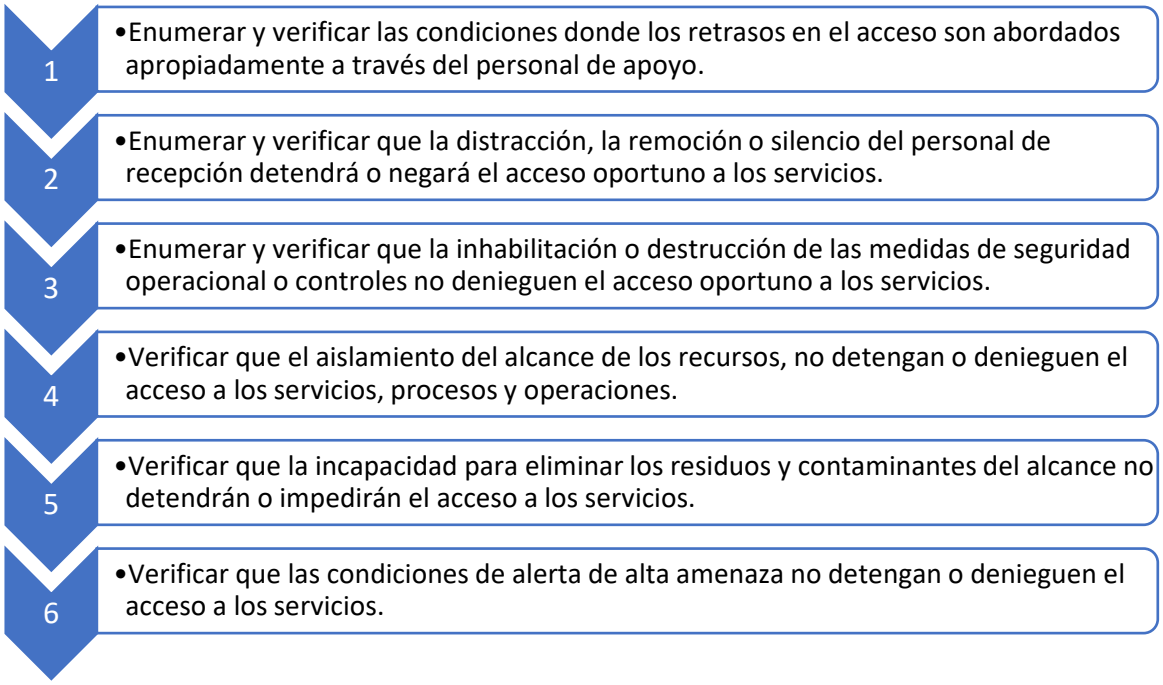
	❖ uso de claves personalizadas, que se recomienda memorizar y no compartir con ninguna persona. ❖ Para tener acceso al Data Center se debe contar con el código y la tarjeta magnética.

Fuente: Elaboración Propia

El valor numérico de **Subyugación** es de: **LC_{Su} = 2**, en vista de que si se usan claves y otros métodos de autenticación para acceder al objetivo.

3.5.2.4 Continuidad (LC_{Ct})

La Continuidad se evalúa siguiendo este proceso:



Los resultados se detallan en la tabla 23:

Tabla 23: Resultados del control Continuidad del Canal Físico

Continuidad		
Retrasos en el acceso	Personal de apoyo Medio automatizado	❖ Si es abordado No es abordado
Personal de recepción	Distracción Remoción Silencio	❖ No deniega el acceso ❖ No deniega el acceso ❖ No deniega el acceso

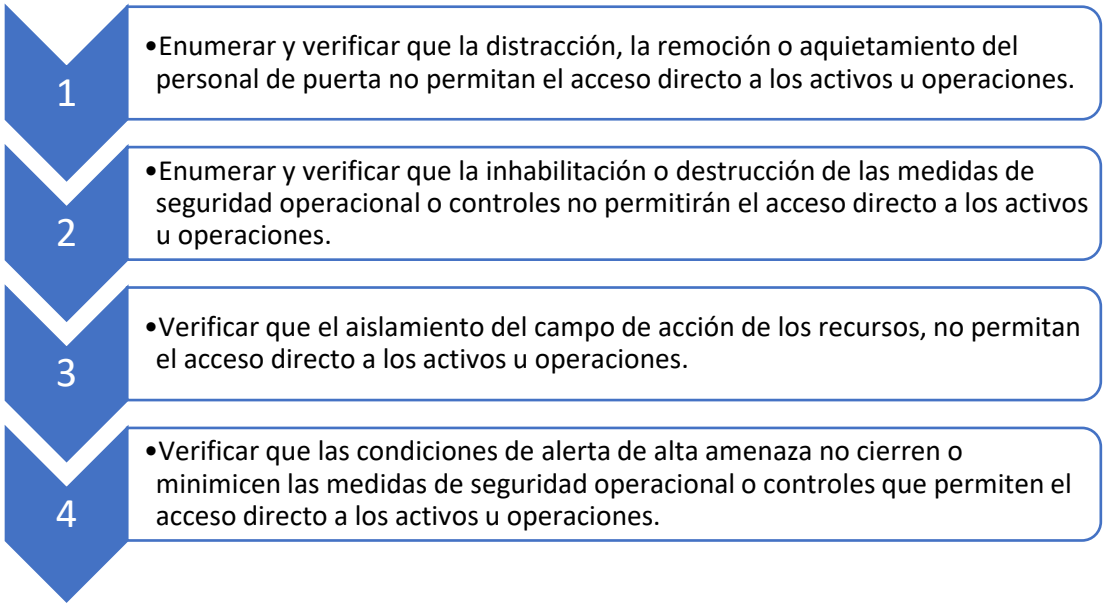
Medidas de seguridad operacional	Inhabilitación o destrucción	Denieguen el acceso
Aislamiento de los recursos	Combustible Energía eléctrica Alimentos Agua Comunicaciones	❖ No detiene el acceso Detiene el acceso ❖ No detiene el acceso ❖ No detiene el acceso Detiene el acceso
Eliminación de residuos	Residuos Contaminantes	❖ No impiden el acceso ❖ No impiden el acceso
Alerta de alta amenaza	Una alerta de este tipo, obliga a que se realice una evacuación total de la institución, por tal motivo se detienen todos los servicios, procesos y operaciones que se llevan a cabo en la UPEC.	

Fuente: Elaboración Propia

En base a los resultados obtenidos se llega al valor numérico de la **Continuidad, LC_{Ct} =** 9, debido a que los retrasos son abordados oportunamente por el personal de apoyo, y las anomalías en el personal de recepción no deniegan el acceso, además el aislamiento de determinados recursos no detiene el acceso a los servicios así como también los problemas con la eliminación de residuos tampoco impide el acceso.

3.5.2.5 Resistencia (LC_{Re})

Este control se debe abordar de la siguiente manera:



EL análisis de estos puntos se resume en la tabla 24:

Tabla 24: Resultados del control Resistencia del Canal Físico

Resistencia		
Personal de recepción	Distracción Remoción Aquietamiento	❖ No permite el acceso ❖ No permite el acceso ❖ No permite el acceso
Medidas de Seguridad Operacional	Inhabilitación o destrucción	Si permite el acceso
Aislamiento de recursos	Combustible Energía Alimentos Agua Comunicaciones	❖ No permite el acceso Si permite el acceso ❖ No permite el acceso ❖ No permite el acceso Si permite el acceso
Alerta de alta amenaza	Al evacuar toda la universidad se puede tener acceso directo con todos los activos de la universidad, a excepción del centro de datos.	

Fuente: Elaboración Propia

La asignación numérica para la **Resistencia** es de **LC_{Re} = 7,** porque el personal de recepción no influye en el acceso a los activos, además aislar determinados recursos tampoco es razón para permitir el acceso a los activos.

3.5.2.6 No-repudio (LC_{NR})

"Enumerar y examinar el uso o insuficiencias de los monitores y sensores e identificar correctamente y registrar el acceso o la interacción con los activos para una evidencia específica a desafiar el repudio. Documentar la profundidad de la interacción que es registrada."(Herzog, 2010)

Los resultados para este control se muestran en la tabla 25:

Tabla 25: Resultados del control No-repudio del Canal Físico

No-repudio	
Monitores y Sensores	❖ Se utiliza sistema de video-vigilancia en el campus universitario.

Fuente: Elaboración Propia

El valor numérico para el No-repudio es de **LC_{NR} = 1**, debido a que solo se cuenta con un método para registrar el acceso a los activos y asegurar el No-repudio, la video-vigilancia como se puede apreciar en la imagen 11.

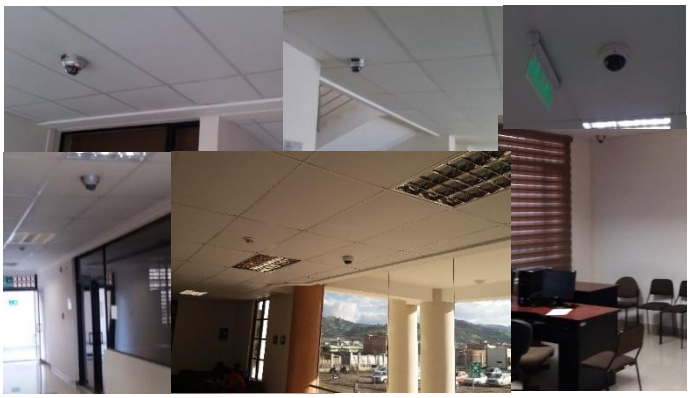


Imagen 16: Algunas cámaras del sistema de video-vigilancia UPEC
Fuente: Elaboración Propia

3.5.2.7 Confidencialidad (LC_{Cf})

"Enumerar y examinar el uso o insuficiencias de todas las señales, la comunicación física, y objetos transportados entre los procesos de alcance interno y externo usando códigos del personal, lenguaje indescifrable, interacciones personales "calladas" o "cercanas" para promover la confidencialidad de la comunicación solamente a aquellos con la clasificación debida de la autorización de seguridad para esa comunicación."(Herzog, 2010)

Los resultados para la confidencialidad se detallan en la tabla 26:

Tabla 26: Resultados del control Confidencialidad del Canal Físico

Confidencialidad	
Confidencialidad de la comunicación	❖ Las reuniones se realizan a puerta cerrada, para evitar que se escuchen las decisiones tomadas y estas no puedan afectar a la institución. ❖ Los documentos se llevan de forma personal, para evitar que terceros se enteren de los tramites que se realizan.

Fuente: Elaboración Propia

La **Confidencialidad** adquiere un valor numérico de **LC_{Cf} = 2**, en vista de que la confidencialidad se realiza usando interacciones directas y en caso de reuniones bajo puerta cerrada.

3.5.2.8 Privacidad (LC_{Pr})

"Enumerar y examinar para el uso o deficiencias de todas las interacciones dentro del campo de acción usando paquetes no marcados o no evidentes, o etiquetadas, las interacciones "calladamente" o a "cuarto cerrado", y dentro de cuartas partes elegidas al azar para ocultar o proteger la privacidad de la interacción y solamente a aquellos con la debida autorización de seguridad para ese proceso o activo."(Herzog, 2010)

El análisis de este control se encuentra en la tabla 27:

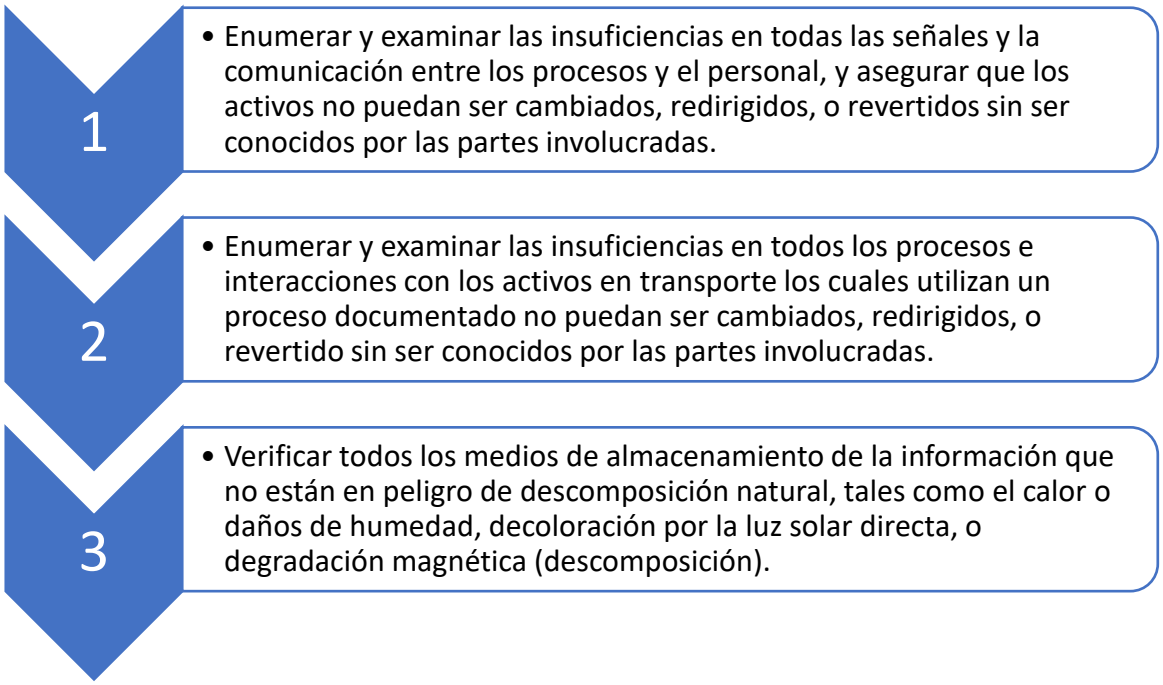
Tabla 27: Resultados del control Privacidad del Canal Físico

Privacidad	
Paquetes no marcados o no evidentes	❖ Los documentos aunque son llevados con precaución, no tienen un identificativo de que sean cruciales para la institución.
Cuarto Cerrado	❖ Al igual que en la confidencialidad, se usa las oficinas a puerta cerrada para evitar la fuga de la información fuera del personal autorizado.

Fuente: Elaboración Propia

La **Privacidad** tiene un valor numérico de **LC_{Pr} = 2**, ya que los documentos importantes no son identificados como tal y las reuniones siempre se realizan a puerta cerrada.

3.5.2.9 Integridad (LC_{It})



Los resultados se detallan en la tabla 28:

Tabla 28: Resultados del control Integridad del Canal Físico

Integridad		
Personal y procesos	Comunicación entre los procesos Proceso documentado	❖ Buena comunicación ❖ Personal
Activos en transporte	Activos	❖ Etiquetas ❖ Inventario
Medios de almacenamiento	❖ Se realiza un mantenimiento constante de todos los activos, en los cuales están presentes los medios de almacenamiento.	

Fuente: Elaboración Propia

En cuanto a la **Integridad** se tiene un valor numérico de: **LC_{It} = 5,** pues si existen buenas maneras para asegurar la integridad de los procesos, y activos de la institución.

3.5.2.10 Alarma (LC_{Al})

"Verificar y enumerar la utilización de un sistema de alerta localizado en todo el alcance, ingreso o mensaje para cada puerta de acceso en una situación sospechosa observada por el

personal en caso de sospecha de intentos de burla, actividad fraudulenta, infracción, o violación. Asegurarse que los sensores / sistemas estén instalados de acuerdo a las normas nacionales, regionales o internacionales y regularmente probados para cubrir todos los puntos de acceso."(Herzog, 2010)

Este control esta detallado en la tabla 29:

Tabla 29: Resultados del control Alarma del Canal Físico

Alarma	
Sistema de alerta	❖ El único método para constar intrusión son las cámaras que son monitoreadas constantemente por el personal de seguridad.

Fuente: Elaboración Propia

El valor numérico para la **Alarma** es de: $\mathbf{LC_{Al} = 1}$, debido a que las cámaras son el único método utilizado para detectar intrusos.

Con los valores de los 10 controles que estipula la auditoria, se procede a calcular el valor total de la Suma de Controles, aplicando la ecuación 2:

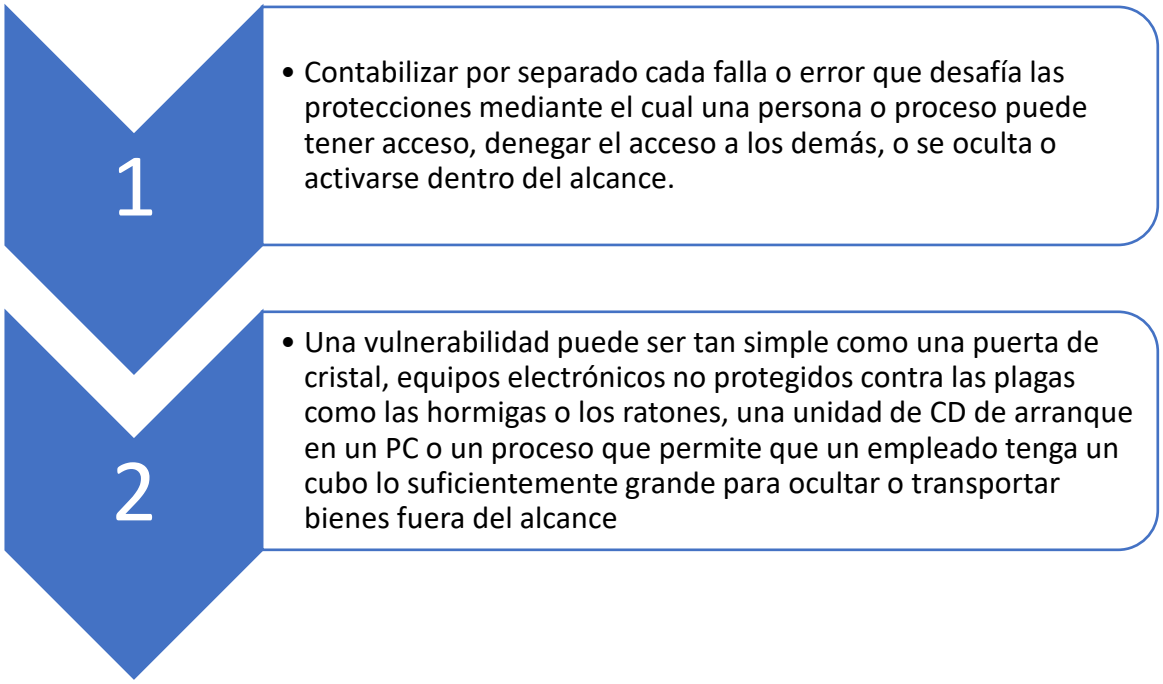
$$\boldsymbol{LC_{sum} = LC_{Au} + LC_{Id} + LC_{Re} + LC_{Su} + LC_{Ct} + LC_{NR} + LC_{Cf} + LC_{Pr} + LC_{It} + LC_{Al}}$$

$$\boldsymbol{LC_{sum} = 2 + 7 + 7 + 2 + 9 + 1 + 2 + 2 + 5 + 1}$$

$$\boldsymbol{LC_{sum} = 38}$$

3.5.3 Limitaciones

3.5.3.1 Vulnerabilidad (L_V)



Por medio de la observación directa se obtuvieron los resultados detallados en la tabla 30:

Tabla 30: Resultados de las vulnerabilidades del Canal Físico

Vulnerabilidades	
Falla o error	❖ El número de guardias no es el suficiente para cubrir toda la instalación de la UPEC. ❖ Las puertas donde se ubican los racks permanecen sin seguro la mayor parte del tiempo. ❖ No existe control de plagas para proteger los equipos electrónicos. ❖ Los empleados tienen la facilidad para extraer diferentes activos fuera del campus universitario. ❖ Las estaciones de trabajo no están empotradas para evitar que sean sustraídas.

Fuente: Elaboración Propia

Las **Vulnerabilidades** presentan un valor numérico de: $L_V = 5$, por los ítem enumerados en los cuales se hace evidencia de las vulnerabilidades más importantes que posee la UPEC.

3.5.3.2 Debilidad (L_W)

"Contabilizar cada defecto o error en los controles para la interactividad: la autenticación, la indemnización, la resistencia, el sometimiento y la continuidad."(Herzog, 2010)

Tabla 31: Resultados de las debilidades del Canal Físico

Debilidad	
Autenticación	❖ No se puede controlar todos los activos que tiene la UPEC.
Indemnización	❖ Los acuerdos firmados no pueden ser controlados en su totalidad. ❖ Aunque si existen señales de peligro no cubren todas las instalaciones. ❖ La video-vigilancia no es perfecta, debido a que es monitoreada por una sola persona.
Resistencia	❖ Se puede circular libremente por todas las instalaciones.
Subyugación	❖ A pesar de las recomendaciones del encargado del área de redes y telecomunicaciones, parte del personal tiene las contraseñas pegadas en los monitores.
Continuidad	No se presentan anomalías en este control.

Fuente: Elaboración Propia

Con este análisis se presenta un valor para la **Debilidad** de: **L_W = 6**, gracias a que se presentan varias debilidades en los controles especificados por la metodología.

3.5.3.3 Preocupación (L_C)

"Una preocupación puede ser un mecanismo de bloqueo de la puerta cuyos controles y tipos de claves de operación son públicos, un generador de respaldo sin medidor de potencia o indicador de combustible, un proceso de equipos que no requiere que el empleado para firmar la salida de materiales cuando se reciben, o una alarma de incendio no lo suficientemente fuerte para ser escuchado por los trabajadores de la máquina con tapones para los oídos."(Herzog, 2010)

Los resultados están detallados en la tabla 32:

Tabla 32: Resultados de las preocupaciones del Canal Físico

Preocupación	
No-repudio	❖ Al ser una sola persona quien monitoree, puede pasar por alto algunos eventos.
Confidencialidad	No se presentan problemas
Privacidad	No se presentan problemas
Integridad	❖ Las etiquetas pueden ser removidas. ❖ La persona que realiza el inventario puede contabilizar mal los activos.
Alarma	No se presentan problemas

Fuente: Elaboración Propia

La **Preocupación** tiene un valor numérico de $\mathbf{L_C = 3}$, en los controles de No-repudio e integridad es donde se presentan estas limitaciones.

3.5.3.4 Exposición (L_E)

"Una exposición puede ser una ventana que permite divisar activos y procesos o un medidor de potencia que muestra la cantidad de energía que consume un edificio y su fluctuación en el tiempo."(Herzog, 2010)

La exposición se encuentra detallada en la tabla 33:

Tabla 33: Resultados de las exposiciones del Canal Físico

Exposición	
Visibilidad	Algunos departamentos tienen visibilidad por medio de ventanas.
Acceso	No se presentan problemas

Fuente: Elaboración Propia

Para este punto se presenta un valor numérico de $\mathbf{L_E = 1}$.

3.5.3.5 Anomalía (L_A)

"En PHYSSEC, una anomalía puede ser pájaros muertos descubiertos en el techo de un edificio en torno a los equipos de comunicaciones."(Herzog, 2010)

Tabla 34: Resultados de las anomalías del Canal Físico

Anomalía	
Visibilidad	No se presentan problemas

Fuente: Elaboración Propia

3.5.4 Calculadora RAV

A continuación se puede apreciar los resultados obtenidos para el canal físico que estipula la metodología.

Tabla 35: Resultados obtenidos para el canal Físico

Métricas de Seguridad Física

OSSTMM version 3.0

Rellene en los campos en blanco los valores numéricos para OPSEC, Controles y Limitaciones con los resultados de la prueba de seguridad. Consulte OSSTMM 3 (www.osstmm.org) para obtener más información.

OPSEC			
Visibilidad	7		
Acceso	11		
Confianza	1		
Total (Porosidad)	19		

CONTROLES			
Clase A		Ausentes	
Autenticación	2	17	
Indemnización	7	12	
Resistencia	7	12	
Subyugación	2	17	
Continuidad	9	10	
Total Clase A	27	68	
Clase B		Ausentes	
No-Repudio	1	18	
Confidencialidad	2	17	
Privacidad	2	17	
Integridad	5	14	
Alarma	1	18	
Total Clase B	11	84	
		Ausentes Verdaderos	
Total todos los Controles	38	152	
Cobertura Total	20,00%	80,00%	

LIMITATIONS		Item Value	Total Value
Vulnerabilidades	5	9,00	45,00
Debilidades	6	4,58	27,47
Preocupaciones	3	5,42	16,26
Exposiciones	1	1,49	1,49
Anomalías	0	0,78	0,00
Total # Limitaciones	15		90,23

OPSEC	10,75
Controles Verdaderos	6,66
Controles Totales	6,66
Cobertura Verdadera A	28,42%
Cobertura Verdadera B	11,58%
Cobertura Verdadera Total	20,00%
Limitaciones	15,645242
Seguridad Δ	-19,74
Proteccion Verdadera	80,26

Seguridad Actual: 80,19 ravs

Luego de ingresar los valores obtenidos en la calculadora RAV, se obtienen que la Seguridad Actual de la UPEC en el canal Físico es de **80,19 RAVS**, lo que se interpreta en que se posee una deficiencia de aproximadamente el 20%, con lo cual se interpreta que la vulnerabilidad que tiene la institución en caso de un ataque es bastante elevada. Los motivos principales para tener una deficiencia que supere el 10% es que los controles para la autenticación, No-repudio y alarma son escasos, por lo cual deben ser los controles que se aborden con mayor prioridad.

Por otra parte la **Seguridad Δ,** toma un valor negativo de **-19,74,** este valor es interpretado como la insuficiencia de barreras físicas para proteger los activos de la institución, además muestra que los controles que se encuentran aplicados tienen falencias por lo cual necesitan ser mejorados para que estos cubran de manera eficiente los activos que posee la universidad.

3.6 Pruebas de Seguridad Inalámbrica

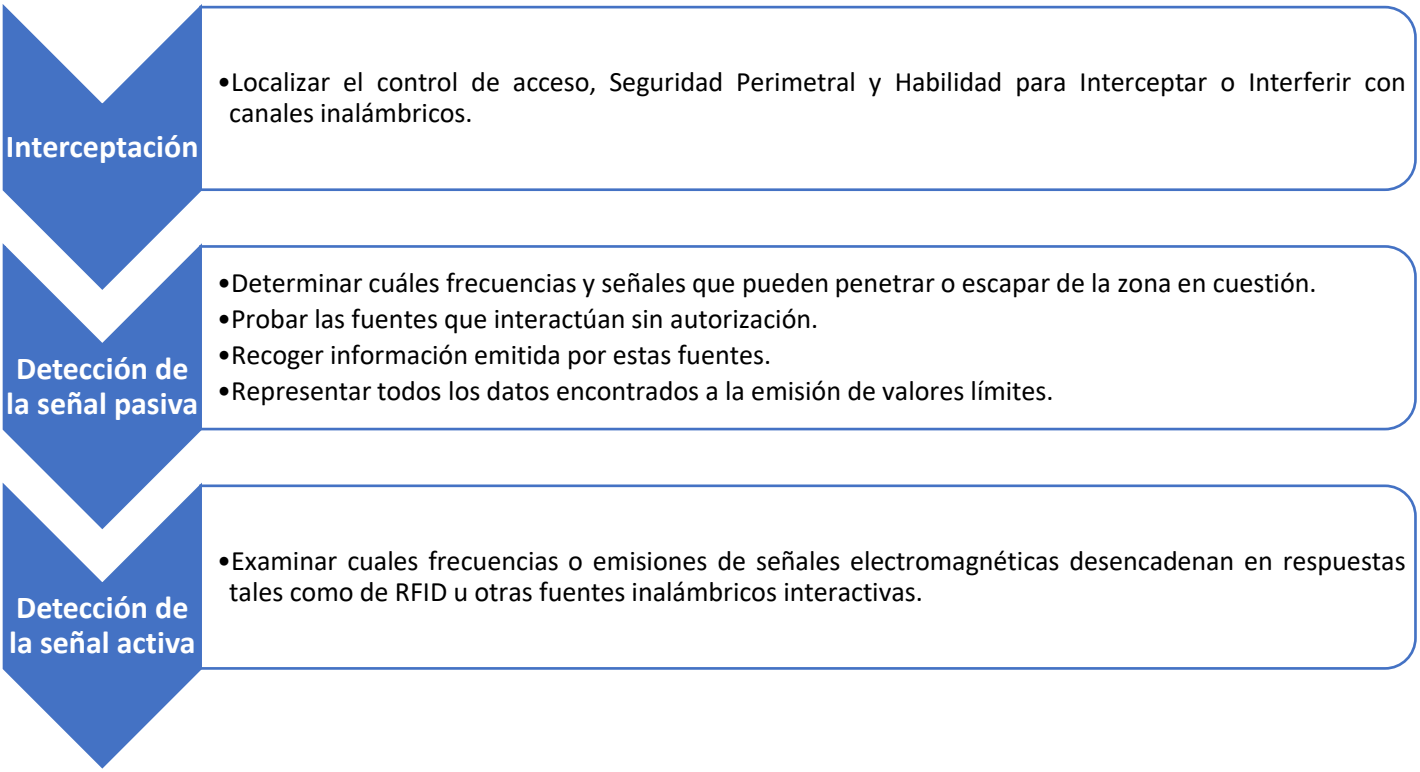
Este canal cubre la interacción del analista dentro del rango de proximidad de los objetivos. Mientras algunos servicios consideran este simplemente como "escaneo", los verdaderos objetivos de cumplimiento de las pruebas de seguridad en este canal son pruebas de barrera físicas y lógicas y medición de la brecha con el estándar de seguridad requerida esbozada en la política de la compañía, regulaciones de la industria, o la legislación regional.

3.6.1 Seguridad Operacional

Para obtener la seguridad operacional se debe analizar la visibilidad, el acceso y la confianza; claro está enfocado al canal que está siendo auditado, en este caso el Inalámbrico.

3.6.1.1 Visibilidad (P_V)

Para realizar este procedimiento se debe toma en cuenta lo siguiente:



Luego de realizar el respectivo análisis, los resultados son detallados en la tabla 36.

Tabla 36: Resultados de Visibilidad del canal Inalámbrico

Visibilidad		
Interceptación	Control de acceso Seguridad Perimetral Interferir canales inalámbricos	❖ Se usa parcialmente. ❖ Firewall Si se interfieren
Detección de la señal pasiva	Frecuencia Señales Fuentes sin autorización	❖ 2,4 GHz ❖ Wi-Fi ❖ Hotspot creadas por estudiantes en las laptops o celulares.
Detección de la señal activa	RFID Otras fuentes inalámbricas	No están presentes No están presentes

Fuente: Elaboración Propia

La **Visibilidad** adquiere un valor de **P_V = 5**, sumando los ítems señalados con las viñetas, los cuales fueron obtenidos por medio de una entrevista al encargado del área de redes y telecomunicaciones, y escaneando las redes wi-fi presentes en la UPEC.

3.6.1.2 Acceso (P_A)

Para analizar este punto se deben seguir las siguientes indicaciones:

Evaluar el acceso administrativo a los dispositivos inalámbricos	•Determinar si los puntos de acceso están apagados durante parte del día cuando no están en uso.
Evaluar la configuración de dispositivos	•Probar y documentar el uso de antenas direccionales y de alta señal que los dispositivos inalámbricos son establecidos en los ajuste de la potencia más baja posible para mantener el funcionamiento suficiente que mantendrá las transmisiones dentro de la límites seguros de la organización.
Evaluar la Configuración, autenticación y cifrado de redes inalámbricas	•Verificar que el identificador del set de servicio por defecto del punto de acceso (SSID) haya sido cambiado.
Control de Acceso	•Evaluar los controles de acceso, seguridad perimetral, y la capacidad para interceptar la comunicación, determinando el nivel de los controles de acceso físico a los puntos de acceso y dispositivos que los controlan.

Los resultados se muestran en la tabla 37.

Tabla 37: Resultados de Acceso del canal Inalámbrico

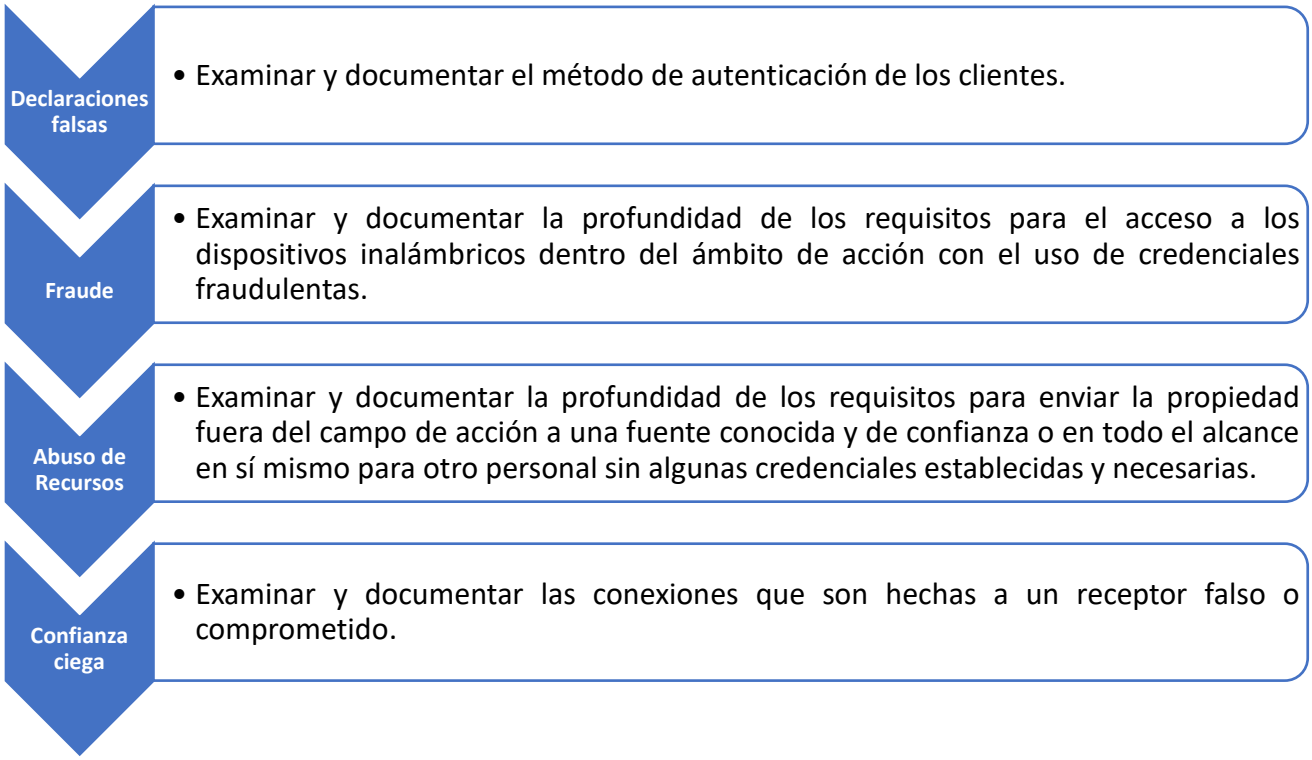
Acceso	
Acceso Administrativo	❖ Los puntos de acceso están encendidos las 24 horas del día.
Configuración Dispositivos	❖ Se usan antenas direccionales No se hace ajuste de la potencia
Cifrado	❖ Los SSID de todos los puntos de acceso han sido cambiados.
Control de acceso	El acceso físico a los AP es relativamente fácil debido a que no se usan cajas de seguridad.

Fuente: Elaboración Propia

El valor numérico para el **Acceso** es de $\mathbf{P_A = 4}$, debido a que los AP están encendidos las 24 horas del día, usan antenas direccionales, y están configurados adecuadamente en cuanto a seguridad se refiere.

3.6.1.3 Confianza (P_T)

Las pruebas de confianzas entre el personal dentro del alcance donde se la confianza se refiere al acceso a la información o propiedad física sin la necesidad de la identificación o autenticación.



Los resultados de Confianza son detallados en la tabla 38:

Tabla 38: Resultados de Confianza del canal Inalámbrico

Confianza	
Declaraciones Falsas	❖ Los estudiantes se autentican con usuario y contraseña en la red Wi-fi eduroam. ❖ Los docentes se controlan por medio de la dirección MAC de sus dispositivos. ❖ El personal administrativo, maneja su propia red wi-fi dependiendo del área en que se encuentre. ❖ Los invitados tienen acceso a una red protegida con contraseña.
Fraude	❖ Los requisitos son bastante robustos.
Abuso de Recursos	❖ Solo se puede acceder a las redes wi-fi establecidas para cada área, por lo que no es posible usar otra que no esté asignada.
Confianza Ciega	❖ No se presentan repetidores falsos.

Fuente: Elaboración Propia

El valor numérico para la **Confianza** es de: $\mathbf{P_T = 7}$, gracias a que la seguridad de las redes Wi-fi son bastante seguras, y solo están disponibles para la institución como tal.

Con los valores de los 3 puntos que plantea la seguridad operacional, se procede con el cálculo del valor de $\mathbf{OpSec_{sum}}$ o la **porosidad** del canal inalámbrico, aplicando la ecuación 1:

$$\mathbf{OpSec_{sum} = P_V + P_A + P_T}$$

$$\mathbf{OpSec_{sum} = 5 + 4 + 7}$$

$$\underline{\mathbf{OpSec_{sum} = 16}}$$

3.6.2 Controles

3.6.2.1 Autenticación (LC_{Au})

Enumerar y probar las insuficiencias de los métodos de autenticación y autorización.

Estos resultados se muestran en la tabla 39:

Tabla 39: Resultados para el control de Autenticación del canal Inalámbrico

Autenticación		
Claves	Autenticación	❖ RSNA-PSK ❖ RSNA ❖ WPA-PSK Open
	Cifrado	❖ CCMP Ninguno
Autorización	❖ Para acceder a las redes wi-fi, se necesita ser parte de la institución, caso contrario no se les brindara el acceso. A excepción de la red wi-fi para invitados.	

Fuente: Elaboración Propia

El valor numérico para la **Autenticación** es de **$LC_{Au} = 5$**, en vista de que se tiene una buena seguridad en cuestión de autenticación.

3.6.2.2 Indemnización (LC_{Id})

"Documentar y enumerar que los objetivos y servicios que están protegidos contra el abuso o elusión de la política de los empleados, estén asegurados al robo o daños, o uso de obligaciones y renuncias de permisos. Verificar la legalidad y la adecuación del idioma en las renuncias."(Herzog, 2010)

El análisis de este control se muestra en la tabla 40:

Tabla 40: Resultados para el control de Indemnización del canal Inalámbrico

Indemnización	
Protección	Los equipos no están protegidos contra ninguna especificación dictada por la metodología.

Fuente: Elaboración Propia

Debido a la ausencia de la **Indemnización**, el valor numérico es de: **LC_{Id} = 0.**

3.6.2.3 Subyugación (LC_{Su})

"Enumerar y poner a prueba las insuficiencias de todos los canales a utilizar o activar los controles de pérdida que no están activados por defecto."(Herzog, 2010)

Los resultados para la subyugación se muestran en la tabla 41:

Tabla 41: Resultados para el control de Subyugación del canal Inalámbrico

Subyugación	
Configuración	La única configuración que se realiza es la de crear la red wi-fi y brindarle seguridad, pero no se toman en cuenta los valores como los canales o la potencia pues estos valores están por defecto.

Fuente: Elaboración Propia

El valor numérico en la Subyugación es de: **LC_{Su} = 0**, debido a la ausencia de este control.

3.6.2.4 Continuidad (LC_{Ct})

"Enumerar y examinar las insuficiencias desde el objetivo en relación con el retraso al acceso y el tiempo de respuesta del servicio a través del personal de apoyo o medios automatizados para un acceso alternativo."(Herzog, 2010)

El resultado se puede apreciar en la tabla 42:

Tabla 42: Resultados para el control de Continuidad del canal Inalámbrico

Continuidad	
Tiempo de respuesta	❖ En caso de presentarse una anomalía en la red wi-fi, el tiempo de respuesta es mínimo y se soluciona el problema lo más pronto posible.

Fuente: Elaboración Propia

El valor numérico para la C**ontinuidad** es de: **LC_{Ct} = 1**, pues los problemas se solucionan con prontitud.

3.6.2.5 Resistencia (LC_{Re})

Mapear y documentar el proceso que se realiza por los guardias desconectar los canales por incumplimiento o problemas de seguridad como un análisis de las deficiencias con la regulación y política de seguridad."(Herzog, 2010)

El análisis de este control se encuentra en la tabla 43:

Tabla 43: Resultados para el control de Resistencia del canal Inalámbrico

Resistencia	
Desconectar canales	❖ En caso de incumplimiento, se niega el servicio y se castiga conforme a la falta.

Fuente: Elaboración Propia

El valor numérico para la **Resistencia** es de: **$LC_{Re} = 1$**.

3.6.2.6 No-repudio (LC_{NR})

"Enumerar y poner a prueba el uso o insuficiencias de los daemons y sistemas para identificar correctamente y registrar el acceso o interacciones a la propiedad para una evidencia específica que permita impugnar el repudio, y documentar la profundidad de la interacción registrada y el proceso de identificación."(Herzog, 2010)

El resultado se encuentra en la tabla 44:

Tabla 44: Resultados para el control de No-repudio del canal Inalámbrico

No-repudio	
Acceso	❖ Los AP cisco permitir monitorear constantemente los usuarios que acceden a la red wi-fi.

Fuente: Elaboración Propia

El **No-repudio** toma un valor numérico de: **$LC_{NR} = 1$**.

3.6.2.7 Confidencialidad (LC_{Cf})

"Enumerar y examinar el uso de equipos para amortiguar las señales de transmisión electromagnética fuera de la empresa y los controles en el lugar para asegurar y encriptar las transmisiones inalámbricas."(Herzog, 2010)

El análisis para la confidencialidad e se detalla en la tabla 45:

Tabla 45: Resultados para el control de Confidencialidad para el canal Inalámbrico

Confidencialidad	
Equipos para amortiguar las señales electromagnéticas	No se usan.

Fuente: Elaboración Propia

El valor numérico de la Confidencialidad es de: **$LC_{Cf} = 0$**.

3.6.2.8 Privacidad (LC_{Pr})

"Determinar el nivel de los controles de acceso físico a los puntos de acceso y dispositivos que los controlan (cerraduras con llave, lectores de tarjetas, cámaras, etc.)."(Herzog, 2010)

Los resultados para la privacidad se encuentran en la tabla 46:

Tabla 46: Resultados para el control Privacidad del canal Inalámbrico

Privacidad	
Acceso físico	No están protegidos físicamente de ninguna manera.

Fuente: Elaboración Propia

El valor numérico para la privacidad es de: **$LC_{Pr} = 0$**.

3.6.2.9 Integridad (LC_{It})

"Determinar que los datos sólo puedan ser consultados y modificados por aquellos que están autorizados y garantizar que el adecuado cifrado esté en uso para garantizar la firma y la confidencialidad de las comunicaciones."(Herzog, 2010)

Los resultados para la integridad se encuentran en la tabla 47:

Tabla 47: Resultados para el control Integridad del canal Inalámbrico

Integridad	
Consulta de datos	❖ Las contraseñas usadas son bastante robustas. ❖ Si se usa cifrado.

Fuente: Elaboración Propia

Para la integridad se tiene un valor de $LC_{It} = 2$.

3.6.2.10 Alarma (LC_{Al})

"Verificar y enumerar el uso de un sistema de alerta localizada o en todo el alcance, registro, o mensaje para cada puerta de acceso sobre cada canal donde una situación sospechosa es observada por el personal en caso de sospecha de intentos de elusión, la ingeniería social, o una actividad fraudulenta."(Herzog, 2010)

Los resultados para la integridad se encuentran en la tabla 48:

Tabla 48: Resultados para el control Alarma del canal Inalámbrico

Alarma	
Sistema de alerta	❖ No poseen ningún sistema de alerta.

Fuente: Elaboración Propia

Para la alarma se tiene un valor de $LC_{Al} = 1$.

Con los 10 valores que estipula la auditoria, se procede a calcular el valor total de la Suma de Controles, aplicando la ecuación 2:

$$\boldsymbol{LC_{sum} = LC_{Au} + LC_{Id} + LC_{Re} + LC_{Su} + LC_{Ct} + LC_{NR} + LC_{Cf} + LC_{Pr} + LC_{It} + LC_{Al}}$$

$$\boldsymbol{LC_{sum} = 5 + 0 + 1 + 0 + 1 + 1 + 0 + 0 + 2 + 0}$$

$$\boldsymbol{LC_{sum} = 10}$$

3.6.3 Limitaciones

3.6.3.1 Vulnerabilidad (L_V)

"Una vulnerabilidad puede ser un hardware que puede ser sobrecargado y quemado por las versiones de mayor potencia de la misma frecuencia o una frecuencia cercana, un receptor estándar sin configuraciones especiales que puede tener acceso a los datos de la señal, un receptor que puede ser obligado a aceptar una señal de terceros en lugar de la prevista, o un punto de acceso inalámbrico cuando cae su conexión cerca de un horno microondas."(Herzog, 2010)

Los resultados para la vulnerabilidad se encuentran en la tabla 49:

Tabla 49: Resultados para la limitación Vulnerabilidad del canal Inalámbrico

Vulnerabilidad
❖ AP estándar residencial

Fuente: Elaboración Propia

En la institución se utilizan AP residenciales, por lo cual no se pueden administrar de la mejor manera, es por esto que se le asigna un valor numérico a la vulnerabilidad de **$L_V = 1$.**

3.6.3.2 Debilidad (L_W)

"Una debilidad puede ser un AP inalámbrico de autenticación de usuarios basado en direcciones MAC (que se puede suplantar) o una tarjeta de seguridad RFID que ya no recibe las señales y por lo tanto deja "abierta" después de recibir una señal procedente de una fuente de energía alta."(Herzog, 2010)

La autenticación no se basa solo en direcciones MAC, pues son parte de la red EDUROAM y los lugares con acceso de tarjetas RFID usan la tarjeta y adicionalmente una clave de acceso.

- **Para la autenticación los controles ausentes son la vulnerabilidad de los routers TP-Link caseros los cuales tienen habilitadas configuraciones por defecto.**
- **Para la indemnización no existen documentos que aseguren lo estipulado por OSSTMM.**

Para los demás controles no se encontraron fallas que comprometan la seguridad de la institución. Por tal motivo a la debilidad se le otorga un valor numérico de **L_W = 2.**

3.6.3.3 Preocupación (L_C)

Una preocupación puede ser un punto de acceso inalámbrico que utiliza el cifrado de datos débil o un abridor de puertas de infrarrojos que no puede leer el remitente en la lluvia.

Tabla 50: Resultados para la limitación Preocupación del canal Inalámbrico

Preocupación
❖ AP TP-Link sin configuraciones especiales.

Fuente: Elaboración Propia

Debido al uso de los routers TP-Link, se pueden vulnerar mediante el uso del WPS, es por eso que la preocupación tiene una valor numérico de **L_C = 1.**

3.6.3.4 Exposición (L_E)

Una exposición puede ser una señal que interrumpe otra maquinaria o un dispositivo de infrarrojos cuyo funcionamiento es visible por las cámaras de vídeo estándar con capacidad de noche.

No se encontraron este tipo de anomalías en la institución, por lo que el valor numérico para la anomalía es de **L_E = 0.**

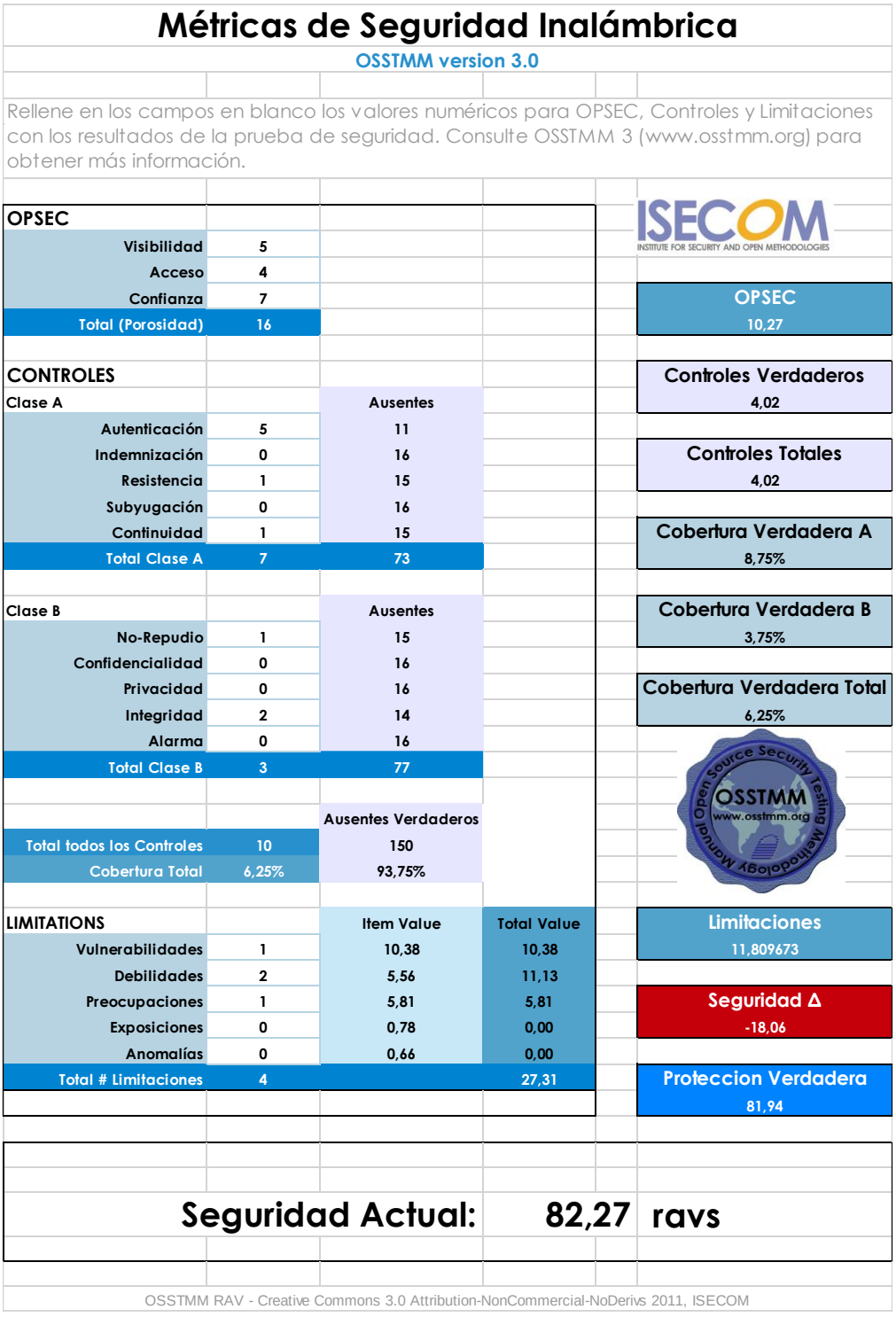
3.6.3.5 Anomalía (L_A)

Una anomalía puede ser una señal local que no puede ser correctamente situada ni ningún daño conocido.

No se encontraron anomalías por lo cual se le otorga un valor numérico de **$L_A = 0$.**

3.6.4 Calculadora RAV

A continuación se puede apreciar los resultados obtenidos para el canal inalámbrico que estipula la metodología.



Métricas de Seguridad Inalámbrica

OSSTMM version 3.0

Rellene en los campos en blanco los valores numéricos para OPSEC, Controles y Limitaciones con los resultados de la prueba de seguridad. Consulte OSSTMM 3 (www.osstmm.org) para obtener más información.

OPSEC			
Visibilidad	5		
Acceso	4		
Confianza	7		
Total (Porosidad)	16		

CONTROLES			
Clase A		Ausentes	
Autenticación	5	11	
Indemnización	0	16	
Resistencia	1	15	
Subyugación	0	16	
Continuidad	1	15	
Total Clase A	7	73	
Clase B		Ausentes	
No-Repudio	1	15	
Confidencialidad	0	16	
Privacidad	0	16	
Integridad	2	14	
Alarma	0	16	
Total Clase B	3	77	
		Ausentes Verdaderos	
Total todos los Controles	10	150	
Cobertura Total	6,25%	93,75%	

LIMITATIONS			
		Item Value	Total Value
Vulnerabilidades	1	10,38	10,38
Debilidades	2	5,56	11,13
Preocupaciones	1	5,81	5,81
Exposiciones	0	0,78	0,00
Anomalías	0	0,66	0,00
Total # Limitaciones	4		27,31

OPSEC	10,27
Controles Verdaderos	4,02
Controles Totales	4,02
Cobertura Verdadera A	8,75%
Cobertura Verdadera B	3,75%
Cobertura Verdadera Total	6,25%
Limitaciones	11,809673
Seguridad Δ	-18,06
Proteccion Verdadera	81,94

Seguridad Actual: 82,27 ravs

Luego de ingresar los valores obtenidos en la calculadora RAV, se obtiene que la Seguridad Actual de la UPEC en el canal Inalámbrico es de **82,27 RAVS**, lo que se interpreta en que se posee una deficiencia de aproximadamente el 18%, esto debido a que la vulnerabilidad de las comunicaciones inalámbricas. Una de las principales causas es el uso de AP residenciales. Los controles para la indemnización, subyugación, confidencialidad, privacidad y alarma son prácticamente nulos, por lo cual deben ser los controles que se aborden con mayor prioridad.

Por otra parte la **Seguridad Δ,** toma un valor negativo de **-14,35,** este valor es interpretad como la insuficiencia de controles que posee la institución en cuanto al talento humano, además muestra que los controles que se encuentran aplicados tienen falencias por lo cual necesitan ser mejorados para que estos se adecúen a las necesidades de seguridad que la universidad requiere.

3.7 Pruebas de Seguridad de las Telecomunicaciones

3.7.1 Seguridad Operacional

3.7.1.1 Visibilidad (P_V)

Enumeración e indexación de los objetivos en el alcance a través de la interacción directa e indirecta con o entre los sistemas vivos.

Red de Topografía

(a) Esquema de la topología de las redes de telecomunicaciones dentro del alcance.

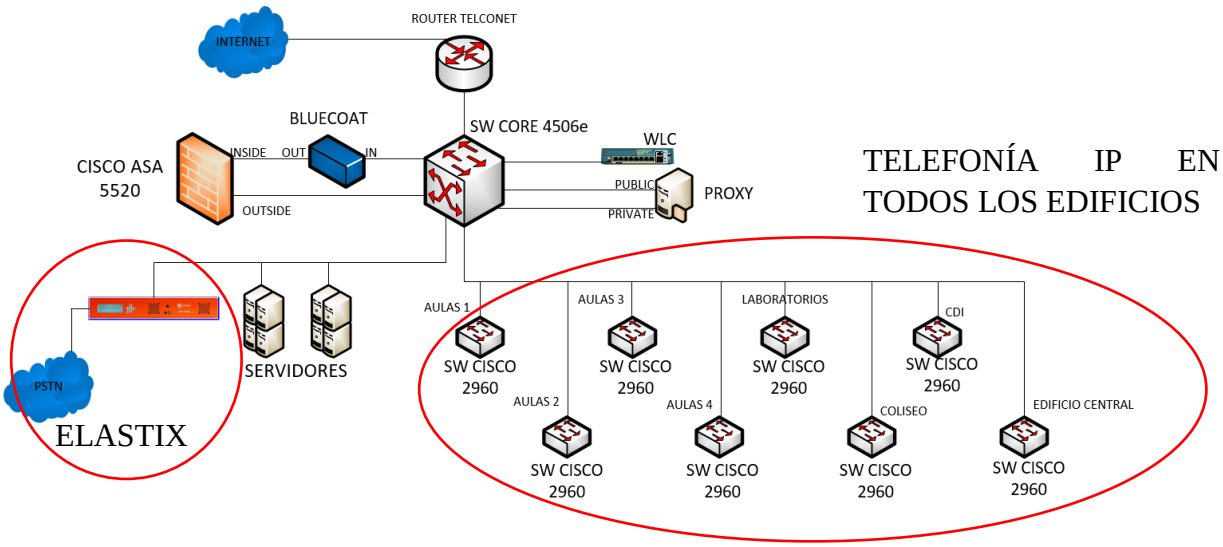


Imagen 17: Topología red interna UPEC

Fuente: Elaboración Propia

En la UPEC se cuenta con el servicio de **telefonía IP** el cual está conectado con la PSTN, este servicio está disponible solo para el personal autorizado y se usa contraseña para su acceso.

Enumeración

(a) Las pruebas PBX: Enumerar los sistemas de telefonía dentro del campo de acción.

(b) La prueba del buzón de voz: Encontrar los buzones de voz dentro del alcance.

(c) La prueba de fax: Enumerar los sistemas de fax dentro del campo de acción.

(d) Encuesta Módem: Encontrar todos los sistemas con módems interactivos y escuchar dentro del campo de acción.

(e) Pruebas de Servicios de Acceso Remoto: Enumerar sistemas RAS dentro del alcance.

(f) Copia de seguridad líneas de pruebas RDSI: enumerar los dispositivos de red de copia de seguridad con líneas RDSI dentro del campo de acción.

(g) Prueba de narración IP: Enumerar los sistemas de VoIP dentro del campo de acción.

(h) Conmutación de paquetes de pruebas de redes X.25: Encontrar vivo y sistemas accesibles y vivos dentro del alcance, registro de sus códigos de respuesta.

Tabla 51: Resultados para Visibilidad del canal Telecomunicaciones

Enumeración	
PBX	❖ Telefonía IP Elastix
Buzón de voz	❖ Si tienen buzón de voz
Fax	No cuentan con este servicio
Modem	❖ PSTN
RAS	❖ SSH y escritorio remoto
RDSI	No cuentan con este servicio
Narración IP	No cuentan con este servicio
Redes X.25	No cuentan con este servicio

Fuente: Elaboración Propia

El valor numérico para la **Visibilidad** es **Pv = 4,** por los servicios presentes en la UPEC.

3.7.1.2 Acceso (P_A)

(a) Las pruebas de PBX: Encontrar los sistemas PBX que están permitiendo la administración remota o el acceso mundial para el terminal de mantenimiento, ya sea a través de marcación de teléfono o de la red IP.

(b) La prueba de voz del buzón: Encontrar los buzones de correo de voz que son accesibles al mundo.

(c) Las pruebas FAX: Encontrar sistemas de fax que están permitiendo la administración remota o acceso mundial a la terminal de mantenimiento.

(d) d) Encuesta Módem: Probar y documentar los protocolos de autenticación en uso (por ejemplo: terminales, PAP, CHAP, otros).

(e) Pruebas de Servicios de Acceso Remoto: probar y documentar los protocolos de autenticación en uso (por ejemplo: terminales, PAP, CHAP, otros).

(f) Pruebas de líneas de copia de seguridad (RDSI): probar y documentar los protocolos de autenticación en uso (por ejemplo: terminales, PAP, CHAP, otros).

(g) Prueba de narración IP: Verificar la posibilidad de llevar a cabo el fraude de llamadas telefónicas, espionaje de llamadas o rastreo, de llamadas, la suplantación de CLID y de denegación de servicio, el uso de ataques dirigidos a las redes convergentes, elementos de la red VoIP, señalización y protocolos de transporte de medios de comunicación.

(h) Conmutación de paquetes de pruebas de redes X.25: Encontrar sistemas que están permitiendo la administración remota, el acceso a otros servicios a través de vías específicas, o de cobro revertido, verificar cuantos canales virtuales (VCs) y los canales virtuales permanentes (PVCs) están en uso y como son manejados (CUG,

mapeo de subdirecciones, detección de llamadas entrantes X.25, filtrado basado en NUA, etc.).

Tabla 52: Resultados para el Acceso del canal Telecomunicaciones

Acceso	
PBX	No es accesible
Buzón de voz	No es accesible
Fax	No cuentan con este servicio
Modem	❖ Las líneas telefónicas son manejadas por CNT
RAS	❖ Son accesibles desde fuera
RDSI	No cuentan con este servicio
Narración IP	No cuentan con este servicio
Redes X.25	No cuentan con este servicio

Fuente: Elaboración Propia

El valor numérico para el **Acceso** es **P_A = 2,**

3.7.1.3 Confianza (P_T)

Las pruebas de confianzas entre sistemas dentro del alcance, donde la confianza se refiere al acceso a la información o propiedad física sin necesidad de credenciales de autenticación.

Suplantación

(a) Probar y documentar los métodos de acceso en uso que no requieren la presentación de credenciales de autenticación.

(b) Probar y documentar la profundidad de los requisitos para la interacción y el acceso a la propiedad dentro del alcance mediante la suplantación de una fuente de confianza (ejemplo: CLID y suplantación X.25 NUA).

Abuso de Recursos

(a) Probar y documentar la profundidad de los requisitos para tomar la propiedad fuera del alcance de una fuente conocida y de confianza o en todo el alcance a sí mismo sin ninguna credencial establecida, requerida.

(b) Probar y documentar la propiedad disponible desde fuera del alcance debido a fugas de información.

Tabla 53: Resultados para la Confianza del canal Telecomunicaciones

Confianza	
Suplantación	No se puede acceder a estos recursos sin ser identificado
Abuso de recursos	❖ No se puede controlar la fuga de información por parte del personal

Fuente: Elaboración Propia

El valor numérico para la **Confianza** es de $\mathbf{P_T = 1,}$ debido a el abuso de recursos por la fuga de información.

Con los valores de los 3 puntos que plantea la seguridad operacional, se procede con el cálculo del valor de $\mathbf{OpSec_{sum}}$ o la **porosidad** del canal Telecomunicaciones, aplicando la ecuación 1:

$$\mathbf{OpSec_{sum} = P_V + P_A + P_T}$$

$$\mathbf{OpSec_{sum} = 4 + 2 + 1}$$

$$\underline{\mathbf{OpSec_{sum} = 7}}$$

3.7.2 Controles

3.7.2.1 Autenticación ($\mathbf{LC_{Au}}$)

(a) Enumerar los recursos de telecomunicaciones que requieren autenticación y verificar todas las formas aceptables de privilegios para interactuar o recibir acceso.

(b) Verificar los métodos de autorización y la identificación requerida.

(c) Asegurarse que las cuentas administrativas no tengan defecto o credenciales fáciles de adivinar.

(d) Asegurarse que las cuentas de usuario no tengan defecto o credenciales fáciles de adivinar.

(e) Verificar y probar las protecciones contra la fuerza bruta y ataques de tipo diccionario.

(f) Verificar y probar la contraseña de comprobaciones de complejidad y el buzón de voz tamaño PIN, la caducidad de contraseñas, y la frecuencia de los controles de cambio.

(g) Probar las credenciales "conocidas" en todos los puntos de acceso enumerados, para verificar los controles de la reutilización de la contraseña.

(h) Verificar el formato utilizado para el almacenamiento de credenciales de autenticación y documentar el texto sin formato o contraseñas ininteligibles y algoritmos de cifrado débiles.

(i) Verificar el formato utilizado para la transmisión de las credenciales de autenticación a través de la red y el documento de texto sin formato o contraseñas ininteligibles y algoritmos de cifrado débiles.

(j) Verificar que la información de autenticación si la tentativa, éxito, o falla. Es debidamente registrada.

Tabla 54: Resultados para el control Autenticación del canal Telecomunicaciones

Autenticación	
Autenticación	❖ Todos los recursos requieren autenticación para su acceso.
Métodos de autenticación	❖ Contraseña y ser parte del personal de la UPEC.
Cuentas administrativas	❖ No están con configuración por defecto
Cuentas de Usuario	❖ No están con configuración por defecto
Protección	❖ Las contraseñas son robustas
Cambios de contraseña	No se realizan
Reutilización de contraseñas	Si se pueden reutilizar
Almacenamiento de credenciales	❖ Solo se almacenan en el Elastix
Transmisión de credenciales	❖ Se realizan personalmente
Registro de autenticación	No se lleva un registro

Fuente: Elaboración Propia

El valor numérico para la **Autenticación** es de **LC_{Au} = 7.**

3.7.2.2 Indemnización (LC_{Id})

(a) Documentar y enumerar los objetivos y servicios que están protegidos contra el abuso o elusión de la política de los empleados, estar asegurados por robo o daños, o usar la responsabilidad y limitaciones de permisos.

(b) Verificar el efecto de las limitaciones de responsabilidad sobre la seguridad o medidas de protección.

(c) Examinar el lenguaje de la póliza de seguro para las limitaciones en los tipos de daños o activos.

Tabla 55: Resultados para el control Indemnización del canal Telecomunicaciones

Indemnización	
Elusión de la política de empleados	❖ No se puede eludir porque todo queda registrado en Elastix
Limitaciones de responsabilidad	❖ Al entregar el teléfono ip se firma por la responsabilidad de este bien.
Seguro	No poseen seguro para este activo.

Fuente: Elaboración Propia

El valor numérico para **Indemnización** es de **LC_{Id} = 2.**

3.7.2.3 Subyugación (LC_{Su})

Enumerar y poner a prueba las insuficiencias desde todos los canales a utilizar o activar los controles de pérdida que no están activados por defecto.

Tabla 56: Resultados para el control Subyugación del canal Telecomunicaciones

Subyugación	
Insuficiencias	❖ En Elastix están habilitados los controles de seguridad.

Fuente: Elaboración Propia

El valor numérico para la **Subyugación** es de **LC_{Su} = 1**.

3.7.2.4 Continuidad (LC_{Ct})

(a) Enumerar y probar las deficiencias de los destinatarios en relación con retrasos en el acceso y el tiempo de respuesta del servicio a través del personal de apoyo o medios automatizados para el acceso alternativo.

(b) Enumerar y probar para las deficiencias de destinatarios en relación con cuestiones de calidad de servicio y los requisitos de rendimiento de las tecnologías de telecomunicaciones.

Tabla 57: Resultados para el control Continuidad del canal Telecomunicaciones

Continuidad	
Personal d Apoyo	❖ En caso de presentarse problemas, estos se solucionan a la brevedad posible
QoS	❖ Este servicio se encuentra en su respectiva VLAN en la cual se encuentra aplicado QoS para la voz.

Fuente: Elaboración Propia

La continuidad tiene un valor numérico de **LC_{Ct} = 2**.

3.7.2.5 Resistencia (LC_{Re})

Mapear y documentar el proceso de los guardianes desconectando canales por incumplimiento o problemas de seguridad como un análisis de las deficiencias con la regulación y la política de seguridad.

Tabla 58: Resultados para el control Resistencia del canal Telecomunicaciones

Resistencia	
Deficiencias Políticas de Seguridad	No existe política de seguridad

Fuente: Elaboración Propia

El valor numérico para la resistencia es de **$LC_{Re} = 0$**.

3.7.2.6 No-repudio (LC_{NR})

(a) Enumerar y probar para el uso o insuficiencias de las aplicaciones y sistemas para identificar adecuadamente y registrar el acceso a la propiedad o interacciones a la propiedad para evidencias específicas para desafiar el repudio.

(b) Documentar la profundidad de la interacción grabada y el proceso de identificación.

(c) Verificar que todos los métodos de interacción estén adecuadamente registrados con la identificación apropiada.

(d) Identificar los métodos de identificación los cuales repudian la derrota.

Tabla 59: Resultados para el control No-Repudio del canal Telecomunicaciones

No-repudio	
Aplicaciones	No se usan
Grabación	No se graban
Identificación Apropiada	❖ Se hace uso de teléfonos ip configurados por el encargado del departamento de redes y telecomunicaciones.
Repudio a la derrota	No se aplica

Fuente: Elaboración Propia

El valor numérico para el **No-repudio** es de **$LC_{NR} = 1$.**

3.7.2.7 Confidencialidad (LC_{Cf})

(a) Enumerar todas las interacciones con los servicios dentro del ámbito de las comunicaciones o bienes transportados por el canal mediante líneas seguras, encriptación, interacciones "sosegadas" o "cerradas" para proteger la confidencialidad de la información de propiedad entre las partes involucradas.

(b) Verificar los métodos aceptables utilizados para la confidencialidad.

(c) Probar la resistencia y el diseño de los métodos de cifrado o de ofuscación.

(d) Verificar los límites exteriores de la comunicación la cual puede ser protegida mediante el método aplicado a la confidencialidad.

Tabla 60: Resultados para el control Confidencialidad del canal Telecomunicaciones

Confidencialidad	
Encriptación	No se usa
Confidencialidad	❖ Se hace uso de teléfonos personales
Cifrado	No se usa
Limites exteriores	❖ No son necesarios porque el servicio es para el personal dentro de las instalaciones.

Fuente: Elaboración Propia

El valor numérico para la **Confidencialidad** es de **LC_{Cf} = 2.**

3.7.2.8 Privacidad (LC_{Pr})

Enumerar todas las interacciones con los servicios dentro del ámbito de las comunicaciones o bienes transportados por el canal mediante líneas seguras, encriptación, interacciones "tranquilizadas" o "cerradas" para proteger la privacidad de la interacción y el proceso de proporcionar activos sólo a aquellos dentro de debida autorización de seguridad para ese proceso, comunicación, o activo.

Tabla 61: Resultados para el control Privacidad del canal Telecomunicaciones

Privacidad	
Líneas seguras	No se usan

Fuente: Elaboración Propia

El valor numérico para la **Privacidad** es de **$LC_{Pr} = 0$**.

3.7.2.9 Integridad (LC_{It})

Enumerar y probar de las deficiencias de integridad donde el uso de un proceso documentado, firmas, cifrado, hachís, o marcas para asegurar que el activo no pueda ser cambiado, conmutado, redirigido, o revertido sin ser conocido por las partes involucradas.

Tabla 62: Resultados para el control Integridad del canal Telecomunicaciones

Integridad	
Intervención	❖ No se puede intervenir las líneas sin ser identificados

Fuente: Elaboración Propia

El valor numérico para la **Integridad** es de **$LC_{It} = 1$**.

3.7.2.10 Alarma (LC_{Al})

(a) Verificar y enumerar la utilización de un sistema de alerta localizada o en todo el alcance, registro, o mensaje para cada puerta de acceso a través de cada canal donde una situación sospechosa es elevada en caso de sospecha de intentos de intrusión o actividad fraudulenta y determinar los niveles de recorte.

(b) Revisar los registros de detalles de llamadas entrantes y salientes en busca de signos de abuso o fraude.

(c) Probar y documentar los sistemas de administración de registros.

Tabla 63: Resultados para el control Alarma del canal Telecomunicaciones

Alarma	
Intentos de intrusión	No se realizan alarmas
Detalles de llamadas	❖ Se pueden consultar en el Elastix
Registros	❖ Se consultan en Elastix

Fuente: Elaboración Propia

El valor numérico para la **Alarma** es de **LC_{Al} = 2.**

Con los 10 valores que estipula la auditoria, se procede a calcular el valor total de la Suma de Controles, aplicando la ecuación 2:

$$LC_{sum} = LC_{Au} + LC_{Id} + LC_{Re} + LC_{Su} + LC_{Ct} + LC_{NR} + LC_{Cf} + LC_{Pr} + LC_{It} + LC_{Al}$$

$$LC_{sum} = 7 + 2 + 0 + 1 + 2 + 1 + 2 + 0 + 1 + 2$$

$$LC_{sum} = 18$$

3.7.3 Limitaciones

3.7.3.1 Vulnerabilidad (L_V)

Una vulnerabilidad puede ser una falla en el sistema de pago telefónico que permite sonidos a través del receptor para imitar que la moneda cae, una cabina telefónica que permite a cualquier persona acceder a la línea telefónica de otra persona, un sistema de correo de voz que proporciona mensajes desde cualquier teléfono en cualquier parte, o una máquina de fax que puede consultar de forma remota para volver a enviar la última cosa en la memoria para el número del llamante.

Tabla 64: Resultados para la Limitación vulnerabilidad del canal Telecomunicaciones

Vulnerabilidad	
Falta de pago	Siempre está al día con sus pagos
Buzón de voz	Se usa clave para el buzón de voz

Fuente: Elaboración Propia

El valor numérico para la **Vulnerabilidad** es de **L_V = 0.**

3.7.3.2 Debilidad (L_W)

Una debilidad puede ser una PBX que todavía tiene las contraseñas administrativas por defecto o un banco de módems de acceso telefónico remoto en el que no se registra el número de llamada, hora y duración.

Tabla 65: Resultados para la Limitación Debilidad del canal Telecomunicaciones

Debilidad	
Contraseñas por defecto	Todas las contraseñas han sido cambiadas

Fuente: Elaboración propia

El valor numérico para la **Debilidad** es de **$L_W = 0$.**

3.7.3.3 Preocupación (L_C)

Una preocupación puede ser el uso de una máquina de FAX para el envío de información privada o un sistema de correo de voz que utiliza tonos táctiles para la introducción de un PIN o contraseña.

Tabla 66: Resultados para la Limitación Preocupación del canal Telecomunicaciones

Preocupación	
Introducción de las contraseñas	❖ Mediante teléfono IP

Fuente: Elaboración Propia

3.7.3.4 Exposición (L_E)

Una exposición puede ser una guía de empresas automatizada ordenada alfabéticamente, permitiendo que cualquiera pueda desplazarse por todas las personas y números, o una máquina de fax que almacena los últimos números marcados.

Tabla 67: Resultados para la Limitación Exposición del canal Telecomunicaciones

Exposición	
Guía telefónica	Esta información es de acceso Público.

Fuente: Elaboración Propia

3.7.3.5 Anomalía (L_A)

Una anomalía puede ser una respuesta del módem desde un número que no tiene módem.

Tabla 68: Resultados para la Limitación Anomalía del canal Telecomunicaciones

Anomalía	
Respuestas no autorizadas	No se presentan

Fuente: Elaboración Propia

3.7.4 Calculadora RAV

Métricas de Seguridad de Telecomunicaciones

OSSTMM version 3.0

Rellene en los campos en blanco los valores numéricos para OPSEC, Controles y Limitaciones con los resultados de la prueba de seguridad. Consulte OSSTMM 3 (www.osstmm.org) para obtener más información.

OPSEC			
Visibilidad	4		
Acceso	2		
Confianza	1		
Total (Porosidad)	7		

CONTROLES			
Clase A		Ausentes	
Autenticación	7	0	
Indemnización	2	5	
Resistencia	0	7	
Subyugación	1	6	
Continuidad	2	5	
Total Clase A	12	23	
Clase B		Ausentes	
No-Repudio	1	6	
Confidencialidad	2	5	
Privacidad	0	7	
Integridad	1	6	
Alarma	2	5	
Total Clase B	6	29	
		Ausentes Verdaderos	
Total todos los Controles	18	52	
Cobertura Total	25,71%	74,29%	

LIMITACIONES			
		Item Value	Total Value
Vulnerabilidades	0	8,43	0,00
Debilidades	0	4,29	0,00
Preocupaciones	1	5,14	5,14
Exposiciones	0	0,78	0,00
Anomalías	0	0,25	0,00
Total # Limitaciones	1		5,14

OPSEC	8,10
Controles Verdaderos	5,10
Controles Totales	5,10
Cobertura Verdadera A	34,29%
Cobertura Verdadera B	17,14%
Cobertura Verdadera Total	25,71%
Limitaciones	7,355205
Seguridad Δ	-10,36
Proteccion Verdadera	89,64

Seguridad Actual: 89,45 ravs

Luego de ingresar los valores obtenidos en la calculadora RAV, se obtienen que la Seguridad Actual de la UPEC en el canal Telecomunicaciones es de **89,45 RAVS**, este valor es relativamente aceptable, esto debido a que solo se posee un servicio para este canal. Se posee una deficiencia de aproximadamente el 11%, esto debido a que los controles para la resistencia y la privacidad son prácticamente nulos, por lo cual deben ser los controles que se aborden con mayor prioridad.

Por otra parte la **Seguridad Δ,** toma un valor negativo de **-10,36,** un valor que es negativo pero no tan alarmante, esto como consecuencia de tener un solo servicio, sin embargo los controles que se encuentran aplicados tienen falencias por lo cual necesitan ser mejorados para que estos se adecúen a las necesidades de seguridad que la universidad requiere.

3.8 Pruebas de la Seguridad de las Redes de Datos

3.8.1 Seguridad Operacional

3.8.1.1 Visibilidad (P_V)

La enumeración e indexación de los objetivos en el alcance a través de la interacción directa e indirecta con o entre los sistemas vivos.

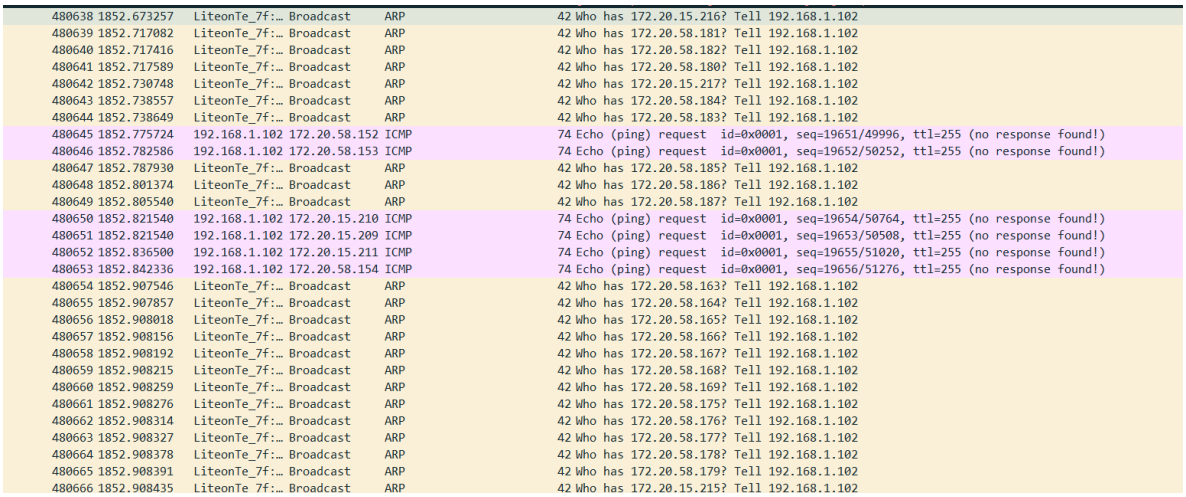
(a) Identificar el segmento(s) de red de destino.

Para identificar el segmento de red se utilizó la herramienta tracert hacia el internet, con lo cual se obtuvo que el segmento de red es 172.20.x.x. Esto se puede apreciar en la imagen:

Imagen 18: Traza hacia internet
Fuente: Elaboración Propia

(b) Verificar y examinar el uso del tráfico y los protocolos de enrutamiento de todos los objetivos.

El protocolo ARP, es el que usa más tráfico en la red, como se puede apreciar en la imagen 14:



480638	1852.673257	LiteonTe_7f:…	Broadcast	ARP	42	Who has 172.20.15.216? Tell 192.168.1.102
480639	1852.717082	LiteonTe_7f:…	Broadcast	ARP	42	Who has 172.20.58.181? Tell 192.168.1.102
480640	1852.717416	LiteonTe_7f:…	Broadcast	ARP	42	Who has 172.20.58.182? Tell 192.168.1.102
480641	1852.717589	LiteonTe_7f:…	Broadcast	ARP	42	Who has 172.20.58.180? Tell 192.168.1.102
480642	1852.730748	LiteonTe_7f:…	Broadcast	ARP	42	Who has 172.20.15.217? Tell 192.168.1.102
480643	1852.738557	LiteonTe_7f:…	Broadcast	ARP	42	Who has 172.20.58.184? Tell 192.168.1.102
480644	1852.738649	LiteonTe_7f:…	Broadcast	ARP	42	Who has 172.20.58.183? Tell 192.168.1.102
480645	1852.775724	192.168.1.102	172.20.58.152	ICMP	74	Echo (ping) request id=0x0001, seq=19651/49996, ttl=255 (no response found!)
480646	1852.782586	192.168.1.102	172.20.58.153	ICMP	74	Echo (ping) request id=0x0001, seq=19652/50252, ttl=255 (no response found!)
480647	1852.787930	LiteonTe_7f:…	Broadcast	ARP	42	Who has 172.20.58.185? Tell 192.168.1.102
480648	1852.801374	LiteonTe_7f:…	Broadcast	ARP	42	Who has 172.20.58.186? Tell 192.168.1.102
480649	1852.805540	LiteonTe_7f:…	Broadcast	ARP	42	Who has 172.20.58.187? Tell 192.168.1.102
480650	1852.821540	192.168.1.102	172.20.15.210	ICMP	74	Echo (ping) request id=0x0001, seq=19654/50764, ttl=255 (no response found!)
480651	1852.821540	192.168.1.102	172.20.15.209	ICMP	74	Echo (ping) request id=0x0001, seq=19653/50508, ttl=255 (no response found!)
480652	1852.836500	192.168.1.102	172.20.15.211	ICMP	74	Echo (ping) request id=0x0001, seq=19655/51020, ttl=255 (no response found!)
480653	1852.842336	192.168.1.102	172.20.58.154	ICMP	74	Echo (ping) request id=0x0001, seq=19656/51276, ttl=255 (no response found!)
480654	1852.907546	LiteonTe_7f:…	Broadcast	ARP	42	Who has 172.20.58.163? Tell 192.168.1.102
480655	1852.907857	LiteonTe_7f:…	Broadcast	ARP	42	Who has 172.20.58.164? Tell 192.168.1.102
480656	1852.908018	LiteonTe_7f:…	Broadcast	ARP	42	Who has 172.20.58.165? Tell 192.168.1.102
480657	1852.908156	LiteonTe_7f:…	Broadcast	ARP	42	Who has 172.20.58.166? Tell 192.168.1.102
480658	1852.908192	LiteonTe_7f:…	Broadcast	ARP	42	Who has 172.20.58.167? Tell 192.168.1.102
480659	1852.908215	LiteonTe_7f:…	Broadcast	ARP	42	Who has 172.20.58.168? Tell 192.168.1.102
480660	1852.908259	LiteonTe_7f:…	Broadcast	ARP	42	Who has 172.20.58.169? Tell 192.168.1.102
480661	1852.908276	LiteonTe_7f:…	Broadcast	ARP	42	Who has 172.20.58.175? Tell 192.168.1.102
480662	1852.908314	LiteonTe_7f:…	Broadcast	ARP	42	Who has 172.20.58.176? Tell 192.168.1.102
480663	1852.908327	LiteonTe_7f:…	Broadcast	ARP	42	Who has 172.20.58.177? Tell 192.168.1.102
480664	1852.908378	LiteonTe_7f:…	Broadcast	ARP	42	Who has 172.20.58.178? Tell 192.168.1.102
480665	1852.908391	LiteonTe_7f:…	Broadcast	ARP	42	Who has 172.20.58.179? Tell 192.168.1.102
480666	1852.908435	LiteonTe_7f:…	Broadcast	ARP	42	Who has 172.20.15.215? Tell 192.168.1.102

Imagen 19: Protocolos monitoreados en Wireshark
Fuente: Elaboración Propia

(c) Verificar las respuestas ICMP de todos los objetivos.

Algunos objetivos tienen respuestas ICMP como se muestra en la figura 15:

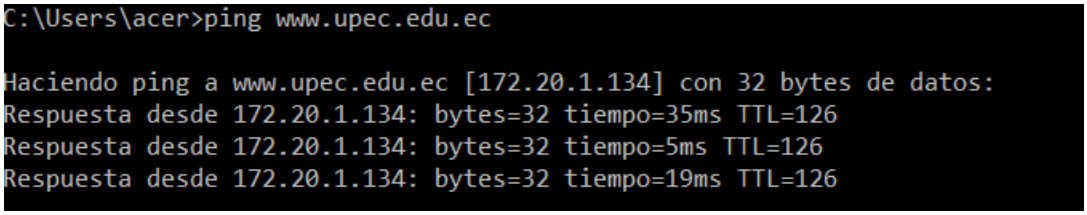


Imagen 20: Respuesta de ICMP, página WEB UPEC
Fuente: Elaboración Propia

(d) Verificar defectos y probables SNMP nombres de la comunidad en uso están de acuerdo a despliegues prácticos de todas las versiones de SNMP.

(e) Usar el sniffing para identificar el protocolo que procede de las respuestas de los servicios de red o peticiones aplicables. Por ejemplo, NetBIOS, ARP, BGP, NFS, OSPF, MPLS, RIPv2, etc

Para verificar este punto se utilizó Wireshark, en el cual se comprobó que el protocolo que procede de las respuestas de los servicios de red es ARP. Esto se muestra en la imagen 16:

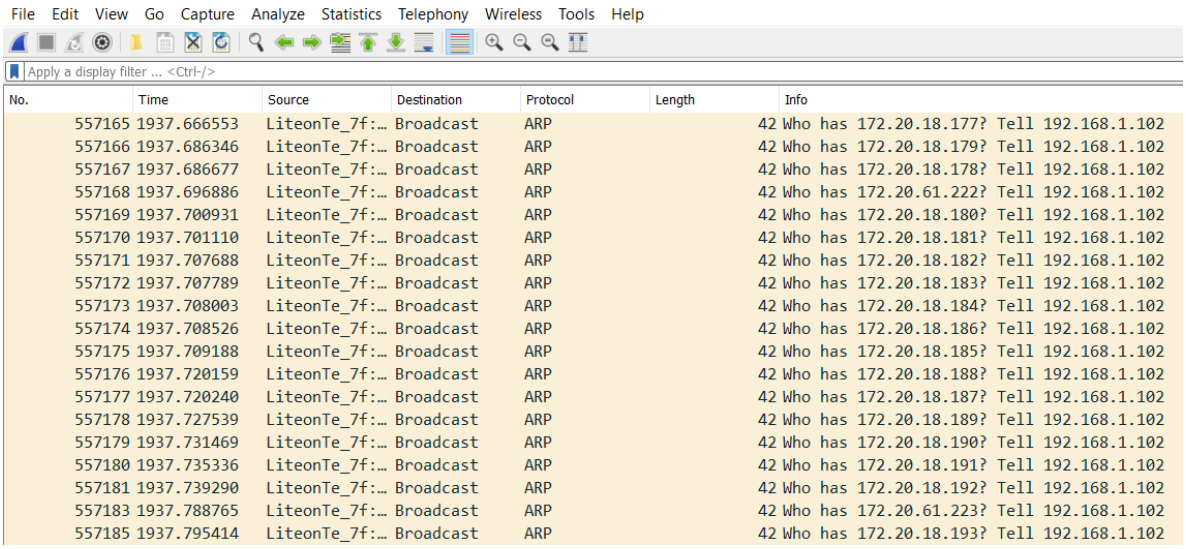


Imagen 21: Protocolo de los servicios de red
Fuente: Elaboración Propia

Los resultados de esta prueba se muestran en la tabla 69:

Tabla 69: Resultados para la Visibilidad del canal Redes de Datos

Visibilidad
❖ El segmento de red es 172.20.x.x ❖ Algunos objetivos tienen respuestas de ICMP ❖ No se poseen defectos de SNMP, porque no se hace uso de ninguna version. ❖ ARP

Fuente: Elaboración Propia

Para la visibilidad se obtiene un valor numérico de $P_V = 4$.

3.8.1.2 Acceso (P_A)

Las pruebas para la enumeración de los principales puntos de acceso dentro del campo de acción.

(a) Solicitar servicios comunes conocidos VPN, incluidos aquellos que utilizan IPSEC e IKE para conexiones desde todas las direcciones.

(b) Solicitar servicios comunes conocidos los cuales utilizan TCP para las conexiones desde todas las direcciones y puertos sin filtrar que no han enviado ninguna respuesta a un SYN TCP

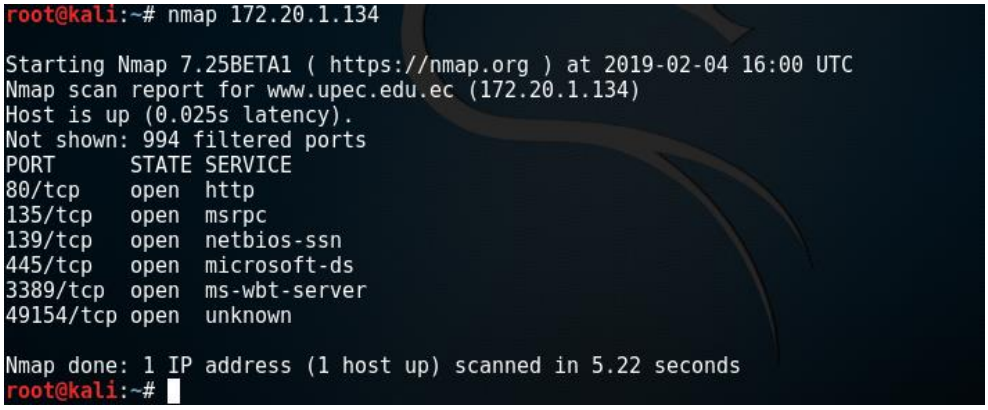


Imagen 22: Puertos TCP Abiertos
Fuente: Elaboración Propia

(c) Relacionar cada puerto abierto a un proceso (servicio), la aplicación (código específico o producto que utiliza el servicio), y el protocolo (los medios para interactuar con dicho servicio o aplicación).

No se pueden relacionar los puertos porque están abiertos sin ninguna restricción y no se tiene registro del uso que se da a cada puerto.

Los resultados de para el acceso se muestran en la tabla 70:

Tabla 70: Resultados para el acceso del canal Redes de Datos

Acceso	
Servicios TCP	❖ Se encuentran abiertos varios puertos
VPN	❖ Si hacen uso de VPN
Puerto abiertos	En el firewall los puertos para la LAN están abiertos. ❖ En el firewall los puertos para la WAN están cerrados, solo se abren los necesarios.

Fuente: Elaboración Propia

Para el acceso se tiene un valor numérico de P_A =3.

3.8.1.3 Confianza (P_T)

Las pruebas de confianzas entre sistemas dentro del alcance donde la confianza se refiere al acceso a la información o propiedad física sin la necesidad de una identificación o autenticación.

Suplantación

(a) Probar las medidas para acceder a la propiedad dentro del campo de acción por la suplantación de la dirección de red.

(b) Verificar si los mecanismos de caché disponibles pueden ser envenenados.

Suplantación de Identidad

(a) Verificar que las direcciones URL para presentaciones y consultas sobre el objetivo sean concisos, dentro del mismo dominio.

(b) Verificar el contenido de destino de datos/ registros / imágenes que no existen en los sitios fuera del objetivo para crear un duplicado del objetivo.

(c) Examinar los registros de dominio de nivel superior para los dominios similares a aquellos identificados dentro del alcance.

(d) Verificar que el destino de usos de personalización en sitios web y correo electrónico en la interacción con los usuarios autenticados.

Los resultados para la confianza se muestran en la tabla 71:

Tabla 71: Resultados para el acceso del canal Redes de Datos

Confianza	
Suplantación	No se puede acceder con la suplantación de ip. No poseen dispositivos de cache.
Suplantación de identidad	❖ El servidor DNS es un servicio contratado. ❖ El correo electrónico es proporcionado por OFFICE 365

Fuente: Elaboración Propia

El valor numérico para la confianza es de $P_T = 2$.

Con los valores de los 3 puntos que plantea la seguridad operacional, se procede con el cálculo del valor de **$OpSec_{sum}$** o la **porosidad** del canal Redes de Datos, aplicando la ecuación 1:

$$\mathbf{OpSec_{sum} = P_V + P_A + P_T}$$

$$\mathbf{OpSec_{sum} = 4 + 3 + 2}$$

$$\underline{\mathbf{OpSec_{sum} = 9}}$$

3.8.2 Controles

3.8.2.1 Autenticación (LC_{Au})

(a) Enumerar la autenticación a la solicitud de accesos y todos los privilegios descubiertos que pueden ser utilizados para proporcionar acceso.

(b) Verificar el método de obtención de la autorización apropiada para la autenticación.

(c) Verificar el método de ser identificado correctamente para ser provista la autenticación.

(d) Verificar la solidez de la autenticación a través de craqueo de la contraseña y volver a aplicar las contraseñas descubiertas a todos los puntos de acceso que requieren autenticación.

Los resultados para la autenticación se muestran en la tabla 72:

Tabla 72: Resultados de la Autenticación para el canal Redes de Datos

Autenticación	
Privilegios	❖ Se debe ser parte de la institución para tener privilegios.
Identificación	❖ Se identifica con la cedula de identidad, la matricula o el contrato. ❖ Las contraseñas son robustas deben contener mayúsculas números y al menos un símbolo.

Fuente: Elaboración Propia

El valor numérico para la autenticación es de $LC_{Au} = 3$.

3.8.2.2 Indemnización (LC_{Id})

(a) Enumerar los objetivos y servicios que están protegidos contra el abuso o elusión de la política de los empleados, están asegurados por robo o daños, o utilizar renuncias de responsabilidad y permisos.

(b) Verificar el efecto de las limitaciones de responsabilidad en la seguridad o medidas de seguridad.

Tabla 73: Resultados de la Indemnización para el canal Redes de Datos

Indemnización
Ningún objetivo ni servicio está protegido o asegurado.

Fuente: Elaboración Propia

3.8.2.3 Subyugación (LC_{Su})

Si un log-in puede hacerse en HTTP, así como HTTPS, pero requiere que el usuario haga esa distinción, entonces se produce un error al contar la Subyugación. Sin embargo, si la aplicación requiere el modo seguro por defecto, tal como un sistema de mensajería interna PKI, entonces cumple con el requisito del control de Subyugación para el alcance.

Tabla 74: Resultados de la Subyugación para el canal Redes de Datos

Subyugación
El sitio web de la institución trabaja como http, por lo cual no se debe hacer ninguna distinción.

Fuente: Elaboración Propia

Los resultados para la Subyugación le dan un valor numérico de $LC_{Su} = 0$.

3.8.2.4 Continuidad (LC_{Ct})

(a) Enumerar y examinar las deficiencias de todos los objetivos con respecto a los retrasos de acceso y los tiempos de respuesta de servicio a través de los sistemas de seguridad.

(b) Verificar los esquemas de bloqueo del proceso de intrusos que no pueden ser usados contra los usuarios válidos.

Tabla 75: Resultados para la continuidad del canal Redes de Datos

Continuidad
❖ Algunos servicios son vulnerables a ataques de denegación de servicios, sin embargo se abordan con la seriedad del caso. No se poseen sistemas de bloqueo de intrusos.

Fuente: Elaboración Propia

Los resultados para la continuidad es $LC_{Ct} = 1$.

3.8.2.5 Resistencia (LC_{Re})

(a) Verificar puntos únicos de fallo (cuellos de botella) en la infraestructura donde el cambio o el fracaso pueden causar una interrupción del servicio.

(b) Verificar el impacto al acceso del objetivo que causará un fallo del sistema o servicio.

(c) Verificar la funcionalidad operacional de los controles para evitar el acceso o permisos por encima de más bajos privilegios posibles en caso de fallo.

(d) Verificar los privilegios disponibles del acceso incluidos por fallos.

Los resultados para la resistencia se muestran en la tabla 76.

Tabla 76: Resultados para la Resistencia del Canal Redes de Datos

Resistencia
❖ No se producen cuellos de botella pues se usa fibra óptica para llegar a cada facultad. ❖ El cableado estructurado se encuentra en buen estado. No se manejan privilegios en caso de fallos. ❖ Para acceder a los dispositivos de red se deben tener las claves de acceso o en su caso acceso físico a los dispositivos.

Fuente: Elaboración Propia

El valor numérico para la Resistencia es de $LC_{Re} = 3$.

3.8.2.6 No-repudio (LC_{NR})

(a) Verificar que todos los métodos de interacciones sean registrados adecuadamente con identificación apropiada.

(b) Identificar los métodos de identificación los cuales repudian la derrota.

Tabla 77: Resultados del No-repudio para el canal Redes de Datos

No-Repudio
❖ Las interacciones realizadas en la red se registran en el firewall de la institución.

Fuente: Elaboración Propia

El resultado para el No-Repudio es de $LC_{NR} = 1$.

3.8.2.7 Confidencialidad (LC_{Cf})

(a) Enumerar todas las interacciones con los servicios dentro del ámbito de las comunicaciones o bienes transportados por el canal mediante líneas seguras, encriptación, interacciones “cerradas” o “calmadas” para proteger la confidencialidad de la información de propiedad entre las partes involucradas.

(b) Verificar los métodos aceptables utilizados para la confidencialidad.

(c) Probar la resistencia y el diseño del método de cifrado o la ofuscación.

Los resultados para la Confidencialidad se muestran en la tabla 78.

Tabla 78: Resultados de la Privacidad Para el canal Redes de Datos

Confidencialidad
❖ Las comunicaciones usan interacciones cerradas

Fuente: Elaboración Propia

Los resultado para la confidencialidad son $LC_{Cf} = 1$.

3.8.2.8 Privacidad (LC_{Pr})

(a) Enumerar los servicios dentro del ámbito de las comunicaciones o bienes transportados utilizando, firmas individuales específicas, identificación personal, interacciones personales "tranquilas" o "a cuarto cerrado" para proteger la privacidad de la interacción y el proceso de proporcionar activos sólo a aquellos dentro de la debida autorización de seguridad para ese proceso, comunicación, o activo.

(b) Relacionar información con TCP no responde y los puertos UDP para determinar si la disponibilidad depende de un tipo particular de contacto o protocolo.

Los resultados para la privacidad se muestran en la tabla 79.

Tabla 79: Resultados para la Privacidad del canal Redes de Datos

Privacidad
❖ La disponibilidad no depende de un tipo particular de protocolo

Fuente: Elaboración Propia

El resultado para la privacidad es de $LC_{Pr} = 1$.

3.8.2.9 Integridad (LC_{It})

Enumerar y las deficiencias de integridad donde utilizando un proceso documentado, firmas, cifrado, hachís, o marcas para asegurar que el activo no puede ser cambiado, redirigido, o revertido sin que sea conocido por las partes involucradas.

Los resultados para la integridad se muestran en la tabla 80.

Tabla 80: Resultados de la Integridad para el canal Redes de Datos

Integridad
❖ Los activos no pueden ser intervenidos

Fuente: Elaboración Propia

3.8.2.10 Alarma (LC_{Al})

Verificar y enumerar la utilización de un sistema de alerta localizado en todo el alcance, registro, o un mensaje para cada puerta de enlace de acceso a través de cada canal donde una situación sospechosa es observada por el personal en caso de sospecha de intentos de elusión, ingeniería social, o una actividad fraudulenta.

Los resultados para la alarma se muestran en la tabla 81.

Tabla 81: Resultados para la Alarma del canal Redes de Datos

Alarma
No se posee un sistema de alarma

Fuente: Elaboración Propia

3.8.3 Limitaciones

3.8.3.1 Vulnerabilidad (L_V)

Una vulnerabilidad puede ser un defecto en el software que permite a un atacante sobrescribir en el espacio de memoria para tener acceso, una falla de cálculo que permite a

un atacante bloquear el CPU en un uso del 100%, o un sistema operativo que permite que los datos suficientes sean copiados en el disco hasta que ya no puede funcionar más.

Los resultados para la vulnerabilidad se muestran en la tabla 82.

Tabla 82: Resultados para la Vulnerabilidad del canal Redes de Datos

Vulnerabilidad
No se puede bloquear CPU haciendo uso del 100% ❖ Los ordenadores no tienen una licencia de antivirus.

Fuente: Elaboración Propia

La vulnerabilidad tiene un resultado de $L_V = 1$.

3.8.3.2 Debilidad (L_W)

Una debilidad puede ser un inicio de sesión que permite intentos ilimitados o una granja de servidores web con el método round-robin DNS para equilibrar la carga sin embargo, cada sistema también tiene un nombre único para enlazar directamente.

Los resultados se muestran en la tabla 83.

Tabla 83: Resultado de la Debilidad para el canal Redes de Datos

Debilidad	
Autenticación	Los inicios de sesión se bloquean por 10 segundos, con ingresos erróneos.
Indemnización	❖ No existen controles a excepción del contrato firmado.
Resistencia	No se presentan inconvenientes
Continuidad	❖ El ping está habilitado por lo cual se pueden hacer ataques de denegación de servicio.
Subyugación	❖ Uso de servidor web no seguro.

Fuente: Elaboración Propia

Para la debilidad se tiene un valor numérico de $L_W = 3$.

3.8.3.3 Preocupación (L_C)

Una preocupación puede ser el uso de certificados de servidor web generadas localmente para HTTPS o archivos que registran sólo los participantes en las operaciones y no la fecha y la hora correcta del registro de transacciones.

Los resultados se muestran en la tabla 83.

Tabla 84: Resultados para la Preocupación del canal Redes de Datos

Preocupación	
No-Repudio	No se encontraron falencias
Privacidad	No se presentaron falencias
Confidencialidad	❖ No se usan líneas seguras
Integridad	No se encontraron falencias
Alarma	❖ EL firewall tiene los puertos abiertos localmente.

Fuente: Elaboración Propia

El resultado numérico para la preocupación es de $L_C = 2$.

3.8.3.4 Exposición (L_E)

Una exposición puede ser una bandera descriptiva y válida acerca de un servicio (banderas de desinformación no son exposiciones) o una respuesta de eco ICMP desde un host.

Los resultados se muestran en la tabla 85.

Tabla 85: Resultados para la Exposición del canal Redes de Datos

Exposición
❖ Algunos host si tienen respuesta de ICMP

Fuente: Elaboración Propia

El valor numérico para la exposición de L_E

3.8.3.5 Anomalía (L_A)

Una anomalía pueden ser respuestas correctas a un sondeo de una dirección IP diferente que fue sondeada o esperado.

Los resultados se muestran en la tabla 86.

Tabla 86: Resultados para la Anomalía del canal Redes de Datos

Anomalía
❖ Si se dan respuestas correctas.

Fuente: Elaboración Propia

El valor numérico para la anomalía es de $L_A = 1$.

3.8.4 Calculadora RAV

Métricas de Seguridad Redes de Datos

OSSTMM version 3.0

Rellene en los campos en blanco los valores numéricos para OPSEC, Controles y Limitaciones con los resultados de la prueba de seguridad. Consulte OSSTMM 3 (www.osstmm.org) para obtener más información.

OPSEC			
Visibilidad	4		
Acceso	3		
Confianza	2		
Total (Porosidad)	9		

CONTROLES			
Clase A		Ausentes	
Autenticación	3	6	
Indemnización	0	9	
Resistencia	3	6	
Subyugación	0	9	
Continuidad	1	8	
Total Clase A	7	38	
Clase B		Ausentes	
No-Repudio	1	8	
Confidencialidad	1	8	
Privacidad	1	8	
Integridad	1	8	
Alarma	0	9	
Total Clase B	4	41	
		Ausentes Verdaderos	
Total todos los Controles	11	79	
Cobertura Total	12,22%	87,78%	

LIMITATIONS			
		Item Value	Total Value
Vulnerabilidades	1	9,78	9,78
Debilidades	3	5,22	15,67
Preocupaciones	2	5,56	11,11
Exposiciones	1	1,35	1,35
Anomalías	1	0,86	0,86
Total # Limitaciones	8		38,77

OPSEC	8,73
Controles Verdaderos	4,18
Controles Totales	4,18
Cobertura Verdadera A	15,56%
Cobertura Verdadera B	8,89%
Cobertura Verdadera Total	12,22%
Limitaciones	12,877838
Seguridad Δ	-17,42
Proteccion Verdadera	82,58

Seguridad Actual: 82,80 ravs

Luego de ingresar los valores obtenidos en la calculadora RAV, se obtienen que la Seguridad Actual de la UPEC en el canal Redes de Datos es de **82,80 RAVS**, lo que se interpreta en que se posee una deficiencia de aproximadamente el 19%, que es la vulnerabilidad que tienen la institución en caso de sufrir un ataque. Los motivos principales para tener una deficiencia que supere el 10% es que los controles para la indemnización, subyugación y alarma son prácticamente nulos, por lo cual deben ser los controles que se aborden con mayor prioridad.

Por otra parte la **Seguridad Δ,** toma un valor negativo de **-17,42,** este valor es interpretado como la insuficiencia de controles que posee la institución en cuanto al canal redes de datos, además muestra que los controles que se encuentran aplicados tienen falencias por lo cual necesitan ser mejorados para que la institución tenga una buna seguridad en caso de sufrir ataques de seguridad.

CAPÍTULO IV

4. Políticas de Seguridad

El presente capítulo se procederá a elaborar las políticas de seguridad informática de la Universidad Politécnica Estatal del Carchi, las cuales están basadas en las vulnerabilidades encontradas en la red interna de la institución luego de haber realizado la auditoria. Además se establecen procedimientos de seguridad, los cuales son establecidos por la Norma ISO/IEC 27001, que servirán para ayudar al cumplimiento de las políticas realizadas.

4.1 Resultados de la auditoría

En la tabla 87 se muestran los resultados finales de la auditoría, los cuales sirven para redactar las políticas de seguridad informática de la institución.

Resultados Finales de la Auditoría					
Canal	**Humano**	**Físico**	**Inalámbrico**	**Telecomunicaciones**	**Redes de Datos**
OpSec	9.48	10.75	10.27	8.10	8.73
Limitaciones	9.96	15.64	11.80	7.35	12.87
Controles Verdaderos	5.59	6.66	4.02	5.10	4.18
Seguridad Δ	-13.86	-19.74	-18.06	-10.36	-17.42
Protección Verdadera	86.14	80.26	81.94	89.64	82.58
Seguridad Actual	86.00	80.19	82.27	89.45	82.80

Tabla 87: Resultados de la Auditoría
Fuente: Elaboración Propia

4.2 Desarrollo de las Políticas

	POLÍTICAS DE SEGURIDAD INFORMÁTICA DE LA UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
Versión:	**1.0**
Revisado por:	**ING. ANDRÉS GUERRERO**
Aprobado por:	**ING. ANDRES GUERRERO** — **Firma:** — **Sello:**
Elaborado por:	**ANDERSON AZA**

1. Objetivo

Proteger la seguridad de la red interna de la Universidad Politécnica Estatal del Carchi, garantizando confiabilidad, disponibilidad e integridad de la misma.

2. Alcance

Estas políticas de seguridad son aplicables para los 5 canales que fueron auditados y deben ser cumplidas por el personal que tenga relación directa con la seguridad de la red interna de la Universidad Politécnica estatal del Carchi.

3. Aplicabilidad

Las políticas de seguridad se deben aplicar de manera obligatoria, con la única excepción en la cual no se cuente con el presupuesto necesario para su aplicación. En caso de existir problemas y no se encuentre la solución con las políticas de seguridad, el Director del

departamento de TIC’s tiene la autoridad para decidir la solución del problema además de modificar, o anular el presente documento.

4. Policías de seguridad Generales

Art 1.- En este documento se establece como se debe manejar la seguridad de la Universidad Politécnica Estatal del Carchi, y fue redactado en base a la auditoría realizada previamente.

Art 2.- La persona encargada de hacer cumplir las políticas de seguridad es el Director del departamento de TIC’s, o su delegado.

Art 3.- Las políticas de seguridad deben ser socializadas con todo el personal de la Universidad Politécnica Estatal del Carchi.

Art 4.- Las políticas de seguridad deben ser revisadas al menos dos veces al año, pues la red interna de la institución está cambiando y se debe actualizar las políticas.

Art 5.- Las contraseñas de todos los sistemas deben contener al menos 8 caracteres, en los cuales se incluyan letras, números y por lo menos un carácter especial.

Art 6.- En caso de incumplir las políticas de seguridad, el Director del Departamento de TIC´s es el responsable de sancionar de acorde con el reglamento interno de la institución.

5. Políticas de seguridad para el canal humano

Art 7.- Solo el personal autorizado tiene la potestad para acceder a las instancias tales como, Data Center, Racks, Estaciones de trabajo.

Art 8.- Para solicitar el permiso para acceder a las áreas restringidas se lo debe realizar mediante un oficio dirigido al Director del departamento de TIC's. Para las áreas que no son competencia del departamento de TIC's, se debe solicitar al encargado de cada departamento.

Art 9.- Los guardias de seguridad deben estar al tanto de las zonas restringidas y de las personas que tienen la autoridad y permiso para acceder.

Art 10.- Para acceder a las estaciones de trabajo de los estudiantes, estos deberán presentar el carnet estudiantil o su cédula en caso de no poseer carnet.

Art 11.- Los permisos deben ser firmados y sellados con el fin de evitar posibles falsificaciones además, se deben confirmar con quien corresponda, para acceder a zonas restringidas, con el fin de evitar el acceso indebido.

Art 12.- Se debe llevar registro de las personas que accedan a las áreas restringidas.

Art 13.- El sistema de video vigilancia debe estar ubicado estratégicamente, con la finalidad de tener visibles las áreas restringidas y evitar accesos indebidos.

Art 14.- En caso de accesos indebidos, se debe abordar al infractor con el personal de seguridad y el Director del departamento de TIC's será quien determine las acciones a tomar, de acuerdo con el reglamento interno de la institución.

Art 15.- Todo el personal de la Universidad Politécnica Estatal del Carchi, debe estar consciente de sus responsabilidades y deberá actuar en favor de la institución en caso de presentarse incidentes.

Art 16.- El personal de la institución no debe divulgar ningún tipo de información, caso contrario será sancionada de acuerdo con el reglamento interno de la institución.

Art 17.- Los empleados de la institución no utilizarán activos corporativos o relaciones comerciales para uso o beneficio personal.

Art 18.- Todo el personal de la institución está obligado a acatar las políticas de seguridad, y los infractores serán sancionados de acuerdo con el reglamento interno.

Art 19.- El talento humano de la institución debe ser capacitado al menos una vez por año en temas de seguridad.

Art 20.- Bajo ninguna circunstancia se deben tener las contraseñas de acceso a los sistemas de la universidad, pegadas en los monitores o teclados de las estaciones de trabajo del personal administrativo.

6. Políticas de seguridad para el canal físico

6.1 Del acceso a zonas restringidas y activos de la institución:

Art 21.- Todas las áreas de la red interna de la UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI**,** son de acceso restringido por tal motivo deben tener medidas de seguridad para proteger la integridad de la institución.

Art 22.- Los guardias de seguridad deben acercarse a las zonas restringidas al menos 2 veces por día, con el fin de resguardar la integridad de las mismas.

Art 23.- El centro de educación infantil debe acatar las políticas de seguridad, pues aunque este fuera del campus es parte de la red interna de la institución.

Art 24.- Para acceder a los activos de la institución se debe presentar una identificación o autorización del jefe del departamento de TIC´s, o del encargado de esa área.

Art 25.- Resguardar los racks de comunicación que se encuentran fuera del data center con la seguridad de por lo menos una cerradura. Y las llaves deben estar en poder de la persona autorizada para esta tarea.

Art 26.- No se pueden llevar los activos de la institución fuera del límite del campus universitario, salvo los casos que sean permitidos por el Director del departamento de TIC's.

Art 27.- Los activos de la institución deben estar asegurados o empotrados con el fin de que estos no sean sustraídos.

Art 28.- El sistema de video vigilancia debe ser monitoreado constantemente, pues de lo contrario no se puede detectar intrusos a tiempo.

6.2 Del acceso al Data Center:

Art 29.- El acceso al Data Center debe ser restringido para el personal no autorizado a excepción de que se posea la debida autorización.

Art 30.- No se permite tomar fotos al interior del Data Center, salvo con la debida aprobación del jefe del Departamento de TIC's.

Art 31.- Esta totalmente prohibido realizar ingresos indebidos que comprometan la seguridad de los activos dentro del Data Center, ingresos tales como, cigarrillo, alimentos, bebidas alcohólicas.

Art 32.- La vigilancia del Data Center debe ser las 24 horas del día, utilizando el sistema de video vigilancia.

Art 33.- Para realizar mantenimiento a los equipos del Data Center, el jefe del departamento de TIC's debe estar presente, o en su caso una persona delegada por él.

Art 34.- El Data Center debe contar con un sistema de respaldo de energía y realizar un mantenimiento periódico del mismo, con el fin de garantizar la continuidad de los servicios de la institución.

Art 35.- El Data Center debe contar con un sistema contra incendios y realizar mantenimientos periódicos, para garantizar la integridad de los equipos que se encuentran en su interior.

6.3 De las reuniones y documentos de la institución:

Art 36.- Todo tipo de reuniones se deben realizar con la puerta cerrada con el fin de que las decisiones tomadas y la información crítica para la institución no puedan ser divulgadas a personas no autorizadas.

Art 37.- Los documentos se deben entregar de forma personal y de ser necesario enviarlos por terceros en sobre cerrado.

7. Políticas de seguridad para el canal Inalámbrico

7.1 De la administración de la red inalámbrica:

Art 38.- Todas las redes inalámbricas deben ser administrables por parte del administrador de la red, por lo cual se deben utilizar equipos robustos, evitando poner puntos de acceso no autorizados, pues estos pueden ser vulnerados.

Art 39.- Los AP deben configurarse de tal forma que no se interfieran entre sí, con el fin de sacar el máximo rendimiento de los mismos.

Art 40.- Ningún punto de acceso debe tener la configuración por defecto, pues son más vulnerables a posibles ataques.

Art 41.- Las contraseñas para acceder a la red inalámbrica deben basarse en el Art. 5 de estas políticas.

Art 42.- Controlar el ancho de banda asignado a cada red Wi-Fi, de acuerdo con la utilidad que se le dé a cada red.

Art 43.- Asegurar físicamente los AP en los sitios en los cuales se encuentran empotrados.

7.2 Del acceso a la red inalámbrica:

Art 44.- Estudiantes, personal administrativo y de servicio, deben acceder a la red destinada para ellos, y las credenciales de acceso deben ser robustas,

Art 45.- La red para persona externas a la institución debe ser controlada con el fin de evitar posibles intrusos.

Art 46.- El uso adecuado de las claves de acceso es de los estudiantes, docentes o personal administrativo pues su uso incorrecto compromete la seguridad de la institución.

8. Políticas de seguridad para el canal Telecomunicaciones

Art 47.- El acceso a la telefonía IP se debe hacer mediante extensiones con contraseñas personalizadas para cada usuario basadas en el Art. 5 de estas políticas.

Art 48.- El buzón de voz debe tener contraseñas personalizadas para cada usuario de la institución y se deben basar en el Art. 5 de estas políticas.

Art 49.- Los RAS solo deben ser accesibles para el administrador de la red, evitando accesos indebidos.

Art 50.- El servicio de telefonía ip debe estar en una Vlan independiente en la cual se maneje QoS.

Art 51.- Los tonos táctiles de los teléfonos ip deben ser desactivados, pues con estos tonos se puede descifrar la contraseña del usuario.

9. Políticas de seguridad para el canal Redes de datos

Art 52.- Se debe realizar mantenimiento constante a los activos de la institución, para que la vida útil de estos sea la óptima.

Art 53.- Se debe llevar un registro de los mantenimientos que se realicen a los activos informáticos de la institución.

Art 54.- Todas las estaciones de trabajo deben estar configuradas de tal manera que eviten la instalación de software no autorizado.

Art 55.- Se deben usar Vlan para segmentar la red física y tener redes lógicamente independientes, con lo cual se mejorará el control de ancho de banda, aplicación de QoS y optimización de la administración.

Art 56.- Se deben manejar los servicios de la institución, en servidores robustos, para garantizar la disponibilidad de los mismos.

Art 57.- Se deben bloquear las respuestas de ICMP de los servidores de la institución, con la finalidad de evitar ataques usando el PING.

Art 58.- Se deben hacer censado de puerto comunes que se utilizan en la red para ser habilitados en el firewall para evitar dejar abiertas puertas traseras que generen ataques.

Art 59.- Todo usuario que pertenezca a la institución tendrá cuentas de correo electrónico, portafolio, estudiantil, docente o administrativo, los cuales serán generados por parte del departamento de TIC's.

Art 60.- Se deben usar los servicios en un entorno seguro, es decir usando certificados SSL.

Art 61.- Limitar a 5 el número intentos de inicio de sesión con claves erróneas, pues se pueden usar herramientas para descifrar la contraseña.

Art 62.- Luego de 5 minutos de inactividad, se debe cerrar la sesión de RAS para evitar posibles intrusiones.

4.3 Procedimientos de seguridad

La norma ISO/IEC 27001 establece realizar procedimientos de seguridad para los siguientes puntos; Control de Documentos, Control de Registros, Auditoria Interna, Acción Correctiva y Preventiva. A continuación se detallan los procedimientos estipulados:

4.3.1 Control de Documentos

Objetivo

Garantizar la integridad y seguridad de la documentación que se maneje dentro de la institución.

Alcance

Aplica a todos los documentos privados de la institución, es decir los documentos que contienen información crítica y que comprometa la seguridad de la misma.

Actividades:

1. Establecer quién es el delegado de aprobar los documentos redactados por los trabajadores de la institución, esto es para las diferentes instancias de la institución.
2. Determinar un formato para los documentos que tengan relación con la seguridad informática.
3. Redactar el documento, en este caso el informe de la auditoria de seguridad informática.
4. Los documentos emitidos por terceros deben ser revisados por el jefe del departamento de TIC’s, o un delegado de la institución.
5. Realizar las correcciones pertinentes de los documentos presentados.
6. Aprobar la documentación.

Diagrama de Flujo:

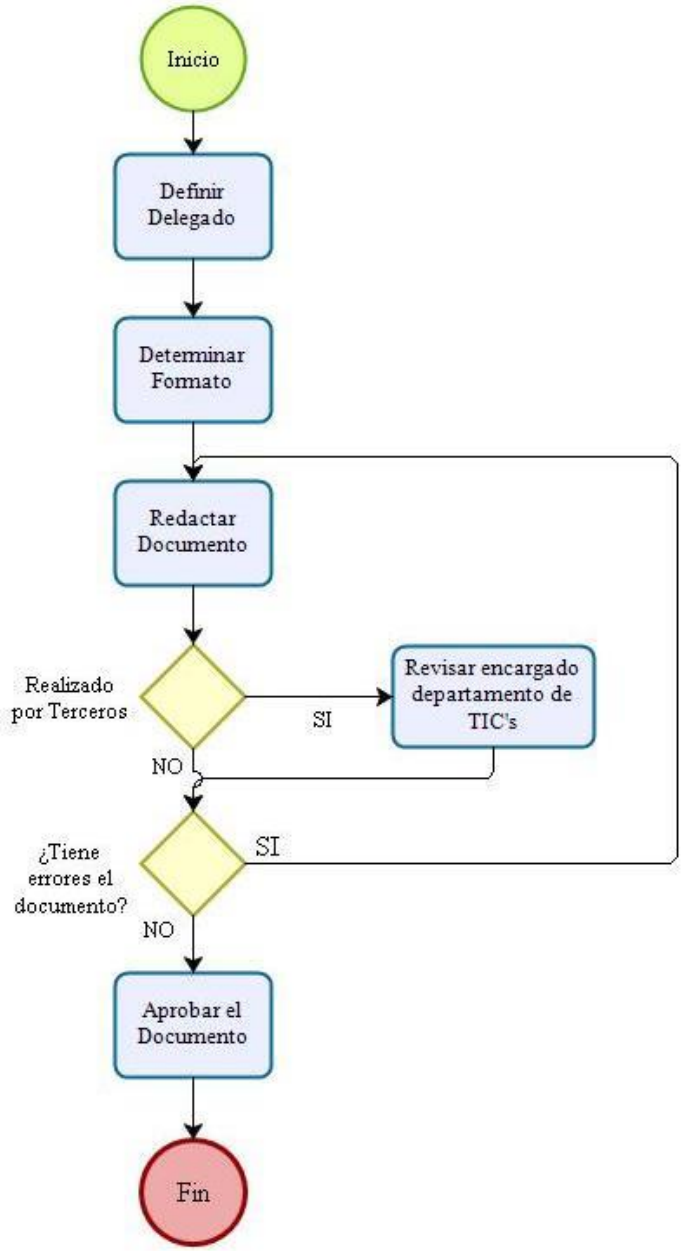


Diagrama de Flujo 1: Control de Documentos
Fuente: Elaboración Propia

4.3.2 Control de Registros

Objetivo

Llevar registro de las personas que tienen acceso a los activos de la institución para de esta manera tener conocimiento de las personas que interactuaron con los equipos y saber si no se usó indebido de los mismos.

Alcance

Aplica a todo el personal que desee acceder a los activos de la institución, ya sea para su uso o para darles mantenimiento.

Actividades

1. Establecer un formato para el registro de acceso, dependiendo si es para uso o para mantenimiento de los activos.
2. Delegar a un encargado de entregar y recibir los activos de la institución.
3. Llenar el registro de acceso a los activos de la institución.
4. Devolver los activos al encargado.
    4.1 En caso de estar en mal estado se procederá con la devolución o reparación del mismo.
5. Comprobar el estado de los activos.
6. Llenar el registro de devolución de los activos.

Diagrama de flujo

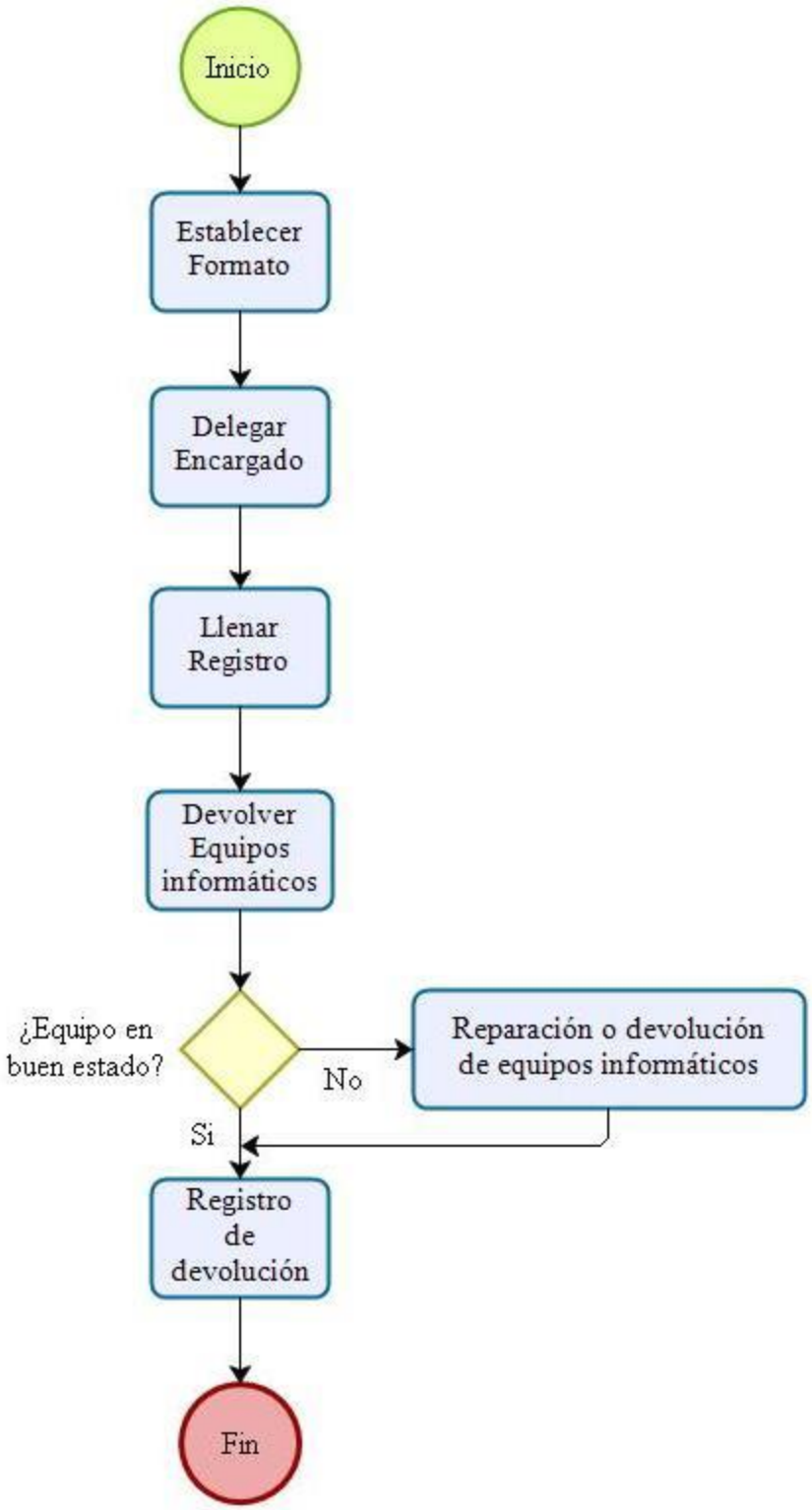


Diagrama de Flujo 2: Control de Registro
Fuente: Elaboración Propia

4.3.3 Auditoria Interna

Objetivo

Definir los procedimientos para realizar una auditoría a la red interna de la Universidad Politécnica Estatal del Carchi, cuando esta sea necesaria.

Alcance

Aplica para una auditoria que se realice dentro de la red interna de la Universidad Politécnica Estatal del Carchi.

Actividades

1. Establecer una metodología para la auditoria de seguridad informática.
2. Analizar la metodología escogida.
3. Definir los elementos necesarios para llevar a cabo la metodología, tanto hardware como software.
4. Realizar la auditoria con la metodología escogida.
5. Documentar el proceso realizado con la auditoria.
6. Analizar los resultados obtenidos.
7. Dependiendo de los resultados obtenidos se procede con el procedimiento ya sea preventivo o correctivo.
8. Elaborar un informe final sobre los resultados obtenidos en la auditoria.

Diagrama de Flujo

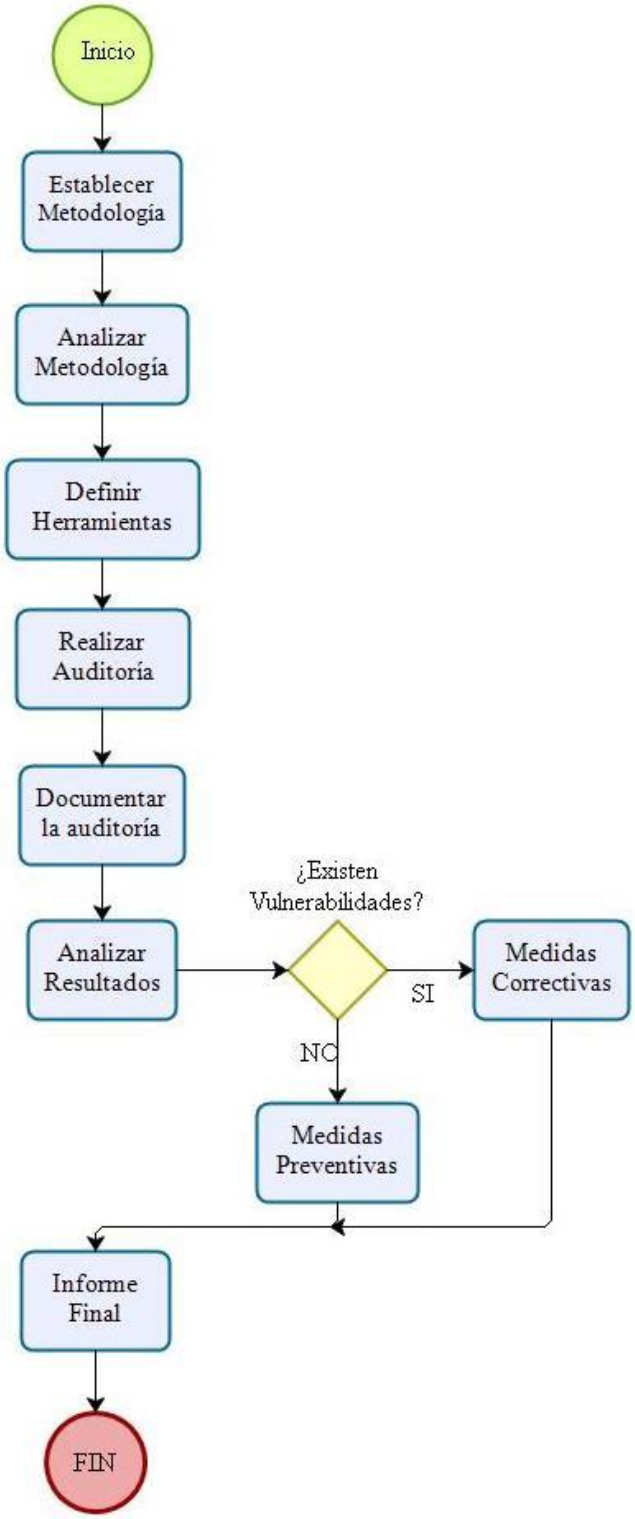


Diagrama de Flujo 3: Auditoria Interna
Fuente: Elaboración Propia

4.3.4 Acción Correctiva

Objetivo

La acción correctiva tiene como objetivo detectar y corregir posibles falencias que se presenten en la red.

Alcance

Las medidas son tomadas a los incidentes que se presenten y se aplican a la red interna de la institución.

Actividades

1. Detectar el incidente.
2. Analizar los incidentes que se presenten en la red interna de la institución.
3. Detectar que parte de la red es la afectada.
4. Analizar el tipo de incidente que se presenta y como abordarlo.
5. Buscar la mejor solución para mitigar las falencias.
6. Mitigar las falencias encontradas.
7. Si las falencias no pueden ser mitigadas, consultar con terceros para solucionar las fallas.
8. Realizar un informe con las soluciones de las falencias.

Diagrama de Flujo

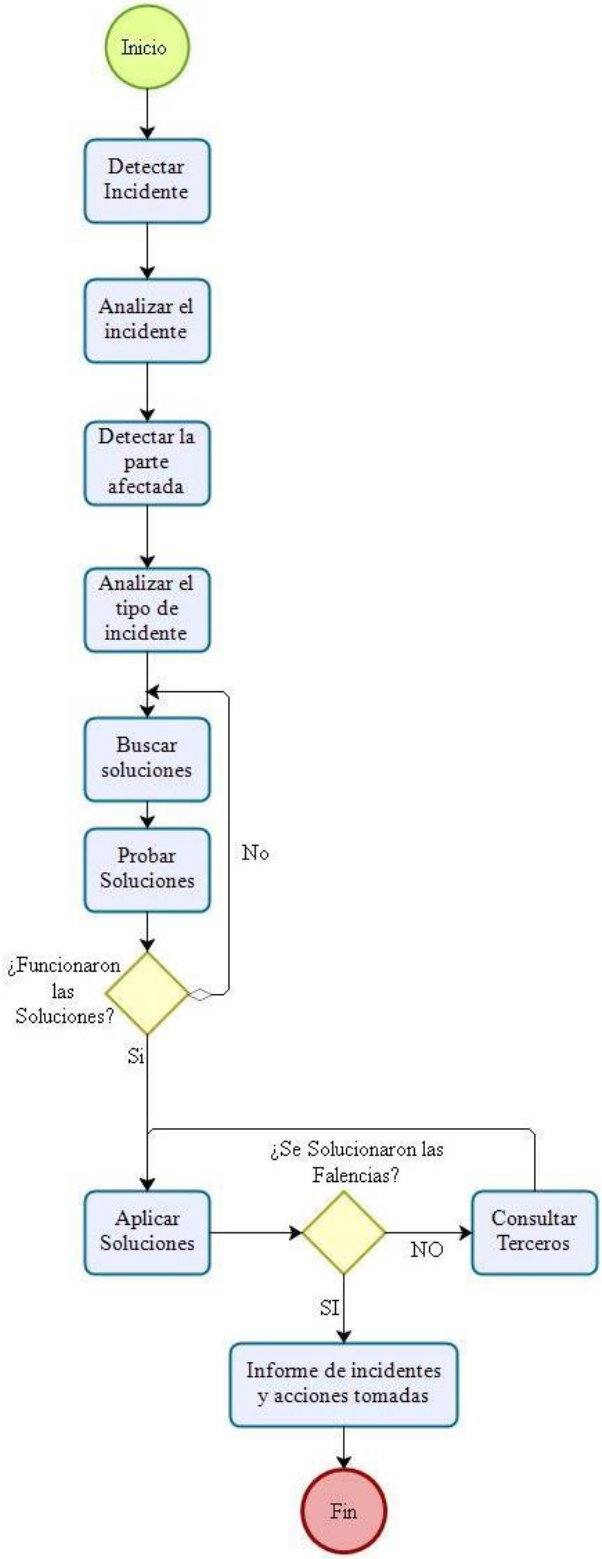


Diagrama de Flujo 4: Acción Correctiva
Fuente: Elaboración Propia

4.3.5 Acción Preventiva

Objetivo

La acción preventiva tiene como objetivo prevenir posibles falencias en la red interna de la institución.

Alcance

Las medidas serán tomadas de acuerdo a la necesidad de la red interna de la institución y deberán ser aprobadas por el director del departamento de TIC's.

Actividades

1. Analizar las partes de la red que necesitan medidas preventivas.
2. Investigar y escoger las medidas preventivas que más le convengan a la institución
3. Aplicar las medidas preventivas.
4. Realizar un informe con las medidas tomadas.

Diagrama de Flujo

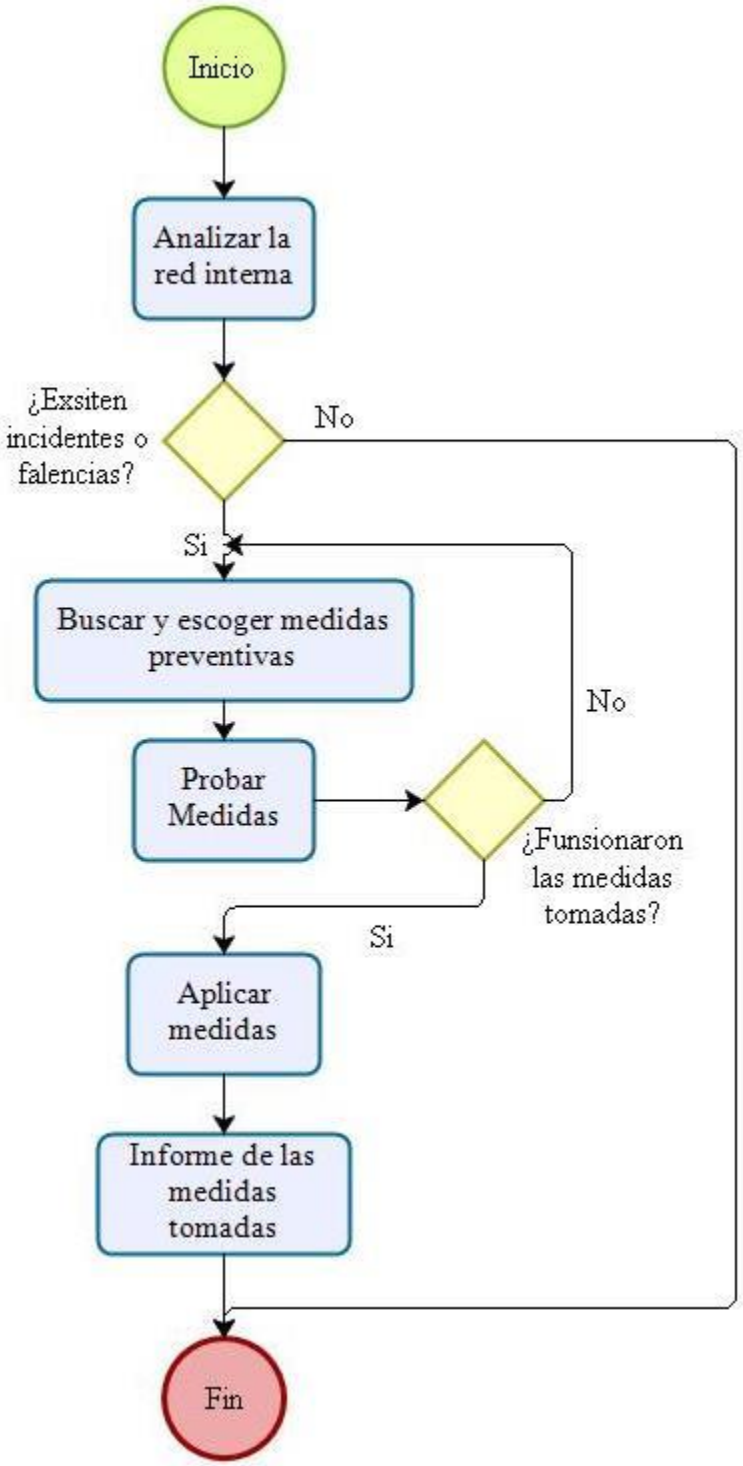


Diagrama de Flujo 5: Medidas Preventivas
Fuente: Elaboración Propia

Además de los procedimientos estipulados por la norma se plantean algunos adicionales que serán de utilidad para cumplir con las políticas de seguridad.

4.3.6 Mantenimiento preventivo equipos informáticos

Objetivo

Mantener en estado óptimo los equipos informáticos de la institución, para prolongar la vida útil de los mismos.

Alcance

Aplica a todos los equipos informáticos de la institución, especialmente estaciones de trabajo.

Actividades

1. Planificar los mantenimientos preventivos.
2. Realizar los mantenimientos preventivos planificados
3. Detectar fallos de los equipos informáticos, en caso de que existan, ya sean de hardware o software.
4. En caso de que los fallos sean de software, buscar las mejores soluciones.
5. En caso de que los problemas sean de hardware, buscar los elementos defectuosos en bodega caso contrario solicitar al Director del departamento de TIC’s se realice la adquisición.
6. Aplicar las soluciones si se encuentran problemas, caso contrario realizar limpieza del equipo.
7. Llenar ficha mantenimiento del equipo.

Diagrama de flujo

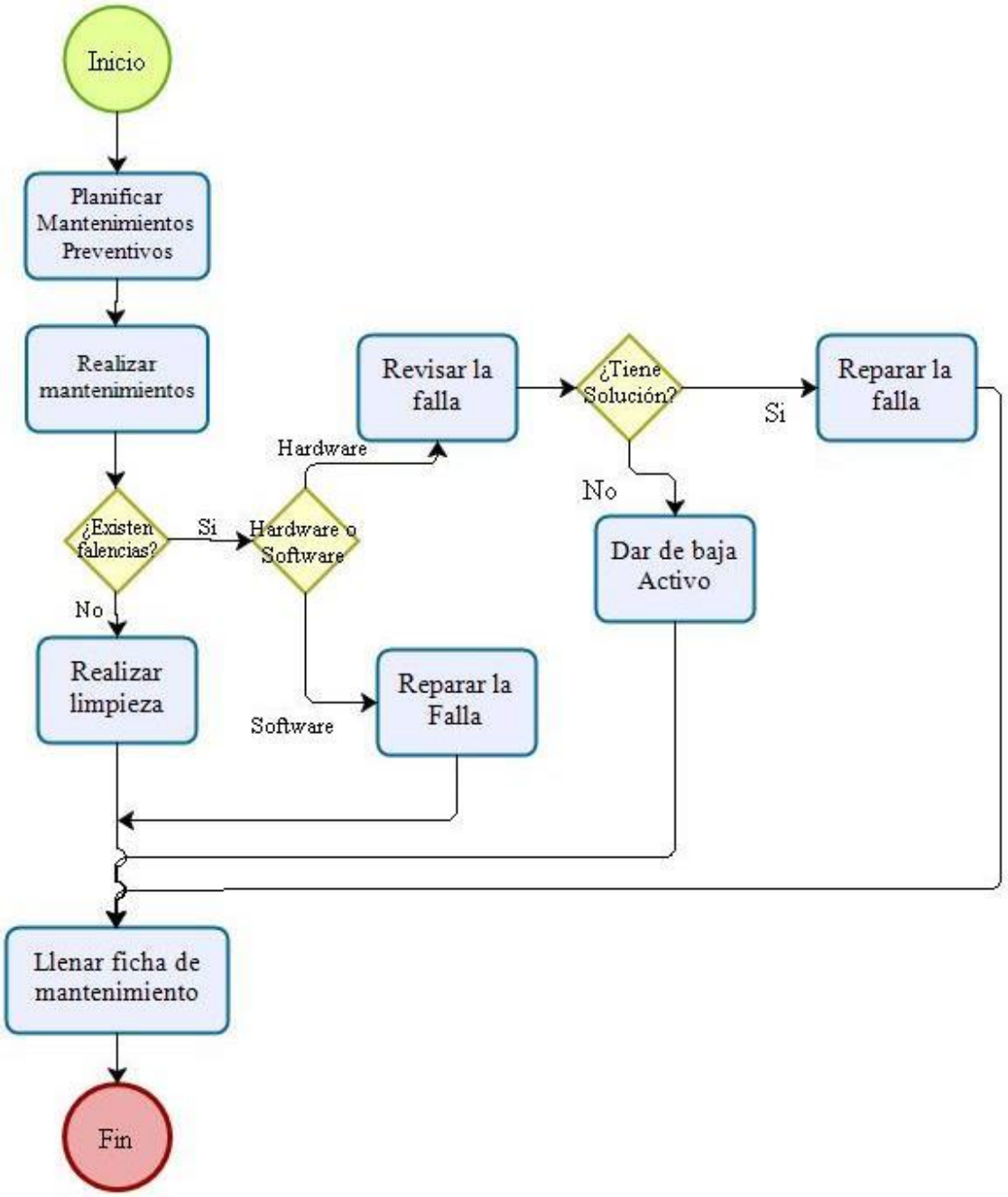


Diagrama de Flujo 6: Mantenimiento Preventivo Equipos Informáticos
Fuente: Elaboración Propia

4.3.7 Mantenimiento correctivo equipos informáticos

Objetivo

Solucionar problemas que se presenten con los equipos informáticos de la institución.

Alcance

Aplica a todos los equipos informáticos de la institución que presenten fallos y sean reportados por parte del personal que los usa.

Actividades

1. El personal informa del equipo que se encuentra fallando.
2. Se busca la razón del fallo.
3. En caso de que los fallos sean de software, buscar las mejores soluciones.
4. En caso de que los problemas sean de hardware, buscar los elementos defectuosos en bodega caso contrario solicitar al Director del departamento de TIC's se realice la adquisición.
5. Aplicar las soluciones.
6. Si el equipo no tiene compostura, se da de baja el activo, caso contrario llenar ficha de mantenimiento del equipo.

Diagrama de flujo

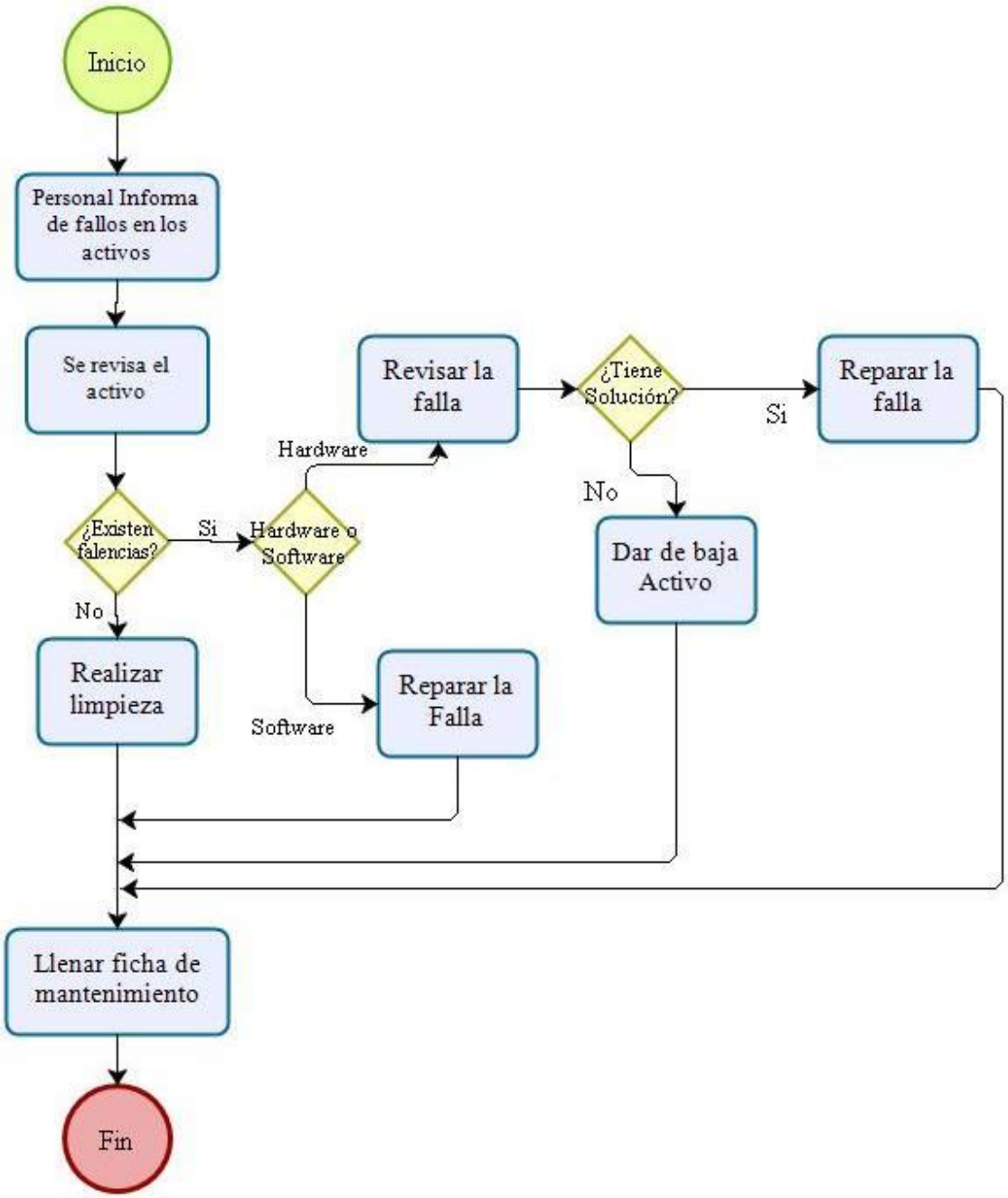


Diagrama de Flujo 7: Mantenimiento Preventivo Equipos Informáticos
Fuente: Elaboración Propia

4.3.8 Filtro de puertos en el firewall

Objetivo

Cerrar los puertos que no se usan en la red interna de la Universidad Politécnica Estatal del Carchi.

Alcance

Aplica a los servicios que se encuentran dentro de la red interna de la institución.

Actividades

1. Identificar los puertos que se utilizan en la red interna
2. Abrir los puerto identificados en el firewall
3. Cerrar todos los puertos que no se están utilizando
4. Llevar un registro de los puertos que se encuentran abiertos y en que IP se encuentran usados.

Diagrama de flujo

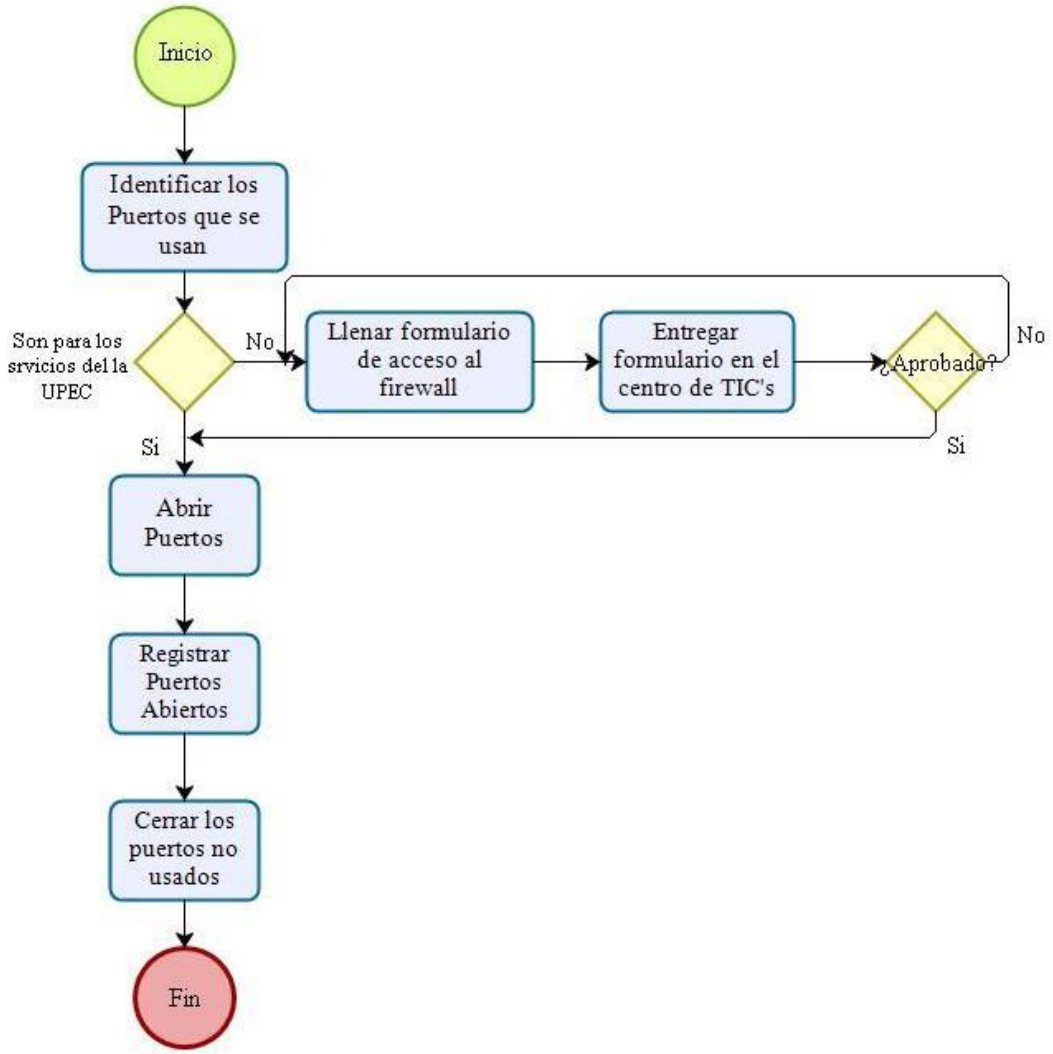


Diagrama de Flujo 8: Filtro de puertos en Firewall
Fuente: Elaboración Propia

4.1.1 Aplicación de certificado SSL, en servidor WEB

Objetivo

Tener un servidor WEB seguro, pues se cifra la información y esta no puede ser interceptada.

Alcance

Aplica al servidor WEB de la institución, el cual aloja toda la información que la universidad da a conocer al público.

Actividades

1. Generar una solicitud de firma de certificado (CSR)
2. Solicitar el certificado SSL, ya sea gratuito o de pago.
3. En caso de elegir certificados de pago, solicitar una proforma.
4. Adquirir los certificados.
5. Descargar los certificados.
6. Instalar el certificado en el servidor.
7. Reiniciar el servidor WEB
8. Comprobar el certificado instalado.

Diagrama de flujo

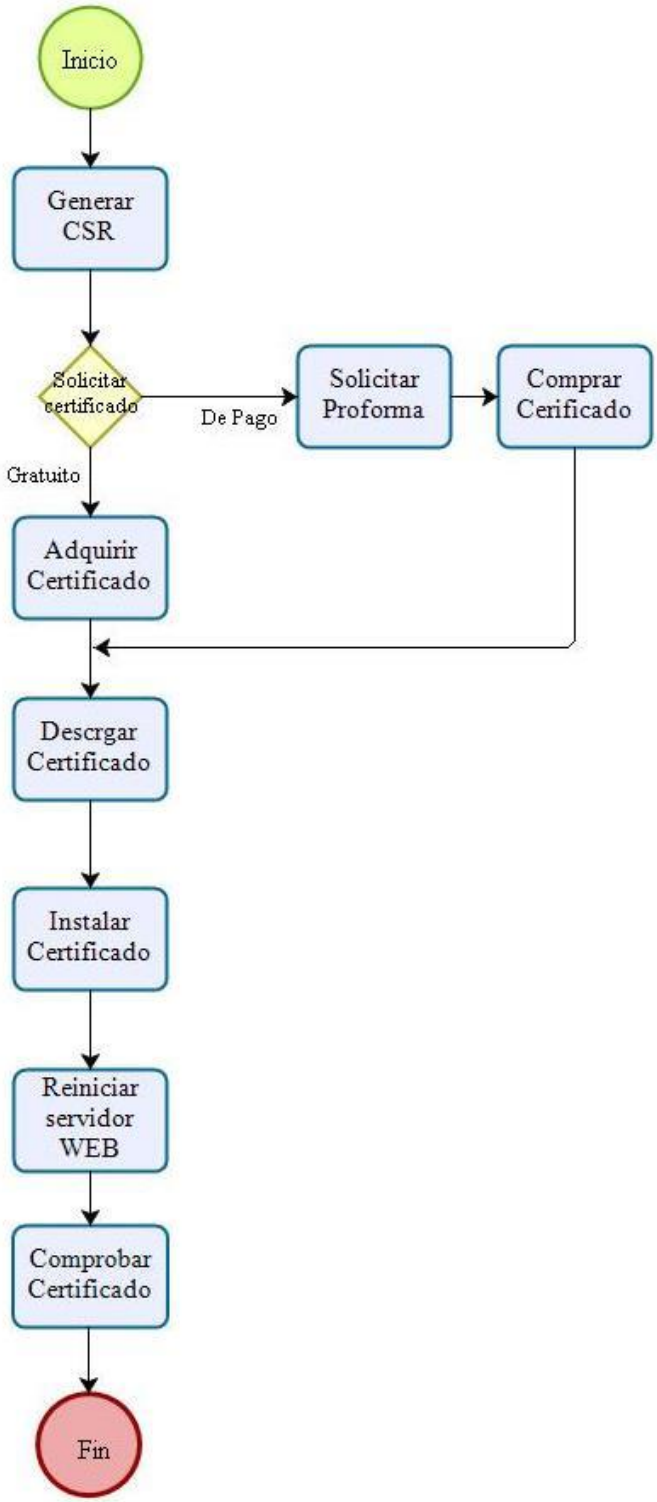


Diagrama de Flujo 9: Certificado SSL
Fuente: Elaboración Propia

4.4 Políticas de seguridad aplicadas en ambiente de prueba

Por cuestiones de presupuesto y en vista de que lagunas políticas están proyectadas a ser realizadas por parte del personal de la institución no fue posible aplicarlas todas, sin embargo a continuación se detalla algunas de las políticas que pudieron ser aplicadas. Cabe recalcar que se realizó un checklist, Anexo 25, para comprobar si las políticas se están aplicando y pueden o no ser eludidas.

4.1.1 Políticas de seguridad generales

En este apartado se detallan las políticas generales y los responsables de su cumplimiento, por lo que se pudo aplicar el Art. 3 el cual menciona que las políticas deben ser socializadas con el personal del departamento de TIC's, esto se puede evidenciar en el Anexo 15. Los demás artículos de este apartado deben ser cumplidos de acuerdo a las circunstancias que se presenten.

4.1.2 Políticas de seguridad para el canal humano

Las políticas de seguridad aplicadas se detallan a continuación:

Art 6. Solo el personal que tenga autorización ingresa a las zonas restringidas: Data Center, Racks, Estaciones de Trabajo.

Esta política es tomada como medida preventiva pues su fin es evitar que personas, que pueden causar daño a la red interna de la UPEC, ingresen a los lugares restringidos.

Lugares restringidos:

- Data Center
- Racks

- Estaciones de Trabajo.

Medidas preventivas:

- Cerrar bajo llave los lugares restringidos.
- En caso de que accedan personas, un delegado del departamento de TIC’s debe estar presente, a excepción de las estaciones de trabajo de los estudiantes en las cuales un docente está encargado de las actividades que se desarrollen.

Aplicar las medidas:

- Las áreas restringidas se encuentran cerradas bajo llave y existe una persona encargada de estas instancias. A continuación se muestran las instancias cerradas bajo llave:

Imagen 23: Laboratorios cerrados bajo llave
Fuente: Elaboración Propia

- Los estudiantes acceden a los laboratorios con la presencia de un docente encargado, como se puede observar en la imagen 21.

Imagen 24: Estudiantes en laboratorio con un docente encargado
Fuente: Elaboración Propia

Art 7. La seguridad privada debe estar al tanto de las zonas restringidas y de las personas que tienen la autoridad y permiso para acceder.

Este artículo es una medida preventiva, para que los guardias eviten que personas no autorizadas accedan a las zonas restringidas.

Medidas preventivas:

- Denegar acceso a personas no autorizadas.

Aplicar medidas:

- El personal de seguridad tiene conocimiento de las personas que tienen la autoridad para ingresar. En el caso de las estaciones de trabajo de los estudiantes, es decir los laboratorios, el ingeniero a cargo debe solicitar el laboratorio con anterioridad.

Art 8. Para acceder a las estaciones de trabajo de los estudiantes, estos deberán presentar el carnet estudiantil.

El carnet estudiantil es una medida preventiva con la cual se puede identificar a los estudiantes.

Medidas preventivas:

- Los estudiantes deben contar con el carnet estudiantil

Aplicar Medidas:

- Los estudiantes tienen carnet estudiantil y deben presentarlo para acceder a estaciones de trabajo de la biblioteca.

Imagen 25: Carnet Estudiantil UPEC
Fuente: UPEC

Art 9. Se debe confirmar las autorizaciones para acceder a zonas restringidas, con el fin de evitar el acceso indebido.

Medidas Preventivas:

- Confirmar las autorizaciones de acceso

Aplicar Medidas:

- Las autorizaciones de acceso están firmadas y selladas.

Art 10. Para solicitar permiso para acceder a las áreas restringidas se lo debe realizar mediante un oficio dirigido al Director del departamento de TIC's.

Medidas Preventivas:

- Realizar oficio para acceder a las áreas restringidas

Aplicar Medidas:

- Se redactan oficios para acceder a las áreas restringidas.

Art 11. Los permisos deben ser firmados y sellados con el fin de evitar posibles falsificaciones

Medias Preventivas:

- Firmar y sellar Permisos

Aplicar Medidas:

- Los permisos son firmados y sellados. Anexo 23.

Art 12. Se debe llevar registro de las personas que accedan a las áreas restringidas.

Esta medida preventiva se realiza con el objetivo de tener un registro de las personas que ingresan a áreas restringidas.

Medidas Preventivas:

- Llevar registro de personas que acceden a las áreas restringidas.

Aplicar medidas:

- Se lleva registro de las personas que ingresan a las zonas restringidas, estas deben ingresar su nombre, numero de cedula y firma como se muestra en el Anexo 16 y Anexo 17.

Art 13. El sistema de video vigilancia debe estar ubicado estratégicamente, con la finalidad de tener visibles las áreas restringidas y evitar accesos indebidos.

Este artículo es una medida preventiva, para monitorear las áreas restringidas de la UPEC.

Medidas Preventivas:

- Sistema de Video Vigilancia

Aplicar medidas:

- El sistema de video vigilancia ya se encontraba ubicado estratégicamente, por lo cual ya se estaba dando cumplimiento.

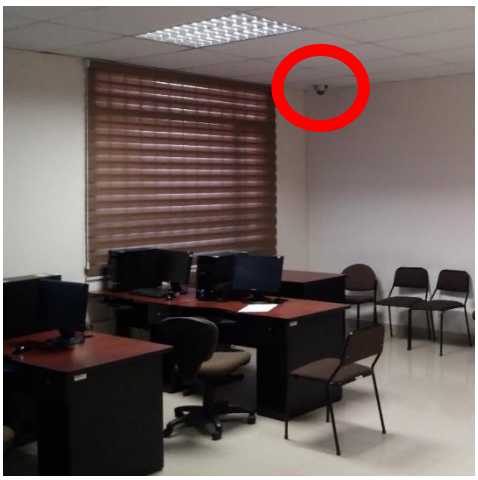


Imagen 26: Cámara ubicada en las estaciones de trabajo de estudiantes

Fuente: Elaboración Propia

Art 15. Bajo ninguna circunstancia se deben tener las contraseñas de acceso a los sistemas de la universidad, pegadas en los monitores o teclados de las estaciones de trabajo del personal administrativo.

Medidas preventivas:

- No pegar contraseñas en ningún lugar de la estación de trabajo

Aplicar medidas:

- No se coloca ninguna contraseña en las estaciones de trabajo pues alguien puede observarla y acceder sin permiso.

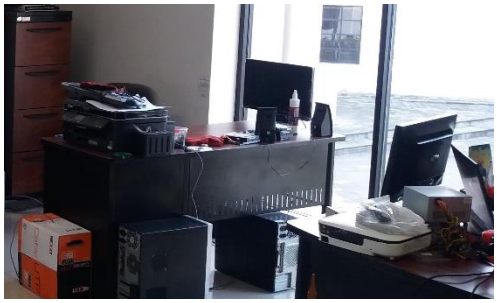


Imagen 27: Estación de Trabajo personal administrativo, sin claves de acceso pegadas
Fuente: Elaboración Propia

4.1.3 Políticas de

Art 17. Los guardias de seguridad deben acercarse a las zonas restringidas al menos 2 veces por día, con el fin de resguardar la integridad de las mismas.

Medidas Preventivas:

- Los guardias deben hacer rondas dos veces por día.

Aplicar Mediadas:

- Los guardias realizan rondas constantemente por todas las instalaciones de la universidad. Esto se evidencia en la imagen:

Imagen 28: Guardias Realizando rondas por la institución
Fuente: Elaboración Propia

Art 20. Resguardar los racks de comunicación con la seguridad de por lo menos una cerradura. Y las llaves deben estar en poder de la persona autorizada para esta tarea.

Medidas preventivas:

- El acceso a los racks debe realizarse mediante cerradura.

Aplicar Medidas:

- Para acceder a los racks se debe tener las llaves de acceso, pues se mantienen bajo puerta cerrada.

Imagen 29: Racks de comunicación bajo llave
Fuente: Elaboración Propia

Art 22. Se debe realizar mantenimiento constante a los activos informáticos de la institución, para que la vida útil de estos sea la óptima.

Medidas Preventivas:

- Realizar mantenimiento a los equipos

Aplicar Medidas:

- Se realiza mantenimiento de los equipos dos veces al año, antes de iniciar cada semestre.

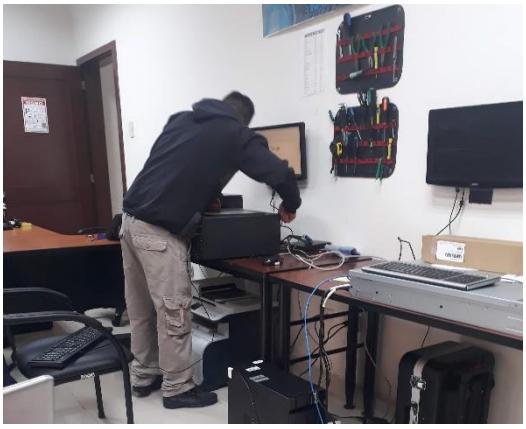


Imagen 30: Personal realizando mantenimiento de equipos informáticos
Fuente: Elaboración Propia

Art 24. El sistema de video vigilancia debe ser monitoreado constantemente, pues de lo contrario no se puede detectar intrusos a tiempo.

Medidas Preventivas:

- Monitorear el sistema de Video Vigilancia

Aplicar Medidas:

El sistema de vigilancia es monitoreado constantemente, no se pudo evidenciar esta medida, debido a que por seguridad no se permitió el acceso.

Art 25. El acceso al Data Center debe ser restringido y solo bajo la debida autorización se podrá acceder.

Medidas Preventivas:

- Solicitar acceso para ingresar al Data Center

Aplicar Medidas:

- Para acceder al Data Center se debe tener autorización. Además esto se puede cumplir debido a que se tiene bloqueado el acceso con tarjeta RFID y claves de acceso.

Imagen 31: Acceso al Data Center con tarjeta RFID y clave

Fuente: Elaboración Propia

Art 32. Todo tipo de reuniones se deben realizar con la puerta cerrada con el fin de que las decisiones tomadas y la información crítica para la institución no puedan ser escuchadas.

Medidas preventivas:

- Realizar reuniones con puerta cerrada.
- Realizar reuniones con cortinas cerradas.

Aplicar medidas:

- Las reuniones se hacen con la puerta cerrada por lo cual no se puede filtrar información.
- Las cortinas se cierran para tener reuniones.

Imagen 32: Oficinas cerradas en reuniones
Fuente: Elaboración Propia

Art 33. Los documentos se deben entregar de forma personal y de ser necesario enviarlos por terceros con sobre cerrado.

Medidas preventivas:

- Entregar documentos de forma personal

Aplicar medidas:

- Los documentos siempre se entregan de forma personal, pues no se cuenta con personal para realizar estos trabajos.

4.1.4 Políticas de seguridad para el canal Inalámbrica

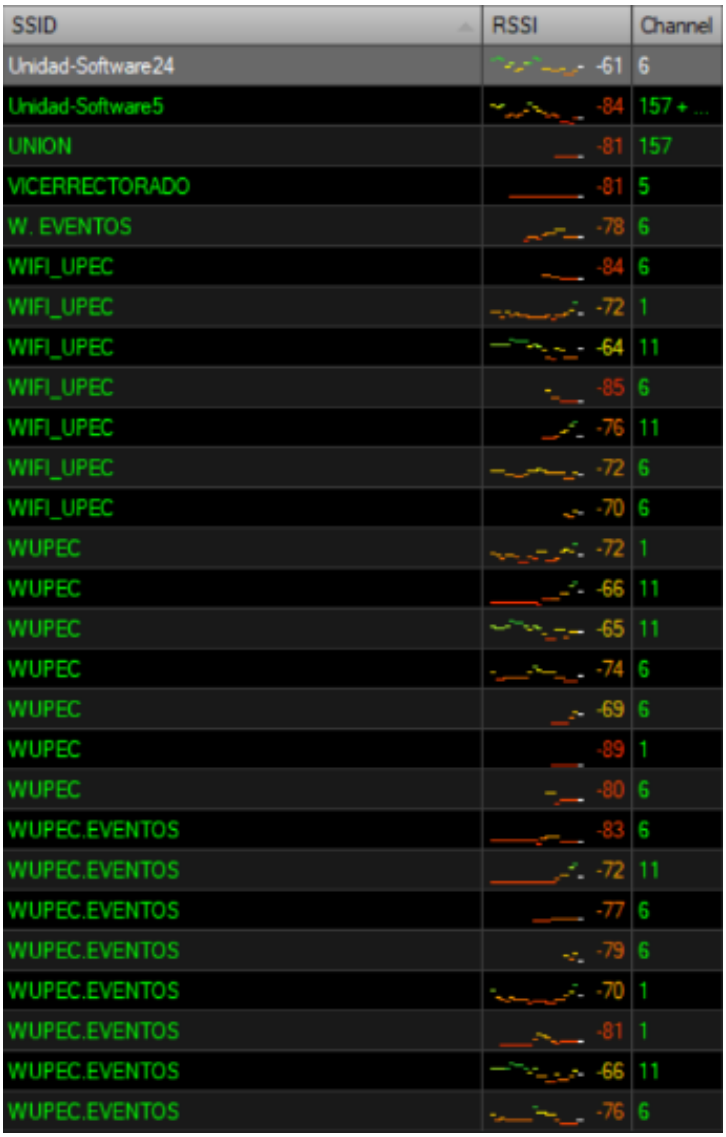
Art 35. Los AP deben configurarse de tal forma que no se interfieran entre sí, con el fin de sacar el máximo rendimiento de los mismos.

Medidas preventivas:

- Configurar AP en canales diferentes

Aplicar Medidas:

- Los AP no se están interfiriendo entre sí, pues se los configuro en canales alejados uno del otro.



SSID	RSSI	Channel
Unidad-Software24	-61	6
Unidad-Software5	-84	157 + ...
UNION	-81	157
VICERRECTORADO	-81	5
W. EVENTOS	-78	6
WIFI_UPEC	-84	6
WIFI_UPEC	-72	1
WIFI_UPEC	-64	11
WIFI_UPEC	-85	6
WIFI_UPEC	-76	11
WIFI_UPEC	-72	6
WIFI_UPEC	-70	6
WUPEC	-72	1
WUPEC	-66	11
WUPEC	-65	11
WUPEC	-74	6
WUPEC	-69	6
WUPEC	-89	1
WUPEC	-80	6
WUPEC.EVENTOS	-83	6
WUPEC.EVENTOS	-72	11
WUPEC.EVENTOS	-77	6
WUPEC.EVENTOS	-79	6
WUPEC.EVENTOS	-70	1
WUPEC.EVENTOS	-81	1
WUPEC.EVENTOS	-66	11
WUPEC.EVENTOS	-76	6

Imagen 33: Redes WIFI UPEC con canales diferentes
Fuente: Elaboración propia

Art 36. Ningún punto de acceso debe tener la configuración que contiene por defecto, pues son más vulnerables a posibles ataques.

Medidas Preventivas:

- No dejar AP con configuración por defecto

Aplicar Medidas:

Todos los AP están configurados, con lo cual no están con las claves por defecto.

SSID	RSSI	Channel	Vendor	Privacy
Unidad-Software24	-61	6		RSNA-CCMP
Unidad-Software5	-84	157 + ...		RSNA-CCMP
UNION	-81	157	Ubiquiti Networks	RSNA-CCMP
VICERRECTORADO	-81	5		RSNA-CCMP
W. EVENTOS	-78	6		RSNA-CCMP
WIFI_UPEC	-84	6		None
WIFI_UPEC	-72	1		None
WIFI_UPEC	-64	11	Cisco Systems	None
WIFI_UPEC	-85	6		None
WIFI_UPEC	-76	11	Cisco Systems	None
WIFI_UPEC	-72	6	Cisco Systems	None
WIFI_UPEC	-70	6		None
WUPEC	-72	1		RSNA-CCMP
WUPEC	-66	11	Cisco Systems	RSNA-CCMP
WUPEC	-65	11	Cisco Systems	RSNA-CCMP
WUPEC	-74	6	Cisco Systems	RSNA-CCMP
WUPEC	-69	6		RSNA-CCMP
WUPEC	-89	1		RSNA-CCMP
WUPEC	-80	6		RSNA-CCMP
WUPEC.EVENTOS	-83	6		RSNA-CCMP
WUPEC.EVENTOS	-72	11	Cisco Systems	RSNA-CCMP
WUPEC.EVENTOS	-77	6		RSNA-CCMP
WUPEC.EVENTOS	-79	6		RSNA-CCMP
WUPEC.EVENTOS	-70	1		RSNA-CCMP
WUPEC.EVENTOS	-81	1		RSNA-CCMP
WUPEC.EVENTOS	-66	11	Cisco Systems	RSNA-CCMP
WUPEC.EVENTOS	-76	6	Cisco Systems	RSNA-CCMP

Imagen 34: AP con claves y nombres diferentes a las predeterminadas

Fuente: Elaboración Propia

Art 37. Las contraseñas deben tener una autenticación y cifrado robustos.

Medidas Preventivas:

- Claves de acceso y cifrado robusto

Aplicar Medidas:

- Las claves son bastante robustas como se muestra a continuación.

MAC Address	SSID	Last Signal	Average Signal	Security Enabled	Connectable	Authentication	Cipher
c8-3a-35-23-4f-90	Docentes-Informatica	25%	25%	Yes	Yes	RSNA-PSK	CCMP
cc-d5-39-9d-8e-23	eduroam	11%	43%	Yes	Yes	RSNA	CCMP
cc-d5-39-9f-15-a3	eduroam	20%	29%	Yes	Yes	RSNA	CCMP
00-3a-99-39-95-33	eduroam	60%	60%	Yes	Yes	RSNA	CCMP
70-10-5c-1f-c9-03	eduroam	57%	41%	Yes	Yes	RSNA	CCMP
cc-d5-39-9f-9f-13	eduroam	46%	66%	Yes	Yes	RSNA	CCMP
cc-d5-39-5c-b8-f3	eduroam	57%	62%	Yes	Yes	RSNA	CCMP
20-3a-07-e0-bc-d3	eduroam	19%	27%	Yes	Yes	RSNA	CCMP
cc-d5-39-9f-a4-63	eduroam	42%	30%	Yes	Yes	RSNA	CCMP
cc-d5-39-9f-a0-83	eduroam	19%	31%	Yes	Yes	RSNA	CCMP
c8-3a-35-52-ab-98	ENGLISH - TEACHERS	13%	13%	Yes	Yes	RSNA-PSK	CCMP
36-de-1a-8c-53-c5	LAPTOP-5O7831FT 8072	35%	35%	Yes	Yes	RSNA-PSK	CCMP
c8-3a-35-52-ab-28	SD_INGLES1	25%	37%	Yes	Yes	WPA-PSK	CCMP
00-0c-42-b9-77-f1	SECMTSUR1	12%	15%	No	Yes	802.11 Open	None
4c-5e-0c-fe-83-01	SurInmaculada	12%	12%	No	Yes	802.11 Open	None
80-2a-a8-22-0c-c0	SWATBELL	13%	13%	No	Yes	802.11 Open	None
60-e3-27-5f-b3-fa	TIC	55%	55%	Yes	Yes	RSNA-PSK	CCMP
1c-3e-84-83-0a-54	Vivis	60%	75%	Yes	Yes	RSNA-PSK	CCMP
cc-d5-39-9f-15-a0	WIFI_UPEC	19%	26%	No	Yes	802.11 Open	None
cc-d5-39-9d-8e-20	WIFI_UPEC	70%	70%	No	Yes	802.11 Open	None
70-10-5c-1f-c9-00	WIFI_UPEC	20%	29%	No	Yes	802.11 Open	None
cc-d5-39-5c-b8-f0	WIFI_UPEC	60%	68%	No	Yes	802.11 Open	None
cc-d5-39-9f-a4-60	WIFI_UPEC	42%	31%	No	Yes	802.11 Open	None
20-3a-07-e0-bc-d0	WIFI_UPEC	46%	46%	No	Yes	802.11 Open	None
cc-d5-39-9f-9f-10	WIFI_UPEC	55%	73%	No	Yes	802.11 Open	None
cc-d5-39-9f-a0-80	WIFI_UPEC	25%	39%	No	Yes	802.11 Open	None
cc-d5-39-9d-8e-21	WUPEC	75%	75%	Yes	Yes	RSNA-PSK	CCMP
70-10-5c-1f-c9-01	WUPEC	20%	20%	Yes	Yes	RSNA-PSK	CCMP
cc-d5-39-9f-15-a1	WUPEC	52%	52%	Yes	Yes	RSNA-PSK	CCMP
00-3a-99-39-95-31	WUPEC	23%	43%	Yes	Yes	RSNA-PSK	CCMP
cc-d5-39-9f-a0-81	WUPEC	39%	35%	Yes	Yes	RSNA-PSK	CCMP
ec-e1-a9-31-3c-00	WUPEC	50%	50%	Yes	Yes	RSNA-PSK	CCMP
cc-d5-39-5c-b8-f1	WUPEC	57%	67%	Yes	Yes	RSNA-PSK	CCMP
20-3a-07-e0-bc-d1	WUPEC	32%	32%	Yes	Yes	RSNA-PSK	CCMP
cc-d5-39-9f-9f-11	WUPEC	90%	76%	Yes	Yes	RSNA-PSK	CCMP
cc-d5-39-9f-a4-61	WUPEC	32%	32%	Yes	Yes	RSNA-PSK	CCMP
cc-d5-39-9f-15-a2	WUPEC.EVENTOS	19%	33%	Yes	Yes	RSNA-PSK	CCMP
cc-d5-39-9d-8e-22	WUPEC.EVENTOS	72%	72%	Yes	Yes	RSNA-PSK	CCMP
00-3a-99-39-95-32	WUPEC.EVENTOS	23%	40%	Yes	Yes	RSNA-PSK	CCMP

Imagen 35: Redes WIFI UPEC
Fuente: Elaboración Propia

4.1.5 Políticas de Seguridad para el canal Telecomunicaciones

Art 43. El acceso a la telefonía IP se debe hacer mediante extensiones con contraseñas personalizadas para cada usuario.

Medidas Preventivas:

- Extensiones deben tener contraseña

Aplicar Medidas:

- Todos los usuarios tienen sus claves personalizadas.

Imagen 36: Extensión con clave de acceso

Fuente: Elastix UPEC

Art 44. El buzón de voz debe tener contraseñas personalizadas para cada usuario de la institución.

Medidas preventivas:

- Colocar contraseña al buzón de voz.

Aplicar medidas:

- El buzón de voz tiene claves para cada usuario, por lo que no es posible acceder a los mensajes sin la clave de acceso.

Art 37. El servicio de telefonía ip debe estar en una Vlan independiente en la cual se aplique QoS

Medidas Preventivas:

- Tener Vlan para voz.

Aplicar medidas:

- Existe una Vlan específica para la telefonía ip, en la cual esta aplicado calidad de servicio para la voz.

Art 38. Los tonos táctiles de los teléfonos ip deben ser desactivados, pues con estos tonos se puede descifrar la contraseña del usuario.

Medidas Preventivas:

- Desactivar tonos táctiles teléfonos IP

Aplicar Medidas:

- Se desactivo los tonos táctiles de todos los teléfonos IP.

4.1.6 Políticas de Seguridad para el canal Redes de Datos

Art 48. Se deben bloquear las respuestas de ICMP de los servidores de la institución, con la finalidad de evitar ataques usando el PING.

Medidas preventivas:

- Bloquear respuestas ICMP de los servidores.

Aplicar Medidas:

- Se bloquearon las respuestas ICMP en los servidores, evitando posibles ataques en la red.

Art 49. Se deben tener abiertos los puertos que se estén utilizando en el firewall pues si se dejan abiertos puertos innecesarios se pueden abrir puertas que generen ataques.

Medidas preventivas:

- Cerrar puerto no usados

Aplicar Medidas:

- Solo los puertos utilizados se encuentran abiertos para de esta manera cerrar posibles puertas traseras.

Art 50. Para crear cuentas de correo electrónico, portafolio, estudiantil, docente y administrativo; se debe ser parte de la institución.

Medidas Preventivas:

Solo se debe crear cuentas de correo y portafolio a los miembros de la UPEC.

Aplicar Medidas:

- Las cuentas se crean solo al personal que está vinculado con la instituciones, ya sea como empleado o estudiante.

Art 51. Las contraseñas de acceso deben ser robustas con el fin de evitar posibles vulneraciones de la seguridad.

Medidas Preventivas:

- Las claves de acceso deben ser robustas

Aplicar medidas:

- Las claves de acceso tienen como requisito usar números, letras y al menos un carácter especial.

CONCLUSIONES

- Una Institución de Educación Superior debe tener una buena seguridad en la red interna sin embargo la UPEC al tener una red relativamente nueva posee debilidades en los 5 canales que se evaluó en la auditoria. Esto implica que la universidad es vulnerable a sufrir ataques tanto lógicos como físicos. El canal que presento mayor vulnerabilidad fue el canal físico pues las barreras que tiene la universidad para proteger los activos son insuficientes y son propensos a ser sustraídos generando pérdidas económicas para la Institución.
- Con la fundamentación bibliográfica se conoció que OSSTMMv3 permite analizar a profundidad la seguridad de la Institución, pues divide el análisis en 5 canales, con lo cual se evalúa la seguridad de cada área por separado, permitiendo conocer resultados puntales de los canales que requieren mayor atención, dando la oportunidad de tomar las medidas más urgentes en primer lugar. Además, permite saber si los controles que se encuentran aplicados son los suficientes para garantizar la integridad de la información y no comprometan la seguridad de la red interna de la UPEC.
- El análisis de la situación actual de la institución se realizó mediante técnicas de observación y persuasión, con lo cual se pudo conocer la estructura de la red interna de la UPEC, la distribución de sus activos, y una vista previa de las falencias más importantes y evidentes de la Universidad, además, fue muy importante como antecedente de la auditoria pues se detalla el estado actual y la seguridad que se maneja en el Data Center, Racks y estaciones de trabajo.

- La auditoría realizada sirve de base para futuras auditorias, pues deja sentados los pasos a seguir para analizar la seguridad de cada canal de la institución, además de herramientas con las cuales se pueden examinar posibles vulnerabilidades en la red.
- Se realizó un informe final con los resultados de la auditoria, el mismo que fue entregado y socializado con los miembros del departamento de TIC's, esto para que el personal que está a cargo de la seguridad de la red interna de la Institución estén informados de las vulnerabilidades encontradas después de realizar la auditoría.
- Las políticas de seguridad se realizaron en base la norma ISO/IEC 27001, y con ellas se podrá mejorar el entorno de seguridad de la universidad, pues abordan las falencias que se encontraron en la red interna, asimismo, sirven para que el personal del departamento de TIC's, por medio de los procesos de seguridad, tengan una guía para abordar los problemas que se presenten; por ese motivo fueron entregadas y socializadas con los miembros del departamento.
- Las políticas fueron aplicadas en un entorno de prueba, con la finalidad de evaluar su funcionamiento y acogida por parte de la institución, para esto se realizó un checklist en el cual se especifica si están siendo cumplidas y si pueden ser eludidas por parte del personal interno de la Universidad.

RECOMENDACIONES

- Se debe prestar especial atención a la seguridad del canal físico de la UPEC, pues es el canal que presentó mayores falencias y compromete la seguridad física de los activos e información de la institución.
- Se recomienda realizar el análisis de la situación actual de la institución al menos dos veces por año, pues su red está cambiando y deben tener clara la estructura de la red interna de la institución y de esta manera poder aplicar los controles necesarios para garantizar sus seguridad.
- Dentro del departamento de TIC´s debería existir una persona encargada netamente de la seguridad informática de la institución y que este pendiente constantemente de las vulnerabilidades que puedan presentarse y de ser necesario aplicar una auditoria dos veces al año.
- El personal del departamento de TIC's debe hacer un análisis periódico de la seguridad informática de la institución y deberán acoger las políticas de seguridad propuestas, pues de esto depende la seguridad de la información que se maneja.
- Las políticas de seguridad deben ser revisadas una vez al año y de ser necesario modificarlas, pues la red interna de la institución se está mejorando y con estas mejoras pueden existir nuevas vulnerabilidades.
- Aunque por falta de recursos económicos no fue posible aplicar todas las políticas de seguridad, la Institución debe designar un presupuesto para que las políticas se implementen en su totalidad y puedan mejorar su seguridad.

- El personal del departamento de TIC´s debe ser capacitado para manejar la seguridad pues la tecnología es cambiante y probablemente en el futuro las mejoras realizadas no serán suficientes.

BIBLIOGRAFÍA

Aguilera, P. (2010). Seguridad Informática. EDITEX.

Allen Harper, J. N. (2015). GRAY HAT HACKING.

Asamblea Nacional de la República del Ecuador. (10 de 02 del 2014). *Código Orgánico Integral Penal*. Retrieved from https://www.justicia.gob.ec/wp-content/uploads/2014/05/c%C3%B3digo_org%C3%A1nico_integral_penal_-_coip_ed._sdn-mjdhc.pdf

Baca Urbina, G. (2016). *Introducción a la seguridad informática*. Distrito Federal, UNKNOWN: Grupo Editorial Patria.

Baudes, G. (2002). Auditoría Informática.

Catoira, F. (2013). Aprendiendo a escanear puertos. Recuperado de: https://www.welivesecurity.com/la-es/2013/11/07/aprendiendo-escanear-puertos-udp/

Congreso Nacional del Ecuador. (28 de 12 de 2006). *Ley de propiedad Intelectual*. Recuperado de: https://www.correosdelecuador.gob.ec/wp-content/uploads/downloads/2015/05/LEY_DE_PROPIEDAD_INTELECTUAL.pdf

Costas, J. (2010). Seguridad Informática. RA-MA S.A.

Chicano, E. (2015). Auditoría de seguridad informática. IFCT0109

Descentralizado de Santa Ana de Cotacachi, basada en la norma NTP-ISO/IEC 17799:2007 y la metodología OSSTMMv2. Universidad Técnica del Norte, Ibarra.

Escrivá Gascó, G., Romero Serrano, R. M., & Ramada, D. J. (2013). *Seguridad informática*. Madrid, ES: Macmillan Iberia, S.A.

Gómez, L. (2012). Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. AENOR

Jaramillo, D. (2 014) Auditoría de seguridad informática para el Gobierno Autónomo

Katz, M. (2013). *Redes y Seguridad*. Buenos Aires: Alfaomega.

Herzog, P. (2010). OSSTMM 3. Manual de la Metodología Abierta de Testeo de Seguridad. In. New York: ISECOM.

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, (17 de 04 del 2002).

Ley Orgánica de Transparencia y Acceso a la Información Pública, (18 de 05 del 2004).

OPENTESTING. (2010). Liberado OSSTMM3. Open Source, Pentesting y Seguridad Informática. https://opentesting.wordpress.com/2010/12/31/liberado-osstmm-3/

Posso, M. (2013). Proyectos, tesis y marco lógico (Noción Ed. Primera ed.). Quito

Piattini, M.; Navarro, E.; Ruiz, M. (2011). Auditoría de tecnologías y sistemas de información. (Alfaomega Ra-Ma Ed. Primera ed.). Madrid.

Racciati, H. (2013). Tiempos de Cambio: OSSTMM 3-Una Introducción. OSSTMM Stallings, W. (2004). Fundamentos de seguridad en redes. PEARSON EDUCATION.

Sanchez, J. (2011). Sistemas y mecanismos de protección. Recuperado de: http://eleclibre.blogspot.com/

Universidad Politécnica Estatal del Carchi. (2005). Misión y Visión UPEC. In.

GLOSARIO DE TÉRMINOS

- **Acceso:** Resultado de una autenticación correcta
- **Activo:** Componente de una empresa que debe ser protegido.
- **Alcance:** El ambiente en el cual se producen interacciones con los activos.
- **Amenaza:** Situación que tienen el potencial para causar daño o perdida de la información.
- **Anomalía:** Actividades que no se encuentran dentro de las operaciones normales de la institución.
- **Ataque:** Actividades que tienen como objetivo quebrantar la seguridad del sistema para obtener información confidencial de la empresa.
- **Auditoría:** Inspección que se lleva a cabo siguiendo una determinada metodología para detectar las fallas de la empresa.
- **Autenticación:** Proceso para comprobar la identidad de los usuarios y activos informáticos.
- **Confianza:** Interacción que no requiere de autenticación entre dos o más usuarios,
- **Disponibilidad:** Característica de un sistema que es accesible y tiene un correcto funcionamiento.
- **Hacker:** Persona que tiene conocimientos para evadir la seguridad de una empresa y acceder a su información.
- **Ingeniería Social:** Técnicas usadas para conseguir información clasificada del personal de una empresa.
- **ISECOM:** Instituto de Seguridad y Metodologías Abiertas.
- **VPN:** Red privada virtual, se usa para conectar varias redes locales por internet.

ACRÓNIMOS

- **ANSI:** Instituto Nacional Estadounidense de Estándares.
- **AP:** Access Point.
- **ARP:** Protocolo de resolución de direcciones.
- **CSR:** Solicitud de firma de certificado.
- **HTTP:** Protocolo de transferencia de hipertexto.
- **HTTPS:** Protocolo seguro de transferencia de hipertexto.
- **ICMP:** Protocolo de mensajes de control de internet.
- **ISO:** Organización Internacional de Normalización.
- **LAN:** Red de área local.
- **MAC:** Control de acceso al medio.
- **RAS:** Servicios de acceso remoto.
- **SSID:** Nombre de Red Inalámbrica.
- **TIA:** Asociación de industrias de telecomunicaciones.
- **UPEC:** Universidad Politécnica Estatal del Carchi.
- **VPN:** Red privada virtual.

ANEXOS

Anexo 1: Datasheet del Switch de Core 4506e

Data Sheet

Cisco Catalyst 4500 Series Switch

Overview

The Cisco® Catalyst® 4500 Series Switches enable Borderless Networks, providing high performance, mobile, and secure user experiences through Layer 2-4 switching investments. They enable security, mobility, application performance, video, and energy savings over an infrastructure that supports resiliency, virtualization, and automation. Cisco Catalyst 4500 Series Switches provide borderless performance, scalability, and services with reduced total cost of ownership (TCO) and superior investment protection.

The Cisco Catalyst 4500 (Figure 1) has a centralized forwarding architecture that enables collaboration, virtualization, and operational manageability through simplified operations. With forward and backward compatibility spanning multiple generations, the new Cisco Catalyst 4500E Series provides exceptional investment protection and deployment flexibility to meet the evolving needs of organizations of all sizes. The Cisco Catalyst 4500E Series platform has 10 Gigabit Ethernet (GE) uplinks and supports Power over Ethernet Plus (PoE+) and Universal PoE (UPOE), enabling customers to future proof their network.

E-Series chassis come in four different form factors: 3-slot (4503-E), 6-slot (4506-E), 7-slot (4507R+E), and 10-slot (4510R+E). 4503-E, 4506-E, 4507R+E, and 4510R+E chassis are extremely flexible and support either 24 or 48 Gbps per line-card slot. Integrated resiliency in the Cisco Catalyst 4500E Series includes 1 + 1 supervisor engine redundancy (10-slot and 7-slot chassis only), redundant fans, software-based fault tolerance, and 1 + 1 power supply redundancy. Integrated resiliency in both hardware and software minimizes network downtime, helping to ensure workforce productivity, profitability, and customer success.

Figure 1. Cisco Catalyst 4500E Series

Cisco Catalyst 4503-E Cisco Catalyst 4507R+E Cisco Catalyst 4510R+E Cisco Catalyst 4506-E

The Cisco Catalyst 4500E Series extends control to the network edge with intelligent network services, including sophisticated quality of service (QoS), predictable performance, advanced security, comprehensive management, and integrated resiliency. Scalability of these intelligent network services is made possible with dedicated, specialized resources known as ternary content-addressable memory (TCAM). Ample TCAM resources (up to 384,000 entries) enable "high feature capacity", which provides wire-speed routing and switching performance independent of provisioning of services such as QoS and security.

Cisco Catalyst 4500E Series Chassis

The Cisco Catalyst 4500E Series offers four chassis options and four supervisor engine options (Table 1). It provides a common architecture that can scale up to 388 ports. The Cisco Catalyst redundant R+E chassis offer high availability by supporting 1 + 1 redundant supervisor engines with subsecond failover time and full-image In-Service Software Upgrades (ISSUs). Nonstop forwarding with stateful switchover (NSF/SSO) and ISSU help ensure continuous packet forwarding during supervisor engine switchover to help ensure high availability for collaboration applications and voice over IP (VoIP). Using the same line cards as the widely deployed Cisco Catalyst 4000 Series Switches and classic Cisco Catalyst 4500 Series Switches, the Cisco Catalyst 4500E Series furthers Cisco's commitment to affordable enterprise and branch-office scalability.

Table 1. Cisco Catalyst 4500E Series Chassis Features

Feature	Cisco Catalyst WS-C4503-E Chassis	Cisco Catalyst WS C4506-E Chassis	Cisco Catalyst WS C4507R+E Chassis	Cisco Catalyst WS C4510R+E Chassis
Total number of slots	3	6	7	10
Line-card slots	2	5	5	8
Supervisor engine slots	1[1]	1[1]	2[2]	2[2]
Dedicated supervisor engine slot numbers	1	1	3 and 4	5 and 6
Supervisor engine redundancy	No	No	Yes	Yes Supervisor Engines V-10GE, 6-E, 7-E, and 8-E)
Supervisor engines supported	Supervisor Engines 8-E, 8L-E, 7-E, 7L-E, 6-E, and 6L-E	Supervisor Engines 8-E, 8L-E, 7-E, 7L-, 6-E, and 6L-E	Supervisor Engines 8-E, 8L-E, 7-E, 7L-E, 6-E, and 6L-E	Supervisor Engines 8-E, 7-E, and 6-E[4]
Maximum PoE per slot	1500W	1500W	1500W	1500W slots 1 and 2; 750W slots 3, 4, and 7-10
Bandwidth scalability per line-card slot	Up to 48 Gbps on all slots	Up to 48 Gbps on all slots	Up to 48 Gbps on all slots[5]	Up to 48 Gbps on all slots[5]
Number of power supply bays	2	2	2	2
AC input power	Yes	Yes	Yes	Yes
DC input power	Yes	Yes	Yes	Yes
Integrated PoE	Yes	Yes	Yes	Yes
Minimum number of power supplies	1	1	1	1
Power supplies supported	• 1000W AC • 1400W AC • 1300W ACV • 2800W ACV • 4200W ACV • 6000W ACV • 9000W ACV • 1400W DC (triple input) • 1400W-DC-P	• 1000W AC • 1400W AC • 1300W ACV • 2800W ACV • 4200W ACV • 6000W ACV • 9000W ACV • 1400W DC (triple input) • 1400W-DC-P	• 1000W AC • 1400W AC • 1300W ACV • 2800W ACV • 4200W ACV • 6000W ACV • 9000W ACV • 1400W DC (triple input) • 1400W-DC-P	• 1400W AC • 2800W ACV • 4200W ACV • 6000W ACV • 9000W ACV • 1400W DC (triple input) • 1400W-DC-P
Number of fan-tray bays	1	1	1	1
Location of 19-inch rack-mount	Front	Front	Front	Front
Location of 23-inch rack-mount	Front (option)	Front (option)	Front (option)	Front (option)

[1] Slot 1 is reserved for supervisor engine only; slots 2 and higher are reserved for line cards.

[2] Slots 3 and 4 are reserved for supervisor engines only in Cisco Catalyst 4507R+E; slots 1-2 and 5-7 are reserved for line cards.

Anexo 2: Datasheet del CISCO ASA 5520

Data Sheet

Cisco ASA 5500 Series Adaptive Security Appliances

Cisco® ASA 5500 Series Adaptive Security Appliances deliver a robust suite of highly integrated, market-leading security services for small and medium-sized businesses (SMBs), enterprises, and service providers—in addition to providing unprecedented services flexibility, modular scalability, feature extensibility, and lower deployment and operations costs.

Cisco ASA 5500 Series Adaptive Security Appliances are purpose-built solutions that integrate world-class firewall, unified communications security, VPN, intrusion prevention (IPS), and content security services in a unified platform. The series builds upon proven technologies from Cisco PIX® 500 Series Security Appliances, Cisco IPS 4200 Series Sensors, and Cisco VPN 3000 Series Concentrators.

Cisco ASA 5500 Series Adaptive Security Appliances are a key component of the Cisco Self-Defending Network. The Cisco ASA 5500 Series provides intelligent threat defense that stops attacks before they penetrate the network perimeter, controls network and application activity, and delivers secure remote access and site-to-site connectivity. The result is a powerful multifunction network security appliance family that provides security breadth, precision, and depth for protecting business networks of all sizes, while reducing the overall deployment and operations costs associated with implementing comprehensive multilayer security.

Figure 1. Cisco ASA 5500 Series Adaptive Security Appliances

The Cisco ASA 5500 Series helps businesses increase effectiveness and efficiency in protecting their networks and applications, while delivering exceptional investment protection through the following elements:

- **Market-proven security capabilities**—The Cisco ASA 5500 Series integrates multiple full-featured, high-performance security services, including application-aware firewall, SSL and IPsec VPN, IPS, antivirus, antispam, antiphishing, and web filtering services. These technologies deliver strong network- and application-layer security, user-based access control, worm mitigation, malware protection, improved employee productivity, instant messaging and peer-to-peer control, and secure remote user and site connectivity.

- **Extensible integrated services architecture**—The Cisco ASA 5500 Series offers businesses strong, adaptive protection from the fast-evolving threat environment through its unique combination of hardware and software extensibility and its powerful Modular Policy Framework (MPF). The innovative extensible multiprocessor design and software architecture of the Cisco ASA 5500 Series enables businesses to easily install additional high-performance security services through security services modules (SSMs) and security services cards (SSCs). This provides businesses with outstanding investment protection, while enabling them to expand the security services profile of their Cisco ASA 5500 Series, as their security and performance needs grow. All these services are easily managed through the powerful Cisco Modular Policy Framework, which allows businesses to create highly customized security policies while making it simple to add new security and networking services into their existing policies.
- **Reduced deployment and operations costs**—The Cisco ASA 5500 Series enables standardization on a single platform to reduce the overall operational cost of security. A common environment for configuration simplifies management and reduces training costs for staff, while the common hardware platform of the series reduces sparing costs. Additional efficiencies are realized by deploying integrated capabilities, obviating the need for the complex designs required to connect standalone solutions.
- **Comprehensive management interfaces**—The graphical Cisco Adaptive Security Device Manager (ASDM), a comprehensive command line interface (CLI), verbose syslog, and Simple Network Management Protocol (SNMP) support round out a rich complement of management options. Multi-unit deployments benefit greatly from Cisco Security Manager, a platform capable of managing distributed deployments of 5 to 5000 devices. The award-winning Cisco Security Monitoring, Analysis, and Response System (Cisco Security MARS) recognizes and correlates real network attacks and then rapidly defines how to stop them, thereby decreasing administrative overhead by reducing false positives and simplifying audit compliance.

The Cisco ASA 5500 Series

The Cisco ASA 5500 Series includes the Cisco ASA 5505, 5510, 5520, 5540, 5550, and 5580 Adaptive Security Appliances—purpose-built, high-performance security solutions that take advantage of Cisco's expertise in developing industry-leading, award-winning security and VPN solutions. Through the Cisco MPF, the Cisco ASA 5500 Series brings a new level of security and policy control to applications and networks. MPF enables highly customizable, flow-specific security policies that have been tailored to application requirements. The performance and extensibility of the Cisco ASA 5500 Series are enhanced through user-installable SSMs. This adaptable architecture enables businesses to rapidly deploy security services when and where they are needed, such as tailoring inspection techniques to specific application and user needs or adding additional intrusion prevention and content security services such as those delivered by the Adaptive Inspection and Prevention (AIP) and Content Security and Control (CSC) SSMs. Furthermore, the modular hardware architecture of the Cisco ASA 5500 Series, along with the powerful MPF, provides the flexibility to meet future network and security requirements, extending the outstanding investment protection provided by the Cisco ASA 5500 Series, and allowing businesses to adapt their network defenses to new threats as they arise.

Anexo 3: Datasheet del Switch Cisco 2960

Data Sheet

Cisco Catalyst 2960-S Series Switches

Product Overview

The Cisco® Catalyst® 2960-S Series Switches are fixed-configuration Gigabit Ethernet switches (Figure 1) that provide enterprise-class Layer 2 switching for campus and branch access applications. They enable reliable and secure business operations with lower total cost of ownership through a range of innovative features including FlexStack, Power over Ethernet Plus (PoE+), and Cisco Catalyst SmartOperations.

Figure 1. Cisco Catalyst 2960-S Series Switches

Product Highlights

Cisco Catalyst 2960-S switches feature:

- 24 or 48 Gigabit Ethernet ports
- 1G Small Form-Factor Pluggable (SFP) or 1G/10G SFP+ slots
- Cisco FlexStack stacking with 20 Gbps of stack throughput (optional)
- IEEE 802.3at-compliant PoE+ for up to 30W of power per port
- Up to 740W of combined PoE/PoE+ budget
- USB interfaces for management and file transfers
- LAN Base or LAN Lite Cisco IOS® Software feature set
- SmartOperations tools that simplify deployment and reduce the cost of network administration
- An enhanced limited lifetime hardware warranty (E-LLW), providing next-business-day replacement

Applications and Benefits

The Cisco Catalyst 2960-S Series is ideal for:

- Deploying cost-effective wired connectivity in traditional desktop workspace environments
- Implementing quality of service (QoS) to provide priority treatment of voice and critical business applications
- Enforcing basic security policies to limit access to the network and mitigate threats
- Reducing total cost of ownership through simplified operations and automation

Switch Configurations

Table 1. Cisco Catalyst 2960-S Series Switches Configurations

Model	10/100/1000 Ethernet Interfaces	Uplink Interfaces	Cisco IOS Software Feature Set	Available PoE Power	FlexStack Stacking
Cisco Catalyst 2960S-48FPD-L	48	2 SFP+	LAN Base	740W	Optional
Cisco Catalyst 2960S-48LPD-L	48	2 SFP+	LAN Base	370W	Optional
Cisco Catalyst 2960S-24PD-L	24	2 SFP+	LAN Base	370W	Optional
Cisco Catalyst 2960S-48TD-L	48	2 SFP+	LAN Base	-	Optional
Cisco Catalyst 2960S-24TD-L	24	2 SFP+	LAN Base	-	Optional
Cisco Catalyst 2960S-48FPS-L	48	4 SFP	LAN Base	740W	Optional
Cisco Catalyst 2960S-48LPS-L	48	4 SFP	LAN Base	370W	Optional
Cisco Catalyst 2960S-24PS-L	24	4 SFP	LAN Base	370W	Optional
Cisco Catalyst 2960S-48TS-L	48	4 SFP	LAN Base	-	Optional
Cisco Catalyst 2960S-24TS-L	24	4 SFP	LAN Base	-	Optional
Cisco Catalyst 2960S-48TS-S	48	2 SFP	LAN Lite	-	No
Cisco Catalyst 2960S-24TS-S	24	2 SFP	LAN Lite	-	No

Cisco FlexStack

Cisco FlexStack provides stacking of up to four 2960-S switches through an optional module (Figure 2).

The FlexStack stack module is hot-swappable and can be added to any Cisco Catalyst 2960-S switch with LAN Base software. Switches connected to a stack will automatically upgrade to the stack's Cisco IOS Software version and transparently join the stack without additional intervention.

Cisco FlexStack and Cisco IOS Software provide true stacking, with all switches in a stack acting as a single switch unit. FlexStack provides a unified data plane, unified configuration, and single IP address for switch management. The advantages of true stacking include lower total cost of ownership and higher availability through simplified management and cross-stack features including EtherChannel, SPAN, and FlexLink. Note that cross-stack features must be disabled before removing the stack module from an active stack member switch.

FlexStack also allows mixed stacking: 2960-S and 2960-SF switches can be combined to provide a combination of Gigabit and Fast Ethernet ports in a single switch stack.

Figure 2. Cisco FlexStack Switch Stack

Power over Ethernet Plus - PoE+

Cisco Catalyst 2960-S switches support both IEEE 802.3af Power over Ethernet (PoE) and IEEE 802.3at PoE+ (up to 30W per port) to deliver lower total cost of ownership for deployments that incorporate Cisco IP phones, Cisco

Anexo 4: Datasheet del WLC Cisco 2500

Data Sheet

Cisco 2500 Series Wireless Controllers

Small to Medium-Sized Enterprise and Branch Office Controller

- Support for up to 75 access points and 1000 clients.
- 802.11n and 802.11ac ready support up to 1 Gbps.
- Payment Card Industry (PCI) support enables certification for scanner and kiosk deployments.

Licensing Flexibility and Investment Protection

- Additional access point licenses may be added over time.

Comprehensive Security

- Full Control and Provisioning of Wireless Access Points (CAPWAP) access point to controller encryption.
- Supports rogue access point detection and detection of denial-of-service attacks.
- Management frame protection detects malicious users and alerts network administrators.

Cisco CleanAir® Technology

- Detects, classifies, locates, and mitigates RF interference to provide performance protection for 802.11n and 802.11ac networks.

Cisco OfficeExtend Solution

- Secure, simple, cost-effective mobile teleworker solution.

Product Overview

The Cisco® 2500 Series Wireless Controller enables systemwide wireless functions in small to medium-sized enterprises and branch offices. Designed for 802.11n and 802.11ac performance, Cisco 2500 Series Wireless Controllers are entry-level controllers that provide real-time communications between Cisco Aironet® access points to simplify the deployment and operation of wireless networks (Figure 1).

Figure 1. Cisco 2500 Series Wireless Controller

As a component of the Cisco Unified Wireless Network, this controller delivers centralized security policies, wireless intrusion prevention system (wIPS) capabilities, award-winning RF management, and quality of service (QoS) for voice and video. Delivering 802.11ac performance and scalability, the Cisco 2500 Series provides low total cost of ownership and flexibility to scale as network requirements grow.

The Cisco 2504 Wireless Controller supports Cisco Application Visibility and Control (AVC), the technology that includes Cisco's Network-Based Application Recognition 2 (NBAR-2) engine. N-BAR-2 does deep packet inspection (DPI) to classify applications and tie into quality of service (QoS) to either drop or mark the traffic, thereby prioritizing business-critical applications in the network. Cisco AVC uses NetFlow Version 9 to export the flows to Cisco Prime™ Infrastructure or a third-party NetFlow Collector. The Cisco 2504 Wireless Controller also supports Bonjour Services Directory, which enables Bonjour (Apple) Services to be advertised and utilized in a separate Layer 3 network. Wireless Policy engine is a wireless profiler and policy feature on the Cisco 2500 Series Wireless Controller that enables profiling of wireless devices and enforcement of policies such as VLAN assignment, QoS, ACL, and time-of-day-based access.

Cisco 2500 Series Wireless Controller-based access point licensing offers flexibility with 5, 15, 25, or 50 access points. Additional access point support can be added in increments of 1, 5, or 25.

Table 1 lists the features and benefits of the Cisco 2500 Series Wireless Controllers.

Table 1. Cisco 2500 Series Wireless Controller Features and Benefits

Feature	Benefits
Scalability	• Supports up to 75 access points • Supports up to 1000 clients
Ease of Deployment	• For quick and easy deployment Access Points can be connected directly to 2504 Wireless LAN Controller via two PoE (Power over Ethernet) ports
High Performance	• Wired-network speed and nonblocking performance for 802.11n and 802.11ac networks. Supports up to 1 Gbps throughput
RF Management	• Provides both real-time and historical information about RF interference impacting network performance across controllers, via systemwide Cisco CleanAir® technology integration
Comprehensive End-to-End Security	• Offers CAPWAP-compliant Datagram Transport Layer Security (DTLS) encryption to help ensure full-line-rate encryption between access points and controllers across remote WAN/LAN links
End-to-end Voice	• Supports Unified Communications for improved collaboration through messaging, presence, and conferencing • Supports all Cisco Unified Wireless IP Phones for cost-effective, real-time voice services
High-Performance Video	• Integrates Cisco VideoStream technology as part of the Cisco medianet framework to optimize the delivery of video applications across the WLAN
PCI Integration	• Part of Payment Card Industry (PCI) certified architecture, and are well-suited for retail customers who deploy transactional data applications such as scanners and kiosks
OfficeExtend	• Supports corporate wireless service for mobile and remote workers with secure wired tunnels to the Cisco Aironet® 600, 1130, 1140 or 3500 Series Access Points • Extends the corporate network to remote locations with minimal setup and maintenance requirements • Improves productivity and collaboration at remote site locations • Separate service set identifier (SSID) tunnels allow both corporate and personal Internet access • Reduced carbon dioxide emissions from a decrease in commuting • Higher employee job satisfaction from ability to work at home • Improves business resiliency by providing continuous, secure connectivity in the event of disasters, pandemics, or inclement weather
Enterprise Wireless Mesh	• Allows access points to dynamically establish wireless connections without the need for a physical connection to the wired network • Available on select Cisco Aironet access points, Enterprise Wireless Mesh is ideal for warehouses, manufacturing floors, shopping centers, and any other location where extending a wired connection may prove difficult or aesthetically unappealing
Environmentally Responsible	• Organizations may choose to turn off access point radios to reduce power consumption during off-peak hours
Mobility, Security and Management for IPv6 & Dual-Stack Clients	• Secure, reliable wireless connectivity and consistent end-user experience • Increased network availability by proactive blocking of known threats • Equips administrators for IPv6 troubleshooting, planning, client traceability from a common wired and wireless management system
Guest Anchor and Wired Guest Access	• Supports up to 15 guest anchor Ethernet over IP (EoIP) tunnels for path isolation of guest traffic from enterprise data traffic • Extends the guest access services to the wired clients on par with other WLAN Controllers

Product Specifications

Table 2 lists the product specification for Cisco 2500 Series Wireless Controllers.

Table 2. Product Specifications for the Cisco 2500 Wireless Controller

Item	Specification
Wireless Standards	IEEE 802.11a, 802.11ac, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, 802.11k, 802.11n, 802.11r, 802.11u, 802.11w, 802.11ac
Wired/Switching/Routing	IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX specification, 1000BASE-T, and IEEE 802.1Q VLAN tagging

Anexo 5: Datasheet TL-WR940N

TP-LINK®

450Mbps Wireless N Router

TL-WR940N

Features:

- Wireless N speed up to 450Mbps makes it ideal for bandwidth consuming or interruption sensitive applications like video streaming, online gaming and VoIP
- Wireless On/Off Button allows users to simply turn their wireless radio on or off
- Easily setup a WPA encrypted secure connection at a push of the WPS button
- WDS wireless bridge provides seamless bridging to expand your wireless network
- IP based bandwidth control allows administrators to determ in how much bandwidth is allotted to each PC
- Parental control allows parents or administrators to establish restricted access policies for children or staff
- Supports virtual server, special application and DMZ host ideal for creating a website within your LAN
- Offers Auto-mail function for system log, convenient for managing the router
- Backward compatible with 802.11b/g products
- Easy Setup Assistant provides quick & hassle free installation
- Sleek exterior, can be mounted on a wall or placed horizontally on a table or desk

Description:

The TL-WR940N Wireless N Router is a combined wired/wireless network connection device designed specifically for small business, office and home networking requirements. It provides a simple, very fast, pleasing way to access internet or Ethernet without cables for work or fun. It complies with the IEEE 802.11n (Draft 2.0) standard with wireless transmission speeds of up to 450Mbps. The router features 4 10/100M switch ports to achieve the most effective data transmission. TL-WR940N adopts MIMO as well as SST™ technologies, has three external fixed Omni directional antennas providing even better wireless performance, transmission rates, stability and coverage. TL-WR940N also provides a Wireless On/Off button that allows users to easily turn on/off the router's wireless radio whenever necessary.

450Mbps Wireless N Router TL-WR940N

Specifications:

HARDWARE FEATURES	
Interface	4 10/100Mbps LAN Ports 1 10/100Mbps WAN Port
Button	Wireless On/Off Button, WPS/Reset Button, Power On/Off Button
External Power Supply	12V / 1A
Wireless Standards	IEEE 802.11n, IEEE 802.11g, IEEE 802.11b
Antenna	3 * 5dBi Fixed Omni Directional Antenna
Dimensions (W x D x H)	7.9 x 5.5 x 1.2 in. (200 x 140 x 28mm)
WIRELESS FEATURES	
Frequency	2.4-2.4835GHz
Signal Rate	11n: Up to 450Mbps(dynamic) 11g: Up to 54Mbps(dynamic) 11b: Up to 11Mbps(dynamic)
EIRP	<20dBm(EIRP)
Reception Sensitivity	270M: -68dBm@10% PER 130M: -68dBm@10% PER 108M: -68dBm@10% PER 54M: -68dBm@10% PER 11M: -85dBm@8% PER 6M: -88dBm@10% PER 1M: -90dBm@8% PER
Wireless Functions	Enable/Disable Wireless Radio, WDS Bridge, WMM, Wireless Statistics
Wireless Security	WEP, WPA / WPA2, WPA-PSK / WPA2-PSK
Guest Network	2.4GHz guest network × 1
SOFTWARE FEATURES	
WAN Type	Dynamic IP/Static IP/PPPoE/ PPTP(Dual Access)/L2TP(Dual Access)/BigPond
DHCP	Server, Client, DHCP Client List, Address Reservation
Quality of Service	WMM, Bandwidth Control
Port Forwarding	Virtual Server, Port Triggering, UPnP, DMZ
Dynamic DNS	DynDns, Comexe, NO-IP
VPN Pass-Through	PPTP, L2TP, IPSec (ESP Head)
Access Control	Parental Control, Local Management Control, Host List, Access Schedule, Rule Management
Firewall Security	DoS, SPI Firewall IP Address Filter/MAC Address Filter/Domain Filter IP and MAC Address Binding
Management	Access Control Local Management Remote Management
Protocols	Supports IPv4 and IPv6

Anexo 6: Datasheet AP CISCO 3500e

Data Sheet

Cisco Aironet 3500p Access Point

Cisco Aironet® 3500p Access Point

- Ideal for high-density stadium and arena deployments
- Delivers more wireless capacity to enable a better fan experience, and 3G/4G cellular offload
- Purpose-built directional, narrow-beamwidth external antennas for targeted coverage and minimal interference
- Rugged metal housing and extended operating temperature

Cisco CleanAir Technology

Self-Healing and Self-Optimizing Wireless

- Classifies over 20 different types of interference, including non-Wi-Fi interference, within 5 to 30 seconds
- Automatic remedial action and less manual intervention

Troubleshooting Forensics for Faster Interference Resolution and Proactive Action

- Cisco CleanAir technology provides real-time, raw spectrum data to help with difficult-to-diagnose interference problems
- Air Quality Index provides a snapshot of network performance and the impact of interference
- Historic interference information for back-in-time analysis and faster problem solving
- 24/7 monitoring with remote access reduces travel and speeds resolution

Robust Security and Policy Enforcement

- Industry's first access point with non-Wi-Fi detection for off-channel rogues
- Supports rogue access point detection and detection of denial-of-service attacks
- Set policies to prohibit devices that interfere **with the Wi-Fi network or jeopardize network** security

Cisco® Aironet® 3500p Access Points are the newest members of the 3500 Series with Cisco CleanAir technology - the industry's first system to create a self-healing, self-optimizing 802.11n wireless network.

High-Density Deployments

The RF spectrum is limited, with mobile users demanding an increasing amount of capacity for video and other high-bandwidth applications. In environments such as stadiums and arenas, providing consistent and reliable Wi-Fi access can be challenging, especially as more mobile devices are packed into a confined area and high or nonexistent ceilings for access point installation. The 3500p is designed with custom configuration settings and narrow-bandwidth, high-gain external antennas to provide targeted coverage for high-density deployments. This special system of directional antennas and power settings allow an organization to deploy more access points closer together, enabling more capacity, lower co-channel interference, and a better user experience. Because of the unique antenna and power settings, FCC regulations require the Cisco Aironet 3500p Access Point to be installed by a certified professional.

RF Excellence

Building on the Cisco Aironet heritage of RF excellence, the 3500p model delivers industry-leading performance for secure and reliable wireless connections. Enterprise-class chipsets and optimized radios deliver a robust mobility experience using Cisco M-Drive technology, which includes:

- Cisco CleanAir technology to intelligently detect and mitigate RF interference for high-performance 802.11n
- Cisco ClientLink technology to improve reliability and coverage for legacy clients

- Cisco BandSelect technology to improve 5-GHz client connections in mixed-client environments
- Cisco VideoStream technology, which uses multicast to improve rich-media applications

All of these features help ensure the best possible end-user experience on the wireless network.

Cisco also offers the industry's broadest selection of 802.11n antennas, delivering optimal coverage for a variety of deployment scenarios.

Scalability

The Cisco Aironet 3500p Access Point is a component of the Cisco Unified Wireless Network, which can scale up to 18,000 access points with full Layer 3 mobility across central or remote locations on the enterprise campus, in branch offices, and at remote sites. The Cisco Unified Wireless Network is the industry's most flexible, resilient, and scalable wireless network architecture, delivering secure access to mobility services and applications and offering the lowest total cost of ownership and investment protection by integrating seamlessly with the existing wired network.

Product Specifications

Table 1 lists the product specifications for Cisco Aironet 3500p Access Points.

Table 1. Product Specifications for Cisco Aironet 3500p Access Points

Item	Specification
Part Numbers	**Cisco Aironet 3500p Access Point** **Controller-Based Access Point** **The Cisco Aironet 3500p: high-density environments, with narrow-beamwidth, high-gain, antennas** • AIR-CAP3502P-x-K9 - Dual-band controller-based 802.11a/g/n • AIR-CAP3502P-xK910 - Eco-pack (dual-band 802.11a/g/n) 10 quantity access points **Cisco SMARTnet® Service for the Cisco Aironet 3500p model with external antennas** • CON-SNT-CAP352Px - SMARTnet 8x5xNBD 3500p access point (dual-band 802.11 a/g/n) • Qty(10) CON-SNT-CAP352Px10 - SMARTnet 8x5xNBD 10 quantity eco-pack 3500p access point (dual-band 802.11a/g/n) **Cisco Wireless LAN Services** • AS-WLAN-CNSLT - Cisco Wireless LAN Network Planning and Design Service • AS-WLAN-CNSLT - Cisco Wireless LAN 802.11n Migration Service • AS-WLAN-CNSLT - Cisco Wireless LAN Performance and Security Assessment Service **Regulatory domains: (x = regulatory domain)** Customers are responsible for verifying approval for use in their individual countries. To verify approval and to identify the regulatory domain that corresponds to a particular country, visit: http://www.cisco.com/go/aironet/compliance. Not all regulatory domains have been approved. As they are approved, the part numbers will be available on the Global Price List.
Software	Cisco Unified Wireless Network Software Release 7.0 or later (autonomous IOS not supported)
802.11n Version 2.0 (and Related) Capabilities	• 2x3 multiple-input multiple-output (MIMO) with two spatial streams • Maximal ratio combining (MRC) • Legacy beamforming • 20- and 40-MHz channels • PHY data rates up to 300 Mbps • Packet aggregation: A-MPDU (Tx/Rx), A-MSDU (Tx/Rx) • 802.11 dynamic frequency selection (DFS) • Cyclic shift diversity (CSD) support

Anexo 7: Acuerdo de confidencialidad

ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN

COMPARECIENTES: EN LA CIUDAD DE TULCÁN A LOS 05 DÍAS DEL MES DE FEBRERO DEL AÑO 2018, CONVIENEN CELEBRAR EL PRESENTE ACUERDO DE CONFIDENCIALIDAD POR UNA PARTE LA UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI A QUIEN EN LO SUCESIVO SE DENOMINARÁ "EL RECEPTOR" REPRESENTADO EN ESTE ACTO POR ANDRÉS GUERRERO CON CEDULA DE IDENTIDAD 0401232871 Y POR LA OTRA, ANDERSON HUMBERTO AZA MIMALCHI CON CEDULA DE IDENTIDAD 0401873096, A QUIEN EN LO SUCESIVO SE LE DENOMINARÁ "EL DIVULGANTE", EN SU EN SU PROPIO NOMBRE Y DERECHO, AL TENOR DE LAS DECLARACIONES Y CLÁUSULAS SIGUIENTES:

PRIMERA.- Objeto. El presente Acuerdo se refiere a la información que EL RECEPTOR proporcione al DIVULGANTE, ya sea de forma oral, gráfica, escrita, o en cualquier tipo de documento, misma que deberá estar advertida como información confidencial para la realización del proyecto de titulación del DIVULGANTE con el tema: Auditoría de seguridad informática en la red interna de la Universidad Politécnica Estatal del Carchi, basada en la norma ISO/IEC 27001 y la metodología OSSTMMv3.

SEGUNDA.- OBLIGACIÓN

1. EL DIVULGANTE únicamente utilizará la información facilitada por EL RECEPTOR para el fin mencionado en la Estipulación anterior, comprometiéndose EL DIVULGANTE a mantener la más estricta confidencialidad respecto de dicha información, para el correcto cumplimiento de las obligaciones del DIVULGANTE para con EL RECEPTOR.

2. EL DIVULGANTE no podrá reproducir, modificar, hacer pública o divulgar a terceros la información objeto del presente Acuerdo sin previa autorización escrita y expresa del RECEPTOR.

3. De igual forma, EL RECEPTOR adoptará respecto de la información objeto de este Acuerdo las mismas medidas de seguridad que adoptaría normalmente respecto a la información confidencial de su propia Institución, evitando en la medida de lo posible su pérdida, robo o sustracción.

TERCERA.- Sin perjuicio de lo estipulado en el presente Acuerdo, ambas partes aceptan que la obligación de confidencialidad no se aplicará en los siguientes casos:

a) Cuando la información se encontrara en el dominio público en el momento de su suministro al DIVULGANTE o, una vez suministrada la información, ésta acceda al dominio público sin infracción de ninguna de las Estipulaciones del presente Acuerdo.

b) Cuando la información ya estuviera en el conocimiento del DIVULGANTE con anterioridad a la firma del presente Acuerdo y sin obligación de guardar confidencialidad.

c) Cuando la legislación vigente o un mandato judicial exija su divulgación. En ese caso, EL DIVULGANTE notificará al RECEPTOR de tal eventualidad y hará todo lo posible por garantizar que se dé un tratamiento confidencial a la información.

d) En caso de que EL DIVULGANTE pueda probar que la información fue desarrollada o recibida legítimamente de terceros, de forma totalmente independiente a su relación con EL RECEPTOR.

CUARTA.- Los derechos de propiedad intelectual de la información objeto de este Acuerdo pertenecen al RECEPTOR y el hecho de revelarla al DIVULGANTE para el fin mencionado en la Estipulación Primera no cambiará tal situación.

En caso de que la información resulte revelada o divulgada o utilizada por EL DIVULGANTE de cualquier forma distinta al objeto de este Acuerdo, ya sea de forma dolosa o por mera negligencia, habrá de indemnizar al RECEPTOR los daños y perjuicios ocasionados, sin perjuicio de las acciones civiles o penales que puedan corresponder a este último.

QUINTA.- Las partes se obligan a devolver cualquier documentación, antecedentes facilitados en cualquier tipo de soporte y, en su caso, las copias obtenidas de los mismos, que constituyan información amparada por el deber de confidencialidad objeto del presente Acuerdo en el supuesto de que cese la relación entre las partes por cualquier motivo.

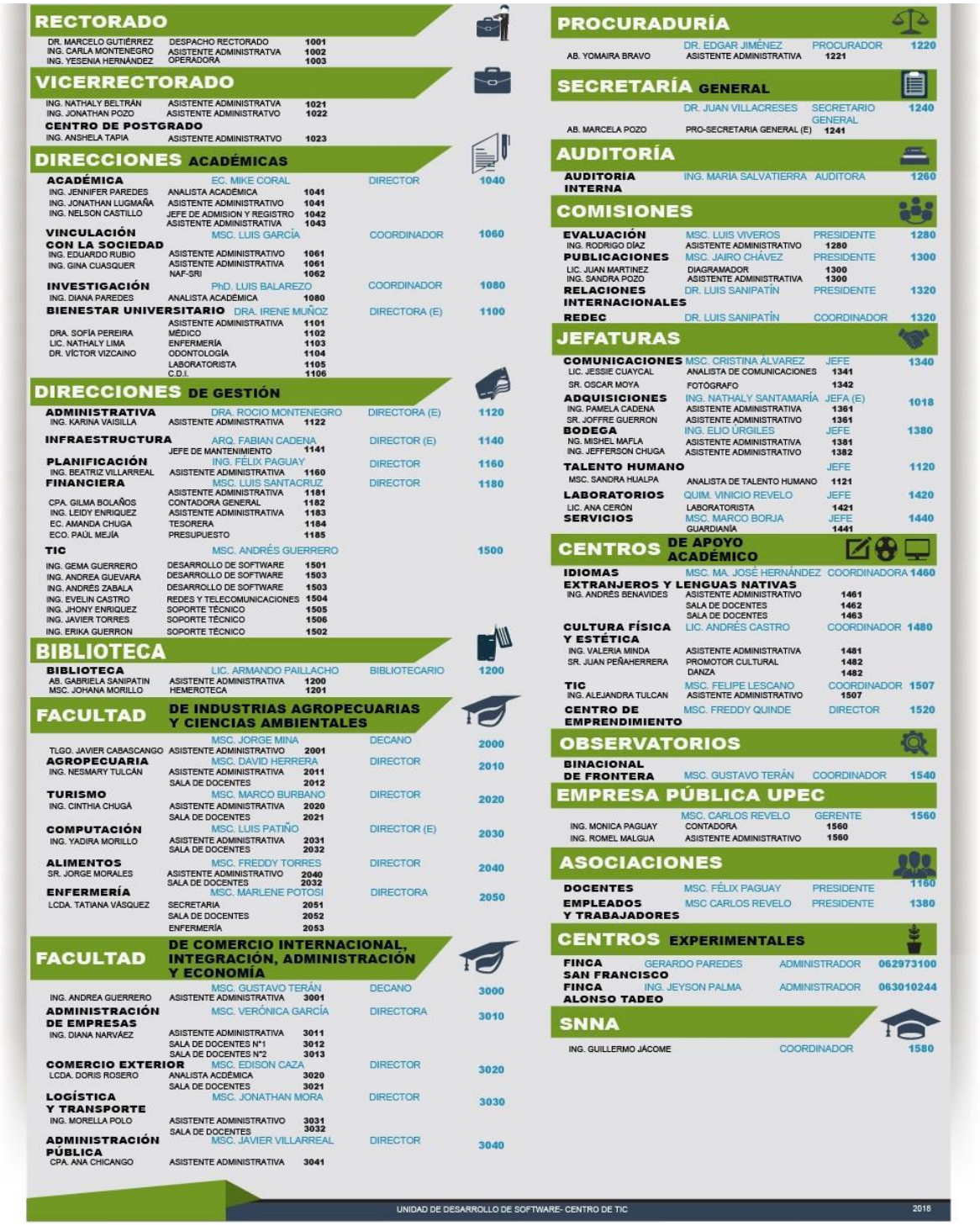
SEXTA.- El presente Acuerdo entrará en vigor en el momento de la firma del mismo por ambas partes, extendiéndose su vigencia hasta un plazo de 2 años después de finalizada la relación entre las partes o, en su caso, la prestación del servicio.

SÉPTIMA.- En caso de cualquier conflicto o discrepancia que pueda surgir en relación con la interpretación y/o cumplimiento del presente Acuerdo, las partes se someten expresamente a los Juzgados y Tribunales de la Provincia del Carchi, con renuncia a su fuero propio, aplicándose la legislación vigente.

Y en señal de expresa conformidad y aceptación de los términos recogidos en el presente Acuerdo, lo firman las partes por duplicado ejemplar y a un solo efecto en el lugar y fecha al comienzo indicados.

POR EL RECEPTOR	POR EL DIVULGANTE
Andrés Guerrero	Anderson Humberto Aza Mimalchi

Anexo 8: Directorio UPEC



RECTORADO

DR. MARCELO GUTIÉRREZ	DESPACHO RECTORADO	1001
ING. CARLA MONTENEGRO	ASISTENTE ADMINISTRATVA	1002
ING. YESENIA HERNÁNDEZ	OPERADORA	1003

VICERRECTORADO

ING. NATHALY BELTRÁN	ASISTENTE ADMINISTRATVA	1021
ING. JONATHAN POZO	ASISTENTE ADMINISTRATVO	1022

CENTRO DE POSTGRADO

ING. ANSHELA TAPIA	ASISTENTE ADMINISTRATVO	1023

DIRECCIONES ACADÉMICAS

ACADÉMICA		EC. MIKE CORAL	DIRECTOR	1040
ING. JENNIFER PAREDES	ANALISTA ACADÉMICA	1041		
ING. JONATHAN LUGMAÑA	ASISTENTE ADMINISTRATIVO	1041		
ING. NELSON CASTILLO	JEFE DE ADMISION Y REGISTRO	1042		
	ASISTENTE ADMINISTRATIVA	1043		
VINCULACIÓN CON LA SOCIEDAD		MSC. LUIS GARCÍA	COORDINADOR	1060
ING. EDUARDO RUBIO	ASISTENTE ADMINISTRATIVO	1061		
ING. GINA CUASQUER	ASISTENTE ADMINISTRATIVA	1061		
	NAF-SRI	1062		
INVESTIGACIÓN		PhD. LUIS BALAREZO	COORDINADOR	1080
ING. DIANA PAREDES	ANALISTA ACADÉMICA	1080		
BIENESTAR UNIVERSITARIO		DRA. IRENE MUÑOZ	DIRECTORA (E)	1100
	ASISTENTE ADMINISTRATIVA	1101		
DRA. SOFÍA PEREIRA	MÉDICO	1102		
LIC. NATHALY LIMA	ENFERMERÍA	1103		
DR. VÍCTOR VIZCAINO	ODONTOLOGÍA	1104		
	LABORATORISTA	1105		
	C.D.I.	1106		

DIRECCIONES DE GESTIÓN

ADMINISTRATIVA		DRA. ROCIO MONTENEGRO	DIRECTORA (E)	1120
ING. KARINA VAISILLA	ASISTENTE ADMINISTRATIVA	1122		
INFRAESTRUCTURA		ARQ. FABIAN CADENA	DIRECTOR (E)	1140
	JEFE DE MANTENIMIENTO	1141		
PLANIFICACIÓN		ING. FÉLIX PAGUAY	DIRECTOR	1160
ING. BEATRIZ VILLARREAL	ASISTENTE ADMINISTRATIVA	1160		
FINANCIERA		MSC. LUIS SANTACRUZ	DIRECTOR	1180
	ASISTENTE ADMINISTRATIVA	1181		
CPA. GILMA BOLAÑOS	CONTADORA GENERAL	1182		
ING. LEIDY ENRIQUEZ	ASISTENTE ADMINISTRATIVA	1183		
EC. AMANDA CHUGA	TESORERA	1184		
ECO. PAÚL MEJÍA	PRESUPUESTO	1185		
TIC		MSC. ANDRÉS GUERRERO		1500
ING. GEMA GUERRERO	DESARROLLO DE SOFTWARE	1501		
ING. ANDREA GUEVARA	DESARROLLO DE SOFTWARE	1503		
ING. ANDRÉS ZABALA	DESARROLLO DE SOFTWARE	1503		
ING. EVELIN CASTRO	REDES Y TELECOMUNICACIONES	1504		
ING. JHONY ENRIQUEZ	SOPORTE TÉCNICO	1505		
ING. JAVIER TORRES	SOPORTE TÉCNICO	1506		
ING. ERIKA GUERRON	SOPORTE TÉCNICO	1502		

BIBLIOTECA

BIBLIOTECA		LIC. ARMANDO PAILLACHO	BIBLIOTECARIO	1200
AB. GABRIELA SANIPATIN	ASISTENTE ADMINISTRATIVA	1200		
MSC. JOHANA MORILLO	HEMEROTECA	1201		

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

		MSC. JORGE MINA	DECANO	2000
TLGO. JAVIER CABASCANGO	ASISTENTE ADMINISTRATIVO	2001		
AGROPECUARIA		MSC. DAVID HERRERA	DIRECTOR	2010
ING. NESMARY TULCÁN	ASISTENTE ADMINISTRATIVA	2011		
	SALA DE DOCENTES	2012		
TURISMO		MSC. MARCO BURBANO	DIRECTOR	2020
ING. CINTHIA CHUGÁ	ASISTENTE ADMINISTRATIVA	2020		
	SALA DE DOCENTES	2021		
COMPUTACIÓN		MSC. LUIS PATIÑO	DIRECTOR (E)	2030
ING. YADIRA MORILLO	ASISTENTE ADMINISTRATIVA	2031		
	SALA DE DOCENTES	2032		
ALIMENTOS		MSC. FREDDY TORRES	DIRECTOR	2040
SR. JORGE MORALES	ASISTENTE ADMINISTRATIVO	2040		
	SALA DE DOCENTES	2032		
ENFERMERÍA		MSC. MARLENE POTOSI	DIRECTORA	2050
LCDA. TATIANA VÁSQUEZ	SECRETARIA	2051		
	SALA DE DOCENTES	2052		
	ENFERMERÍA	2053		

FACULTAD DE COMERCIO INTERNACIONAL, INTEGRACIÓN, ADMINISTRACIÓN Y ECONOMÍA

		MSC. GUSTAVO TERÁN	DECANO	3000
ING. ANDREA GUERRERO	ASISTENTE ADMINISTRATIVA	3001		
ADMINISTRACIÓN DE EMPRESAS		MSC. VERÓNICA GARCÍA	DIRECTORA	3010
ING. DIANA NARVÁEZ	ASISTENTE ADMINISTRATIVA	3011		
	SALA DE DOCENTES N°1	3012		
	SALA DE DOCENTES N°2	3013		
COMERCIO EXTERIOR		MSC. EDISON CAZA	DIRECTOR	3020
LCDA. DORIS ROSERO	ANALISTA ACDÉMICA	3020		
	SALA DE DOCENTES	3021		
LOGÍSTICA Y TRANSPORTE		MSC. JONATHAN MORA	DIRECTOR	3030
ING. MORELLA POLO	ASISTENTE ADMINISTRATIVO	3031		
	SALA DE DOCENTES	3032		
ADMINISTRACIÓN PÚBLICA		MSC. JAVIER VILLARREAL	DIRECTOR	3040
CPA. ANA CHICANGO	ASISTENTE ADMINISTRATIVA	3041		

PROCURADURÍA

		DR. EDGAR JIMÉNEZ	PROCURADOR	1220
AB. YOMAIRA BRAVO	ASISTENTE ADMINISTRATIVA	1221		

SECRETARÍA GENERAL

		DR. JUAN VILLACRESES	SECRETARIO GENERAL	1240
AB. MARCELA POZO	PRO-SECRETARIA GENERAL (E)	1241		

AUDITORÍA

AUDITORIA INTERNA		ING. MARIA SALVATIERRA	AUDITORA	1260

COMISIONES

EVALUACIÓN		MSC. LUIS VIVEROS	PRESIDENTE	1280
ING. RODRIGO DÍAZ	ASISTENTE ADMINISTRATIVO	1280		
PUBLICACIONES		MSC. JAIRO CHÁVEZ	PRESIDENTE	1300
LIC. JUAN MARTINEZ	DIAGRAMADOR	1300		
ING. SANDRA POZO	ASISTENTE ADMINISTRATIVA	1300		
RELACIONES INTERNACIONALES		DR. LUIS SANIPATÍN	PRESIDENTE	1320
REDEC		DR. LUIS SANIPATÍN	COORDINADOR	1320

JEFATURAS

COMUNICACIONES		MSC. CRISTINA ÁLVAREZ	JEFE	1340
LIC. JESSIE CUAYCAL	ANALISTA DE COMUNICACIONES	1341		
SR. OSCAR MOYA	FOTÓGRAFO	1342		
ADQUISICIONES		ING. NATHALY SANTAMARÍA	JEFA (E)	1018
ING. PAMELA CADENA	ASISTENTE ADMINISTRATIVA	1361		
SR. JOFFRE GUERRON	ASISTENTE ADMINISTRATIVO	1361		
BODEGA		ING. ELIO URGILES	JEFE	1380
NG. MISHEL MAFLA	ASISTENTE ADMINISTRATIVA	1381		
ING. JEFFERSON CHUGA	ASISTENTE ADMINISTRATIVO	1382		
TALENTO HUMANO			JEFE	1120
MSC. SANDRA HUALPA	ANALISTA DE TALENTO HUMANO	1121		
LABORATORIOS		QUIM. VINICIO REVELO	JEFE	1420
LIC. ANA CERÓN	LABORATORISTA	1421		
SERVICIOS		MSC. MARCO BORJA	JEFE	1440
	GUARDIANÍA	1441		

CENTROS DE APOYO ACADÉMICO

IDIOMAS EXTRANJEROS Y LENGUAS NATIVAS		MSC. MA. JOSÉ HERNÁNDEZ	COORDINADORA	1460
ING. ANDRÉS BENAVIDES	ASISTENTE ADMINISTRATIVO	1461		
	SALA DE DOCENTES	1462		
	SALA DE DOCENTES	1463		
CULTURA FÍSICA Y ESTÉTICA		LIC. ANDRÉS CASTRO	COORDINADOR	1480
ING. VALERIA MINDA	ASISTENTE ADMINISTRATIVA	1481		
SR. JUAN PEÑAHERRERA	PROMOTOR CULTURAL	1482		
	DANZA	1482		
TIC		MSC. FELIPE LESCANO	COORDINADOR	1507
ING. ALEJANDRA TULCAN	ASISTENTE ADMINISTRATIVO	1507		
CENTRO DE EMPRENDIMIENTO		MSC. FREDDY QUINDE	DIRECTOR	1520

OBSERVATORIOS

BINACIONAL DE FRONTERA		MSC. GUSTAVO TERÁN	COORDINADOR	1540

EMPRESA PÚBLICA UPEC

		MSC. CARLOS REVELO	GERENTE	1560
ING. MONICA PAGUAY	CONTADORA	1560		
ING. ROMEL MALGUA	ASISTENTE ADMINISTRATIVO	1560		

ASOCIACIONES

DOCENTES		MSC. FÉLIX PAGUAY	PRESIDENTE	1160
EMPLEADOS Y TRABAJADORES		MSC CARLOS REVELO	PRESIDENTE	1380

CENTROS EXPERIMENTALES

FINCA SAN FRANCISCO	GERARDO PAREDES	ADMINISTRADOR	062973100	
FINCA ALONSO TADEO	ING. JEYSON PALMA	ADMINISTRADOR	063010244	

SNNA

ING. GUILLERMO JÁCOME	COORDINADOR	1580	

UNIDAD DE DESARROLLO DE SOFTWARE- CENTRO DE TIC 2018

Anexo 9: Reporte del Canal Humano de la UPEC

Reporte de la Prueba de Seguridad Humana

Certificación de la Verificación de Seguridad OSSTMM 3.0

OSSTMM.ORG - ISECOM.ORG

ID del Auditor	040187309-6	**Fecha**	16/01/2018
Auditor Principal	Anderson Humberto Aza M.	**Duración de la Prueba**	Dos semanas
Alcance y Relación	Personal de la UPEC	**Vectores**	Empleados que tienen interacción con la red interna
Canales	Humano	**Tipo de Prueba**	Ingeniería Social

Soy responsable de la información contenida en este reporte y he verificado personalmente que toda la información es fundamentada y verdadera

FIRMA DE RESPONSABLE

SELLO DE LA INSTITUCION

Observaciones: Para probar este canal se aplicaron 15 encuestas a algunos empleados de la institución, se anexa la tabulación en la parte inferior. Adicional a las encuestas se recogió más datos usando la persuasión y la observación.

VALORES DE LA SEGURIDAD OPERACIONAL		**VALORES DE LOS CONTROLES**	
Visibilidad	7	**Autenticación**	5
Acceso	4	**Indemnización**	1
Confianza	3	**Resistencia**	3
VALORES DE LAS LIMITACIONES		**Subyugación**	0
Vulnerabilidad	1	**Continuidad**	0
Debilidad	1	**No-Repudio**	3
Preocupación	0	**Confidencialidad**	4
Exposición	0	**Privacidad**	2
Anomalía	0	**Integridad**	2
		Alarma	3
OpSec	9,90	**Controles Verdaderos**	5,59
Limitaciones	8,83	**Seguridad Δ**	-13,14

Protección Verdadera	86.86	**Actual Security**	86.68

Tabulación de encuestas sobre la seguridad del canal Humano en la UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

La información obtenida de las encuestas es netamente de uso estadístico para uso de un estudiante que se encuentra realizando el trabajo de titulación en la red interna de la UPEC, y no afectara al encuestado en ningún aspecto.

PREGUNTAS	RESPUESTAS		
	SI	NO	N/A
1. ¿Tienen acceso otras personas a su estación de trabajo?	0	12	3
2. ¿Se puede acceder a las estaciones de trabajo de la institución sin ningún tipo de credenciales?	8	5	2
3. ¿Posee clave de acceso su estación de trabajo?	13	2	0
4. ¿Tiene la clave de acceso escrita y a la vista de terceros?	9	6	0
5. Cuando sale de la estación de trabajo, ¿Deja cerrando la sesión?	10	5	0
6. Al culminar el día, ¿Apaga su estación de trabajo?	15	0	0
7. Cuando su estación de trabajo tiene errores, ¿Acude al centro de TIC's?	13	0	2
8. ¿Alguna vez ha perdido información de su estación de trabajo?	4	11	0
9. ¿En su contrato, existe algún acuerdo de no divulgación de la información?	15	0	0
10. ¿Piensa usted que la información de la institución es 100% segura?	8	5	2
11. ¿Cambia frecuentemente las claves de acceso a su estación de trabajo?	2	13	0
12. ¿Tiene antivirus su estación de trabajo?	5	4	6
13. ¿Alguna vez se han mostrado alertas por virus?	3	5	7
14. ¿Guarda respaldos de los archivos que tiene en su estación de trabajo?	5	10	0
15. ¿Navega por internet en su estación de trabajo?	15	0	0
16. ¿Ha llevado información de la institución fuera de su estación de trabajo?	8	7	0
17. ¿Usa el correo electrónico convencional para compartir información de la institución?	5	10	0
18. ¿Usa redes sociales para compartir información de la institución?	0	15	0
19. ¿Usa dispositivos ajenos a la institución para almacenar información?	2	13	0
20. ¿Comparte información de la institución por medio de llamadas telefónicas?	5	10	0
21. ¿Confía en el personal de seguridad, para garantizar la integridad de las estaciones de trabajo?	7	5	3
22. ¿Existen cámaras de seguridad en las cercanías a las estaciones de trabajo?	9	2	4
23. ¿Alguna vez sustrajo activos informáticos fuera de la institución?	0	15	0

24. ¿Existe inventario de las estaciones de trabajo de la institución?	8	2	5

CHECKLIST

Dirigida: Canal Humano de la UPEC

Técnica: Observación y Persuasión	**Fecha: 16/01/2018**	
Firma del Representante:	**Sello de la Institución:**	
1. Seguridad Operacional	**SI**	**NO**
Rectorado y vicerrectorado tienen acceso al Data Center	X	
Dirección de TIC's tiene acceso al Data Center	X	
Dirección de TIC's tiene acceso a los racks	X	
Tiene el personal limitaciones para acceder a las estaciones de trabajo		X
Los demás departamentos de la institución pueden acceder al Data Center y racks.		X
Pueden personas ajenas a la institución acceder a las estaciones de trabajo	X	
Pueden ingresar dispositivos electrónicos a la institución	X	
Cuenta con seguridad privada la institución	X	
2. Controles	**SI**	**NO**
Se requieren autenticación para acceder a los equipos informáticos de la institución		**X**
Existe acuerdo de confidencialidad para los empleados de la institución		**X**
Tiene correo electrónico seguro la institución	**X**	
Se puede acceder a los racks sin autorización	**X**	

Se tiene acceso a los equipos inalámbricos sin autorización	**X**	
Se lleva registro de acceso en la institución		**X**
Posee comunicaciones seguras la institución		**X**
Existen procesos eficientes en la comunicación dentro de la institución	**X**	
Se usan firmas y sellos para los documentos	**X**	
Existe sistema de video vigilancia	**X**	
Cuentan con antivirus en las estaciones de trabajo	**X**	
1. Limitaciones	**SI**	**NO**
El personal nuevo puede divulgar información clasificada	**X**	
Se puede comprobar que los empleados cumplen con el contrato firmado		**X**
Los turnos de los guardias son rotativos	**X**	
Se lleva registro de ingreso a la institución		**X**
Los guardias de seguridad poseen información relevante para la UPEC		**X**

Anexo 10: Reporte del Canal Físico de la UPEC

Reporte de la Prueba de Seguridad Física

Certificación de la Verificación de Seguridad OSSTMM 3.0

OSSTMM.ORG - ISECOM.ORG

ID del Auditor	040187309-6	Fecha	02/02/2018
Auditor Principal	Anderson Humberto Aza M.	Duración de la Prueba	Dos semanas
Alcance y Relación	Espacio Físico de la UPEC	Vectores	Data Center, Racks, Estaciones de Trabajo
Canales	Físico	Tipo de Prueba	Observación y Persuasión

Soy responsable de la información contenida en este reporte y he verificado personalmente que toda la información es fundamentada y verdadera

FIRMA DE RESPONSABLE

SELLO DE LA INSTITUCIÓN

Observaciones: Para probar este canal se tomaron fotografías de los lugares de acceso, además del checklist correspondiente.

VALORES DE LA SEGURIDAD OPERACIONAL		VALORES DE LOS CONTROLES	
Visibilidad	7	Autenticación	2
Acceso	11	Indemnización	7
Confianza	1	Resistencia	7
VALORES DE LAS LIMITACIONES		Subyugación	2
Vulnerabilidad	5	Continuidad	9
Debilidad	6	No-Repudio	1
Preocupación	3	Confidencialidad	2
Exposición	1	Privacidad	2
Anomalía	0	Integridad	5
		Alarma	1
OpSec	10,75	Controles Verdaderos	6,66
Limitaciones	15,64	Seguridad Δ	-19,74

Protección Verdadera	80.26	Seguridad Actual	80.19

A continuación se muestran los lugares de acceso a la institución, en la imagen 1, se muestra el acceso principal a la Universidad, en la imagen 2 se puede observar la vía de acceso al Data Center de la institución, en la imagen 3 se observa el acceso a los racks sin ninguna seguridad que garantice su integridad y finalmente en la imagen 4 se aprecia el acceso a los laboratorios sin ninguna seguridad pues las puertas se encuentran abiertas.

Imagen 37: Puerta principal de la UPEC
Fuente: Elaboración Propia

Imagen 38: Vía de acceso al Data Center
Fuente: Elaboración Propia

Imagen 39: Acceso a los Racks
Fuente: Elaboración Propia

Imagen 40: Acceso a los laboratorios
Fuente: Elaboración Propia

CHECKLIST

Técnica: Observación y Persuasión	**Fecha: 03/02/2018**	
Firma del Representante: 	**Sello de la Institución:** 	
1. Seguridad Operacional	**SI**	**NO**
El campus es de acceso público	**X**	
Existen objetivos fuera del alcance	**X**	
Se cuenta con normas de tráfico	**X**	
Cuenta con directorio telefónico	**X**	
Cuenta con barreras para ruido	**X**	
Cuenta con barreras para calor	**X**	
Cuenta con barreras para frio	**X**	
Cuenta con barreras para humedad	**X**	
Cuenta con barreras para humo	**X**	
Cuenta con barreras para olores	**X**	
Cuenta con barreras para luz dañina	**X**	
Se puede acceder sin identificación	**X**	
2. Controles	**SI**	**NO**
Se requiere autorización para acceder al Data Center	**X**	
Se requiere autorización para acceder a los rack		**X**
Se requiere autorización para acceder a las estaciones de trabajo		**X**
Se puede llevar equipo informático dentro de la institución	**X**	
Se pueden llevar los activos informáticos fuera de la institución	**X**	
Se lleva registro de los artículos que son introducidos o retirados de la universidad		**X**
Se puede eludir el contrato	**X**	
Se usan señales de advertencia o peligro	**X**	
Se usan cámaras	**X**	
Se usan avisos de entrada restringida	**X**	
Tiene seguridad el acceso al Data Center	**X**	

Deniega el acceso a la institución, la distracción, remoción o silencio del personal de recepción.		**X**
Deniega el acceso aislarla de recursos como energía eléctrica	**X**	
Las reuniones se realizan a puerta cerrada	**X**	
Los documentos son llevados de forma personal	**X**	
Se identifican los documentos de acuerdo a su importancia	**X**	
Se lleva inventario de los equipos informáticos	**X**	
1. Limitaciones	**SI**	**NO**
Es suficiente el número de guardias para la institución	**X**	
Existe control de plagas		**X**
Se encuentran empotradas las estaciones de trabajo		**X**
Se controla el cumplimiento del contrato al 100%		**X**
Las señales de peligro cubren toda la institución		**X**
Existen limitaciones para circular en el campus		**X**
Las oficinas cuentan con cortinas	**X**	
Posee el Data Center sistema contra incendios		**X**
Posee el Data Center respaldos de energía		**X**

Anexo 11: Reporte del Canal Inalámbrico de la UPEC

Reporte de la Prueba de Seguridad Inalámbrica

Certificación de la Verificación de Seguridad OSSTMM 3.0

OSSTMM.ORG - ISECOM.ORG

ID del Auditor	040187309-6	Fecha	19/02/2018
Auditor Principal	Anderson Humberto Aza M.	Duración de la Prueba	Dos semanas
Alcance y Relación	Todo el Campus de la UPEC	Vectores	Red Inalámbrica UPEC
Canales	Inalámbrico	Tipo de Prueba	Entrevista, y software de detección de redes Wi-Fi

Soy responsable de la información contenida en este reporte y he verificado personalmente que toda la información es fundamentada y verdadera

FIRMA DE RESPONSABLE

SELLO DE LA INSTITUCIÓN

UNIVERSIDAD TÉCNICA ESTATAL DE CARCHI - UPEC CENTRO TIC - TULCÁN

Observaciones: Para probar este canal se escanearon las redes Wi-Fi de la institución, además se realizó una entrevista al encargado del departamento de TIC's.

VALORES DE LA SEGURIDAD OPERACIONAL		VALORES DE LOS CONTROLES	
Visibilidad	5	Autenticación	5
Acceso	4	Indemnización	0
Confianza	7	Resistencia	1
VALORES DE LAS LIMITACIONES		Subyugación	0
Vulnerabilidad	1	Continuidad	1
Debilidad	2	No-Repudio	1
Preocupación	1	Confidencialidad	0
Exposición	0	Privacidad	0
Anomalía	0	Integridad	2
		Alarma	0
OpSec	10,27	Controles Verdaderos	4.02
Limitaciones	11.81	Seguridad Δ	-18.06

Protección Verdadera	81.94	Seguridad Actual	82.27

Informe de la entrevista sobre la seguridad del canal Inalámbrico en la UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Entrevistador: Anderson Humberto Aza Mimalchi	**Entrevistado: Ing. Javier Torres**
Técnica: Entrevista	**Fecha: 21/02/2018**
Firma del Representante:	**Sello de la institución:**

El objetivo de la entrevista es obtener información de la seguridad en la red inalámbrica de la Universidad Politécnica Estatal del Carchi y se realiza como parte de la auditoria que se está llevando a cabo.

PREGUNTAS REALIZADAS

a. ¿Se usa control de acceso, para ingresar a las redes Wi-Fi de la institución?

b. ¿Se pueden interferir las redes inalámbricas presentes en la institución?

c. ¿Qué frecuencia se utiliza para las redes Wi-Fi?

d. ¿Se pueden generar señales Wi-Fi no autorizadas dentro de la institución?

e. ¿Existen señales inalámbricas diferentes al Wi-Fi?

f. ¿Se apagan los AP, o estos están encendidos las 24 horas del día?

g. ¿Los AP tienen antenas direccionales?

h. ¿Se ajusta la potencia de salida de los AP, o esta se encuentra en el máximo valor?

i. ¿Los AP están con SSID por defecto?

j. ¿Cuál es el método de autenticación para los estudiantes?

k. ¿Cuál es el método de autenticación para el personal administrativo?

l. ¿Cuál es el método de autenticación para los docentes?

m. ¿Cuál es el método de autenticación para los invitados?

n. ¿Se puede usar redes Wi-Fi que no estén asignadas a cada sector?

o. ¿Se han detectado repetidores falsos?

p. ¿Qué parámetros se configuran en los AP?

q. ¿Cuándo se presentan problemas con los AP, cuanto tardan en abordar el problema?

r. ¿Puede monitorear los usuarios que acceden a la red Inalámbrica?

s. ¿Poseen sistema de alerta para detectar problemas con la red inalámbrica?

t. ¿Utilizan AP residenciales o empresariales?

CONCLUSIONES

Una vez se obtuvo las respuestas por parte del entrevistado, se concluyó lo siguiente:

Las redes inalámbricas de la institución son solo las Wi-Fi y tienen control de acceso para estudiantes, docentes personal administrativo e invitados. Cabe mencionar que las claves de acceso son diferentes en cada red, además los estudiantes tienen su usuario y clave personalizada con la red eduroam.

Al no configurar canal y potencia de salida, las redes Wi-Fi se pueden interferir bajando la calidad de la señal, Por otra parte los AP se encuentran encendidos las 24 horas del día y no se reinician para evitar que se saturen.

Los AP tienen antenas direccionales para de esta manera focalizar la señal Wi-Fi de acuerdo al personal al cual está dirigido. El personal tiene su método de acceso diferente es decir, los estudiantes tienen la red eduroam, los docentes tienen protección con clave y MAC, el personal administrativo tiene su propia red y los invitados tienen una red protegida con contraseña. Por este motivo cada área del personal no puede usar redes que no se le hayan asignado.

No existen sistemas RFID o infrarrojos dentro de la institución, la única señal inalámbrica es el Wi-Fi, para navegar por internet.

En cuanto a los equipos utilizados para generar las señales Wi-Fi se usan equipos CISCO, aunque para los departamentos administrativos se está haciendo uso de router residenciales, los cuales no prestan las garantías de seguridad recomendada.

Físicamente es fácil acceder a los AP, pues estos no se encuentran empotrados y es fácil sustraerlos de la institución, además estos no se encuentran asegurados contra robos o daños por lo que en caso de hurto o daño la institución debe asumir los costos. La única forma de resguardar la seguridad de los AP es el sistema de video vigilancia, sin embargo no es 100 % confiable debido a que una sola persona monitorea este servicio.

EVIDENCIA DEL ESCANEO DE LAS REDES WI-FI

En este apartado se puede observar imágenes en las cuales se encuentran las redes Wi-Fi de la institución, con su tipo de autenticación y cifrado. Esto se realizó tanto dentro de la institución como fuera de ella. Además, se muestra la ubicación de los equipos tanto dentro de las oficinas como fuera de ellas.

Imagen 1: AP CISCO ubicado en la pared en el edificio principal.
Fuente: Elaboración Propia

Imagen 2: AP TP-LINK ubicado en una de las oficinas de la institución
Fuente: Elaboración Propia

MAC Address	SSID	Last Signal	Average Signal	Security Enabled	Connectable	Authentication	Cipher	RSSI	Channel Number	Maximum Speed
60-e3-27-5f-b5-0a	ADQUISICIONES	22%	43%	Yes	Yes	RSNA-PSK	CCMP	-84	1	54 Mbps
74-29-af-48-a9-af	AHP	57%	41%	Yes	Yes	RSNA-PSK	CCMP	-72	6	54 Mbps
4e-4e-03-96-03-24	Alcatel Pixi 4 (4)	18%	23%	Yes	Yes	RSNA-PSK	CCMP	-87	6	54 Mbps
c0-bd-d1-9d-f4-de	AndroidAPE	11%	27%	Yes	Yes	RSNA-PSK	CCMP	-92	6	54 Mbps
68-a3-c4-fd-28-1f	Anto	28%	37%	Yes	Yes	RSNA-PSK	CCMP	-81	6	54 Mbps
c8-3a-35-52-ab-80	AUDIOVISUALES	92%	81%	Yes	Yes	WPA-PSK	CCMP	-58	6	54 Mbps
88-a5-bd-0f-a5-58	CCTV MARINA	9%	9%	Yes	Yes	RSNA-PSK	CCMP	-93	8	54 Mbps
2c-54-2d-38-18-d7	CDEI	70%	74%	Yes	Yes	RSNA-PSK	CCMP	-67	11	54 Mbps
e4-68-a3-d7-7b-62	CNT/D2NET	19%	19%	Yes	Yes	RSNA-PSK	CCMP	-86	1	54 Mbps
30-52-cb-08-11-4a	DESKTOP-4BT7TH6 9420	23%	23%	Yes	Yes	RSNA-PSK	CCMP	-83	1	54 Mbps
60-e3-27-5f-a6-f2	DIR-ACADEMICA	28%	43%	Yes	Yes	RSNA-PSK	CCMP	-81	1	54 Mbps
c8-3a-35-57-da-08	DIRECCION_EAEM	22%	31%	Yes	Yes	RSNA-PSK	CCMP	-84	7	54 Mbps
60-e3-27-5f-b4-88	DIRECCION_TIC	39%	55%	Yes	Yes	RSNA-PSK	CCMP	-78	6	54 Mbps
46-d2-44-01-83-5d	DIRECT-4401035D	62%	65%	Yes	Yes	RSNA-PSK	CCMP	-70	6	54 Mbps
00-3a-99-39-95-33	eduroam	20%	21%	Yes	Yes	RSNA	CCMP	-85	11	54 Mbps
00-3a-99-70-a5-a3	eduroam	87%	61%	Yes	Yes	RSNA	CCMP	-60	6	54 Mbps
00-3a-99-76-e6-33	eduroam	19%	58%	Yes	Yes	RSNA	CCMP	-86	11	54 Mbps
00-3a-99-85-76-d3	eduroam	55%	66%	Yes	Yes	RSNA	CCMP	-73	6	54 Mbps
00-3a-99-85-9e-e3	eduroam	25%	46%	Yes	Yes	RSNA	CCMP	-82	11	54 Mbps
34-a8-4e-f8-c1-c3	eduroam	100%	91%	Yes	Yes	RSNA	CCMP	-45	1	54 Mbps
40-01-7a-dd-c7-53	eduroam	23%	19%	Yes	Yes	RSNA	CCMP	-83	1	54 Mbps
64-d8-14-b3-c9-a3	eduroam	52%	68%	Yes	Yes	RSNA	CCMP	-74	6	54 Mbps
88-75-56-ed-91-a3	eduroam	20%	23%	Yes	Yes	RSNA	CCMP	-85	1	54 Mbps
a8-9d-21-72-00-73	eduroam	22%	24%	Yes	Yes	RSNA	CCMP	-84	1	54 Mbps
c0-25-5c-8e-d1-f3	eduroam	18%	36%	Yes	Yes	RSNA	CCMP	-87	6	54 Mbps
c4-0a-cb-a4-3a-83	eduroam	19%	35%	Yes	Yes	RSNA	CCMP	-86	1	54 Mbps
cc-d5-39-9f-94-b3	eduroam	67%	81%	Yes	Yes	RSNA	CCMP	-68	11	54 Mbps
cc-d5-39-9f-95-43	eduroam	72%	71%	Yes	Yes	RSNA	CCMP	-66	1	54 Mbps
ec-e1-a9-30-bc-e3	eduroam	23%	52%	Yes	Yes	RSNA	CCMP	-83	11	54 Mbps
f4-1f-c2-1f-c7-b3	eduroam	35%	40%	Yes	Yes	RSNA	CCMP	-79	11	54 Mbps
e8-93-09-31-db-86	Eve J1	39%	40%	Yes	Yes	RSNA-PSK	CCMP	-78	6	54 Mbps
60-36-dd-2a-13-96	hola =D	100%	89%	Yes	Yes	RSNA-PSK	CCMP	-45	11	54 Mbps
f0-43-47-26-8c-d2	HUAWEI-8CD2	18%	27%	Yes	Yes	RSNA-PSK	CCMP	-87	1	54 Mbps
c0-56-27-44-87-25	INSCRIPCIONES	80%	51%	Yes	Yes	RSNA-PSK	CCMP	-63	11	54 Mbps
	INTERNET CNT	100%	100%	Yes	Yes	RSNA-PSK	CCMP			0 Mbps
14-b9-68-2b-7b-6c	INTERNET CNT	32%	32%	Yes	Yes	RSNA-PSK	CCMP	-80	11	54 Mbps
5a-59-f9-89-84-34	isabella	20%	42%	Yes	Yes	RSNA-PSK	CCMP	-85	1	54 Mbps
ba-81-98-54-b8-fc	JIMMY-6279	20%	27%	Yes	Yes	RSNA-PSK	CCMP	-85	11	54 Mbps
54-35-30-2c-da-62	Kvn_Andr's	28%	37%	Yes	Yes	RSNA-PSK	CCMP	-81	11	54 Mbps

Imagen 3: Redes inalámbricas escaneadas dentro de la institución
Fuente: Elaboración Propia

MAC Address	SSID	Last Signal	Average Signal	Security Enabled	Connectable	Authentication	Cipher	RSSI	Channel Number	Maximum Speed
bc-66-41-89-47-64	Casa	25%	22%	Yes	Yes	RSNA-PSK	CCMP	-82	3	54 Mbps
00-3a-7d-20-1c-53	eduroam	90%	85%	Yes	Yes	RSNA	CCMP	-59	11	54 Mbps
ec-e1-a9-30-bc-e3	eduroam	9%	12%	Yes	Yes	RSNA	CCMP	-93	11	54 Mbps
c8-3a-35-52-ab-98	ENGLISH - TEACHERS	32%	29%	Yes	Yes	RSNA-PSK	CCMP	-80	6	54 Mbps
c0-25-e9-a9-5f-e4	FABIAN1	9%	9%	Yes	Yes	RSNA-PSK	CCMP	-93	4	54 Mbps
ec-08-6b-41-57-78	Gerando Chunes	16%	17%	Yes	Yes	RSNA-PSK	CCMP	-88	7	54 Mbps
84-be-52-b6-63-7b	HUAWEI_P9lite_9335	35%	38%	Yes	Yes	RSNA-PSK	CCMP	-79	6	54 Mbps
4c-5e-0c-6e-c0-e3	JERLEO	28%	33%	Yes	Yes	RSNA-PSK	CCMP	-81	1	54 Mbps
2e-59-8a-54-0f-7c	LG X cam_9971	65%	54%	Yes	Yes	RSNA-PSK	CCMP	-69	6	54 Mbps
fc-42-03-c5-43-6d	Stiven	90%	57%	Yes	Yes	RSNA-PSK	CCMP	-59	6	54 Mbps
e0-aa-96-ed-f1-9a	Tivo	72%	57%	Yes	Yes	RSNA-PSK	CCMP	-66	1	54 Mbps
c4-e9-84-82-af-bc	W.COLISEO	67%	73%	Yes	Yes	RSNA-PSK	CCMP	-68	2	54 Mbps
00-3a-7d-20-1c-50	WIFI_UPEC	87%	85%	No	Yes	802.11 Open	None	-60	11	54 Mbps
ec-e1-a9-30-bc-e0	WIFI_UPEC	11%	11%	No	Yes	802.11 Open	None	-92	11	54 Mbps
00-3a-7d-20-1c-51	WUPEC	87%	84%	Yes	Yes	RSNA-PSK	CCMP	-60	11	54 Mbps
ec-e1-a9-31-3c-00	WUPEC	16%	15%	Yes	Yes	RSNA-PSK	CCMP	-88	6	54 Mbps
00-3a-7d-20-1c-52	WUPEC.EVENTOS	85%	85%	Yes	Yes	RSNA-PSK	CCMP	-61	11	54 Mbps

Imagen 4: Redes inalámbricas escaneadas fuera de la institución
Fuente: Elaboración propia

Anexo 12: Reporte del Canal Telecomunicaciones de la UPEC

Reporte de la Prueba de Telecomunicaciones

Certificación de la Verificación de Seguridad OSSTMM 3.0

OSSTMM.ORG - ISECOM.ORG

ID del Auditor	040187309-6	Fecha	05/03/2018
Auditor Principal	Anderson Humberto Aza M.	Duración de la Prueba	Dos semanas
Alcance y Relación	TELEFONIA IP UPEC	Vectores	TELEFONIA IP UPEC
Canales	Telecomunicaciones	Tipo de Prueba	Entrevista

Soy responsable de la información contenida en este reporte y he verificado personalmente que toda la información es fundamentada y verdadera

FIRMA DE RESPONSABLE

SELLO DE LA INSTITUCIÓN

Observaciones: Se anexa la entrevista realizada al administrador de red

VALORES DE LA SEGURIDAD OPERACIONAL		VALORES DE LOS CONTROLES	
Visibilidad	4	Autenticación	7
Acceso	2	Indemnización	2
Confianza	1	Resistencia	0
VALORES DE LAS LIMITACIONES		Subyugación	1
Vulnerabilidad	0	Continuidad	2
Debilidad	0	No-Repudio	1
Preocupación	1	Confidencialidad	2
Exposición	0	Privacidad	0
Anomalía	0	Integridad	1
		Alarma	2
OpSec	8,10	Controles Verdaderos	5,10
Limitaciones	7,35	Seguridad Δ	-10,36

Protección Verdadera	89,64	Seguridad Actual	89,45

Informe de la entrevista sobre la seguridad del canal Telecomunicaciones en la UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Entrevistador: Anderson Humberto Aza Mimalchi	**Entrevistado: Ing. Javier Torres**
Técnica: Entrevista	**Fecha: 07/03/2018**
Firma del Representante:	**Sello de la institución:**

El objetivo de la entrevista es obtener información de la seguridad en la red inalámbrica de la Universidad Politécnica Estatal del Carchi y se realiza como parte de la auditoria que se está llevando a cabo.

PREGUNTAS REALIZADAS

a. ¿Utilizan telefonía IP en la institución?

b. ¿Usan buzón de voz en la institución?

c. ¿Tienen RAS en la institución?

d. ¿Poseen RDSI, Narración IP o redes X.25 en la institución?

e. ¿Qué servicios son accesibles desde fuera de la institución?

f. ¿Se puede controlar el abuso de recursos en la telefonía IP?

g. ¿Utilizan autenticación para los servicios que utilizan?

h. ¿Cómo se realiza la transmisión de contraseñas?

i. ¿Tienen habilitados controles de seguridad en sus servicios?

j. ¿Aplican calidad de servicio en sus servicios?

k. ¿Poseen políticas de seguridad?

CONCLUSIONES

Luego de realizar la entrevista, se puede apreciar que el único servicio que se posee la institución en este canal es la telefonía IP, el cual es accesible mediante contraseña y solo dentro de la institución. Sin embargo no se puede controlar el abuso de recursos pues el personal de la institución puede usar el servicio para uso personal. Este servicio se encuentra gestionado con QoS en una Vlan independiente.

Por otra parte los servicios que poseen tienen contraseña la cual se transmite de forma personal, para evitar que personas no autorizadas accedan a estos servicios prestados por la institución.

Anexo 13: Reporte del Canal Redes de Datos de la UPEC

Reporte de la Prueba de Redes de Datos

Certificación de la Verificación de Seguridad OSSTMM 3.0

ID del Auditor	040187309-6	Fecha	19/03/2018
Auditor Principal	Anderson Humberto Aza M.	Duración de la Prueba	Dos semanas
Alcance y Relación	Equipos de comunicación de la UPEC	Vectores	DATA CENTER
Canales	Redes de Datos	Tipo de Prueba	Software de auditoria

Soy responsable de la información contenida en este reporte y he verificado personalmente que toda la información es fundamentada y verdadera

FIRMA DE RESPONSABLE

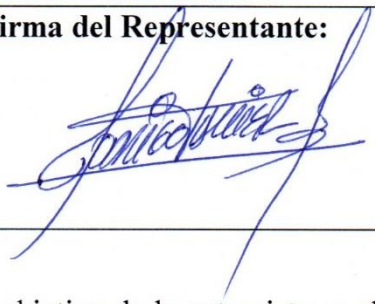
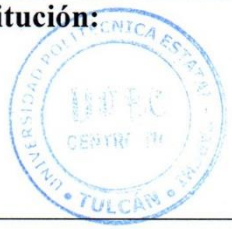
SELLO DE LA INSTITUCIÓN

Observaciones: Se anexa la entrevista realizada al administrador de red

VALORES DE LA SEGURIDAD OPERACIONAL		VALORES DE LOS CONTROLES	
Visibilidad	4	Autenticación	3
Acceso	3	Indemnización	0
Confianza	2	Resistencia	3
VALORES DE LAS LIMITACIONES		Subyugación	0
Vulnerabilidad	1	Continuidad	1
Debilidad	3	No-Repudio	1
Preocupación	2	Confidencialidad	1
Exposición	1	Privacidad	1
Anomalía	1	Integridad	1
		Alarma	0
OpSec	8,73	Controles Verdaderos	4,18
Limitaciones	12,87	Seguridad Δ	-17,42

Protección Verdadera	82,58	Seguridad Actual	82,80

Informe de la entrevista sobre la seguridad del canal Inalámbrico en la UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Entrevistador: Anderson Humberto Aza Mimalchi	**Entrevistado: Ing. Javier Torres**
Técnica: Entrevista	**Fecha: 21/02/2018**
Firma del Representante: 	**Sello de la institución:** 

El objetivo de la entrevista es obtener información de la seguridad en la red inalámbrica de la Universidad Politécnica Estatal del Carchi y se realiza como parte de la auditoria que se está llevando a cabo.

PREGUNTAS REALIZADAS

a. ¿Hacen uso de VPN para conexiones remotas'

b. ¿En el firewall se encuentran filtrados los puertos?

c. ¿Tienen servicios contratados?

d. ¿Qué correo electrónico utilizan?

e. ¿Cómo es la conexión del Data Center a los edificios de la universidad?

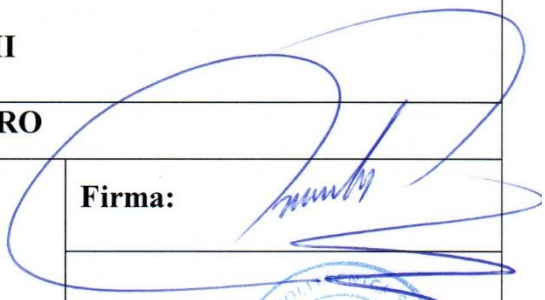
f. ¿Posen antivirus de paga en las estaciones de trabajo?

CONCLUSIONES

La institución posee VPN para acceder remotamente a su red interna, por otra parte en el firewall no filtran los puertos localmente por lo cual son vulnerables a sufrir posibles ataques. Cabe mencionar que el servicio de DNS es contratado por lo cual se encuentra fuera de la red interna, de igual forma que el correo electrónico.

Para conectar los edificios con el datacenter se hace uso de fibra óptica con el fin de evitar los cuellos de botella, lo cual es muy provechoso para la institución.

Anexo 14: Informe Final de la Auditoria

INFORME FINAL DE LA AUDITORÍA DE SEGURIDAD INFORMÁTICA EN LA UNIVERSIDAD POLITECNICA ESTATAL DEL CARCHI		
Revisado por:	**ING. ANDRÉS GUERRERO**	
Aprobado por:	**ING. ANDRÉS GUERRERO**	**Firma:**  **Sello:** 
Elaborado por:	**ANDERSON AZA**	

1. Introducción

La auditoría se realizó con el fin de detectar vulnerabilidades en la red interna de la Institución, pues debido a que existen muchas personas mal intencionadas (Hackers), que se dedican a explotar las debilidades de seguridad informática en la red, los cuales pueden obtener información confidencial de la institución o denegar los servicios informáticos que la universidad ofrece. La auditoría se realizó en base a la metodología OSSTMMv3, con lo cual se analizaron 5 canales, los cuales son: Humano, Físico, Inalámbrico, Telecomunicaciones y Redes de Datos.

En el presente documento se detallan las resultados finales obtenidos luego de realizar la auditoria de seguridad informática en la red interna de la Universidad Politécnica Estatal del Carchi.

2. Actividades realizadas

Para el desarrollo de la auditoria se utilizaron las siguientes métricas operacionales:

- **Canal Humano**

Para el canal humanos las principales actividades que se desarrollaron son las siguientes:

- Detectar el personal autorizado para acceder a las diferentes áreas de la institución.
- Detectar si se requiere autenticación para interactuar con los activos de la institución.
- Intentar acceder a los racks de comunicación sin ningún tipo de autorización.
- Detallar los privilegios que son requeridos para ingresar al Data Center
- Investigar si los documentos internos llevan firmas y sellos con el fin de evitar falsificaciones.
- Observar si se posee un número de guardias adecuado y si poseen sistema de video vigilancia.

- **Canal Físico**

En el canal Físico las principales actividades desarrolladas son las siguientes:

- Detectar los objetivos dentro y fuera del alcance de la Institución.
- Tratar de encontrar la ubicación de los activos más importantes de la institución.
- Detectar las normas de seguridad que se tienen para asegurar los activos de la institución.
- Determinar los tipos de autorización que se requieren para tener acceso a la red interna de la institución

- Investigar si los activos pueden ser llevados fuera de institución sin solicitar ningún tipo de permiso.
- Verificar si se da un mantenimiento adecuado a los equipos informáticos de la institución.
- Verificar los métodos que se poseen para detectar la intrusión de personas indebidas.
- Detectar las fallas que se poseen para tener asegurados los activos de la institución.

➢ **Canal Inalámbrico**

Las actividades que se llevaron a cabo se detallan a continuación:

- Detectar el control de acceso que se lleva a cabo en la red inalámbrica.
- Indagar si existen fuentes no autorizadas.
- Investigar la autenticación que es requerida para acceder a la red Wi-Fi de la institución.
- Investigar si lo AP utilizados son lo bastante robustos para uso institucional.
- Revisar si se posee control de ancho de banda n cada red Wi-Fi.
- Comprobar si se puede monitorear las estaciones que acceden a la red Wi-Fi.
- Revisar si las redes Wi-Fi pueden ser vulneradas.

➢ **Canal Telecomunicaciones**

Para el canal telecomunicaciones las principales actividades que se realizaron son las siguientes:

- Se detectó los servicios que se utilizan en la institución.

- Detectar la manera de acceder a los servicios y si esta es segura.
- Detectar los métodos de autenticación
- Revisar el uso que se le da a los servicios que presta la institución.
- Revisar si se aplica QoS y si estos servicios están en una Vlan independiente.
- Detectar si los teléfonos IP pueden ser intervenidos.

➢ **Canal Redes de Datos**

Para el canal redes de datos las principales actividades que se realizaron son las siguientes:

- Identificar el segmento de red utilizado.
- Verificar los protocolos utilizados.
- Verificar respuestas ICMP a los objetivos.
- Revisar los puertos que se encuentran abiertos.
- Revisar el tipo de contraseñas que se usan.
- Revisar si el servidor web utiliza certificados SSL.
- Revisar si las interacciones de la red son registradas.
- Revisar si la institución posee sistema de detección de intrusos IDS o sistema de prevención de intrusos IPS.

3. Resultados

➢ **Canal Humano**

Luego de ingresar los valores obtenidos en la calculadora RAV, se obtienen que la Seguridad Actual de la UPEC en el canal Humano es de 85,53 RAVS, lo que se interpreta

en que se posee una deficiencia de aproximadamente el 15%, lo cual no significa que la institución vaya a ser atacada, sino que muestra la vulnerabilidad de la institución en caso de un ataque. Los motivos principales para tener una deficiencia que supere el 10% es que los controles para la indemnización, subyugación y continuidad son prácticamente nulos, por lo cual deben ser los controles que se aborden con mayor prioridad.

Por otra parte la Seguridad Δ, toma un valor negativo de -14,35, este valor es interpretado como la insuficiencia de controles que posee la institución en cuanto al talento humano, además muestra que los controles que se encuentran aplicados tienen falencias por lo cual necesitan ser mejorados para que estos se adecúen a las necesidades de seguridad que la universidad requiere.

- **Canal Físico**

Luego de ingresar los valores obtenidos en la calculadora RAV, se obtienen que la Seguridad Actual de la UPEC en el canal Físico es de 80,19 RAVS, lo que se interpreta en que se posee una deficiencia de aproximadamente el 20%, con lo cual se interpreta que la vulnerabilidad que tiene la institución en caso de un ataque es bastante elevada. Los motivos principales para tener una deficiencia que supere el 10% es que los controles para la autenticación, No-repudio y alarma son escasos, por lo cual deben ser los controles que se aborden con mayor prioridad.

Por otra parte la Seguridad Δ, toma un valor negativo de -19,74, este valor es interpretado como la insuficiencia de barreras físicas para proteger los activos de la institución, además muestra que los controles que se encuentran aplicados tienen falencias por lo cual necesitan ser mejorados para que estos cubran de manera eficiente los activos que posee la universidad.

- **Canal Inalámbrico**

Luego de ingresar los valores obtenidos en la calculadora RAV, se obtiene que la Seguridad Actual de la UPEC en el canal Inalámbrico es de **82,27 RAVS**, lo que se interpreta en que se posee una deficiencia de aproximadamente el 18%, esto debido a que la vulnerabilidad de las comunicaciones inalámbricas. Una de las principales causas es el uso de AP residenciales. Los controles para la indemnización, subyugación, confidencialidad, privacidad y alarma son prácticamente nulos, por lo cual deben ser los controles que se aborden con mayor prioridad.

Por otra parte la **Seguridad Δ,** toma un valor negativo de **-14,35,** este valor es interpretad como la insuficiencia de controles que posee la institución en cuanto al talento humano, además muestra que los controles que se encuentran aplicados tienen falencias por lo cual necesitan ser mejorados para que estos se adecúen a las necesidades de seguridad que la universidad requiere.

- **Canal Telecomunicaciones**

Luego de ingresar los valores obtenidos en la calculadora RAV, se obtienen que la Seguridad Actual de la UPEC en el canal Telecomunicaciones es de 89,45 RAVS, este valor es relativamente aceptable, esto debido a que solo se posee un servicio para este canal. Se posee una deficiencia de aproximadamente el 11%, esto debido a que los controles para la resistencia y la privacidad son prácticamente nulos, por lo cual deben ser los controles que se aborden con mayor prioridad.

Por otra parte la Seguridad Δ, toma un valor negativo de -10,36, un valor que es negativo pero no tan alarmante, esto como consecuencia de tener un solo servicio, sin embargo los

controles que se encuentran aplicados tienen falencias por lo cual necesitan ser mejorados para que estos se adecúen a las necesidades de seguridad que la universidad requiere.

- **Canal Redes de Datos**

Luego de ingresar los valores obtenidos en la calculadora RAV, se obtienen que la Seguridad Actual de la UPEC en el canal Redes de Datos es de 82,80 RAVS, lo que se interpreta en que se posee una deficiencia de aproximadamente el 19%, que es la vulnerabilidad que tienen la institución en caso de sufrir un ataque. Los motivos principales para tener una deficiencia que supere el 10% es que los controles para la indemnización, subyugación y alarma son prácticamente nulos, por lo cual deben ser los controles que se aborden con mayor prioridad.

Por otra parte la Seguridad Δ, toma un valor negativo de -17,42, este valor es interpretado como la insuficiencia de controles que posee la institución en cuanto al canal redes de datos, además muestra que los controles que se encuentran aplicados tienen falencias por lo cual necesitan ser mejorados para que la institución tenga una buna seguridad en caso de sufrir ataques de seguridad.

Anexo 15: Registro del personal al cual fueron impartidas las falencias y políticas de seguridad

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

REGISTRO DEL PERSONAL AL CUAL FUERON IMPARTIDAS LAS FALENCIAS Y LAS POLITICAS DE SEGURIDAD

Nombres	Apellidos	Firma
Omar Darwin	Guerrero Pozo	
JAVIER TORRES	TORRES BOLAÑOS	
Edison Manuel	Tarapues Quespaz	
Samanta Gabriela	Pozo Guerron	

Sello de la institución:

Anexo 16: Hoja de Registro de acceso a Laboratorios

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Registro de Acceso a los laboratorios

Fecha	Hora	Docente	Laboratorio	Firma

Anexo 17: Hoja de Registro de acceso a Data Center y Racks

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI Registro de Acceso a los Data Center y Racks					
Fecha	**Hora**	**Nombre**	**Área**	**Motivo**	**Firma**

Anexo 18: Ficha de mantenimiento de equipos informáticos

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI FICHA DE MANTENIMIENTO DE EQUIPOS INFORMÁTICOS			
Responsable:		**Fecha Mantenimiento:**	
INFORMACIÓN DEL EQUIPO			
Tipo			
Modelo			
N° de serie			
Estado actual:			
Procedimientos de Software realizados:			
Procedimientos de Hardware realizados:			
Observaciones:			
Firma:		**Sello:**	

Anexo 19: Formulario para dar de baja equipos informáticos

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI FORMULARIO PARA DAR DE BAJA EQUIPOS INFORMÁTICOS DAÑADOS	
RESPONSABLE:	
FECHA:	
EQUIPO DEFECTUOSO:	
NUMERO DE SERIE:	
PROCEDIMIENTOS REALIZADOS:	
RAZONES PARA DAR DE BAJA:	
FIRMA:	**SELLO:**

Anexo 20: Ficha posterior al acceso al Data Center

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI FICHA POSTERIOR AL ACCESO AL DATA CENTER	
Visitante:	
Correo:	
Teléfono:	
Fecha de acceso:	
Hora de ingreso:	
Motivos de acceso al Data Center:	
Actividades realizadas:	
Hora de salida:	
Persona que supervisó la visita:	
Firma Visitante:	**Firma Supervisor:**

Anexo 21: Formulario de registro de equipo para acceso al firewall

	UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI **FORMULARIO DE REGISTRO DE EQUIPO PARA ACCESO AL FIREWALL DE LA UPEC**					
Tipo de Solicitud: (Marque con una X)	**Nueva:**		**Modificación:**			
Solicitante:						
Correo:		**Teléfono:**				
Equipo:						
Ubicación:						
Sistema Operativo:						
Dirección IP:						
Servicios Solicitados:	**LAN**		**WAN**			
	Servicios	**Puertos**	**Servicios**	**Puertos**		
Usos que se le va a dar al equipo:						
Firma del Solicitante:						
Fecha de entrega:						
Tiempo de registro:						
PARA USO DEL DEPARTAMENTO DE TIC´s						
Resolución de Aprobación:	**Aprobado:**		**No aprobado:**			
Observaciones:						
Fecha de Resolución:						
Firma Director Departamento de TIC´s:		**Sello:**				

Anexo 22: Formulario de registro para acceder a la red inalámbrica

<table>
<tr><td colspan="3">UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FORMULARIO DE REGISTRO PARA ACCEDER A LA RED INALÁMBRICA DE LA UPEC</td></tr>
<tr><td>Instrucciones generales:</td><td colspan="2">Presentar la clave de acceso que se desea para la red de estudiantes.
La clave debe contener mínimo 8 caracteres, combinando números, letras y por lo menos 1 carácter especial.
Llenar el formulario según corresponda
Presentar el formulario en el departamento de TIC’s</td></tr>
<tr><td>Términos de uso:</td><td colspan="2">Para la utilización de la red inalámbrica, se debe ser parte de la institución, con excepción de la red inalámbrica para invitados.
No se debe hacer uso indebido de la red inalámbrica de la institución.
en caso de anomalías el departamento de TIC´s puede suspender el acceso a la red inalámbrica.</td></tr>
<tr><td colspan="3">Datos Generales</td></tr>
<tr><td>Nombres:</td><td colspan="2"></td></tr>
<tr><td>Cédula:</td><td colspan="2"></td></tr>
<tr><td>Facultad/Carrera:</td><td colspan="2"></td></tr>
<tr><td>Correo Institucional:</td><td colspan="2"></td></tr>
<tr><td>Teléfono:</td><td colspan="2"></td></tr>
<tr><td>Datos estudiantes:</td><td>Clave de Acceso:</td><td></td></tr>
<tr><td rowspan="4">Datos personal Administrativo:</td><td>Dependencia:</td><td></td></tr>
<tr><td>Cargo:</td><td></td></tr>
<tr><td>Dirección MAC 1:</td><td></td></tr>
<tr><td>Dirección MAC 2:</td><td></td></tr>
<tr><td colspan="3"></td></tr>
<tr><td rowspan="3">Datos docentes:</td><td>Nombramiento/Contrato:</td><td></td></tr>
<tr><td>Dirección MAC 1:</td><td></td></tr>
<tr><td>Dirección MAC 2:</td><td></td></tr>
</table>

Anexo 23: Autorización de Acceso

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Ley No. 2006-36 Publicada en el Segundo Suplemento del Registro Oficial No. 244 del 5 de abril del 2006

Memorando N°. UPEC–CTIC - 2017–275-M

Tulcán, 18 de Septiembre del 2017

***ASUNTO**: Carta de Aceptación.*

Ing. Daniel Jaramillo

COORDINADOR DE LA CARRERA DE INGENIERIA EN ELECTRONICA Y REDES DE COMUNICACIÓN.

De mi consideración:

Me dirijo a usted, en la oportunidad de aceptar al señor **Aza Mimalchi Anderson Humberto**, C.I **0401873096**, estudiante de la **Universidad Técnica del Norte,** de la carrera de **Ingeniería en Electrónica y Redes de Comunicación**, para realizar su tema de investigación **"AUDITORIA DE SEGURIDAD INFORMATICA EN LA RED INTERNA DE LA UNIVERSIDAD POLITECNICA ESTATAL DEL CARCHI"** y que además pueda tener acceso a la infraestructura de la red interna de la UPEC, en el Centro de TIC en la Unidad de Redes y Telecomunicaciones, bajo la supervisión del Ing. Javier Torres.

Particular que informo para los fines pertinentes.

Atentamente,

Ing. Andrés Guerrero.

DIRECTOR DEL CENTRO DE TIC DE LA UPEC

"EDUCACIÓN PARA EL DESARROLLO Y LA INTEGRACIÓN"

Av. Universitaria y Antisana Telfs: (06) 2224-079 / 2224-080 Fax ext.: 1313
www.upec.edu.ec e-mail: info@upec.edu.ec

Anexo 24: Oficio de solicitud de Acceso

UNIVERSIDAD TÉCNICA DEL NORTE
UNIVERSIDAD ACREDITADA RESOLUCIÓN 002-CONEA-2010-129-DC
Resolución N° 001-073-CEAACES-2013-13

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS
CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

Ibarra, 04 de septiembre del 2017
Oficio UTN-CIERCOM-2017-110

Doctor
Hugo Ruiz
RECTOR UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
Tulcán

Cordial Saludo:

Solicito de la manera más comedida, se digne autorizar para que el señor Anderson Humberto Aza Mimalchi, portador de la cédula de ciudadanía 040187309-6, alumno de la carrera de Ingeniería en Electrónica y Redes de Comunicación, tenga acceso a la infraestructura de la red interna de la universidad, bajo la supervisión del departamento de TICs, con la finalidad que pueda desarrollar su tema de investigación: "AUDITORÍA DE SEGURIDAD INFORMÁTICA EN LA RED INTERNA DE LA UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI, BASADA EN LA NORMA ISO/IEC 27001 Y LA METODOLOGÍA OSSTMMv3". El docente que supervisará el desarrollo de esta actividad es el ingeniero Edgar Maya, Director de tesis.

Por su gentileza en atender este pedido, le agradezco inmensamente.

Atentamente,

CIENCIA Y TÉCNICA AL SERVICIO DEL PUEBLO

INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN
CIERCOM
COORDINACIÓN

Ing. Daniel Jaramillo V.
COORDINADOR

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
INGRESO DE DOCUM.
Fecha: 14-09-2017
Procedencia: UTN
Hora: 9:40
Recibido por:

Copia: Ing. Edgar Maya
Silvia

Anexo 25: Checklist de las políticas de seguridad luego de ser aplicadas

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CACHI CHECKLIST POLITICAS DE SEGURIDAD UPEC					
Elaborado por:	**Anderson Aza**		**Fecha:**	**25/02/2019**	
Políticas Evaluadas	**¿Se están aplicando?**		**¿Se pueden Eludir?**		**Observación**
	SI	**NO**	**SI**	**NO**	
Art 5		✓	✓		
Art 7	✓			✓	
Art 9	✓			✓	
Art 15	✓		✓		
Art 18	✓			✓	
Art 20	✓		✓		
Art 25	✓			✓	
Art 26	✓		✓		
Art 29	✓			✓	
Art 30	✓			✓	
Art 31	✓			✓	
Art 35		✓	✓		
Art 38	✓			✓	
Art 40	✓			✓	
Art 41	✓			✓	
Art 42	✓			✓	
Art 50	✓			✓	

Art 51	✓		✓		
Art 57	✓			✓	
Art 58	✓			✓	
Art 59	✓			✓	
APROBADO POR: **ING. ANDRES GUERRERO**					
FIRMA:			**SELLO:**		

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CACHI

CHECKLIST POLITICAS DE SEGURIDAD UPEC

Elaborado por:	**Anderson Aza**		**Fecha:**	**27/02/2019**	
Políticas Evaluadas	**¿Se están aplicando?**		**¿Se pueden Eludir?**		**Observación**
	SI	**NO**	**SI**	**NO**	
Art 5		✓	✓		Los empleados cambiaron claves sin cumplir el art.
Art 7	✓			✓	
Art 9	✓			✓	
Art 15	✓		✓		
Art 18	✓			✓	
Art 20	✓		✓		Aun tienen las claves pegadas
Art 25	✓			✓	
Art 26	✓		✓		
Art 29	✓			✓	
Art 30	✓			✓	
Art 31	✓			✓	
Art 35		✓	✓		
Art 38	✓			✓	
Art 40	✓			✓	
Art 41	✓			✓	
Art 42	✓			✓	
Art 50	✓			✓	
Art 51	✓		✓		

Art 57	✓			✓	
Art 58	✓			✓	
Art 59	✓			✓	
APROBADO POR: **ING. ANDRES GUERRERO**					
FIRMA:			**SELLO:**		

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CACHI CHECKLIST POLITICAS DE SEGURIDAD UPEC					
Elaborado por:	**Anderson Aza**		**Fecha:**	**07/03/2019**	
Políticas Evaluadas	**¿Se están aplicando?**		**¿Se pueden Eludir?**		**Observación**
	SI	**NO**	**SI**	**NO**	
Art 5	✓		✓		
Art 7	✓			✓	
Art 9	✓			✓	
Art 15	✓		✓		
Art 18	✓			✓	
Art 20	✓		✓		
Art 25	✓			✓	
Art 26	✓		✓		
Art 29	✓			✓	
Art 30	✓			✓	
Art 31	✓			✓	
Art 35		✓	✓		
Art 38	✓			✓	
Art 40	✓			✓	
Art 41	✓			✓	
Art 42	✓			✓	
Art 50	✓			✓	
Art 51	✓		✓		

Art 57	✓			✓	
Art 58	✓			✓	
Art 59	✓			✓	
APROBADO POR: **ING. ANDRES GUERRERO**					
FIRMA:			**SELLO:**		

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CACHI

CHECKLIST POLITICAS DE SEGURIDAD UPEC

Elaborado por:	**Anderson Aza**		**Fecha:**	**08/03/2019**	
Políticas Evaluadas	**¿Se están aplicando?**		**¿Se pueden Eludir?**		**Observación**
	SI	**NO**	**SI**	**NO**	
Art 5	✓			✓	Algunos empleados hacen caso omiso
Art 7	✓			✓	
Art 9	✓			✓	
Art 15	✓		✓		No se puede entrodar a todo el personal
Art 18	✓			✓	
Art 20	✓		✓		Algunos empleado aun pegan las claves
Art 25	✓			✓	
Art 26	✓		✓		
Art 29	✓			✓	
Art 30	✓			✓	
Art 31	✓			✓	
Art 35		✓	✓		No hay presupuesto
Art 38	✓			✓	
Art 40	✓			✓	
Art 41	✓			✓	
Art 42	✓			✓	
Art 50	✓			✓	
Art 51	✓		✓		

Art 57	✓			✓	
Art 58	✓			✓	Se están migrando los servidores y se reconfigurará el firewall
Art 59	✓			✓	
APROBADO POR: **ING. ANDRES GUERRERO**					
FIRMA:			**SELLO:**		