UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

APLICACIÓN DE LA METODOLOGÍA OSSTMM PARA LA SEGURIDAD DE LA RED INALÁMBRICA DE LA UNIVERSIDAD TÉCNICA DEL NORTE MEDIANTE HERRAMIENTAS DE KALI LINUX

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS COMPUTACIONALES

Autor:

Jhomar Klever Narváez Bonilla

Director:

Ing. Marco Remigio Pusdá Chulde Msc.

Ibarra, 2019

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

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

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO	
CÉDULA DE IDENTIDAD:	100381124-5
APELLIDOS Y NOMBRES:	Narváez Bonilla Jhomar Klever
DIRECCIÓN:	Ibarra, Calle 17 de julio
EMAIL:	jknarvaezb@utn.edu.ec
TELÉFONO MÓVIL:	0990890326

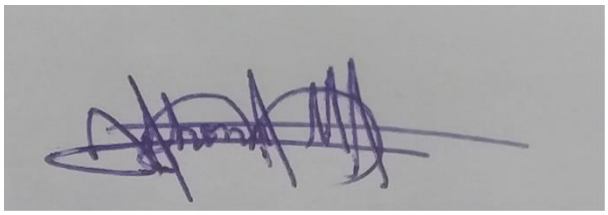
DATOS DE LA OBRA	
TÍTULO:	APLICACIÓN DE LA METODOLOGÍA OSSTMM PARA LA SEGURIDAD DE LA RED INALÁMBRICA DE LA UNIVERSIDAD TÉCNICA DEL NORTE MEDIANTE HERRAMIENTAS DE KALI LINUX
AUTOR:	Narváez Bonilla Jhomar Klever
FECHA:	Junio 2019
PROGRAMA:	☒ **PREGRADO** ☐ **POSGRADO**
TITULO POR EL QUE OPTA:	INGENIERÍA EN SISTEMAS COMPUTACIONALES
ASESOR /DIRECTOR:	ING. MARCO REMIGIO PUSDÁ CHULDE MSC.

2. CONSTANCIAS

El autor 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 el titular 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.

Ibarra, a los 4 días del mes de junio de 2019.

EL AUTOR:



_____

Narváez Bonilla Jhomar Klever

CERTIFICACIÓN

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN DEL DIRECTOR DEL TRABAJO

MSc. Marco Pusdá, DIRECTOR DEL PRESENTE TRABAJO DE TITULACIÓN

Certifico:

Que, el presente trabajo de titulación **"APLICACIÓN DE LA METODOLOGÍA OSSTMM PARA LA SEGURIDAD DE LA RED INALÁMBRICA DE LA UNIVERSIDAD TÉCNICA DEL NORTE MEDIANTE HERRAMIENTAS DE KALI LINUX"** fue realizado en su totalidad por la Sr. Jhomar Klever Narváez Bonilla, bajo mi supervisión.

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

MSc. Marco Pusdá

DIRECTOR DE TESIS

CERTIFICACIÓN

UNIVERSIDAD TECNICA DEL NORTE

Universidad Acreditada resolución 002-CONEA-2010-129-DC

Resolución No. 001-073-CEAACES-2013-13

DIRECCION DE DESARROLLO TECNOLOGICO E INFORMATICO

DIRECTOR DE LA DIRECCIÓN DE DESARROLLO TECNOLÓGICO E INFORMÁTICO

CERTIFICA

QUE: El señor JHOMAR KLEVER NARVAEZ BONILLA con cédula identidad 1003811245 estudiante de la Facultad de Ingeniería en Ciencias Aplicadas – de la Carrera de Ingeniería en Sistemas Computacionales, ha desarrollado con los datos entregados de la Dirección de Desarrollo Tecnológico e Informático, el Proyecto de Tesis "**APLICACIÓN DE LA METODOLOGÍA OSSTMM PARA LA SEGURIDAD DE LA RED INALÁMBRICA DE LA UNIVERSIDAD TÉCNICA DEL NORTE, MEDIANTE HERRAMIENTAS DE KALI LINUX".**

QUE: El estudio del proyecto fue entregado al Ingeniero Vinicio Guerra – Analista de Redes de la Dirección de Desarrollo Tecnológico e Informático el 20 de mayo del 2019.

Es todo cuanto puedo certificar, facultando al interesado hacer uso de este certificado como estime conveniente, excepto para trámites judiciales.

Ibarra, 23 de mayo del 2019

Atentamente
CIENCIA Y TECNICA AL SERVICIO DEL PUEBLO

UNIVERSIDAD TECNICA DEL NORTE
IBARRA - ECUADOR
DEPARTAMENTO DE INFORMATICA

Ing. Juan Carlos García
DIRECTOR

Av. 17 de Julio 5 – 21 y José María Córdova
Ciudadela Universitaria Barrio El Olivo
Teléfono: (06) 2997800 ext. 7040 Casilla 199
www.utn.edu.ec
Ibarra - Ecuador

DEDICATORIA

Dedico este trabajo de titulación, en primera instancia al Todopoderoso quien me ha dado la fortaleza suficiente para poder seguir adelante, inclusive en los momentos más difíciles, cuando he estado a punto de caer él me ha dado la fortaleza para continuar; a mi madre Esther Bonilla, mi padre Isidro Narváez quienes me inculcaron valores y nunca dejaron de apoyarme para que el cumplimento de este objetivo se hiciera realidad. A mis hermanos y hermanas Víctor, Manolo, Silvia, Fernanda, Mayra quienes siempre han sido un ejemplo en mi vida, que con su, apoyo y preocupación han estado a mi lado siempre. Y por último pero no menos importante, a Carolina quien ha estado, siempre inquebrantable a mi lado, dándome todo su apoyo, comprensión y cariño, alguien que le da a la palabra amor y compañía un nuevo significado.

AGRADECIMIENTOS

Agradezco a la Universidad Técnica del Norte por brindarme conocimientos a través de los profesores que con su profesionalismo y dedicación impartieron enseñanzas a lo largo de la carrera.

Mi agradecimiento a personas que con su don de gente supieron orientarme en la construcción y desarrollo del Tema de este trabajo, me refiero a Ing. Vinicio Gerra Administrador de Redes y Comunicaciones del Departamento DDTI y mi Tutor Ing. Marco Pusdá por el apoyo, confianza y la orientación investigativa y arquitectura de las ideas plasmadas en el desarrollo de esa idea que da su génesis en la presente Tesis.

Un especial agradecimiento a mis compañeros, amigos que he podido cultivar en la universidad quienes con su pensamiento y confianza han depositado en mí, la más grande fortuna, su amistad y fraternidad.

RESUMEN

El presente proyecto consiste en la realización de una auditoria de seguridad informática para la red inalámbrica de la Universidad Técnica del Norte, siguiendo la metodología OSSTMM en su versión 3 y utilizando herramientas del sistema operativo Kali Linux, con el objetivo de detectar posibles vulnerabilidades y deficiencias en la infraestructura tecnológica de la red inalámbrica.

En el primer capítulo, se presenta la fundamentación teórica en la que se describen los aspectos importantes de la seguridad informática y la metodología OSSTMM versión 3 y otros fundamentos relacionados con la seguridad informática.

En el segundo capítulo, se describe las herramientas de Kali Linux a ser utilizadas para cumplir los objetivos de este trabajo.

En el tercer capítulo, se analiza, aplica y documenta el proceso de la metodología OSSTMM versión 3 utilizando herramientas de Kali Linux.

En el cuarto capítulo, se detallan los resultados obtenidos en la aplicación de la metodología OSSTMM v3 y las herramientas de Kali Linux con las vulnerabilidades y deficiencias encontradas y las posibles medidas correctivas a implementar dentro de la institución.

Al final del documento se presentan las conclusiones y recomendaciones que se basan en los resultados obtenidos de las pruebas de seguridad de la red.

PALABRAS CLAVES: Osstmm, Kali Linux, rav, seguridad informática, vulnerabilidades.

ABSTRACT

The present project consists in the realization of a computer security audit for the informatic security of the Técnica del Norte University, following the methodology OSSTMM in its version 3 and using tools of the operating system Kali Linux, with the Objective of detecting possible vulnerabilities and weaknesses in the technological infrastructure of the wireless network.

The first chapter describes, the theoretical foundation in which describes the important aspects of informatic security and methodology OSSTMM version 3 and other fundaments related to computer security.

In the second chapter, it describes the tools of Kali Linux to be used to fulfill the objectives of this work.

In the third chapter, it analyzes, applies and documents the process of the methodology OSSTMM version 3 using tools of Kali Linux.

In the fourth chapter, there are detailed the results obtained in the application of the methodology OSSTMM v3 and the tools of Kali Linux with the vulnerabilities and weaknesses found and the possible remedial measures to implement within the institution.

At the end of the document presents the conclusions and recommendations that are based on the obtained results of the tests for network security.

Key words: Osstmm, Kali Linux, rav, Informatic security, vulnerabilities.

Tabla de contenido

Índice de Tablas

Índice de Figuras

Introducción

1.1 Antecedentes

La seguridad informática, se define como un conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información, dentro de la seguridad informática podemos encontrar elementos y técnicas tanto hardware, como software, así como dispositivos físicos y medios humanos (María Ramos & hurtado, 2011).

Debido al uso de la red inalámbrica con frecuencia conlleva asumir riesgos asociados con la interferencia de la señal, tales como la interceptación y la intrusión, los mismos que pueden quebrantar la seguridad de una red inalámbrica (Touhill & Touhill, 2014).

El Manual de la Metodología Abierta de Testeo de Seguridad (OSSTMM), metodología del Institute for Security and Open Methodologies (ISECOM) permite evaluar la seguridad en redes con testeos de intrusión, a través de Hacking Ético (Walker, 2016).

Kali Linux es una distribución derivada de Debian, un sistema operativo de distribución libre. Especializado en pruebas de penetración (pentesting), provee software para auditar la seguridad de una red o el equipo en el que se ejecuta, y analiza los resultados después del ataque (lo que es conocido como informática forense) (Hertzog & Mas, 2016).

1.2 Situación actual

En la actualidad las empresas tienen que hacer frente a una mayor demanda de accesos inalámbricos, ya sea por parte de clientes, proveedores o empleados. Desafortunadamente, las redes inalámbricas son el elemento más vulnerable de la infraestructura de TI (CARPENTIER, 2016).

Actualmente en la red inalámbrica de la Universidad Técnica del Norte permite conectar a cualquier dispositivo inalámbrico que capte la señal de un AP (Punto de acceso inalámbrico), lo que posibilita la navegación gratis en la Internet, pero a la vez, la conectividad de los usuarios dificulta el acceso a los servicios en línea en ciertos periodos de tiempo, desconociendo las causas de la interrupción de la red.

El crecimiento de aplicaciones de escritorio, aplicaciones web, incremento de usuarios en la universidad, hace que la red este expuesta a posibles ataques informáticos, y como resultado a daños graves o irreversibles a los servicios, equipos informáticos y perdida de información. generando inconformidad en los usuarios.

1.3 Justificación

Justificación tecnológica.

Teniendo en cuenta que la tecnología es dinámica y completamente cambiante, un análisis necesita ser reforzado después de un periodo máximo de doce meses, si se hacen cambios, aunque sean mínimos, a nivel de software, hardware o de infraestructura tecnológica, o incluso, si se llega a cambiar de personal, es necesario que como medida preventiva se realicen nuevamente las pruebas de penetración con el fin de garantizar la máxima seguridad en la institución, independientemente del tiempo transcurrido desde la última vez (Vieites, 2014).

Justificación teórica.

Ejemplificar el estado de las medidas de seguridad en redes inalámbricas mediante la metodología abierta de testeo de seguridad OSSTMM, y de esta manera encontrar los puntos más vulnerables y poder recomendar las medidas correctivas necesarias que permitan mejorar la eficiencia de la red.

1.4 Problema

¿Qué tipo de vulnerabilidades existen en la red inalámbrica de la Universidad Técnica del Norte?, Figura 1.

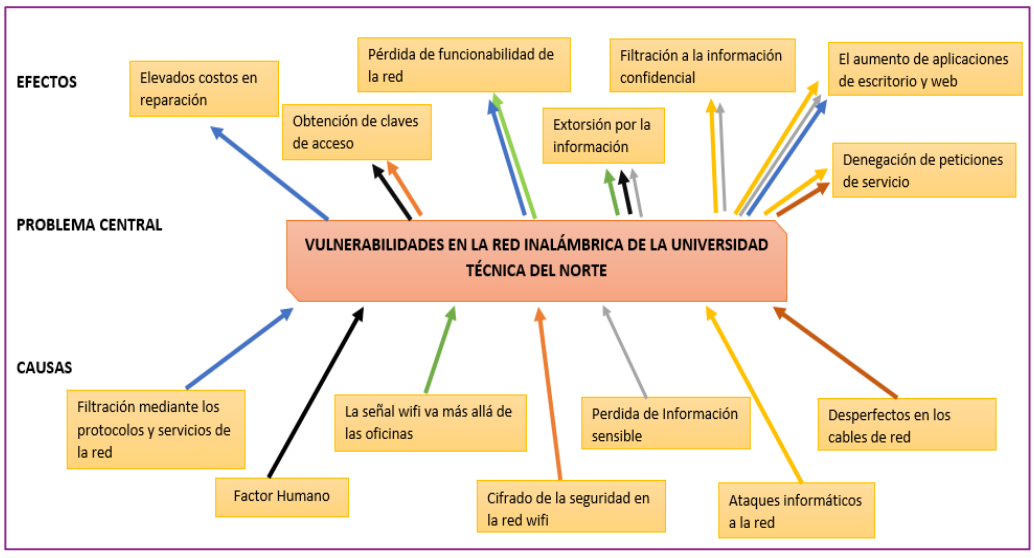


Fig. 1. Árbol de Problemas

Fuente: Propia

1.5 Objetivo

Aplicar la metodología OSSTMM para la verificación de la seguridad en la red inalámbrica de la Universidad Técnica del Norte.

1.5.1 Objetivos Específicos

- Identificar y fundamentar los conceptos que se relacionan con seguridad en redes.
- Definir las herramientas de Kali Linux con mayor adaptabilidad basadas en la metodología OSSTMM.
- Reconocer las amenazas, vulnerabilidades y riesgos de la red inalámbrica de la Universidad Técnica del Norte.
- Elaboración de un documento con los hallazgos vulnerables encontrados en el estudio.

1.6 Alcance

Se realizará la verificación de la red inalámbrica de la Universidad Técnica del Norte aplicando la metodología OSSTMM (manual de la metodología abierta de testeo de seguridad) en su versión 3, debido a las ventajas que esta ofrece. Evaluando y analizando las secciones: (Heredero, Agius, Romero, & Salgado, 2012).

- Seguridad de la información.
- Seguridad de los Procesos.
- Seguridad en las tecnologías de Internet.
- Seguridad en las Comunicaciones.
- Seguridad Inalámbrica.
- Seguridad Física.

Esta metodología abarca toda la seguridad operativa basada en diferentes áreas o canales como lo describe el manual. (Simpson, 2012). Y se muestra en la Figura 2.

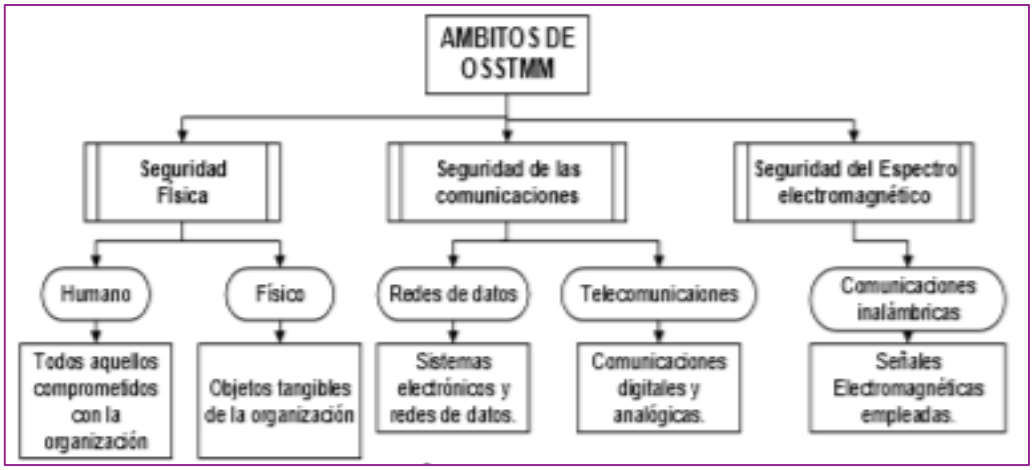


Fig. 2. Ámbitos de OSSTMM

Fuente: (RAULT et al., 2015)

Se utilizará el Sistema Operativo Kali Linux y se escogerán en su primera fase las herramientas que más adaptación tengan con la metodología planteada, una vez que se detecta las vulnerabilidades de la infraestructura de la red inalámbrica, se determina la estrategia con la cual se realizará el testeo de intrusión, a través de Hacking Ético, como se muestra en la figura 3.

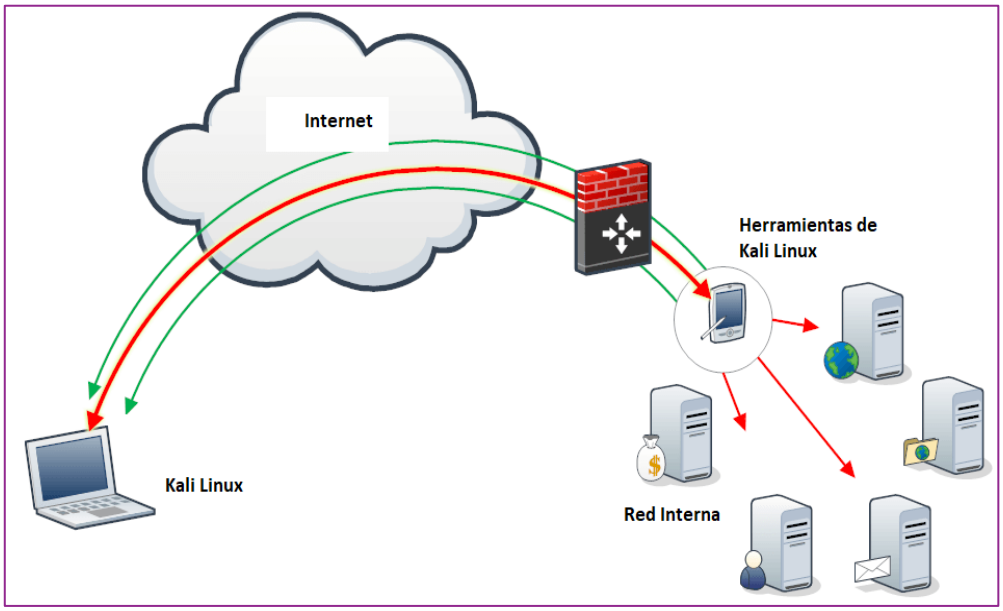


Fig. 3. Arquitectura del Análisis con Kali Linux

Fuente: Propia

CAPÍTULO 1

Fundamentación Teórica

Introducción

En el presente capítulo se describe el fundamento teórico mediante el cual ayudará a la investigación del presente proyecto de titulación, se describe conceptos básicos acerca de la seguridad informática, Ethical Hacking, redes inalámbricas, riesgos informáticos, el procedimiento para realizar una auditoria informática con las herramientas de OSSTMM en versión 3 y descripción del Sistema Operativo Kali Linux.

1.7 Seguridad Informática

"Es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable" (López, 2010, pág. 9). Su principal objetivo es minimizar y gestionar los riesgos y detectar los posibles problemas y amenazas a la seguridad. Carmona Romera (2011) afirma:

> La seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran:
>
> - La información, que se ha convertido en uno de los activos más importantes y valiosos dentro de una organización.
> - La infraestructura computacional.
> - Los usuarios, que son las personas que gestionan la información. (pág.99).

1.7.1 Red informática

Es un conjunto de ordenadores y periféricos conectados entre sí, que permiten que se transmita información y se compartan varios recursos, recursos como: aplicaciones, base de datos, impresoras, archivos compartidos, entre otros, para que una red pueda funcionar, tiene que contar con el hardware necesario: router, cableado, tarjetas de red, repetidores, entre otros, en fin, una red, más que varios ordenadores conectados, la conforman muchas personas que solicitan, facilitan e intercambian información y a la vez experiencias a través de sistemas de comunicación (Darín & Academy, 2016).

> La distribución de recursos se multiplica a través de arquitecturas que incluyen diferentes capas, los recursos que dispone el usuario se emplean para organizar la información recibida cuando una capa intermedia administra las aplicaciones, estas se

han vuelto independientes de los datos y se distribuyen en distintos niveles. (DORDOIGNE, 2015, pág. 25)

La figura 4 representa una arquitectura de tres capas.

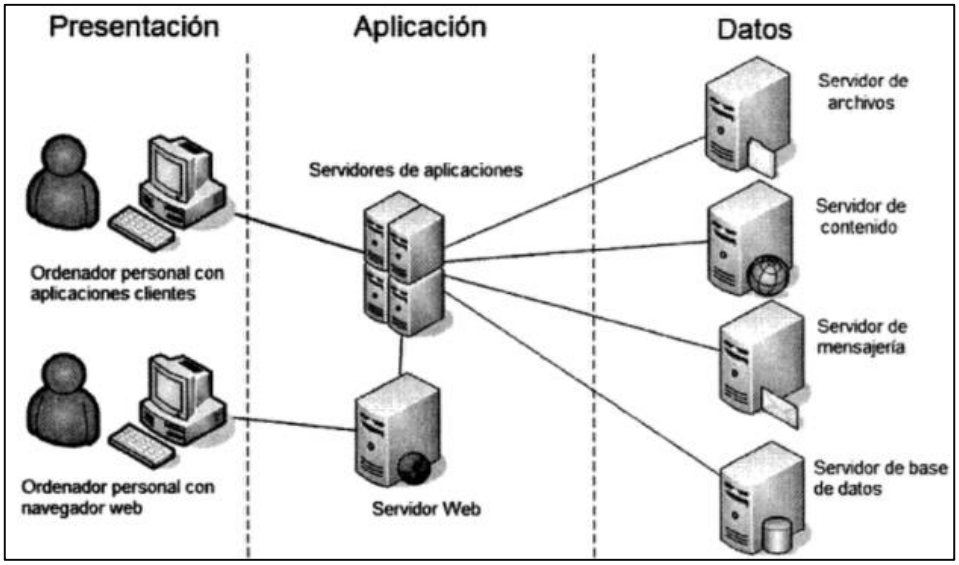


Fig. 4. Arquitectura de tres capas
Fuente: (DORDOIGNE, 2015)

1.7.2 Importancia de la seguridad informática.

La seguridad informática se tiene que considerar como una norma muy importante y de manejo delicado dentro de una organización o institución por lo que no debe aislarse de los demás procesos que se manejan en ella, la inseguridad supone perdida de la información y perjuicios económicos, según (RAMOS & HURTADO, 2011) la seguridad informática es “Un conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información en un sistema informático” (pág. 2). Su principal objetivo es proteger la infraestructura y la información, así como los datos.

1.7.3 Principios importantes de la seguridad informática.

La seguridad informática está basada en la confidencialidad, integridad, disponibilidad, autenticación y no repudio. Las interpretaciones o significados de estos aspectos pueden variar de acuerdo con el entorno, pero básicamente se relacionan con la protección de las amenazas a la seguridad del sistema.

Confidencialidad.

> Se define como el hecho de que los sistemas de información estén únicamente al alcance del conocimiento de las personas, organizaciones o mecanismos autorizados, en los momentos autorizados y de una manera autorizada, para prevenir errores de confidencialidad se debe diseñar un control de acceso al sistema: quién puede acceder, a qué parte del sistema, en qué momento y para realizar qué tipo de operaciones. (López, 2010, pág. 10)

Integridad.

Este principio garantiza la autenticidad y precisión de la información sin importar el momento en que, ésta se solicita, para prevenir riesgos se debe dotar al sistema de mecanismos que prevengan y detecten cuándo se produce un fallo de integridad y que puedan tratar y resolver los errores que se han descubierto (López, 2010).

Disponibilidad.

> La metodología Magerit define como: grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado. Situación que se produce cuando se pueda acceder a un sistema de información en un periodo de tiempo considerado aceptable. Se debe aplicar medidas que resguarden la información creando copias de seguridad y mecanismos para restaurar datos que se hubiesen dañado o destruido de forma accidental. (López, 2010, pág. 11)

Autenticación.

Consiste en la confirmación de la identidad de un usuario, de un servicio, de una aplicación; es decir, la garantía de que un interlocutor es realmente quien dice ser, se definen dos tipos de autenticación: la de origen de datos en la que se relaciona con la conexión entre redes y la autenticación de entidad de par, en la que se presenta en una asociación sin conexión. Según Urbina (2016) Afirma: “la red, por medio de sus procedimientos, debe garantizar que se establezca un intercambio de datos o de información con la entidad requerida por el usuario, y no con otra que esté suplantando a la entidad real requerida” (pág. 15).

No repudio o irrenunciabilidad.

Costas Santos (2014) afirma que:

El no repudio está relacionado con la autenticación y permite probar la participación de las partes en una comunicación. Existen dos posibilidades:

- No repudio en origen: el emisor no puede negar el envío. La prueba la crea el propio emisor y la recibe el destinatario.
- No repudio en destino: el receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. En este caso la prueba irrefutable la crea el receptor y la recibe el emisor. (pág. 12).

A la relación de estas características se presentan en la figura 5.

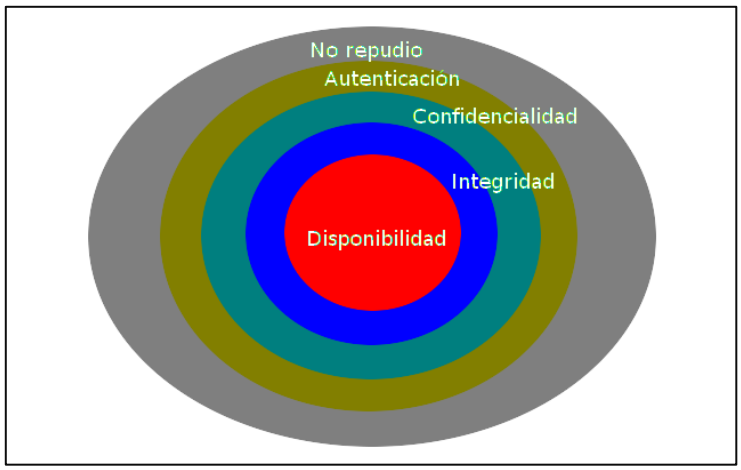


Fig. 5. Relación de los servicios de seguridad

Fuente: (Costas Santos, 2014)

En los diferentes servicios de seguridad, unos dependen de otros jerárquicamente, así si no existe el de nivel interior, no puede aplicarse el exterior. De esta manera, la disponibilidad se convierte en el primer requisito de seguridad, cuando existe ésta, se puede disponer de confidencialidad, que es imprescindible para conseguir integridad, imprescindible para poder obtener autenticación y por último el no repudio que solo se obtiene si se produce previamente la autenticación. (Costas Santos, 2014, pág. 19)

1.8 Seguridad de la Información.

En materia de seguridad de la información e informática, es importante conocer varios términos, mismos que se detallan a continuación:

1.8.1 Activos.

Son los recursos que pertenecen al propio sistema de información o que están relacionados con este, necesario para que la organización alcance los objetivos planteados, es decir, todo aquello que tenga valor y que pueda ser protegido frente a un percance a futuro (López, 2011).

En la figura 6, el analista debe de contar con conocimientos avanzados sobre los riesgos de los activos a proteger para poder evaluar la criticidad de las vulnerabilidades encontradas y cuál será la probabilidad de amenaza por parte de los atacantes (Roman, 2017).

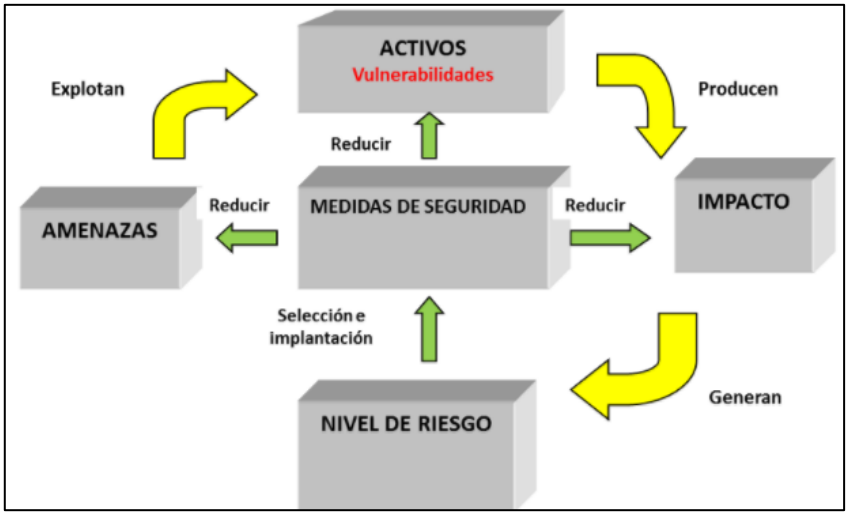


Fig. 6. Medidas de seguridad de los activos

Fuente: (Roman, 2017)

Datos.

Constituye el núcleo en una organización, se considera que los activos se encuentran al servicio de la protección de los datos, se encuentran organizados en base de datos, cada tipo de dato tiene diferente estudio de recuperación frente a un eventual deterioro o perdida.

Software.

Conformado por el sistema operativo y las aplicaciones informáticas instaladas en el equipo de un sistema de información, gestionan los datos para proporcionar un propósito o fin para el que fue establecido.

Hardware.

Se refiere a todos los equipos (servidores y terminales) que contienen al software, permitiendo su funcionamiento y que a su vez sirven de almacenamiento para la información del sistema.

Personal.

Son el recurso humano que se encuentran interactuando con el sistema informático, como son los administradores, programadores y usuarios, las fallas más habituales en las aplicaciones suceden por el factor humano.

1.8.2 Riesgos informáticos.

En informática, las organizaciones no desean sufrir un ataque interno o externo en sus sistemas de información, pero los ataques casi siempre suceden, de manera que esa probabilidad se materializa, "la organización siempre está amenazada de sufrir algún daño en su sistema informático, daño que puede provocar pérdidas de muchos tipos, y las amenazas son mayores cuando los sistemas de información presentan puntos débiles llamados vulnerabilidades" (Baca Urbina, 2016, pág. 23).

Riesgos de integridad.

"Este tipo abarca todos los riesgos asociados con la autorización, completitud y exactitud de la entrada, procesamiento y reportes de las aplicaciones utilizadas en una organización" (González, 2003, pág. 3). La información puede ser modificada por quien está autorizado, con la finalidad de asegurar la consistencia de los datos de manera interna o externa (Bigelow, 2003).

Riesgos de acceso.

Se dirigen al inapropiado e inadecuado acceso a los sistemas, datos e información, estos riesgos comprenden: los riesgos asociados con la integridad de la información en los sistemas de bases de datos y los riesgos relacionados a la confidencialidad de la información, este tipo de riesgos puede ocurrir en los niveles de la estructura de la seguridad de la información, como son: administración de información, entorno de procesamiento, redes y nivel físico (González, 2003).

Riesgos de infraestructura.

Se refiere a que en las organizaciones el hardware, software, redes, personas y procesos, no cuentan con una estructura de información tecnológica efectiva que puedan soportar de manera adecuada las necesidades de los negocios con un costo eficiente y rentable, estos riesgos tienen relación con los procesos de la información tecnológica las que definen, desarrollan, mantienen y operan un entorno de procesamiento de información y los sistemas asociadas con servicio al cliente, pago de cuentas, entre otras (González, 2003).

Otros Riesgos.

La figura 7 muestra otros riesgos a los cuales se encuentran inmersos los sistemas de información.

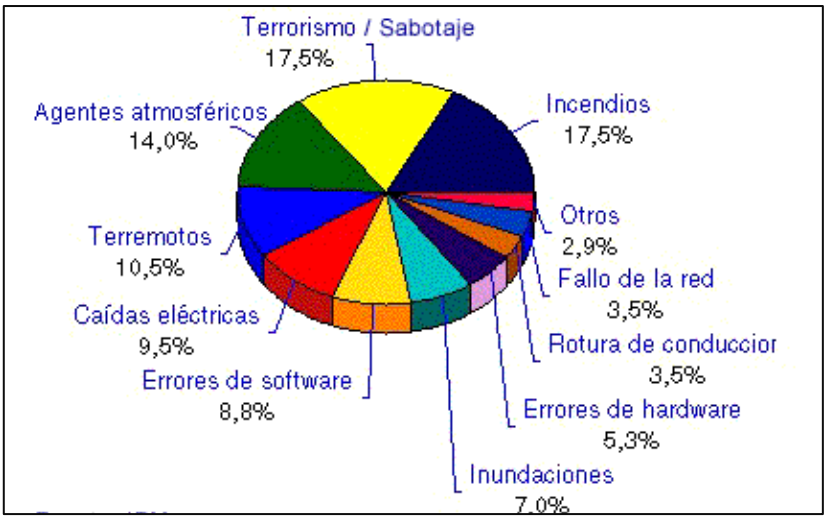


Fig. 7. Tipos de Riesgos

Fuente: (Lascano, & Jeanett, 2010)

1.8.3 Metodologías de evaluación de riesgo.

Magerit.

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas, creada por el Consejo Superior de Informática de España alineada a la familia ISO/IEC 27000, Ofrece un método estructurado y sistemático ayudando a un analista a la realización de un análisis de gestión de riesgo (Dirección General de Modernización Administrativa, 2012).

Los objetivos de MAGERIT según (Gómez Vieites, 2014) son:

- Concienciar a los responsables de los Sistemas de Información de la existencia de riesgos y de la necesidad de adoptar las medidas para limitar su impacto.
- Ofrecer un método sistemático para analizar tales riesgos.
- Planificar control. las medidas oportunas para mantener los riesgos identificados bajo control
- Facilitar todos los procesos de evaluación, auditoría, certificación o acreditación.

Donde el sistema de información se estudia las fortalezas, riesgos y amenazas para analizar sus debilidades y establecer planes de acción correctivas. La figura 8 muestra la estructura de la metodología.

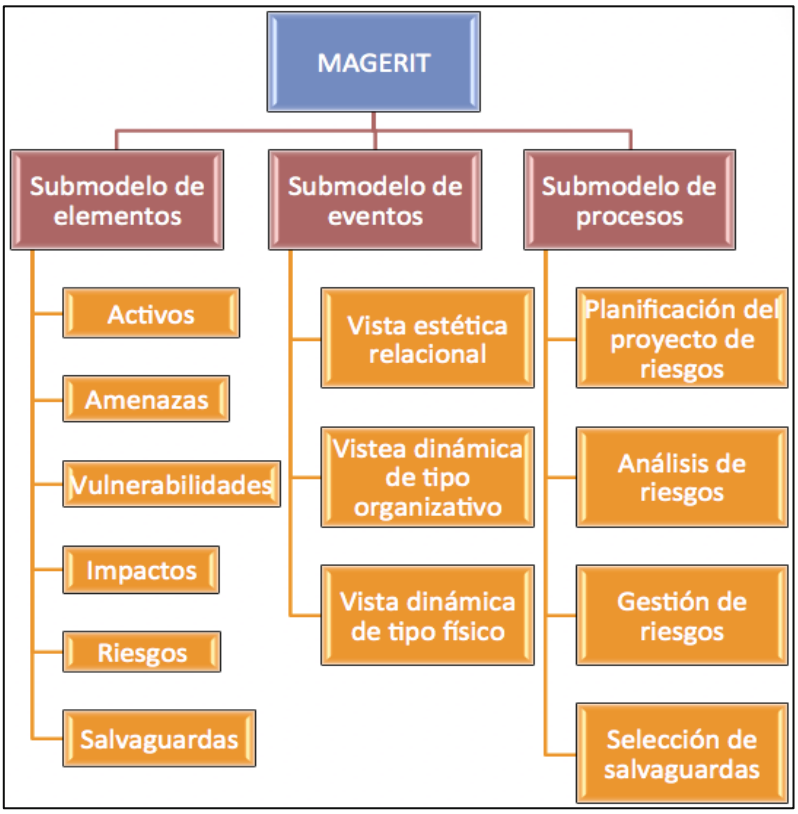


Fig. 8. Estructura de bloques del modelo MAGERIT

Fuente: (Gutiérrez de Mesa & Pagés Arévalo, 2008)

Elementos de Magerit.

Análisis de Riegos.

Permite identificar los tipos de amenazas que se encuentran presentes en los sistemas de Información llamados (activos); para determinar las vulnerabilidades, el grado de impacto que puede tener una organización (Freitas, 2009).

Gestión de Riesgos.

Con los resultados obtenidos en el análisis de riesgo, la gestión de riesgos permite implementar las salvaguardas de seguridad de mayor adaptación y qué tan eficaces son ante amenazas, permitiendo una prevención y control de los riesgos encontrados en el análisis reduciendo al mínimo sus posibles perjuicios (D. Bracho & Rincón, 2010).

Ámbito de aplicación.

Magerit ofrece una herramienta libre para el análisis de riesgo llamada PILAR (Proceso Informático Lógico para el Análisis de Gestión de Negocios), la cual dispone de una biblioteca estándar de propósito general y capaza de realizar calificaciones de seguridad respecto de normas ampliamente conocidas como la ENS (Esquema Nacional de Seguridad), se puede aplicar en Gobiernos, Organismos, Organizaciones grandes, Organizaciones comerciales y no comerciales.

Octave.

Desarrollada por la Universidad Carnegie Mellon en el año 2001, es una metodología de Análisis y Gestión de Riesgos, conocido por sus siglas como (OCTAVE), es flexible y estudia los riesgos en base a tres principios Confidencialidad, Integridad y Disponibilidad, requiere la participación de todos los niveles de la organización y las personas implicadas de forma directa en los activos críticas de información, su objetivo es ayudar a las organizaciones a mejorar su capacidad de gestión identificando y evaluando los riesgos que afectan la seguridad dentro de una organización (Diaz Moreno, 2013).

Para cumplir las necesidades de seguridad de la organización de la información Está compuesta por tres fases como se muestra en la figura 9:

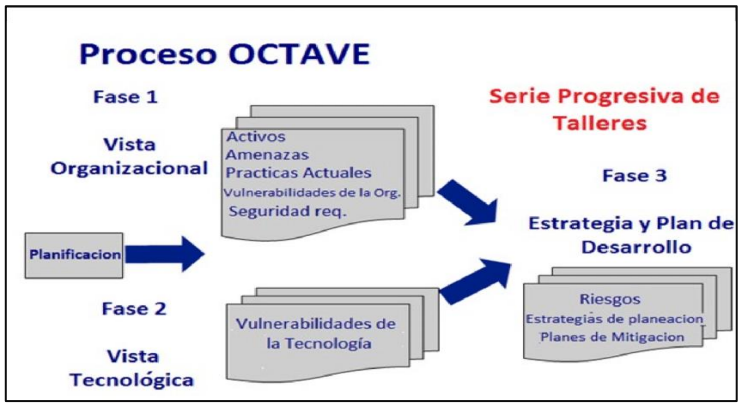


Fig. 9. Fases de la metodología Octave

Fuente: (Domínguez Chávez, 2015)

Las fases están divididas en varios procesos y cada proceso tiene talleres dirigidos o realizados por un equipo de analistas.

- **Fase 1**.

Se refiere a la recopilación, consolidación y el análisis de la información obtenida en los distintos niveles de la organización, el equipo de análisis determina cuales son los activos críticos y que se está haciendo para protegerlos (Kapczyński, Tkacz, & Rostanski, 2012).

- **Fase 2.**

En esta fase se realiza una evaluación de la infraestructura de información, los analistas los principales componentes operacionales y las vulnerabilidades que pueden dar lugar a una acción no autorizada hacia los activos. (Kapczyński et al., 2012).

- **Fase 3.**

Se identifica los riesgos en los activos críticos y se decide la acción a realizar, el quipo analista basados en la información recolectada crea una estrategia y planes de mitigación (Kapczyński et al., 2012).

1.8.4 Criptografía

Criptografía es una palabra que proviene del griego y significa “arte de escribir con clave secreta o de un modo enigmático, la criptografía es un grupo de técnicas que tratan sobre protección de la información” (Jalca et al., 2018, pág. 95).

“La ciencia de generar los mensajes cifrado es la criptografía y la descifrar los mensajes se conoce criptoanálisis. Ambas forman la llamada criptografía” (Jalca et al., 2018, pág. 95).

A los mensajes originales también se les llama texto claro o común. El descifrado es el proceso inverso del cifrado. El proceso cifrado-descifrado se muestra en la figura 10.

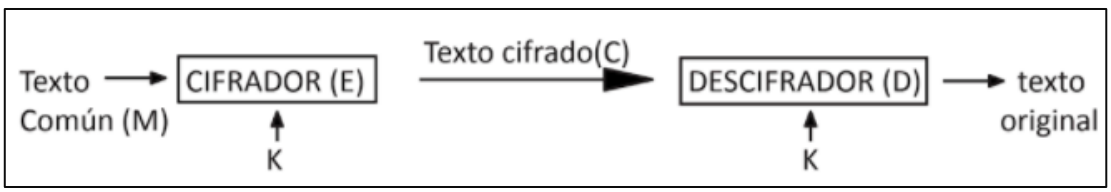


Fig. 10. Criptosistema

Fuente: (Jalca et al., 2018)

Según (Jalca et al., 2018), un criptosistema se puede definir como una quíntupla (M, C, K, E, D), donde:

- **M**: es el conjunto de todos los mensajes sin cifrar (texto claro).
- **C**: es el conjunto de todos los posibles mensajes cifrados (criptogramas).
- **K**: es el conjunto de claves que se puede emplear en el criptosistema.
- **E**: es el conjunto de transformaciones de cifrado que se aplica a cada elemento de M para obtener un elemento de C.
- **D**: es el conjunto de transformaciones de descifrado. (pág. 95).

"El cifrado es la transformación de datos o mensajes en alguna forma no legible y su objetivo es mantener la información oculta para aquellos a los cuales no está dirigido. Un mensaje cifrado se le llama texto cifrado" (Jalca et al., 2018, pág. 95)

1.8.5 Conceptos básicos para un Ethical Hacking.

Los conceptos básicos que se deben manejar al momento de realizar un Ethical Hacking son los que garantizan el éxito para mejorar el sistema de seguridad en una red.

Definición de hacker.

Por lo general ante la sociedad se piensa que es una persona que comete delitos informáticos, pero esto no es así, la definición correcta es la siguiente:

Un hacker es una persona con profundos conocimientos sobre una tecnología, RAULT (2015) Afirma que:

> es una persona mañosa, apasionada, con tendencia a la curiosidad y a la sed de aprender que a la voluntad de hacer daño. Es un especialista en seguridad informática, que utiliza sus conocimientos por el gusto y la necesidad de saber más o difundir la información (pág. 24).

Un hacker busca primero el funcionamiento del sistema a nivel de hardware y software para descubrir el modo de codificación de las ordenas del programa, para luego modificar la información en su propio uso o para investigación total del sistema.

Definición de hacker ético.

Se refiere a un experto en informática y sistemas que utilizan sus conocimientos de hacking con fines de defensa en seguridad de la información, “la función del Ethical hacker es determinar lo que un intruso puede hacer sobre un sistema y la información, y velar por su protección” (Héctor Jara y Federico G. Pacheco, 2012, pág. 41).

Pentest.

Un test de penetración consiste en una simulación de un ataque real a un sistema o una red informática con la intención de encontrar debilidades y reparar problemas de seguridad (Colobran Huguet, Arqués Soldevilla, & Marco Galindo, 2008).

1.8.6 Tipos de ataques.

Un ataque informático consiste en aprovechar debilidades, fallas en el software o en el hardware para intenta tomar el control, desestabilizar, dañar a un sistema informático o red para obtener un beneficio.

Ataques al sistema operativo

Consiste en la búsqueda de fallas en el software base de todo el resto de los sistemas, de esta manera se puede explotar y tomar el control del sistema en caso de haber encontrado alguna vulnerabilidad, un atacante aprovecha las configuraciones estándar, las implementaciones que se le realiza al sistema operativo a las distintas tecnologías. Por ejemplo “un sistema que tuviera un fallo en la implementación de cierta tecnología de cifrado, lo cual haría que el cifrado fuera débil, sin que se tratara de un problema en el propio algoritmo de cifrado ni en la aplicación que lo utilizara” (Héctor Jara y Federico G. Pacheco, 2012, pag 47).

Ataques a las aplicaciones

En este caso, existen cientos y miles líneas de código en los diferentes sistemas informáticos, siendo casi eminente una falla de seguridad entre sus líneas, las que son aprovechadas por los atacantes, otro factor en el que se basa un atacante es la masividad de las aplicaciones, ejemplo: un programa para leer un archivo de tipo PDF es utilizado por millones de personas la que representa un mejor objetivo a diferencia de otro tipo de archivo menos conocido utilizado por pocas personas (Héctor Jara y Federico G. Pacheco, 2012).

Errores en configuración

Constituye un punto sensible, dado que por más seguro sea un software ya sea el sistema operativo o las aplicaciones, una mala configuración estándar puede tornarlo en un punto de entrada por el atacante, ejemplo: “un antivirus con una configuración deficiente podría hacer que cumpliera su función de manera poca efectiva, provocando que una buena herramienta terminara por traducirse en una mala solución y, por ende, en una brecha de seguridad” (Héctor Jara y Federico G. Pacheco, 2012, pag 51). En el ámbito corporativo, como resultado de realizar un exhaustivo análisis de sus propios sistemas, surgen la necesidad de implementar una serie de configuraciones mínimas para obtener un nivel mejorado de seguridad.

Errores en protocolos

En este caso, las fallas están directamente en los protocolos, dado que existen centenares de protocolos, existen a la vez, posibilidades de encontrar fallas en ellos, “el problema más grave es que un error en el diseño de uno implica que las situaciones sean potencialmente incorregibles, y que deben realizarse modificaciones a distintos niveles para resolverlos, incluyendo a veces su variación total o parcial” (Héctor Jara y Federico G. Pacheco, 2012, pag 53).

1.8.7 Tipos de pentesting.

La figura 11 muestra los tres tipos de pruebas de penetración o pentesting más conocidos.

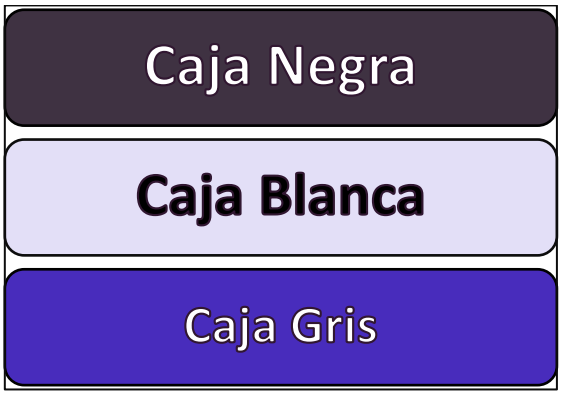


Fig. 11. Tipos de pentesting

Fuente: Elaboración propia

- **Test de caja negra**

El método consiste en una serie de pruebas que evalúan exclusivamente las entradas y salidas del sistema de información, el auditor de seguridad no tiene ningún conocimiento del funcionamiento interno del sistema, actuará como si fuera un atacante, probando una tras otra las distancias puertas en busca de una vulnerabilidad que pueda explotar, este tipo de test tiene como ventaja de que son rápidos, realistas y menos caros, sin embargo, no son exhaustivas las vulnerabilidades más profundas y ocultas pueden ser pasadas por alto (RAULT et al., 2015).

- **Test de caja blanca**

Antes de realizar esta prueba el auditor de seguridad deberá recopilar toda la información que sea posible para la evaluación de la seguridad y de las vulnerabilidades del sistema de información: código fuente de las aplicaciones archivos de configuración, entre otras, este tipo de pruebas son más minuciosas, detectan las vulnerabilidades más profundas y los resultados obtenidos son más precisos, sin embargo, requieren de muchos y costosos recursos (Chicano Tejada, 2014).

- **Test de caja gris**

En este método el auditor de seguridad tiene conocimiento limitado de los detalles internos del sistema con el fin de identificar el mayor número de amenazas posibles reales, se realiza la prueba del sistema objetivo en un marco de vigilancia aleatoria (Medina, 2015).

1.9 Auditoria Informática.

1.9.1 Objetivo fundamental de la auditoria informática.

Se lleva a cabo la evaluación de normas, controles, técnicas y procedimientos que se han establecidos en una organización para adquirir confiabilidad, oportunidad, seguridad y confidencialidad de la información que se procesa a través de los sistemas de información, el objetivo es conseguir información fidedigna del estado del sistema, de esta manera conseguir un documento final con la detección de las debilidades y la identificación de amenazas con una definición clara de las causas de estas situaciones (Chicano Tejada, 2014).

1.9.2 Tipos de auditoria informática.

Realizar auditorías con determinada frecuencia asegura y determina la integridad de los controles aplicados a los distintos sistemas de información.

Los servicios de auditoria pueden ser de distinta índole:

Auditoria de seguridad interna.

Este tipo de auditoria intenta detectar los riesgos y debilidades de la estructura del sistema de información, se analiza cualquier vía de ataque que pueda provocar un daño, perdida o una alteración a la información sensible de una organización y ofrece soluciones disminuyendo las posibilidades de un ataque interno, se contrasta el nivel de seguridad de las redes locales y corporativas de carácter interno (Costas Santos, 2014).

Auditoria de código de aplicaciones.

Se refiere al análisis del código tanto de aplicaciones web, como de cualquier tipo de aplicación, ejemplo: un sitio web en la que mediante un análisis externo a la web se comprueba vulnerabilidades como la inyección de código SQL, Cross Site Request/Reference Forgery (CSRF), entre otras vulnerabilidades, este tipo de auditorías se realiza independientemente del lenguaje empleado (Costas Santos, 2014).

Auditoria de las comunicaciones.

“Se refiere a la auditoria de los procesos de autenticación y cifrado en los sistemas de comunicación, al uso eficiente de redes internas y externas y al uso de cualquier dispositivo empleado por la empresa para comunicarse de manera interna y externa” (Baca Urbina, 2016 pág. 295).

Auditoria de seguridad perimetral.

En este tipo de análisis, el perímetro de la red local o corporativa es estudiado y se analiza el grado de seguridad que ofrece desde el exterior hacia la red interna sobrepasando las barreras de seguridad, de esta manera, las vulnerabilidades que puedan existir quedaran a la vista del analista para una posterior corrección (Costas Santos, 2014).

1.9.3 Amenazas y vulnerabilidades.

Vulnerabilidades.

Vieites (2014) afirma que: “Es cualquier debilidad en el sistema informático que pueda permitir a las amenazas causarle daños y producir pérdidas en la organización” (pág. 74). Las vulnerabilidades pueden darse por fallas de diseño, por errores en la implementación o por falta de mantenimiento, por una codificación deficiente, entre otros motivos, Se suele emplear

una escala cuantitativa o cualitativa para una determinada vulnerabilidad en un equipo o recurso: bajo, moderado y alta, como se describe En la tabla 1.1

TABLA 0.1 Escala propuesta para medir el impacto del daño en una organización

IMPACTO DE DAÑO	CARACTERÍSTICA
Alto	○ Perdida o inhabilitación de recursos críticos. ○ Interrupción de los procesos de negocio. ○ Daños en la imagen y reputación de la organización. ○ Robo o revelación de información estratégica o especialmente protegida.
Moderado	○ Perdida o inhabilitación de recursos críticos, pero que cuentan con elementos de respaldo. ○ Caída notable en el rendimiento de los procesos de negocio en la actividad normal de la organización. ○ Robo o revelación de información confidencial, pero no considerada estratégica.
Bajo	○ Perdida o inhabilitación de recursos secundarios. ○ Disminución de rendimiento de los procesos de negocio. ○ Robo o relevancia de información interna no publicada.

Fuente: (Gómez Vieites, 2014)

Amenazas.

Una amenaza tiene el potencial de causar un daño o una pérdida a un sistema de información, una amenaza sólo existe en caso de que una vulnerabilidad pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información, Situaciones como: falta de capacitación a los usuarios y concientización en el uso de las tecnologías, mejoras de técnicas de ingeniería social y la creciente rentabilidad ataques informáticos, han provocado el aumento de amenazas intencionales (Costas Santos, 2014).

En general, las principales amenazas y ataques a las cuales se enfrenta un equipo o la información Se muestran en la tabla 1.2:

TABLA 0.2 Técnicas de ataques cibernéticos

TÉCNICAS	CARACTERÍSTICAS
Malware	Programas malintencionados (virus, espías, gusanos, troyanos, etc.) que afectan a los sistemas con pretensiones como: controlarlo o realizar acciones remotas, dejarlo inutilizable, reenvío de spam, etc.
Ingeniería social	Obtener información confidencial como credenciales (usuario-contraseña), a través de la manipulación y la confianza de usuarios legítimos. El uso de dichas credenciales o información confidencial servirá para la obtención de beneficios económicos mediante robo de cuentas bancarias, reventa de información o chantaje.
Scam	Estafa electrónica por medio del engaño como donaciones, transferencias, compra de productos fraudulentos, etc. Las cadenas de mail engañosas pueden ser scam si hay pérdida monetaria y hoax (bulo) cuando solo hay engaño.
Spam	Correo o mensaje basura, no solicitados, no deseados o de remitente no conocido, habitualmente de tipo publicitario, enviados en grandes cantidades que perjudican de alguna o varias maneras al receptor. Suele ser una de las técnicas de ingeniería social basada en la confianza depositada en el remitente, empleadas para la difusión de scam, phishing, hoax, malware, etc.
Sniffing	Rastrear monitorizando el tráfico de una red para hacerse con información confidencial.
Spoofing	Suplantación de identidad o falsificación, por ejemplo, encontramos IP, MAC, tabla ARP, web o mail Spoofing.
Pharming	Redirigir un nombre de dominio (domain name) a otra máquina distinta falsificada y fraudulenta.
Phishing	Estafa basada en la suplantación de identidad y la ingeniería social para adquirir acceso a cuentas bancarias o comercio electrónico ilícito.

Password cracking	Descifrar contraseñas de sistemas y comunicaciones. Los métodos más comunes son mediante sniffing, observando directamente la introducción de credenciales (shoulder surfing), ataques de fuerza bruta, probando todas las combinaciones posibles, y de diccionario, con un conjunto de palabras comúnmente empleadas en contraseñas.
Botnet	Conjunto de robots informáticos o bots, que se ejecutan de manera autónoma y automática, en multitud de host, normalmente infectados, permite controlar todos los ordenadores/servidores infectados de forma remota. Sus fines normalmente son rastrear información confidencial o incluso cometer actos delictivos.
Denegación de servicio o Denial of Service (DoS)	Causar que un servicio o recurso sea inaccesible a los usuarios legítimos. Una ampliación del ataque Dos es el llamado ataque distribuido de denegación de servicio, también llamado ataque DDoS, a través de una botnet, siendo esta técnica el ciberataque más usual y eficaz.

Fuente: (Costas Santos, 2014)

1.10 Redes Inalámbricas.

Las redes de área local inalámbricas (Wireless Local Area Networks o WLAN), permite a los dispositivos informáticos la transmisión de información a través de ondas electromagnéticas (Álvarez Marañón & Pérez García, 2004). En la figura 12 se muestra una red empresarial típica.

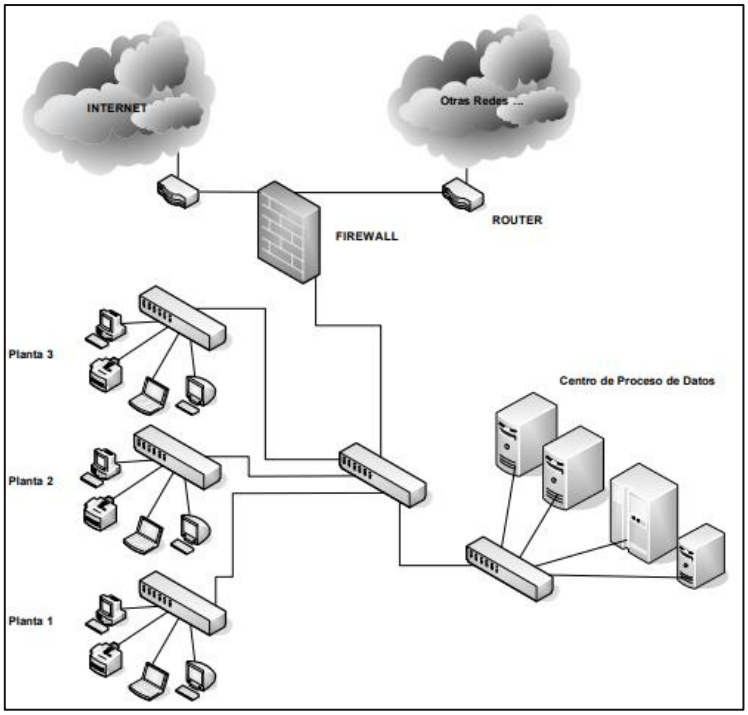


Fig. 12 Una red empresarial típica

Fuente: Álvarez Marañón & Pérez García, 2004)

Esta tecnología ofrecen muchas ventajas a comparación con las redes conectadas por cable como: (Costas Santos, 2014)

Ventajas

- La capacidad de brindar conectividad en cualquier momento y lugar, es decir mayor disponibilidad y acceso a redes.
- La instalación de la tecnología inalámbrica es simple y económica.
- La tecnología inalámbrica permite que las redes se amplíen fácilmente, sin limitaciones de conexiones de cableado, por lo que es fácilmente escalable.

1.10.1 La seguridad en las redes inalámbricas.

Robles & Ortega (2014) indican que:

Las redes inalámbricas son muy vulnerables a la captura de información por parte de usuarios no autorizados, sobre todo porque cualquier equipo ubicado dentro del radio de acción de la red tiene capacidad de obtener los mensajes enviados por equipos que sí están autorizados, ésta captura de tráfico la pueden realizar los equipos que

> dispongan de adaptadores inalámbricos con capacidad para funcionar en modo promiscuo además de tener instalado un programa de captura de tráfico (pág. 513).

"El modo promiscuo consiste en que el adaptador de red recibe los mensajes y los procesa, aunque éste no sea su destinatario, hay que tener en cuenta que no todos los adaptadores inalámbricos disponen de este modo de funcionamiento" (Robles & Ortega, 2014, pág. 513).

1.10.2 Protocolos utilizados en redes inalámbricos.

Protocolo WEP

El protocolo por sus siglas Wired Equivalent Privacy (WEP) que en español significa Privacidad Equivalente a Cableado, es el sistema de cifrado incluido en el estándar IEEE 802.11i como protocolo que permite cifrar la información de redes inalámbricas, no fue creado por expertos en seguridad o criptografía, así que pronto se demostró que era vulnerable ante los problemas de cifrado RC4 (Cerra Mariel, 2010).

El propósito del protocolo WEP fue brindar un nivel de seguridad a las redes inalámbricas comparable al de las redes alambradas tradicionales, la vida del protocolo WEP fue muy corta; un diseño deficiente y poco transparente condujo ataques muy efectivos a su implantación, pocos meses después de que fuera publicado, el protocolo fue considerado obsoleto. (Arturo, 2015).

> El inconveniente del cifrado WEP radica en que se establece una clave de cifrado estático que no cambia con el tiempo, a no ser que los administradores de la red se preocupen en cambiarla con determinada frecuencia. Un intruso puede utilizar programas especializados de fuerza bruta para obtener la clave de cifrado y acceder a la red. (Robles & Ortega, 2014, pág. 514)

Protocolo WPA

El protocolo por sus siglas Wi-Fi Protected Access (WPA) que en español significa Acceso Wi-Fi protegido, se trata de un sistema más robusto que WEP, aprobado en abril del 2003 por la Alianza WiFi (Wi-Fi Alliance), dentro del estándar IEEE 802.11i, WPA destaca por su compatibilidad con el hardware ya instalado en el mercado; las tarjetas de red y puntos de acceso, que utilizaban el algoritmo simétrico RC4 del protocolo WEP como base para el cifrado de las transmisiones (Vieites, 2014).

WPA emplea un nuevo protocolo de cifrado conocido como (TKIT) Temporal Key Integrity Protocol, que permite reforzar la seguridad de las claves y proteger la red contra los ataques

por falsificación o por repetición, en WPA se utilizan claves de cifrado de 128 bits que se pueden asignar de forma dinámica por usuarios y por sesión, por lo que este sistema es mucho más robusto a ataques de fuerza bruta, superando además el problema de las claves estáticas y de tamaño reducido del protocolo WEP (Vieites, 2014).

WPA2

> El protocolo por sus siglas Wi-Fi Protected Access 2 (WPA2) que en español significa Acceso Wi-Fi 2 protegido, es un sistema para proteger a las redes inalámbricas eliminando las vulnerabilidades detectadas en WPA. La nueva generación de puntos de acceso en el protocolo WPA2 utiliza el algoritmo de cifrado (AES) por sus siglas en inglés (Advanced Encryption Standard), El AES es un sistema de cifrado de por bloques con claves de 128, 192, 256 bits. (MIRANDA, 2005, pág. 156)

1.11 Herramientas de seguridad Kali Linux.

1.11.1 Introducción.

Kali Linux inicio en versión beta en el año 2006 en tipo LiveCD's (sistema operativo almacenado en un medio extraíble, tradicionalmente un CD) posteriormente los creadores de BackTrack revolucionaron el sistema operativo con herramientas de auditoria en redes y sistemas, en 2013 Offensive Security da por terminado el soporte y actualización del nuevo sistema operativo, se puede decir que es una completa reestructuración de BackTrack Linux desde la base hacia arriba (Alamanni, 2015)

Está basada en los estándares de desarrollo Debian, utilizada para realizar auditorías de seguridad y pruebas de penetración, Kali Linux contiene gran cantidad de herramientas para identificar fallas o vulnerabilidades, capturar información, explorarlas, escalar privilegios y cubrir las huellas, contiene un gran cantidad de herramientas obtenidas desde fuentes relacionadas en seguridad y análisis forense, trae preinstalado más de seiscientos programas, el equipo de Kali Linux está conformado por un entorno seguro con un grupo pequeño de personas quienes pueden modificar, actualizar los paquetes e interactuar con los repositorios oficiales también firman los paquetes utilizados, la distribución se la realiza en imágenes de disco (ISO) compiladas en arquitecturas (32/64 bits y ARM) (offensive security, 2018).

1.11.2 Motivos para utilizar Kali Linux.

Es un Sistema operativo orientado a seguridad informática de penetración avanzada, diseñado para actos de incursión y de testeo de vulnerabilidades, todas las aplicaciones contenidas están firmadas por el desarrollador que lo compiló y desarrolló (offensive security, 2018).

Desde una perspectiva facilita el trabajo a los administradores de sistemas y redes, permitiendo auditar a los sistemas y las redes por completo.

1.11.3 Ventajas

- Está orientado para tareas de auditoria informática y análisis forense, permite descubrir los potenciales rastros de los atacantes y por donde es atacado el sistema operativo, su uso y desarrollo tiene una finalidad educativa y ética.
- El software es de distribución libre, multilenguaje y se puede realizar las adaptaciones necesarias para obtener herramientas destinadas a realizar tareas específicas.
- Tiene más de seiscientas herramientas asociadas con la seguridad informática en las que se destacan; nmap que permite escanear los puertos de un sistema, aircrack-ng para la seguridad de las redes inalámbricas
- La instalación se la puede realizar de distintas maneras, mediante el Bus universal en Serie (USB), máquina virtual y modo fijo en una partición del disco duro.

1.12 Metodologías de pruebas de penetración.

1.12.1 Metodología PTES.

Por sus siglas Penetration Testing Execution Standard que en español sería Estándar de Ejecución de Tests de Intrusión, fue creada por expertos en la industria de la auditoria informática, el principal objetivo es “La realización de un proceso de Test de intrusión que cubra el proceso desde el principio hasta el final. Comienza con la parte de acuerdos y autorizaciones previas a las pruebas, y termina explicando cómo se debe realizar el informe” (Santoyo, 2015).

Características.

A continuación, se enumeran las principales características. (Lago, 2017).

- Tiene instrucciones detalladas sobre cómo realizar muchas de las tareas que son requeridas para analizar con precisión la seguridad de un entorno.

- Fácil de entender y puede adaptarse a las necesidades de pruebas requeridas por él analista.

Fases de la metodología PTES:

El estándar consta de siete secciones principales, estas cubren todo lo relacionado con un test de intrusión desde el pre-compromiso, la comunicación inicial y el razonamiento detrás de un pentest, a través de la recopilación de inteligencia y las fases de modelado de amenazas donde los auditores están trabajando entre bastidores para comprender mejor la organización que están testando, pasando por la investigación de vulnerabilidades, la explotación y la publicación de la explotación, donde la experiencia técnica de los auditores entran en juego y se combinan con la comprensión del negocio, y finalmente el informe, que captura todo el proceso, de manera que tenga sentido para el cliente y le proporcione más valor como se muestra en la figura 13 (Cristian Borghello, 2017).

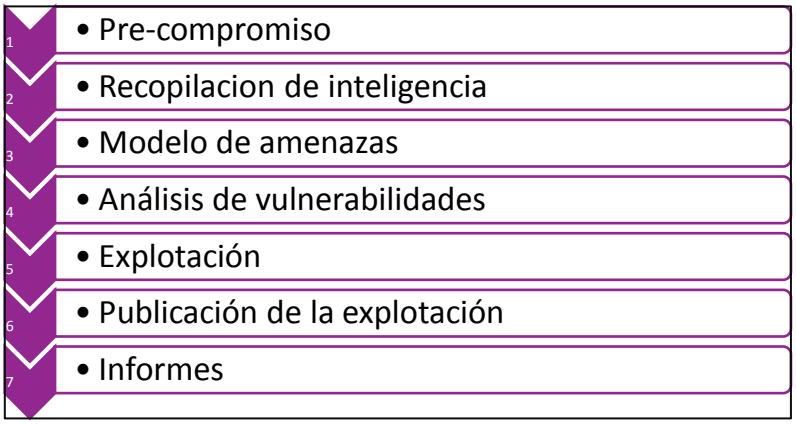


Fig. 13 Fases de la metodología PTES

Fuente: (MediaWiki, 2011)

1.12.2 Metodología NIST SP 800-115

Esta metodología como bien indica su nombre ha sido desarrollada por el Instituto Nacional de Normas y Tecnologías (National Institute of Standards and Technology) de Estados Unidos, La misión de este instituto es promover la innovación y la competencia industrial en Estados Unidos mediante avances en metodologías, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida. (Santoyo, 2015, pág. 18)

Entre las numerosas metodologías que dispone, se encuentra la SP 800-1157 que se titula Technical Guide to Information Security Testing and Assessment. El objetivo de esta es proveer de una metodología para llevar a cabo pruebas y evaluaciones de seguridad, además proponer estrategias para mitigar los fallos. Contiene recomendaciones prácticas para diseñar, implementar y mantener los procesos y procedimientos asociados con la seguridad. No es una guía que entre en mucha profundidad o detalle, si no que repasa los aspectos fundamentales de una auditoria de seguridad (Santoyo, 2015, pág. 19).

Características.

Según la NIST SP 800-115, las pruebas de intrusión pueden ser utilizadas para determinar:

- La manera en que el sistema tolera los patrones de ataques del mundo real.
- El nivel de sofisticación que un atacante necesita para comprometer con efectividad el sistema.
- Las medidas adicionales que se deben emplear para mitigar las amenazas contra el sistema.
- La habilidad de los defensores para detectar los ataques y responder apropiadamente a estos.

Fases de la metodología NIST SP 800-115.

El NIST, SP 800-115, divide una prueba de penetración en 4 fases como se muestra en la figura 14:

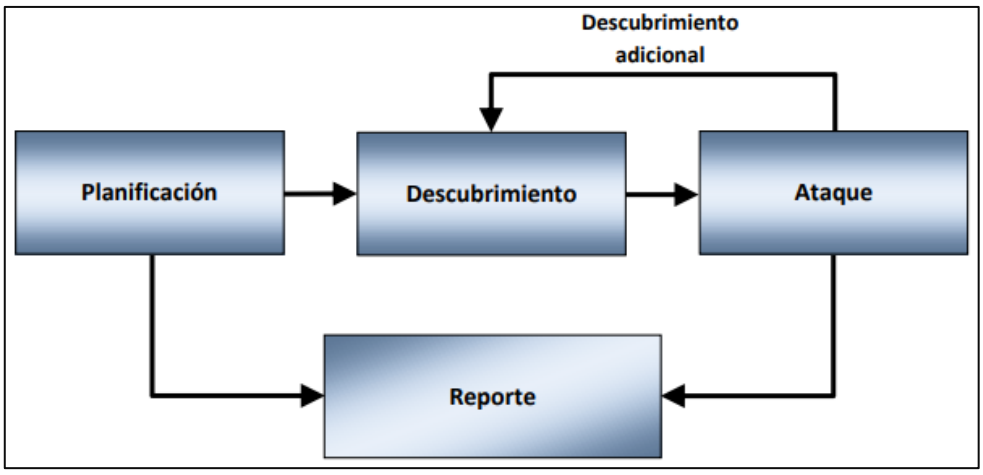


Fig. 14 Fases de la metodología NIST SP 800-115

Fuente: (AGUSTÍN LÓPEZ LÓPEZ, 2011)

- **Fase de Planificación.**

"Consiste en establecer los objetivos y las reglas de la prueba de penetración, para encaminar todo el proceso hacia un resultado satisfactorio para la organización que se va a auditar" (AGUSTÍN LÓPEZ LÓPEZ, 2011, pág. 11).

- **Fase de Descubrimiento.**

Se realiza el escaneo y recopilación de información de la infraestructura informática de la organización (AGUSTÍN LÓPEZ LÓPEZ, 2011).

"Se realiza el descubrimiento de vulnerabilidades a partir de la información recopilada de servicios, base tecnológica y otras informaciones que permitan realizar búsquedas en bases de datos de vulnerabilidades públicas o propias" (Henry Raúl González Brito, 2017).

- **Fase de Ataque.**

A partir de las vulnerabilidades o fallas identificadas previamente, el analista trata de aprender más acerca de la red específica y aprovechar las vulnerabilidades identificadas, si el analista es capaz de explotar una vulnerabilidad, puede instalar más herramientas en el sistema para obtener información y/o accesos adicionales, para determinar el nivel de acceso que un atacante podría adquirir. (AGUSTÍN LÓPEZ LÓPEZ, 2011, pág. 16).

- **Fase de Reporte.**

"En la fase de reporte, se describe las vulnerabilidades identificadas, se indica el proceso utilizado para la explotación de las mismas y finalmente se proporciona una guía de cómo mitigar las debilidades encontradas" (AGUSTÍN LÓPEZ LÓPEZ, 2011, pág. 17).

1.12.3 Metodología OSTTMM

Introducción.

El Manual de la Metodología Abierta de Testeo de Seguridad por sus siglas en inglés "Open Source Security Testing Methodology Manual", creado en el año 2001 por Pete Herzog, Director Ejecutivo de ISECOM (Instituto para la Seguridad y Metodologías Abiertas) una organización internacional sin ánimo de lucro (ISECOM, 2015).

Está es una metodología que permite evaluar la seguridad operacional de ubicaciones físicas, las interacciones humanas y todas las formas de comunicación como inalámbricas, cableadas, analógicas y digitales, es actualizada constantemente por expertos en el tema de seguridad y es considerado uno de los mejores manuales para pruebas de seguridad y métrica, se enfoca en los detalles técnicos de los elementos que necesitan ser comprobados, y el análisis va desde el proceso de comprobación, verificación hasta la evaluación de los resultados obtenidos, OSSTMM es un estándar profesional más completo y utilizado a la hora de realizar pruebas de seguridad de redes y en sistemas informáticos a través de testeos de intrusión con Hacking Ético, este manual permite el cumplimiento de normas y de mejores prácticas como las establecidas en la ISO 27001 - 27002 e ITIL entre otras (ISECOM, 2015).

Propósito manual.

- "Proveer de una metodología científica que permita evaluar a la organización, realizando pruebas sobre la seguridad operacional de adentro hacia afuera" (Aldo Valdez Alvarado, 2013, pág. 2).
- "Proveer guías para el auditor de sistemas informáticos, enfocadas a la certificación de la organización en cuanto a los requisitos del ISECOM" (Aldo Valdez Alvarado, 2013, pág. 2).

El Documento contiene una serie de descripciones específicas para la realización de un test de seguridad operacional, en las que se incluyen aspectos humanos, físicos, telecomunicaciones, medios inalámbricos y redes, y cualquier otra descripción derivada de una métrica real, como se muestra en la tabla 1.3.

TABLA 0.3 Ámbitos de OSSTMM

Clase	Canal	Descripción
Seguridad Física (PHYSSEC)	Humano	Comprende elementos humanos de la comunicación en donde la interacción es física o psicológica.
	Físico	Comprende el elemento tangible de la seguridad donde la interacción requiere esfuerzos físicos o de un transmisor de energía para manipular.

Seguridad Inalámbrica (SPECSEC)	Inalámbricos	Comprende todas las comunicaciones electrónicas, señales y emanaciones que tienen lugar sobre el espectro electromagnético.
Seguridad en las Comunicaciones (COMSEC)	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 pública.
	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.

Fuente: (C. L. Bracho & Cuzme, 2017)

La información de cada uno de los canales auditados se encuentra resumida en el Rav, que no es nada más que el balance de la porosidad, los controles y las limitaciones.

Características.

A continuación, se enumeran las principales características. (Lago, 2017).

- El RAV, calcula el valor actual de seguridad basado en seguridad operativa, pérdida de control, y limitaciones. El resultado, representa el estado actual de la seguridad del objetivo.
- Practicar la metodología OSSTMM ayuda a reducir los casos de falso negativo y falso positivo y provee mediciones de seguridad reproducibles
- La metodología es actualizada regularmente con nuevas tendencias de seguridad, normativas y planteamientos éticos.
- Asegura que la evaluación será llevada a cabo a fondo y resultados recogidos serán consistentes, cuantificables y de confianza.

1.12.4 Comparativa de las metodologías.

La Tabla 1.4 presenta la comparativa de las metodologías: OSSTMM, PTES y NIST SP 800-115.

TABLA 0.4 Comparativa de las metodologías

	OSSTMM	PTES	NIST SP 800-115
Ámbito operacional	Sí	No	No
Ámbito físico	Sí	No	No
Ámbito social	Sí	No	Sí
Guía técnica	No	Si	No
Métricas	Si	No	No
Informes	Sí	Sí	Sí
Gestión de proyecto	No	Sí	No

Fuente: Elaboración Propia.

El análisis comparativo de las metodologías OSSTMM, PTES, NIST SP 800-115; se lo realiza en base a varios factores: (Ortega & Leonel, 2017).

Ámbito operacional

Se Trata sobre los ámbitos de aplicación de las metodologías, de donde se puede rescatar que OSSTMM cumple en separar la seguridad de la información en un ámbito operacional, es decir buscar las limitaciones que poseen sus controles. (Ortega & Leonel, 2017).

Ámbito físico

En las metodologías PTES y NIST SP 800-115 se pueden aplicar técnicas de ingeniería social (Ortega & Leonel, 2017).

- **Guía técnica**

Este factor se refiere a que sí la metodología cuenta con una guía técnica de aplicación de las pruebas, de donde se puede rescatar que PTES cuenta con una guía detallada de

pruebas; pero OSSTMM, aunque no cuenta con una guía, dicta ejemplos de las pruebas que se deberían efectuar a lo largo de su contenido (Ortega & Leonel, 2017).

- **Métricas**

Una ventaja significativa con la que debe contar una metodología es de disponer de algún tipo de métrica que permita hacer un análisis cuantitativo del estado de la seguridad informática de la organización donde se efectué el proceso de la auditoría; y sólo OSSTMM cuenta con dichas métricas operacionales (Ortega & Leonel, 2017).

- **Informes**

Una vez que se haya concluido con el proceso de la auditoría, se debe contar con un informe donde se plasmen los resultados obtenidos de la misma (Ortega & Leonel, 2017).

- **Gestión de proyecto**

Se debe tomar en cuenta un aspecto que no es de mucha trascendencia para el auditor sobre la parte previa y posterior al proyecto puesto que esta tarea debe ser realizada por un Manager o Comercial de la organización (Ortega & Leonel, 2017).

CAPÍTULO 2

Herramientas de Kali Linux

2.1 Herramientas de Verificación del Tráfico de Red

Programas como tcpdump, Snort y Wireshark permiten al sistema y a los administradores de red ver el tráfico de una red proporcionando datos valiosos cuando se pretende buscar problemas en la red. En realidad, los programas de detección de intrusión de red como los mencionados anteriormente están basados en tecnología de husmeo y se utilizan para ver el comportamiento anormal al rastrear de una forma pasiva el tráfico de una red.

2.1.1 Wireshark

Historia

Wireshark conocido como Ethereal fue desarrollado inicialmente por Gerald Combs y se lanzó después de varias pausas en desarrollo en julio de 1998 como versión 0.2.0, a los pocos días empezaron a llegar parches, informes de errores y palabras de aliento y Ethereal estaba en camino hacia el éxito, la lista de personas que han contribuido en el programa Wireshark es demasiado extensa desde sus inicios hasta la actualidad, y la mayoría de los contribuyentes comenzaron con un protocolo que necesitaban de Wireshark o que ya no manejaban, así que copiaron un disector existente y contribuyeron con el código al equipo (Gerald Combs, 2018).

En 2008, Wireshark finalmente llegó a la versión 1.0, esta versión fue la primera que se consideró completa, con las características mínimas implementadas, en 2015 se lanzó Wireshark 2.0, que contó con una nueva interfaz de usuario, en la actualidad es una herramienta imprescindible a la hora de realizar una auditoría a la red (Gerald Combs, 2018)

Definición.

“Wireshark es una aplicación multiplataforma se distribuye bajo licencia GPL de libre distribución” (Moreno Pérez & Santos González, 2014). (Díaz) 2014 afirma: “Wireshark Permite analizar su tráfico y los paquetes de datos enviados de ida y vuelta, además que permite analizar cientos de protocolos distintos (pág. 96).

Wireshark “Se puede instalar en todos los sistemas operativos, Linux, Windows, Solaris, Mac OS, etc, esto es lo que lo hace tan popular” (Gómez Beas, 2014, pág. 109). Posee

versión gráfica como se muestra en la figura 15, y una versión de línea de comandos, “la herramienta gráfica se incluye con decodificadores de protocolos que son muy amplios y actualizados, la versión de línea de comandos se denomina tethereal, y requiere que el controlador Winpcap esté instalado en el sistema remoto” (Scambray & McClure, 2009, pág. 200).

Los equipos y redes a menudo tienen cierta cantidad de datos transferidos a los dispositivos dentro de la red, entonces los administradores de red establecerán una línea base, o una cantidad establecida de tráfico considerada normal, cuando el tráfico está fuera de esta línea sin razón, empiezan a buscar posibles intrusos o malware. (Orloff, 2009, pág. 100).

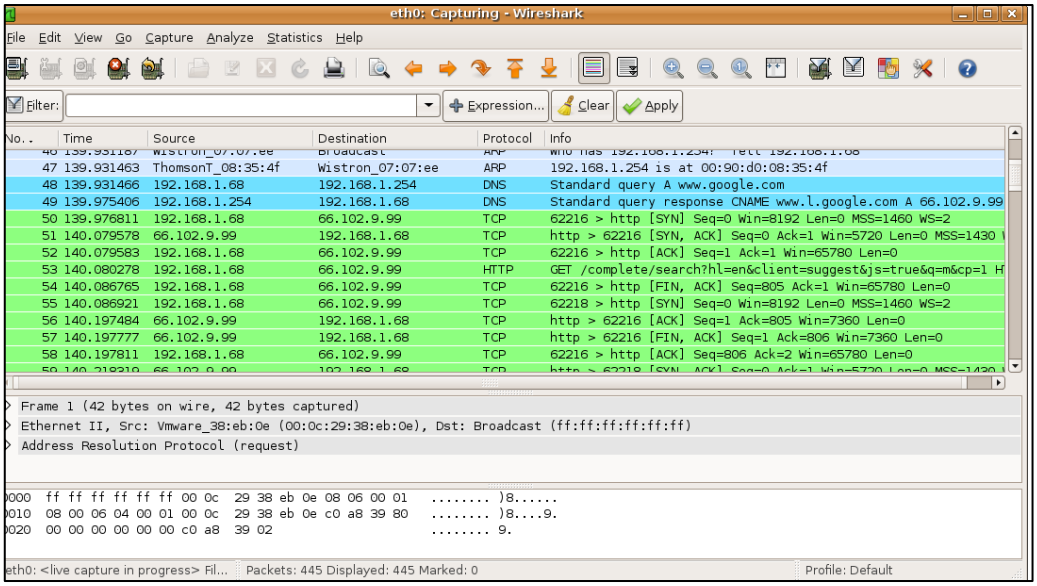


Fig. 15. Interfaz Gráfica de Wireshark

Fuente: Propia

Características

Dispone de las características siguientes: (Chicano Tejada) 2014 afirma que:

- Captura los paquetes directamente desde una interfaz de red.
- Permite obtener información detallada del protocolo utilizado en el paquete de datos capturado.
- Puede importar y/o exportar los registros capturados desde/hacia otras aplicaciones.
- Busca los registros de información que cumplan con un criterio establecido previamente por el usuario.
- Ofrece informes y estadísticas (pág. 133).

Permite identificar y analizar el tráfico de red en un momento determinado entre estas características destacan: (Chicano Tejada) 2014:

- Permite analizar más de 480 protocolos.
- Captura directamente los paquetes de datos desde una interfaz de red.
- Con el análisis del paquete capturado, se obtiene información del protocolo utilizado.
- Permite importar y/o exportar los paquetes de datos capturados a otras aplicaciones.
- Filtra los paquetes de datos atendiendo a unos criterios definidos por el usuario.
- Ofrece estadísticas del tráfico de red.
- Es una herramienta gratuita.
- Examina los datos de la red de un archivo de captura guardado en disco y permite analizar la información capturada mediante los detalles y sumarios de cada paquete.
- Se puede utilizar en varios sistemas operativos como Windows, Linux, Unix, etc.
- No está disponible en español (pag 205)**.**

2.1.2 Tcpdump

Es una herramienta de línea de comandos como se muestra en la figura 16, imprescindible para cualquier administrador de sistemas, original de Linux, el código es de libre distribución (Barceló Ordinas, Íñigo Griera, & Llorente Viejo, 2008).

tcpdump permite.

> Analizar el tráfico de la red por medio de conexión (LAN o punto a punto), Al contrario de lo que su nombre indica, Captura todo el tráfico de la red y es capaz de interpretar los paquetes no sólo en el ámbito TCP, sino también en el IP, LAN, y aplicación (para aplicaciones comunes (Barceló Ordinas, Íñigo Griera, & Llorente Viejo, 2008).

Los paquetes leídos se muestran en pantalla o se pueden almacenar en un fichero del disco para ser manipulados posteriormente por otra herramienta avanzada u esta misma herramienta, es necesario privilegios para ejecutarla, porque se necesita poner la tarjeta de red en modo promiscuo para que acepte todos los paquetes, (Roa Buendía, 2013). Es fácil de instalar y tiene muchas opciones para los paquetes capturados en la red.

Fig. 16. Línea de comandos Tcpdump

Fuente: Propia

2.1.3 Snort

(Chicano Tejada) 2014 afirma que:

> Se trata de una de las herramientas más utilizadas para detectar intrusiones en la red, aunque también es frecuentemente utilizada como analizador, Dispone de un motor bastante potente para la detección de intrusiones, ataques y realizar escaneos de puertos para registrar todos los eventos destacables y generar alertas en aquellos eventos que supongan (pág. 201).

"Permite analizar todo el flujo de paquetes que atraviesan por los interfaces de red de un sistema para comprobar mediante firmas si son o no ataques, Snort dispone de varios frontales gráficos para facilitar su manejo" (Álvarez Marañón & Pérez García, 2004, pág. 348), como se muestra en la figura 17.

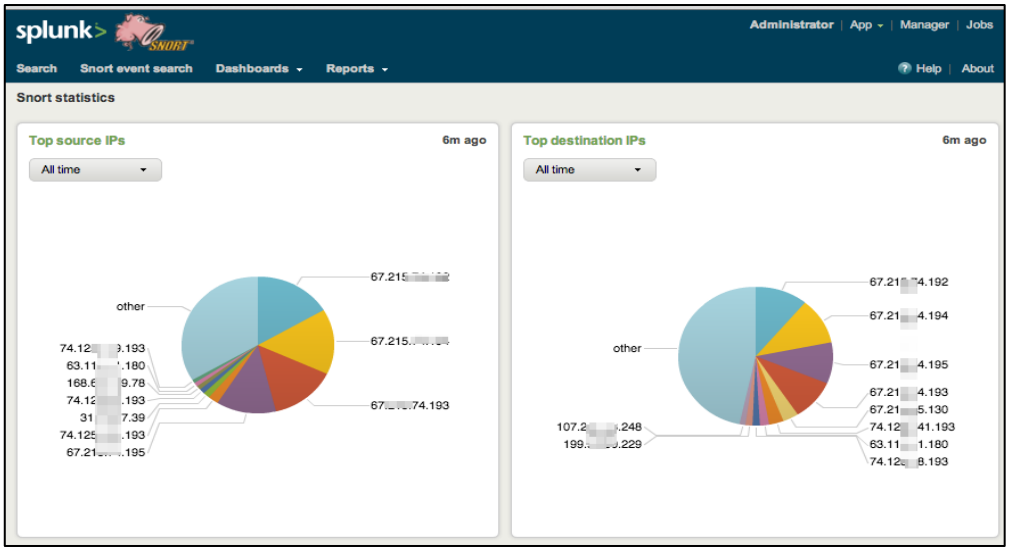


Fig. 17. Interfaz gráfica de Snort

Fuente: Propia

2.1.4 Porque utilizar Wireshark

Se ha escogido la herramienta Wireshark como mejor herramienta de visualización del tráfico de la red por sus características como lo muestra la tabla 2.1.

TABLA 0.1 Comparativa de las herramientas de visualización del tráfico de red

	Snort	**tcpdump**	**Wireshark**
Analizador de protocolos de red.	si	si	si
Interfaz gráfica de usuario	si	no	Si
Sistema de detección de intrusos en una Red.	si	no	No
Software gratuito	si	Si	si
Informe detallado de resultados	si	si	si
Crear estadísticas	no	no	si
Abrir y guardar datos de paquetes capturados	no	si	si
Sistema Robusto	no	no	si

Soporte de la mayoría de los protocolos	no	no	si
Captura de paquetes en tiempo real	si	si	si

Fuente: Propia

2.2 Herramientas de Verificación de Puertos

Introducción

"Un puerto es una interfaz (consistente en un numero denominado número de puerto) para comunicarse con un programa a través de la red" (Romero, 2010, pág. 101). En las tareas de auditoría de seguridad informática, también ese importante conocer los puertos y servicios que se utilizan cada vez que se envía y se recibe datos dentro de una red.

La variedad de herramientas con funciones de análisis de red, puertos y servicios es muy amplia, siendo muchas de ellas de código abierto y compatibles con varios sistemas operativos. De estas herramientas, se mencionan a Nmap, Nessus y Netcat, las cuales se describen a continuación.

2.2.1 Nmap

Nmap (Network Mapper) Es una utilidad libre de código abierto utilizada para la exploración de redes y la auditoria de sistemas y aplicaciones, es una herramienta muy optimizada en la que permite realizar grandes comprobaciones de red en tiempos cortos (Sanz Mercado, 2008)*.*

Historia

Desarrollado desde cero y realizada en código C, Nmap nació con la idea de unificar en una sola herramienta multitud de escáneres de puertos de código abierto como: Julian Assange Scanner, Reflscan SYN Scanner, FIN Scanner y entre otros, tratando de superar las limitaciones que por separado tenía cada uno de ellos, esta herramienta fue escrita por un hacker llamado Gordon Lyon. («Nmap: the Network Mapper - Free Security Scanner», s. f.)

Durante el transcurso del tiempo, la herramienta Nmap y la comunidad a su alrededor han crecido de una manera significativa, lo que ha dotado a la herramienta de nuevas características y funcionalidad, convirtiéndola hoy por hoy en una suite de prestigio. («Nmap: the Network Mapper - Free Security Scanner», s. f.).

Definición

Nmap (Network Mapper) es una utilidad para la exploración de redes y auditoría de seguridad muy optimizada para realizar grandes comprobaciones de red en tiempos cortos. (Sanz Mercado, 2008)***, "***aunque funciona muy bien contra equipos individuales". (Giménez Albacete, 2014, pag 392)

Su función es escanear un anfitrión buscando puertos TCP y UDP abiertos. Cuando puede hallar uno, Nmap realiza un intento de conexión de manera que puede identificar qué aplicación está activa en ese puerto. Ésta es una manera sencilla y poderosa para que un administrador revise lo que su sistema expone a la red (Shah & Soyinka, 2007), y cuenta con una interfaz gráfica llamada Zenmap figura 18.

"Nmap interpreta la mayoría de los protocolos estándar empleados en la actualidad, lo que le permite devolver información mucho más completa que un listado de puertos abiertos" (Giménez Albacete, 2014, pag 392). También puede determinar qué tipos y versiones de sistemas operativos está utilizando cada host, qué tipo de cortafuegos o filtros de paquetes se están utilizando, etc, (Díaz Orueta, Alzórriz Armendáriz, & Sancristóbal Ruiz, 2014).

Características

Las características destacables de Nmap según (Díaz & Alzórriz & Sancristóbal) 2014 son:

- Flexibilidad: Permite utilizar diferentes técnicas para mapear redes, incluso cuando éstas están protegidas por cortafuegos o filtros de paquetes. Estas técnicas incluyen diferentes mecanismos para el escaneo de puertos, identificación de sistemas operativos, sus versiones, etc.
- Facilita información sobre los servicios que se están ejecutando en el sistema de información.
- Potencia: Nmap ha sido utilizada para escanear redes con cientos de miles de hosts conectados a la misma.
- Documentación: Nmap está ampliamente documentada en varios idiomas. Se puede acceder a dicha documentación desde http:// nmap.org/docs.html (pag 285)

La información extraída con Nmap puede ser utilizada para múltiples usos. Los más habituales son los siguientes: (Nmap: the Network Mapper - Free Security Scanner», s. f.)

- Descubrimiento de subredes.
- Análisis de penetración de redes y equipos.

- Evaluación de la implantación de cortafuegos y de la eficacia de herramientas de detección y prevención de intrusiones.
- Descubrimiento del estado de puertos de comunicaciones.
- Descubrimiento de los servicios disponibles en un servidor, así como de sus versiones.
- Descubrimiento del tipo y versión del sistema operativo instalado en el equipo remoto.
- Obtención de información adicional acerca de servicios y equipos, a través de la ejecución de scripts convenientemente elaborados.

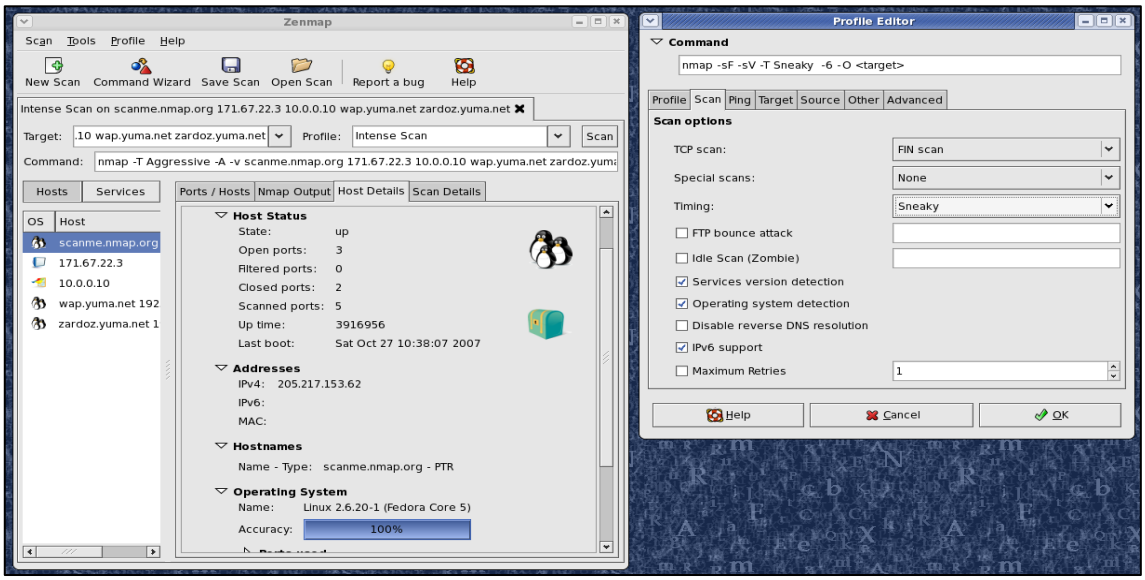


Fig. 18. Interfaz gráfica de Nmap

Fuente: Propia

2.2.2 Nessus

Este es un software parecido a Nmap, ya que es capaz de escanear equipos en busca de potenciales vulnerabilidades mediante un daemon, o incluso realizar los propios escaneados con Nmap, y a través de un cliente Nessus interactuar con el programa. La diferencia con Nmap radica en que una vez que son detectadas las vulnerabilidades del sistema dispone de exploits para atacar dichas vulnerabilidades (Solé Almagro, 2015, pag 206), y cuenta con una interfaz gráfica figura 19.

Tiene una forma distinta de funcionar. Se necesita instalar nessus en un ordenador que a partir de ese momento será un servidor, al cual se puede conectar desde cualquier ordenador (incluso él mismo) con un programa cliente, para así realizar un escaneo al ordenador u ordenadores que se desee (Sanz Mercado, 2008).

“Esta forma de trabajar permite tener una máquina dedicada a la realización de escaneos en red, pudiendo monitorizar desde cualquier ordenador que posea un programa cliente (incluso este último ordenador puede ejecutar el sistema operativo Windows)” (Sanz Mercado, 2008, pág. 88).

Una vez realizada esta operación la idea es exactamente equivalente a la de nmap, es decir, se puede realizar un análisis de un ordenador o de una red, buscando los puertos abiertos y además buscando debilidades en los programas que se ejecutan en estos puertos abiertos. Esto último es otra gran diferencia con respecto a nmap, ya que con nmap se llega hasta encontrar los puertos abiertos, mientras que con nessus se intenta ver si son vulnerables o no los servicios que están ejecutándose, por lo tanto hay que tener mucho más cuidado con este programa, ya que se puede rozar el límite entre lo permitido y lo no permitido si se escanea máquinas que no pertenecen al auditor, se debe tener en cuenta que es posible que la prueba de vulnerabilidades puede provocar una denegación de servicio contra la máquina escaneada. (Sanz Mercado, 2008, pag 88)

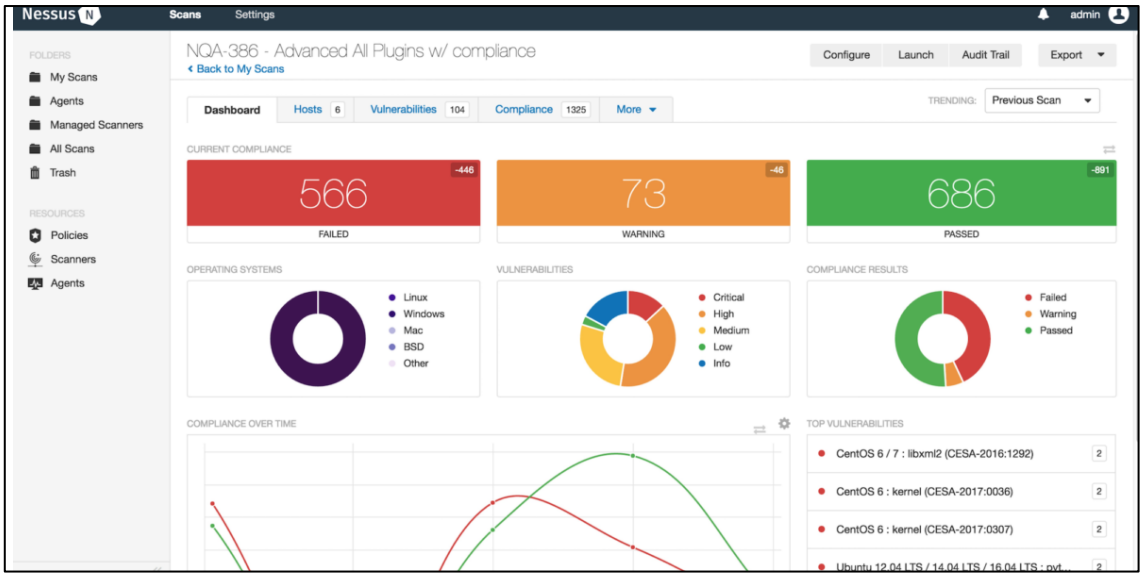


Fig. 19. Interfaz gráfica de Nessus

Fuente: Propia

2.2.3 Netcat

“La herramienta Netcat se ha hecho casi imprescindible en el ámbito de la seguridad informática, hasta tal punto que se denomina comúnmente la navaja suiza de la seguridad de la red, por sus innumerables posibilidades de uso” (Chicano Tejada, 2014, 194).

Netcat “permite utilizar conexiones TCP y UDP desde la línea de comandos Figura 20 (por ejemplo, transmitir un fichero) o comprobar qué puertos tiene abiertos una determinada máquina, entre otros servicios” (Barceló Ordinas, Íñigo Griera, & Llorente Viejo, 2008, pag 44).

No obstante, cabe destacar también otras funciones como(Chicano) 2014:

- Chat: poniendo uno de los equipos en modo servidor y otro equipo en modo cliente.
- Envío y recepción de ficheros: transmitir ficheros de un equipo cliente a un servidor.
- Escaneo de puertos: se puede optar por escanear todos los puertos de un equipo determinado o decidir qué puertos concretos escanear.
- Servidor web: con Netcat, puede utilizarse el equipo servidor un solo fichero HTML de forma puntual.
- Ejecución de la herramienta en modo silencioso.
- Obtención de una shell para conocer las conexiones del equipo con el sistema operativo Unix.

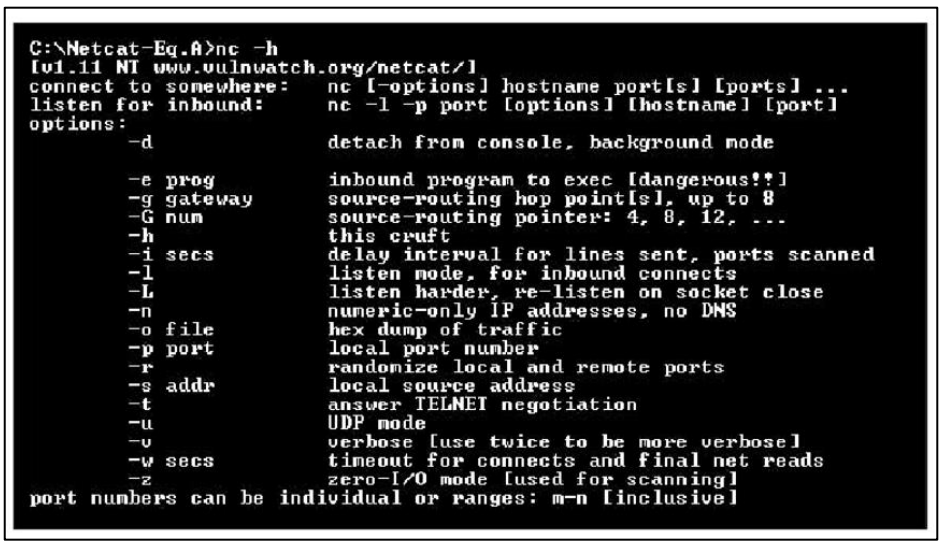


Fig. 20. Línea de comandos de Netcat

Fuente: Propia

2.2.4 Porque utilizar Nmap

Se ha escogido la herramienta Nmap como mejor herramienta de verificación de puertos debido a que es un sistema robusto y el mejor en su área como lo muestra la tabla 2.2.

TABLA 0.2 Comparativa de las herramientas de verificación de puertos

	NESSUS	**NETCAT**	**NMAP**
Escaneo en IPv4 e IPv6	Si	Si	Si
Escaneo de host	Si	No	Si
Denegación de servicios	Si	Si	no
Informe detallado de resultados	Si	No	Si
interfaz gráfica de usuario	Si	No	Si
Generación de tráfico basura en la red.	Si	Si	no
Software gratuito	no	Si	Si
Comprobación de la configuración de los elementos de seguridad (sistema cortafuegos, sistemas de detección de intrusos, entre otros.)	Si	no	Si
Comprobación de la configuración de los elementos de red (fallos, encaminamiento de la red, dispositivos de conectividad, entre otros)	Si	no	Si
Alta velocidad de exploración.	Si	no	Si
Modelo cliente-servidor	Si	Si	no

Fuente: Propia

2.3 Herramientas de Captura de Contraseñas en la Red

La función de este tipo de programas consiste en realizar la captura de paquetes que se envían y reciben a través de la red, a estos programas se les conoce como sniffers, un sniffer es un "programa que registra todo el tráfico de la red en busca de contraseñas y datos relevantes que se transmiten" (Aguilera, 2011, pág. 171), a continuación se describe la utilización de herramientas como son Kismet, asleap y la suite aircrack-ng

2.3.1 Aircrack-ng

Historia

Aircrack-ng es de código abierto realizado en lenguaje ensamblador y lenguaje C desarrollado por Thomas D'Otreppe, esta plataforma se encuentra en la versión 1.4 desarrollada para funcionar en sistemas Linux, tiene gran popularidad y se encuentra en distribuciones como BackTrack (Kali), WifiSlax o WifiWay, dedicadas a la auditoría de seguridad, Aircrack-ng es una bifurcación del proyecto original de Aircrack (Thomas Otreppe, s. f.).

Definición

Aircrack es un analizador de paquetes e inyector de paquetes multiplataforma, es toda una suite de herramientas que, combinadas todas, pueden descifrar contraseñas Wifi de tipo WEP y WPA/WPA2-PSK.

Aircrack-ng puede recuperar claves WEP una vez que se han capturado suficientes paquetes encriptados con su herramienta airodump-ng combinando ataques estadísticos con ataques de fuerza bruta, mientras que, para recuperar claves de tipo WPA/WPA2-PSK se la realiza por medio de un diccionario de palabras preconocidas. (Hurley, Rogers, Thornton, & Baker, 2007).Las herramientas que contiene suite son las siguientes: (Thomas Otreppe, s. f.)

- airbase-ng
- aircrack-ng
- airdecap-ng
- airdecloak-ng
- airdriver-ng
- aireplay-ng
- airmon-ng
- airodump-ng
- airdecloak-ng
- airolib-ng
- airserv-ng
- airtun-ng
- easside-ng
- packetforge-ng

- tkiptun-ng
- wesside-ng

Las herramientas más utilizadas para la Auditoría inalámbrica son:

- Aircrack-ng (Herramienta que descifra claves de los vectores de inicio)
- Airodump-ng (Herramienta de escaneo a la red, y capturas vectores de inicio)
- Aireplay-ng (Herramienta que inyecta tráfico para elevar la captura de vectores de Inicio)
- Airmon-ng (Herramienta para poner la tarjeta inalámbrica en modo Monitor, y poder capturar e inyectar vectores)

La suite está diseñada para trabajar con una distribución Linux, aunque también existe una versión para Windows que no es muy estable debido a conflictos con drivers. Esta suite está diseñada para trabajar con tarjetas inalámbricas cuyo chip sea Atheros y con algunas de chip Railink sin necesidad de configurarlas. Aunque se ha logrado usar la suite en otros chips, con configuraciones especiales en Linux. (Thomas Otreppe, s. f.), en la figura 21 se muestra la interfaz gráfica.

Características

Se enfoca en diferentes áreas de seguridad de la red inalámbrica como: (Thomas Otreppe, s. f.).

- Monitoreo: captura de paquetes y exportación de datos a archivos de texto para su posterior procesamiento por parte de herramientas de terceros.
- Ataque: Repetición de ataques, desautorización, puntos de acceso falsos y otros mediante inyección de paquetes.
- Pruebas: Comprobación de las tarjetas wireless y capacidades del controlador (captura e inyección).
- Agrietamiento: WEP y WPA/WPA2-PSK.

Aircrack-ng es la nueva generación de aircrack con gran cantidad de nuevas funcionalidades como: (Thomas Otreppe, s. f.).

- Aumento de número de tarjetas y drivers soportados
- Aumento del número de sistemas operativos soportados
- Nuevos ataques WEP soportados: PTW (aircrack-ng)
- Ataque de diccionario WEP (aircrack-ng)
- Ataque de fragmentación (aireplay-ng)
- Alta velocidad de crackeo (aircrack-ng)
- Capturar de múltiples tarjetas (airodump-ng)
- Nuevas herramientas: airtun-ng, packetforge-ng (arpforge mejorado), wesside-ng, easside-ng, airserv-ng, airolib-ng, airdriver-ng, airbase-ng, tkiptun-ng y airdecloak-ng

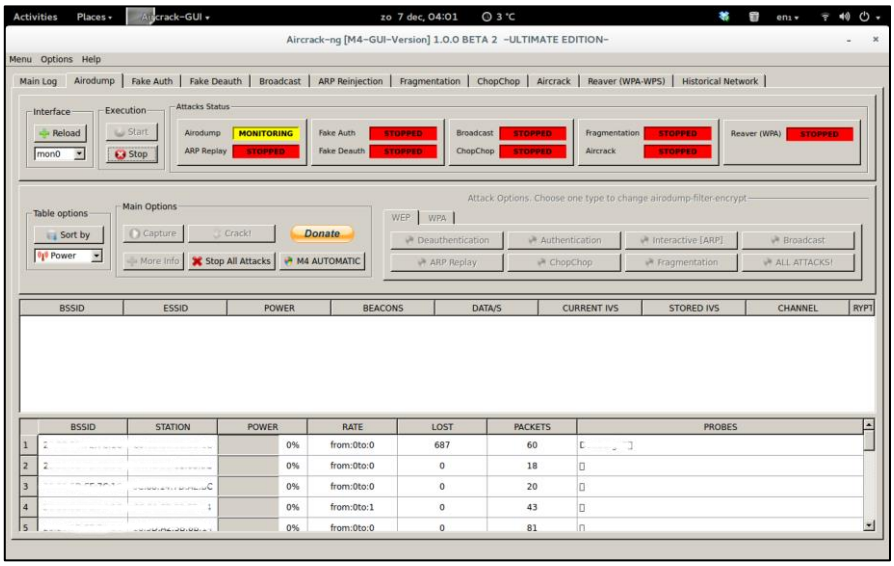


Fig. 21. Interfaz gráfica de Aircrack-ng

Fuente: Propia

2.3.2 Kismet

Kismet fue desarrollado por Mike Kershaw, es un sniffer y un sistema de detección de intrusiones para redes inalámbricas, cuenta con una interfaz gráfica figura 22, y funciona en sistemas operativos como: Linux, FreeBSD, NetBSD, OpenBSD, y Mac OS X. La diferencia de Kismet con otros tipos de sniffers inalámbricos se encuentra en su funcionamiento pasivo. Es decir que no envía paquetes detectables, permitiendo detectar la presencia de varios puntos de acceso y clientes inalámbricos, asociando unos con otros (Mike Kershaw, s. f.).

Para usar Kismet, hay que instalar los controladores personalizados necesarios para la operación de modo de monitores (Modo supervisor o modo del sistema). Esto varía

dependiendo de los chips, la tarjeta inalámbrica, pero Kismet viene con una sola forma de habilitarlos todos para la operación de monitor. (McClure, Scambray, & Kurtz, 2010).

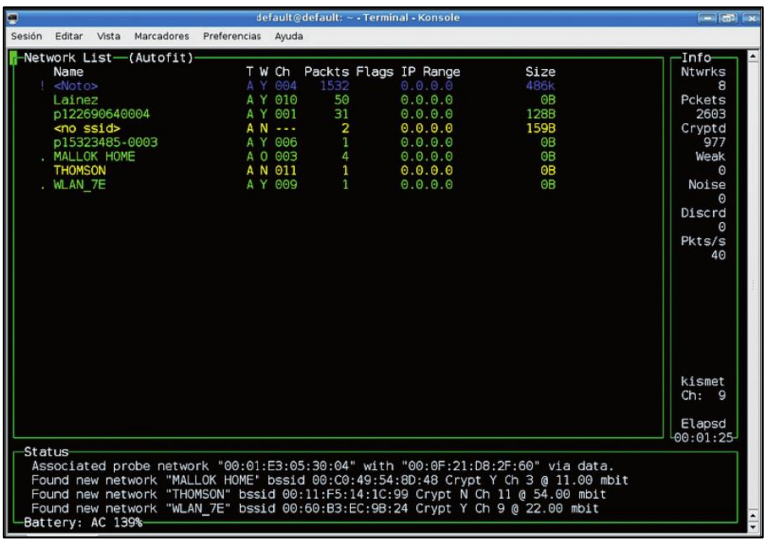


Fig. 22. Interfaz gráfica de Kismet

Fuente: (Chicano Tejada, 2014)

Características:

- Permite exportar todo el tráfico capturado a wireshark
- Disponible en Linux y soporte limitado para Windows
- Permite conexión con GPS, útil para wardriving (Búsqueda de redes desde un vehículo en movimiento)

2.3.3 Asleap

Asleap es una herramienta de seguridad inalámbrica diseñada para capturar y descifrar contraseñas LEAP (protocolo de autenticación ampliable desarrollado por Cisco) débiles de puntos de acceso inalámbricos y las correspondientes tarjetas inalámbricas de Cisco. Asleap está disponible en línea de comandos figura 23, también puede leer tráfico de cualquier tarjeta de red inalámbrica por medio del modo RFMON (modo de monitor), o en caso de que quiera vigilar varios canales de frecuencia, da soporte a saltos. En caso de que se identifique una tarjeta inalámbrica o un punto de acceso, la información obtenida se despliega al usuario casi en tiempo real. Los archivos PCAP o los archivos OmniPeek almacenados pueden utilizarse como entradas, en caso de que se analicen o procesen datos posteriores al tiempo real. (McClure et al., 2010)

La característica única de Asleap es que puede integrarse con Air-Jack para derribar a usuarios inalámbricos autentificados de redes inalámbricas de destino. El beneficio de esta

característica es que pueda des autentificar a cada usuario en una red para forzarlo a que vuelva a autentificar el punto de acceso. Después, cuando el usuario se vuelva a autentificar en un dispositivo de Cisco con LEAP habilitado, su contraseña se olfateará y romperá con Asleap. (McClure et al., 2010, pag 485)

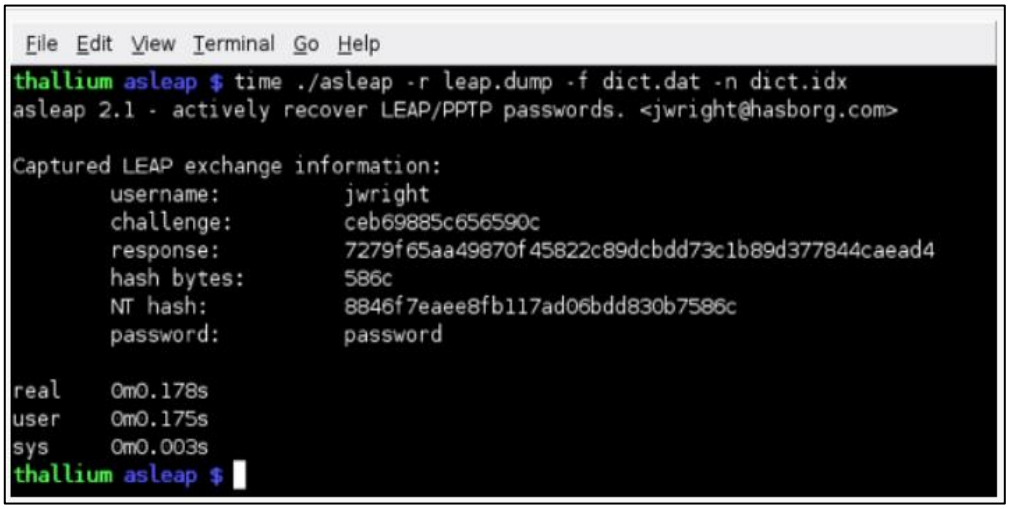


Fig. 23. Línea de comandos Asleap

Fuente: (Chicano Tejada, 2014)

2.3.4 Por qué utilizar Aircrack-ng

Se ha escogido la herramienta Aircrack-ng como mejor herramienta de captura de paquetes dentro de la red por sus características como lo muestra la tabla 2.3.

TABLA 0.3 Comparativa de las herramientas de captura de contraseñas en la red

	Asleap	**Kismet**	**Aircrack-ng**
interfaz gráfica de usuario	No	si	si
Crackeador de redes WEP y WPA/WPA2-PSK	No	no	si
Software gratuito	Si	si	Si
Sistema Robusto	No	no	si
Captura y exportación de paquetes de datos	Si	Si	si
inyección de paquetes	No	No	si
Ataques de diccionario	No	no	si

Fuente: Propia

2.4 Otras herramientas a utilizar

2.4.1 Maltego

Maltego es una herramienta utilizada para la recopilar información por la capacidad que posee para obtener los datos y la manera intuitiva en que son presentados, por eso, a partir de la recopilación la herramienta maltego se encarga de mostrar la información de manera gráfica ordenada y entendible (Hector Jara, s. f.).

2.4.2 Dnsrecon

Es una herramienta desarrollada en Ruby por Carlos Pérez, desarrollador en el proyecto MetaSploit, Dnsrecom es una herramienta de recuperación de información mediante el uso de servidores DNS, se debe especificar a una dirección IP de inicio y una dirección Ip final dejando a elección las redes que se desea escanear, además que permite la recuperación automática de información de todos los TLD (Top Level Domain) asociados a un nombre (RAULT et al., 2015).

2.4.3 Dnsenum

Esta herramienta permite obtener mucha información sobre los servidores DNS de un dominio determinado como: servidor de nombres, transferencia de zona, subdominios, servidores MX, fuerza bruta en DNS (RAULT et al., 2015).

2.4.4 Sparta

Sparta es una aplicación GUI de python su objetivo es simplificar algunas tareas involucradas en las fases de exploración y enumeración durante la realización de una prueba de penetración a la infraestructura de red, permite ahorrar tiempo en la ejecución de diversas herramientas de manera simultánea al tener acceso de “apuntar y hacer clic”, permite ejecutar nmap desde Sparta también importar resultados en forma XML (Antonio Quina, 2015).

CAPÍTULO 3

Aplicación de la Metodología

De acuerdo con el Manual de la Metodología Abierta de Testeo de Seguridad OSSTMM en su versión 3 se plantea en seguir el proceso de cuatro puntos, en el cual no se tiene que mostrar cada paso que se hace, pero si se debe entender cómo se llegó de A, a la C (Pete Herzog, 2010). A continuación se describe el proceso de cuatro puntos:

- **Fase de Inducción**

Cada viaje comienza con una dirección, en esta fase el analista comienza la auditoría entendiendo los requisitos, el alcance y las limitaciones de la auditoría en dicho alcance, a menudo, el tipo de prueba se determina mejor después de esta fase (Pete Herzog, 2010). Para esta fase es necesario realizar una revisión de los requisitos que son necesarios para comenzar con la auditoria, estos son autorización formal escrita por la persona encargada del área de redes y comunicaciones del DDTI, quien cuidará que el proceso se lleve a cabo dentro de los márgenes permitidos por la ley, y que la información obtenida sea únicamente para fines evaluativos.

- **Fase de Interacción**

El analista investigará o agitará el objetivo para desencadenar respuestas para el análisis (Pete Herzog, 2010). Es decir, recopilar información a través de observaciones, entrevistas, encuestas a los encargados de interactuar con los sistemas o con las solicitudes de documentos e información, de tal manera que se pueda evaluar la seguridad actual de un canal a ser auditado: Seguridad operacional, controles y limitaciones.

- **Fase de Indagación**

El analista investiga las emanaciones del objetivo y de las pistas o indicadores de esas emanaciones, un sistema o proceso generalmente dejará una firma de su existencia a través de interacciones con su entorno (Pete Herzog, 2010). En esta fase se aplicarán técnicas escogidas y descritas en cada uno de los canales las cuales son: canal físico, humano, Inalámbrico y redes de datos. Para luego proceder a realizar pruebas que permitan encontrar los valores numéricos por cada ítem o literal dentro de un canal.

- **Fase de Intervención**

Estas pruebas se centran en los recursos de los objetivos requeridos en la aplicación, mismos que se pueden intercambiar, cambiar, sobrecargar, o morir a causa de la penetración o interrupción, esto es a menudo es la fase final de una prueba de seguridad (Pete Herzog, 2010). En esta fase es necesario generar informes para cada canal auditado mediante el uso de la hoja de cálculo propio de la metodología en la que permite valorar la eficiencia o deficiencia de seguridad de un canal.

Además la metodología plantea seis tipos de pruebas: prueba ciega o hacking ético, prueba de penetración o caja negra, caja blanca, caja gris, Tándem e Inversión, (Pete Herzog, 2010). De la cual se eligió la prueba de Caja Gris para el desarrollo de las pruebas de los canales a evaluar: físico, humano, redes de datos y comunicación inalámbrica, de esta metodología. Para que la persona responsable del área de Sistemas y Redes del DDTI de la UTN establezca mecanismos de defensa con anticipación de esta manera permitir al analista obtener datos más reales de la auditoria aplicada, además de brindar cierta información al analista. Para empezar con la auditoria se obtuvo un permiso de la persona responsable del área de Sistemas y Redes del DDTI para poder adquirir la información específica del personal de DDTI.

Métrica Operacional

La métrica proporcionada por la metodología OSSTMM es una medida a escala de la superficie de ataque (RAV), la cual permite medir con valor numérico la cantidad de interacciones no controladas en contra de un objetivo, se calcula mediante el equilibrio cuantitativo entre operaciones, limitaciones y controles la relación existente se evidencia en la tabla 3.1, el RAV no puede decir si un objetivo en particular será atacado, pero sí puede decir contra que ataques puede defenderse con éxito, a que profundidad puede llegar un atacante y cuanto daño puede hacer, tener el RAV es entender qué parte de la superficie de ataque está expuesta, en esta escala está representada de dos maneraras:100 RAV o 100%RAV por simplicidad de comprensión, aunque no es precisamente un porcentaje es el equilibrio perfecto, menos de 100 RAV existe poco control y por lo tanto una mayor superficie de ataque y más de 100 RAV muestra más controles de los que son necesarios, lo que puede ser un problema, ya que los controles a menudo agregan interacciones dentro de un alcance, así como problemas de complejidad y mantenimiento (Pete Herzog, 2010).

TABLA 0.1 Estructura del RAV

Categoría		**Seguridad operacional**	**Limitaciones**
Operaciones		Visibilidad **(PV)**	Exposición **(LE)**
		Acceso **(PA)**	
		Confianza **(PT)**	Vulnerabilidad **(LV)**
Controles	Clase A	Autenticación **(LCAu)**	Debilidad **(LW)**
		identificación **(LCID)**	
		Resistencia **(LCRe)**	
		Subyugación **(LCSu)**	
		Continuidad **(LCCt)**	
	Clase B	No repudio **(LCNR)**	Preocupación **(LC)**
		Confidencialidad **(LCCf)**	
		Privacidad **(LCPr)**	
		Integridad **(LCIt)**	
		Alarma **(LCAl)**	
			Anomalías **(LA)**

Fuente: Elaboración propia

RAV

Una forma simple y sencilla de hacer RAVS es utilizar las hojas de cálculo creadas específicamente para obtener el valor de la superficie de ataque y varias métricas requeridas a partir de los datos obtenidos en las pruebas, esta hoja de cálculo se encuentra disponible en la página web de ISECOM, con la hoja de cálculo el analista sólo necesita ingresar los valores en las casillas blancas vacías y el resto de los cálculos se manejan automáticamente (Pete Herzog, 2010).

En el RAV Se obtiene lo que se sabe de lo que hay para un vector en particular y no se hace suposiciones que rodean lo que no está allí, en el RAV se cuenta todo lo que es visible e interactivo fuera del alcance y permite la interacción no autenticada entre otros objetivos en el alcance, esto se convierte en la primera parte la porosidad, la siguiente parte es calcular los 10 controles tales como autentificación, subyugación, no-repudio, etc., cada control se valora como el 10% de un poro ya que cada uno proporciona 1/10th de los controles totales necesarios para prevenir todos los tipos de ataque, La tercera parte del RAV se basa en las limitaciones encontradas en la protección y los controles, estos también son conocidos como “Vulnerabilidades”, el valor de estas limitaciones proviene de la porosidad y los propios controles establecidos, con todos los conteos completados, el RAV básicamente resta la

porosidad y las limitaciones de los controles (Pete Herzog, 2010). Entonces el RAV se interpreta de la siguiente manera:

R A V = CONTROLES VERDADEROS – POROSIDAD – LIMITACIONES

Ecuación 1: Ecuación de cálculo de la seguridad

Fuente: (Herzog, 2010)

De la estructura del RAV de la tabla 4 se obtienen las siguientes ecuaciones según la metodología OSSTMM.

Porosidad

También conocida como la seguridad operacional del alcance, es el primero de los tres factores que permiten obtener la medición de la seguridad real actual a calcular de los canales: físico, humano, redes de datos y comunicación inalámbrica. Se mide inicialmente como la suma de la visibilidad del alcance **(P_V)**, el acceso **(P_A)** y confianza **(P_T)** (Pete Herzog, 2010).

La fórmula de la ecuación es:

$$OpSec_{sum} = (P_V) + (P_A) + (P_T)$$

Ecuación 2: Ecuación de la porosidad

Fuente: (Herzog, 2010)

Controles

El segundo paso para calcular el valor del RAV es definir los Controles, es decir los mecanismos de seguridad puestos en marcha para proteger la seguridad, para obtener el valor **LC_{sum}** se debe determinar la suma de las 10 categorías de controles divididos en dos grupos de cinco, así controles de Clase A: Autenticación **(TC_{Au}),** Identificación **(TC_{Id}),** Resistencia **(TC_{Re}),** Subyugación **(TC_{Su}),** Continuidad **(TC_{Ct}),** controles de Clase B: No repudio **(TC_{NR}),** Confidencialidad **(TC_{Cf}),** Privacidad **(TC_{Pr}),** Integridad **(TC_{It})** y Alarma **(TC_{Al})** (Pete Herzog, 2010).

La fórmula de la ecuación es:

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

Ecuación 3: Suma de controles

Fuente: (Herzog, 2010)

Para determinar los controles ausentes de la autenticación **(MC_{Au})**, hay que restar la suma de controles de autenticación de la seguridad operacional **($OpSec_{sum}$) − (TC_{Au})** pero siempre se debe tomar en cuenta que los controles ausentes **(MC_{sum})** nunca pueden ser menor que cero (Pete Herzog, 2010). La ecuación para determinar los controles faltantes para la autenticación **(MC_{Au})** está dada por:

$$SI\ OpSec_{sum} - TC <= 0$$

$$ENTONCES\ MC_{Au} = 0$$

$$CASO\ CONTRARIO\ MC_{Au} = OpSec_{sum} - LC_{Au}$$

El total de los controles ausentes **(MC_{sum})**, se debe calcular sumando individualmente cada uno de los 10 Controles, como se muestra en la siguiente ecuación:

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

Ecuación 4: Suma de controles ausentes

Fuente: (Herzog, 2010)

Limitaciones

Las limitaciones se ponderan individualmente, la ponderación de las vulnerabilidades, debilidades y preocupación se basan en una relación entre la porosidad o la suma **($OpSec_{sum}$)**, los controles de pérdida y en el caso de las exposiciones y anomalías, la existencia de otras limitaciones también desempeña un papel, una exposición o anomalía no plantea problemas por sí solo a menos que también esté presente una vulnerabilidad, debilidad o preocupación (Pete Herzog, 2010).

Exposición

La exposición es una acción, falla o error injustificable que proporciona visibilidad directa o indirecta de objetivos o Activos dentro del alcance del canal elegido (Pete Herzog, 2010).

Vulnerabilidad

Es una falla o error que: niega el acceso a los activos a personas o procesos autorizados, permite el acceso privilegiado de los activos a las personas o procesos no autorizados, permitir a personas o procesos no autorizados ocultar activos o a sí mismos dentro del alcance (Pete Herzog, 2010).

Debilidad

La debilidad es la falla o error que interrumpe, reduce, abusa o anula específicamente los efectos de los cinco controles de Clase A: Autenticación **(FC_{Au}),** Identificación **(FC_{Id}),** Resistencia **(FC_{Re}),** Subyugación **(FC_{Su}),** Continuidad **(FC_{Ct})** (Pete Herzog, 2010), la fórmula es:

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

Ecuación 5: Fórmula de Debilidad

Fuente: (Herzog, 2010)

Preocupación

La preocupación es la falla o error que interrumpe, reduce, abusa o anula los efectos del flujo o Ejecución de los cinco controles de Clase B: No repudio **(FC_{NR}),** Confidencialidad **(FC_{Cf}),** Privacidad **(FC_{Pr}),** Integridad **(FC_{It})** y Alarma **(FC_{Al})** (Pete Herzog, 2010). La fórmula es:

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

Ecuación 6: Fórmula de Preocupación

Fuente: (Herzog, 2010)

Anomalía

Es un elemento no identificable o desconocido que no ha sido controlado y no puede ser contabilizado en operaciones normales.

3.1 Pruebas de Seguridad Humana (HUMSEC)

Comprende el elemento humano de la comunicación donde la interacción es física o psicológica, la prueba de este canal requiere la interacción con personas en posiciones de guardián de los activos, este canal cubre la participación de personas, principalmente el

personal operativo dentro del alcance objetivo, el objetivo de las pruebas de seguridad en este canal es la prueba de concienciación de seguridad del personal y la medición de brechas con las políticas de la organización, regulaciones de la industria o la legislación regional (Pete Herzog, 2010).

"La auditoría informática es útil, pero no constituye una ciencia exacta, debe apoyarse en un conjunto de suposiciones" (Derrien, 2009, pág. 7), con este concepto para la elaboración del estudio se consideró en realizar diferentes encuestas a las áreas informáticas más expuestas a ataques, áreas donde existe acceso libre a computadoras como son los laboratorios y donde se maneja información delicada como es el DDTI Debido a que según el artículo 3 de la Institución y la LOTAIP se designa al Director/a de Desarrollo de Tecnológico e Informático es el responsable de atender la información pública en la UTN, los laboratorios de computación en donde existe un alta concurrencia de estudiantes de la casona universitaria en las cinco Facultades.

Las encuestas fueron elaboradas con el fin no comprometer la integridad, confidencialidad de las personas encuestadas, por tanto, para obtener datos más cercanos a la realidad y exactitud las encuestas fueron elaboradas de tipo anónimas, en el anexo 1 se muestran los datos obtenidos para resolver este canal. Los literales o pasos a seguir son interpretados por el autor y director Pete Herzog de la metodología OSSTMM.

se realizó:

- 15 encuestas entre el personal del DDTI y encargados de los laboratorios de las facultades FCCSS, FICAYA, FICA, FECYT y FACAE.
- 10 encuestas a los estudiantes de la UTN.
- Uso de herramientas Kali Linux.

3.1.1 Porosidad

Visibilidad

Enumerar el personal dentro del alcance tanto autorizados y no autorizados a los procesos dentro del objetivo, sin importar el tipo de acceso, tiempo y el método para la obtención de esos datos. En la tabla 3.2 se muestran los datos obtenidos para la visibilidad.

TABLA 0.2 Elaboración de la Visibilidad dentro del canal Humano

Técnica de encuesta:	**Observación y Encuesta**	
Objetivo:	**DDTI**	
Personal:	**Autorizados**	**No Autorizados**
Departamentos/Áreas	**1.-** Dirección Financiera	**11.-** Docentes
	2.- Seguridad y Gestión de Riesgos	**12.-** Investigadores
	3.- Mantenimiento y Construcciones	**13.-** Estudiantes
	4.- Gestión del Talento Humano	**14.-** Personas particulares
	5.- Secretaria General	
	6.- Gestión de Proyectos	
	7.- Comunicación Organizacional	
	8.- Practicantes	
	9.- Bienestar Universitario	
	10.- Centro de Transferencia y Desarrollo Tecnológico	

Fuente: Elaboración propia

La prueba se realizó en un lapso de diez días laborales utilizando técnicas de observación y aplicación de encuestas, donde se obtuvo una lista de acceso del personal autorizado y no autorizado dentro del alcance el DDTI como se detalla la tabla 3.2, por tanto, contabilizando los ítems numéricos se tiene un valor para la visibilidad de **Pv = 14**

Acceso

Realizar pruebas para la enumeración de diferentes puntos de acceso al personal dentro del alcance, si bien el acceso del personal fuera de su estación de trabajo es un verdadero escenario utilizado a menudo para robar la propiedad de la información, esto se puede limitar utilizando interacciones solamente en el alcance para proteger los derechos del personal en su vida privada. En la tabla 3.3 se muestran los datos obtenidos para el acceso.

TABLA 0.3 Elaboración del Acceso dentro del canal Humano

Acceso	
Técnica:	**Encuestas y Observación**
Objetivo:	**DDTI** **Encargados de los laboratorios FICA FCCSS, FICAYA, FECYT y FACAE.**
	1.- computadoras de trabajo

Información Obtenida	**2.-** Dispositivos móviles personales
	3.- Documentos físicos
	4.- Interacción entre personal

Fuente: Elaboración propia

Los diferentes puntos de acceso a los que el personal puede acceder e interactuar dentro del alcance objetivo estan los items mencionados en la tabla 3.3, por tanto, se obtiene un valor numerico de P_A **= 4.**

Confianza

Probar la confianza entre el personal dentro del alcance, donde la confianza se refiere al acceso a la información o a los activos físicos de otros objetivos dentro del alcance. En la tabla 3.4 se detallan los datos obtenidos para la confianza.

TABLA 0.4 Elaboración de la Confianza dentro del canal Humano

Confianza	
Técnica:	**Ingeniería Social y Encuestas**
Objetivo:	**DDTI** **Encargados de los laboratorios FICA FCCSS, FICAYA, FECYT y FACAE.**
Información Obtenida	**1.-** Acceso a oficinas
	2.- Acceso a los activos físicos
	3.- Obtención de credenciales
	4.- Obtención de Imágenes personales
	5.- Obtención de correos personales
	6.- Obtención de cuentas de redes sociales

Fuente: Elaboración propia

La prueba se realizó dentro del alcance (encargados de los laboratorios FICA FCCSS, FICAYA, FECYT y FACAE y el DDTI) mediante la aplicación de encuestas y el uso de la herramienta de recopilación de datos Maltego de Kali Linux para obtener los datos personales como se visualiza en la figura 24, en donde se obtuvo una lista de acceso a la información del personal y a los activos físicos dentro del alcance, contabilizando los ítems numéricos en la tabla 3.4 se tiene un valor numérico de P_T**=6**

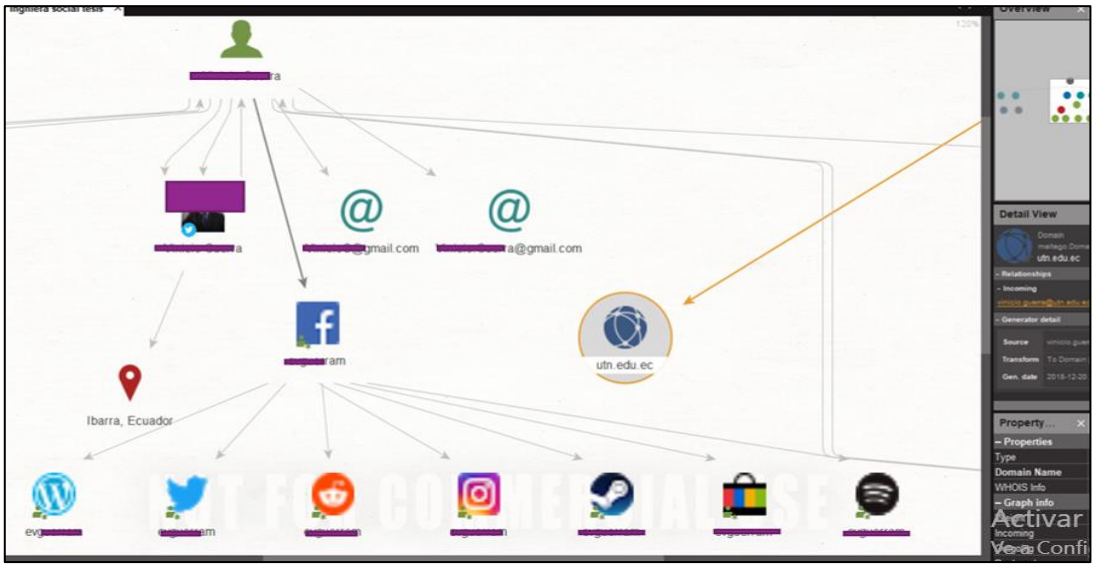


Fig. 24. Elaboración de la Confianza dentro del canal Humano con Maltego

Fuente: Elaboración Propia

3.1.2 Controles

Se deben realizar pruebas para enumerar los tipos de controles utilizados para proteger el valor de los activos de la organización auditada.

Autenticación

Enumerar y probar las deficiencias del personal de recepción y que privilegios se requieren para interactuar con ellos, con el fin de asegurar que sólo las partes identificables, autorizadas y grupos destinados tengan acceso. En la tabla 3.5 se observan los datos obtenidos para la Autenticación.

TABLA 0.5 Elaboración del Control de Autenticación dentro del canal Humano

Autenticación	
Técnica:	**Observación**
Objetivo Área:	**EDIFICIO CENTRAL** **DDTI**
Medios de Interacción Autorizados	**1.-** Solicitud por escrito de una autoridad correlacionada al entorno laboral, perteneciente a la Institución
	Biométrico
	2.- Petición Formal
	3.- Oficio con autorización del Sr Rector
	4.- Correo electrónico Institucional

Fuente: Elaboración propia

La prueba se realizó a través de la técnica de observación dentro del alcance (Edificio Central y el DDTI), se constató que para interactuar con el personal de recepción de los departamentos del edificio central de forma identificable y autorizada de manera que faciliten información comprometida es necesario los ítems marcados en la tabla 3.5, por tanto el valor numérico de la Autenticación es **$LC_{Au}=4$**

Indemnización

Documentar y enumerar el abuso o la elución de las políticas de los empleados, los seguros, acuerdos de no divulgación, no competencia, de responsabilidad, o renuncias de uso/usuario con todo el personal de acceso dentro del alcance. En la tabla 3.6 se muestran los datos obtenidos para la Indemnización.

TABLA 0.6 Elaboración del Control de Indemnización dentro del canal Humano

Indemnización	
Técnica:	**Normativa Institucional**
Objetivo Área:	**Personal Administrativo, Investigativo y Docentes de la UTN**
Leyes Internas Contempladas	**1.-** Firmas actas de responsabilidad
	2.- Amonestación verbal
	3.- Amonestación escrita
	4.- Acuerdo de confidencialidad e integridad
	5.- Seguimiento de una comisión especial de la UTN
	6.- Comisiones de servicio con remuneración

Fuente: Elaboración propia

Se recurrió a la legislación legal y administrativa actuales de la UTN disponibles en sitio web institucional, las normas o leyes que protegen a los activos de la institución están remarcados en los ítems en la tabla 3.6. Según el capítulo 1 artículo 3 del reglamento para el juzgamiento de infracciones y la aplicación de sanciones a las y los estudiantes, profesores o profesoras, investigadores o investigadoras de la UTN cuando un trabajador incumple las políticas internas el primer paso es dar a conocer al Honorable Consejo Universitario encargado de nombrar una comisión especial para dar seguimiento al inconveniente suscitado (Legislación legal UTN, 2012). Además, se resalta que el reglamento interno de la UTN prioriza y enfatiza la seguridad de trabajador u empleado ante un peligro laboral, por tanto el valor numérico de este control es de **$LC_{ID}=6$**

Resistencia

Enumerar y probar las insuficiencias del personal dentro del alcance, para lo cual la eliminación o la tranquilidad del personal de recepción, permitirá el acceso directo a los activos; en otras palabras, a “fallar de forma segura”. En la tabla 3.7 se manifiestan los datos obtenidos para la resistencia.

TABLA 0.7 Elaboración del Control de Resistencia dentro del canal Humano

Resistencia	
Técnica:	**Encuesta**
Objetivo Área:	**DDTI**
Acceso Directo	**1.-** Jefe de Área
	2.- Área de infraestructura
	Secretaria

Fuente: Elaboración propia

Para la resistencia se encontró que puede acceder el jefe del área de manera que el personal no encuentra ninguna anomalía, y hacia al área de los servidores puede acceder el área de infraestructura, por tanto, contabilizando los ítems de la tabla 3.7 se obtiene un valor numérico de $\boldsymbol{LCRe}$ **= 2**

Subyugación

Enumerar y probar las insuficiencias de los activos comunicados a través de canales en los que los controles no son necesarios, se puede eludir o ignorar, como el correo electrónico inseguro o sobre una línea telefónica pública. En la tabla 3.8 se exponen datos encontrados para la subyugación.

TABLA 0.8 Elaboración del Control de Subyugación dentro del canal Humano

Subyugación	
Técnica:	**Encuesta**
Objetivo Área:	**Personal Administrativo, Investigativo y Docentes de la UTN**
Controles no regulados	Uso de correos electrónicos privados
	Uso de redes sociales
	Teléfonos personales

Fuente: Elaboración propia

Aunque existen acuerdos por escrito de la integridad, confidencialidad, la no divulgación de la información por parte de los trabajadores u empleados pertenecientes a la UTN, no existen normas o controles aprobadas en la institución acerca de qué tipo de información se transmita o se reciba cuando se haga uso de redes sociales personales, correo electrónico personales o teléfonos personales, por tanto, el valor numérico de este control es de **$LC_{Su}=0$.**

Continuidad

Enumerar y probar 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 al personal alternativo de recepción. En la tabla 3.9 se muestran los datos obtenidos para la continuidad.

TABLA 0.9 Elaboración del Control de Continuidad dentro del canal Humano

Continuidad	
Técnica:	**Observación y Encuestas**
Objetivo Área:	**Personal Administrativo, Investigativo y Docentes de la UTN**
Ausencia por:	Gira de observación
	Enfermedad o calamidad
	Vacaciones
	Problemas externos
	Reuniones o conferencias
Genera Inconvenientes	**1.-** Directores de departamentos u áreas
	2.- Secretarias
	3.- Personal de apoyo
	Personal de seguridad

Fuente: Elaboración propia

Mediante la técnica de observación y en base a encuestas realizadas se obtiene que el personal de apoyo, secretarias y directores de departamentos generan inconvenientes laborales cuando se encuentra ausente, como se observa en la tabla 3.9 por tanto el valor numérico de la continuidad es **$LC_{Ct}=3$**

No repudio

Enumerar y probar el uso o las deficiencias del personal de recepción para identificar y registrar adecuadamente el acceso o las interacciones con los activos, mostrando evidencias

específicas para desafiar el repudio. Documentar la profundidad de la interacción que se registra. En la tabla 3.10 se muestran los datos obtenidos para el no repudio.

TABLA 0.10 Elaboración del Control de No Repudio dentro del canal Humano

No Repudio		
Técnica:	**Observación y Encuestas**	
Personal de recepción de:	DDTI	No posee Registro
	Encargados de los laboratorios FICA FCCSS, FICAYA, FECYT y FACAE	**1.-** Posee Registro

Fuente: Elaboración propia

Mediante encuestas y observación dentro del alcance objetivo las áreas o departamentos que poseen registros se encuentran los laboratorios de computación de las facultades FICA FCCSS, FICAYA, FECYT y FACAE, como se observa en el anexo 1 por tanto, el valor numérico del No Repudio es **$LC_{NR}=1$**

Confidencialidad

Enumerar y probar el uso o insuficiencias de todos los segmentos de comunicación con el personal dentro del alcance a través de un canal específico, o propiedades transportadas usando líneas seguras, encriptación, interacciones personales “cercanas” o “silenciosas” para proteger la confidencialidad de los activos de información que sólo conocen los que tienen la debida autorización de seguridad de ese activo. En la tabla 3.11 se muestran los datos obtenidos para la confidencialidad.

TABLA 0.11 Elaboración del Control de Confidencialidad dentro del canal Humano

Confidencialidad	
Técnica:	**Observación y Encuesta**
Tipos de Comunicación	Comunicación verbal
	1.- Comunicación escrita
	2.- Quipux
	3.- Correo electrónico Institucional
	Correo electrónico personal
	Redes Sociales
	4.- Método de encriptación
	5.- Vía telefónica institucional

Fuente: Elaboración propia

De los diferentes tipos de comunicaciones existentes dentro de la UTN se remarca que las líneas de comunicación seguras que se manejan en la institución son: la comunicación por escrito, correo electrónico institucional, Quipux, métodos de encriptación de la información y mediante vía telefónica institucional por tanto el valor numérico de la confidencialidad es de **LC_{Cf}=5**

Privacidad

Enumerar y probar el uso o deficiencias de todos los segmentos de comunicación con el personal dentro del alcance a través de un canal o propiedades transportadas utilizando específicamente firmas individuales, identificación personal, interacciones personales "silenciosas" o "a puerta cerrada" para proteger la privacidad de la interacción y el proceso de proporcionar activos sólo a aquellos dentro de la autorización de seguridad adecuada para ese proceso, información o activos físicos. En la tabla 3.12 se detallan los datos obtenidos para el control de privacidad.

TABLA 0.12 Elaboración del Control de Privacidad dentro del canal Humano

Privacidad	
Técnica:	**Observación y Encuestas**
Propiedades seguras transportadas por medio de:	Firmas individuales
	Identificación personal
	1.- Interacciones personales a puerta cerrada

Fuente: Elaboración propia

Las propiedades transportadas dentro de la UTN utilizando específicamente interacciones personales del personal a puerta cerrada y el uso de identificación personal demuestran ser métodos seguros y confiables, mientras que un activo transportado utilizando sólo firmas individuales puede ser suplantada, por tanto, el valor numérico del control de privacidad es de **LC_{Pr}=1.**

Integridad

Enumerar y probar el uso o las deficiencias en todos los segmentos de comunicación con el personal dentro del alcance, donde los activos son transportados por un canal mediante un proceso documentado, firmado, cifrado, encriptado, o marcas para proteger y asegurar que la información de los activos físicos no pueda ser cambiados, conmutados, redirigidos o revertidos sin que sea conocido por las partes involucradas. En la tabla 3.13 se exponen los datos obtenidos para el control de integridad.

TABLA 0.13 Elaboración del Control de Integridad dentro del canal Humano

Integridad	
Técnica:	**Observación y Encuestas**
Activos transportados mediante un proceso documentado eficiente	**1.-** Firmas y sellos
	2.- Cifrado de Datos
	3.- Encriptación
	4.- Firmas electrónicas
	Documentos sin firmas y sellos

Fuente: Elaboración propia

Las propiedades o activos transportadas dentro de la UTN mediante procesos documentados impresos o digitales que hacen uso de: firmas y sellos, cifrado de datos, encriptación, documentos con firmas electrónicas son eficientes y confiables, mientras que los documentos que no presentan firmas y sellos presentan inconsistencias, por tanto, el valor numérico del control de Integridad es **$LC_{It}=4$**

Alarma

Verificar y enumerar el uso de un sistema de advertencias, registro o un mensaje en todo el alcance sobre cada canal donde el personal detecte una situación sospechosa de un intento de evasión, ingeniería social, o una actividad fraudulenta. En la tabla 3.14 se muestran los datos obtenidos para el control de alarma.

TABLA 0.14 Elaboración del Control de Alarma dentro del canal Humano

Alarma	
Técnica:	**Observación y Encuestas**
Métodos existentes frente a una actividad Sospechosa	**1.-** Sistema de alarma
	2.- Personal de seguridad
	3.- Mensajes o llamadas telefónicas personales
	Registros

Fuente: Elaboración propia

Los métodos eficientes y que se utilizan frente a una actividad sospechosa dentro de la UTN están: el uso de sistemas de alarma (anexo 1) en todo el campus universitario, la respuesta del personal de seguridad y las llamadas o mensajes entre el personal, por tanto, el valor numérico del control de Alarma es **$LC_{AI}=3$**

3.1.3 Limitaciones

Exposición

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 la institución que informa a los llamantes que una persona en particular se encuentra enferma o de vacaciones. En la tabla 3.15 se exponen los datos encontrados para la exposición.

TABLA 0.15 Elaboración de la Exposición dentro del canal Humano

Exposición	
Técnica:	**Observación y Encuesta**
Objetivo Área:	**DDTI** **Encargados de los laboratorios FICA FCCSS, FICAYA, FECYT y FACAE.**
Información directa expuesta cuando:	**1.-** Solicitación de información de un empleado por llamada telefónica anónima o personalmente con identidad falsa
	2.- Se realiza manipulación remota a una computadora de trabajo de un empleado
	3.- Registro de acceso es visible hacia los empleados y estudiantes debido a que se realiza en hojas físicas en los laboratorios de las cinco facultades
	4.- Uso de dispositivos de almacenamiento extraíble de una computadora de trabajo hacia otra
	5.- Manipulación de una computadora de trabajo por parte de practicantes

Fuente: Elaboración propia

Los datos obtenidos para esta limitación se muestran en los ítems marcados en la tabla 3.15 proporcionando un valor numérico para la exposición de **L_E=5.**

Vulnerabilidad

Una vulnerabilidad puede ser un sesgo cultural que no permite que un empleado cuestione a otras personas que se ven fuera de lugar o una falta de capacitación que deja a una nueva secretaria para dar información clasificada que es solo para uso interno. En la tabla 3.16 se detallan los datos encontrados para la vulnerabilidad.

TABLA 0.16 Elaboración de la Vulnerabilidad dentro del canal Humano

Vulnerabilidad	
Técnica:	**Observación y Normativa UTN**
Información directa expuesta cuando:	No existe cuestiones laborales por sesgos culturales en la UTN
	1.- Por capacitación de un empleado nuevo se facilita información confidencial de uso interno
	2.- Por preparación del entorno de trabajo a un practicante se facilita información confidencial de uso interno
	3.- Las instituciones públicas como la UTN deben facilitar información de los empleados según la ley de acceso a la información (anexo 1)

Fuente: Elaboración propia

Se resalta que el código de ética de La UTN en su capítulo 3, artículo 4 establece que, la UTN garantiza igualdad de oportunidades para todas las personas, mantiene un criterio democrático libre de toda discriminación con trato justo sin distinguir raza, color, religión, nacionalidad, sexo, edad, discapacidad o condición (Legislación legal UTN, 2012). Los datos obtenidos para esta están marcados en los ítems de la tabla 3.16 contabilizando un valor numérico para la vulnerabilidad de **Lv=3.**

Debilidad

Una debilidad puede ser una falla del proceso de una segunda guardia para asumir el puesto de guardia que corre detrás de un intruso o un clima cultural dentro de una empresa para permitir que amigos ingresen a espacios restringidos, debilidad o errores de los controles de clase A. En la tabla 3.17 se exponen los datos obtenidos para la debilidad.

TABLA 0.17 Elaboración de la Debilidad dentro del canal Humano

Debilidad	
Técnica:	**Observación y Encuestas**
Controles Clase A	**Fallas en los controles**
Autenticación	**1.-** Suplantación de identidad en una solicitud por escrito de una autoridad correlacionada al entorno laboral, perteneciente a la Institución
	2.- El personal puede dejar abierto la sesión en su computadora de trabajo del correo electrónico institucional provocando la manipulación de la información por otra persona
Indemnización	**3.-** Aunque el personal a realizado firmas de actas de responsabilidad de un activo puede ser vulnerado
	4.- Una amonestación verbal presenta falla debido que cuando se hace cambio de autoridad pasa desapercibido

subyugación	**5.-** Mediante el uso de correos electrónicos privados puede filtrarse información comprometida
	6.- Mediante el uso de redes sociales se puede filtrar información comprometida
	7.- Mediante el uso de teléfonos personales puede filtrarse información comprometida

Fuente: Elaboración propia

En la tabla 3.17 se observa las fallas que pueden suscitarse en los controles de clase A, para el control de continuidad y resistencia de las medidas aplicadas no se encontró errores o fallas, de tal manera que aplicando la ecuación 5 y sumando las deficiencias de los controles de los ítems marcados se obtiene un valor numérico de:

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

$$L_w = 2 + 2 + 0 + 3 + 0$$

$$L_w = 7$$

Preocupación

Enumerar las fallas o irregularidades de los controles de la clase B del canal Humano, en la tabla 3.18 se muestran los datos obtenidos para la preocupación.

TABLA 0.18 Elaboración de la Preocupación dentro del canal Humano

Preocupación	
Técnica:	**Observación y Encuestas**
Controles Clase B	**Fallas en los controles**
no repudio	**1.-** los laboratorios de computación FICA FCCSS, FICAYA, FECYT y FACAE, presentan inconsistencias debido a que el registro se lo hace en hojas físicas y en ocasiones no se registra a las personas por la confianza existente (anexo 1)
Confidencialidad	**2.-** puede existir inconsistencia en la comunicación escrita porque se pueden manipular los datos
	3.- puede existir fallas en la comunicación vía telefónica institucional debido a que una persona ajena a su puesto de trabajo puede utilizar un teléfono de otro trabajador para pedir información confidencial al personal de esta u otra área
alarma	**4.-** existe fallas en los guardias debido a que frente a una actividad sospechosa puede pasar desapercibidos

Fuente: Elaboración propia

En los controles marcados en la integridad y privacidad no se encontraron errores o fallas, de tal manera que aplicando la ecuación 6 y sumando las deficiencias de los controles marcados en la tabla 3.18, se obtiene un valor numérico para la preocupación de:

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

$$Lc = 1 + 2 + 0 + 0 + 1$$

$$Lc = 4$$

Anomalía

Contabilizar cada elemento identificable o desconocido que no puede tenerse en cuenta en las operaciones normales, generalmente cuando el origen o el destino del elemento no pueden ser entendidas. Una anomalía puede ser una pregunta que hace un guardia, que puede parecer irrelevante para el trabajo o para una charla estándar. En la tabla 3.19 se muestran los datos obtenidos para la anomalía.

TABLA 0.19 Elaboración de la Anomalía dentro del canal Humano

Anomalía	
Técnica:	**Observación y Encuestas**
Objetivo:	**DDTI, Estudiantes y Encargados de los laboratorios FICA FCCSS, FICAYA, FECYT y FACAE.**
Anomalías	**1.-** Se comparte información del trabajo por cuentas de correo electrónico personal
	2.- Ingreso de personas que no ejercen actividad laboral dentro de la institución
	3.- Ingreso de personal de otros departamentos u áreas no relacionadas con el entorno laboral
	4.- Se desconoce si existen políticas a seguir en caso de que otra persona utilice la computadora de trabajo
	5.- El personal asegura haber recibido información de dudosa procedencia
	6.- Usan dispositivos de almacenamiento extraíbles para compartir información dentro de la Institución
	7.- a diferencia de los trabajadores de la UTN los estudiantes de la institución aseguran que la información de la UTN no se encuentra totalmente segura
	8.- estudiantes aseguran que los activos transportados a través del personal autorizado de la UTN no es un método confiable y seguro

Fuente: Elaboración propia

Como resultado sumando las anomalías de los ítems marcados en la tabla 3.19 se obtiene un valor numérico de **L_A = 8.**

3.1.4 Aplicación del RAV

Para la aplicación del RAV se utilizó la hoja de cálculo propia de la metodología, la cual se encuentra disponible en su sitio oficial www.osstmm.com, los valores se consiguieron a través de técnicas de observación, Ingeniera social, reglamento de la institución y encuestas al personal del DTTI y a encargados de los laboratorios de las facultades FICA FCCSS, FICAYA, FECYT y FACAE de la UTN. En la tabla 3.20 se detallan los valores obtenidos en la prueba de seguridad humana.

TABLA 0.20 Datos Obtenidos para el RAV del canal Humano

Datos Obtenidos para el RAV del Canal Humano (HUMSEC)		
Ítems		**Valor Total**
Porosidad	Visibilidad	**(PV) = 14**
	Acceso	**(PA) = 4**
	Confianza	**(PT) = 6**
Controles	Autenticación	**(LCAu) = 4**
	Indemnización	**(LCID) = 6**
	Resistencia	**(LCRe) = 2**
	Subyugación	**(LCSu) = 0**
	Continuidad	**(LCCt) = 3**
	No repudio	**(LCNR) = 1**
	Confidencialidad	**(LCCf) = 5**
	Privacidad	**(LCPr) = 1**
	Integridad	**(LCIt) = 4**
	Alarma	**(LCAl) = 3**
Limitaciones	Exposición	**LE = 5**
	Vulnerabilidad	**LV = 3**
	Debilidad	**Lw = 7**
	Preocupación	**Lc = 4**
	Anomalía	**LA = 8**

Fuente: Elaboración propia

Análisis de resultados

La Medida de seguridad de la superficie de ataque para canal humano se visualiza en la tabla 3.21.

TABLA 0.21 Calculadora RAV de OSSTMM 3, Prueba de Seguridad Humano

Pruebas de Seguridad Humana

OSSTMM versión 3.0

Inserte en los espacios en blanco los valores numéricos para OPSEC, Controles y Limitaciones con los resultados de la prueba de seguridad. Visite OSSTMM 3 (www.osstmm.org) para más información

OPSEC	
Visibilidad	14
Acceso	4
Confianza	6
Total (Porosidad)	24

CONTROLES		
Clase A		Ausentes
Autenticación	4	20
Indemnización	6	18
Resistencia	2	22
Subyugación	0	24
Continuidad	3	21
Total Clase A	15	105

Clase B		Ausentes
No-Repudio	1	23
Confidencialidad	5	19
Privacidad	1	23
Integridad	4	20
Alarma	3	21
Total Clase B	14	106

		Ausentes Verdaderos
Total Controles	29	211
Cobertura Total	12,08%	87,92%

LIMITACIONES		Valor Numérico	Valor Total
Vulnerabilidad	3	9,791667	29,375000
Debilidad	7	5,375000	37,625000
Preocupación	4	5,416667	21,666667
Exposición	5	1,242708	6,213542
Anomalías	8	0,803125	6,425000
Total # Limitaciones	27		101,3052

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

OPSEC	11,427051
Controles Verdaderos	6,070769
Controles Completos	6,070769
Cobertura Verdadera A	12,50%
Cobertura Verdadera B	11,67%
Total Cobertura Verdadera	12,08%
Limitaciones	16,045429
Seguridad Δ	-21,40
Protección Verdadera	78,60

OSSTMM Open Source Security Testing Methodology Manual
OSSTMM
www.osstmm.org

Seguridad Actual 78,76 ravs

Fuente: Elaboración propia

Los valores numéricos obtenidos dentro del canal son rellenados automáticamente en la hoja de cálculo del RAV perteneciente a la metodología, los valores a rellenar son: valor total de OpSec, valor ausente y valor total del control de clase A y B, valores ausentes y total de Limitaciones, el RAV básicamente resta la porosidad y las limitaciones de los controles como lo indica la ecuación 1. Se resalta el valor numérico de la seguridad Δ enmarcado de color rojo lo que significa una carencia o insuficiencia del 21,40 de los controles adoptados, la cual indica que la información digital y física del DTTI y de la UTN se encuentra parcialmente vulnerable y expuesta a posibles ataques informáticos.

R A V = CONTROLES VERDADEROS – POROSIDAD – LIMITACIONES

RAV = 6,0707 – 11,4270 – 16,0454

RAV = - 21,40

3.2 Pruebas de seguridad física (PHYSSEC)

La prueba de este canal requiere una interacción no comunicativa con las barreras y los seres humanos en las posiciones de cuidadores de los activos, este canal cubre la interacción del analista dentro de la proximidad de los objetivos, el verdadero objetivo de cumplimiento de las pruebas de seguridad en este canal es la prueba de barrera física y lógica y la medición de brechas con el estándar de seguridad requerido como se describe en la política de la organización, regulaciones de la industria o la legislación regional (Pete Herzog, 2010).

"La auditoría informática es útil, pero no constituye una ciencia exacta, debe apoyarse en un conjunto de suposiciones" (Derrien, 2009, pág. 7), con este concepto para la elaboración del estudio se consideró recurrir a técnicas de observación y encuestas dentro de la UTN, la encuesta fue realizada al encargado del área de redes y comunicaciones, en el anexo 2 se detallan los datos conseguidos para resolver este canal. Los literales o pasos a seguir son interpretados por el autor y director Pete Herzog de la metodología OSSTMM.

3.2.1 Porosidad

Visibilidad

Realizar pruebas de enumeración y verificación para la visibilidad de objetivos y activos. En PHYSSEC, los activos también deben incluir suministros como alimentos, agua, combustible, etc. y procesos operativos que pueden afectar a dichos suministros, como la eliminación adecuada de desechos y otros contaminantes, la carga y descarga de los envíos de suministros, los ciclos de descanso, la aclimatación adecuada, etc.

- Localizar y detallar el perímetro de alcance determinado con técnicas de visualización visible y asistida, las áreas de acceso público, los planes y recursos públicos.
- Enumerar y detallar objetivos y activos visibles fuera del alcance.
- Enumerar y detallar los objetivos de las normas de tráfico, el tráfico peatonal, las áreas ocupadas y los sensores visibles fuera del alcance.
- Enumerar las direcciones y las guías telefónicas internas que identifican las ubicaciones de las instalaciones de procesamiento de información confidencial a las que el público no puede acceder fácilmente.
- Localizar y enumerar la ubicación física y el diseño del objetivo, el tamaño y la capacidad de navegación de los obstáculos, barreras y peligros que aumentarán con el tiempo.

En la tabla 3.22 se muestran los datos obtenidos para la visibilidad

TABLA 0.22 Elaboración de la Visibilidad dentro del canal Físico

Visibilidad	
Técnica:	**Observación, Normativa UTN**
Perímetro del Alcance cercano (UTN):	**1.-** Edificio central
	2.- Biblioteca
	3.- Facultades
	4.- Auditorios
	5.- Polideportivo
	6.- Espacios recreativos
	7.- Parqueaderos
	8.- Gimnasio
	9.- Canchas multideportivas
	10.- Piscina
Perímetro cercano fuera del alcance (UTN):	**11.-** Colegio Universitario
	12.- Estadio
	13.- Campus San Vicente de Paul
Normas de tráfico dentro del alcance:	**14.-** Señalética vehicular
	15.- Señalética peatonal
	No existen sensores visibles fuera del alcance
Guías telefónicas y Direcciones	**16.-** Acceso público
Ubicación física del alcance	Objetivo: DDTI

	Edificio central planta baja dentro de Gestión de Talento Humano Informática. No es visible desde el exterior.

Fuente: Elaboración propia

La prueba se realizó recurriendo a la normativa de la institución y mediante técnicas de observación entorno al objetivo principal el campus universitario y DDTI como muestra el anexo 1. De la tabla 3.22 se resalta que: Según el artículo 1 y 7 de difusión de la información pública de la ley orgánica de transparencia y acceso a la información pública (LOTAIP), determina que la información de los trabajadores de una institución pública como es la UTN es de acceso público y estarán publicados en su página web o portal (LOTAIP, 2004). Además, que el objetivo alcance no es visible desde el exterior, por tanto, contabilizando los ítems se obtiene un valor para la visibilidad de **Pv = 16.**

Acceso

Pruebas para la enumeración de puntos de acceso para interactuar con los objetivos y activos dentro del alcance, si bien el acceso a muros y cercas que bordean propiedades fuera del alcance es un escenario real y se usa a menudo en un ataque, esta auditoría se limita a la interacción de alcance solamente para proteger los derechos de propiedad de terceros. En la tabla 3.23 se detallan los datos obtenidos para el acceso.

TABLA 0.23 Elaboración del Acceso dentro del canal Físico

Acceso	
Técnica:	**Observación e Ingeniería social**
Objetivo:	**DDTI**
Acceso físico directo	**1.-** Entrada a personal de Gestión de Talento Humano Informática
	2.- Entrada de personas edificio central
Accesos ajenos	**3.-** Frio
	Calor
	Humedad
	Luz dañina
	4.- Ruido desde el exterior
	Olores perjudícales
	Humo
	Comida
	Bebidas
	Polvo

Fuente: Elaboración propia

La prueba se realizó mediante técnicas de observación e ingeniería social, determinado que para entrar al DDTI existe una entrada principal mediante el edificio central, al igual existe la penetración de frio y ruido del exterior, por tanto, sumando los ítems marcados en la tabla 3.23 se obtiene un valor para el acceso de $P_A = 4$.

Confianza

Probar la confianza entre procesos dentro del alcance donde la confianza se refiere al acceso a los activos sin la necesidad de identificación o autenticación. En la tabla 3.24 se detallan los datos obtenidos para la confianza.

TABLA 0.24 Elaboración de la Confianza dentro del canal Físico

Confianza	
Técnica:	**Observación y encuestas**
Objetivo:	**UTN**
Información Obtenida	**1.-** Acceso a oficinas
	Acceso a los activos físicos
	Obtención de credenciales

Fuente: Elaboración propia

La prueba se realizó en las instalaciones del campus universitario, para el acceso a los activos se requiere una identificación o autorización de una autoridad, por tanto, el valor numérico para la confianza es de $P_T = 1$

3.2.2 Controles

Autenticación

- Enumerar y probar las deficiencias a las que se requieren privilegios para acceder, el proceso de obtención de esos privilegios, y asegurar de que solo se proporcione acceso a las partes identificables y autorizadas.
- Verifique el proceso de autenticación de los elementos que pueden ser llevados dentro del alcance por personal autorizado y no autorizado.
- Verificar el proceso de autenticación de los elementos que pueden ser extraídos fuera del alcance por personal autorizado y no autorizado.
- Verifique el proceso de registro de acceso y los elementos que fueron introducidos y retirados.

En la tabla 3.25 se muestran los datos obtenidos para la confianza dentro del objetivo DDTI.

TABLA 0.25 Elaboración de la Autenticación dentro del canal Físico

Autenticación	
Técnica:	**Observación y encuestas**
Objetivo:	**DDTI**
Privilegios para obtener acceso al objetivo	**1.-** Jefes Departamentales **2.-** Personal de seguridad **3.-** Practicantes **4.-** Personas particulares
Elementos llevados dentro del objetivo	**5.-** Oficios Dispositivos extraíbles **6.-** Solicitudes
Elementos extraídos del objetivo	**7.-** Oficios Dispositivos extraíbles **8.-** Solicitudes
Elementos introducidos y retirados	**9.-** Equipos Informáticos

Fuente: Elaboración propia

Se proporciona aprobación de acceso al lugar con ciertas restricciones a practicantes, jefes departamentales, personas particulares y el personal de seguridad, entre los elementos autorizados que pueden ser llevados y extraídos del DDTI están oficios y solicitudes y equipos informáticos. Sumando los ítems de la tabla 3.25 se obtiene un valor numérico de **LC_{Au}=9.**

Indemnización

- Documentar y enumerar la capacidad de abusar o eludir la política de los empleados, los seguros, la no divulgación, la no competencia, los contratos de responsabilidad o el uso de renuncia de responsabilidad del del personal dentro del alcance.
- Enumerar el uso de señales de advertencia de peligro, vigilancia o alarmas vigentes, problemas de salud y avisos de entrada restringida.
- Verificar el alcance y la finalidad de la acción legal utilizada para mantener la indemnización.

En la tabla 3.26 se muestran los datos obtenidos para la indemnización.

TABLA 0.26 Elaboración de la Indemnización dentro del canal Físico

Indemnización	
Técnica:	**Observación y Encuestas**
Objetivo:	**UTN**
Personal autorizado	política de los empleados Los seguros **1.-** Acuerdo de no divulgación **2.-** contratos de responsabilidad uso de renuncia de responsabilidad
Interior del alcance (Anexo 2)	**3.-** señales de advertencia de peligro **4.-** Cuidado o botón de pánico problemas de salud **5.-** avisos de entrada restringida
Acción legal	**6.-** Se aplica

Fuente: Elaboración propia

Dentro de los controles se puede eludir se encuentran los contratos de responsabilidad puesto que si un activo se encuentra en un mal estado se puede enviar a ser arreglado de manera verbal evitando este control, para la acción legal se recurre a las leyes vigentes en la institución. Por tanto, sumando los ítems de la tabla 3.26 se obtiene un valor numérico para la indemnización de **$LC_{ID}=6$**

Resistencia

- Enumere y verificar que la distracción, la remoción o tranquilización del personal de recepción no permitan el acceso directo a los activos u operaciones.
- Enumerar y verificar que la desactivación o destrucción de las medidas o controles de seguridad operacional no permita el acceso directo a los activos u operaciones.
- Verificar que el aislamiento del alcance de recursos tales como combustible, energía, alimentos, agua, comunicaciones, etc. no permita el acceso directo a activos u operaciones.
- Verificar que las condiciones de amenaza de alerta alta no cierren o minimicen las medidas de seguridad operativas o los controles que permitan el acceso directo a los activos u operaciones.

En la tabla 3.27 se muestran los datos obtenidos para la resistencia dentro de la UTN.

TABLA 0.27 Elaboración de la Resistencia dentro del canal Físico

Resistencia		
Técnica:	**Observación, Ingeniería social y Encuestas**	
Objetivo:	**UTN**	
Personal de recepción	Distracción	Permite el acceso
	Remoción	Permite el acceso
Controles de seguridad operacional	Destrucción	Permite el acceso
	Desactivación	**1.-** No permite el acceso
Falta de Recursos	Combustible	Permite acceso
	Energía eléctrica	Permite acceso
	Alimento	Permite acceso
	Agua	Permite acceso
	Comunicación	**2.-** No Permite el acceso
Condiciones de amenaza alta	**3.-** No permite el acceso	

Fuente: Elaboración propia

En base a la técnica de observación e Ingeniería social se determina de la tabla 3.27 que la distracción del personal y la remoción del personal permite el acceso directo a los activos u operaciones, la desactivación de los controles de seguridad operacional no permite el acceso a los activos u operaciones al igual que la falta de comunicación no permite el acceso, por tanto, el valor numérico para la resistencia es de $\boldsymbol{LCRe}$ **= 3.**

Subyugación

Enumerar y probar las deficiencias en el acceso a los activos no controlados por la fuente que proporciona el acceso (es decir, PIN, fotos de identificación, etc., seleccionados por el actor, registros con los números de identificación escritos por el actor, etc.) en la tabla 3.28 se visualizan los datos obtenidos para la subyugación dentro de La UTN.

TABLA 0.28 Elaboración de la Subyugación dentro del canal Físico

Subyugación		
Técnica:	**Observación, Ingeniería social**	
Objetivo:	**UTN**	
Divulgación de control de acceso por:	Reloj Biométrico	Identificación visible
	PIN	Tarjetas de acceso

Fuente: Elaboración propia

Para el acceso a un área restringida se prohíbe la divulgación de contraseñas o la duplicación de los controles de acceso por parte del personal a cargo, por tanto, el valor numérico para la subyugación es de **LC_{SU}=0.**

Continuidad

- Enumerar y verificar las condiciones en las que los retrasos en el acceso se abordan adecuadamente a través del personal de apoyo o mediante un medio automatizado para el acceso oportuno a servicios, procesos y operaciones.
- Enumerar y verificar que la distracción, la eliminación o el silencio del personal de recepción no detendrán ni denegarán el acceso oportuno a los servicios, procesos y operaciones.
- Enumerar y verificar que la inhabilitación o destrucción de las medidas o controles de seguridad operacional no negarán el acceso oportuno a los servicios, procesos y operaciones.
- Verificar que el aislamiento del alcance de recursos tales como combustible, energía eléctrica, alimentos, agua, comunicaciones, etc. no detenga ni niegue el acceso a los servicios, procesos y operaciones.
- Verifique que la incapacidad para eliminar los residuos y contaminantes del alcance no impedirá ni negará el acceso a servicios, procesos y operaciones.
- Verificar que las condiciones de alerta de amenaza alta no detengan ni denieguen el acceso a servicios, procesos y operaciones.

En la tabla 3.29 se detallan los datos obtenidos para la continuidad dentro de La UTN.

TABLA 0.29 Elaboración de la Continuidad dentro del canal Físico

Continuidad		
Técnica:	**Observación, Ingeniería social y Encuestas**	
Objetivo:	**UTN**	
Retrasos por el personal de apoyo		**1.-** No detiene el acceso
Personal de recepción	Distracción	**2.-** No detiene el acceso
	Silencio	**3.-** No detiene el acceso
	Eliminación	detiene el acceso
Controles de seguridad operacional	Inhabilitación	Detiene el acceso
	Destrucción	Detiene el acceso

Falta de Recursos	Combustible	**4.-** No detiene el acceso
	Energía eléctrica	Detiene el acceso
	Alimento	**5.-** No detiene el acceso
	Agua	**6.-** No detiene el acceso
	Comunicación	Detiene el acceso
Incapacidad de eliminar	Residuos	Detiene el acceso
	Contaminantes	Detiene el acceso
Condiciones de amenaza alta	**7.-** Detiene el acceso	

Fuente: Elaboración propia

El retraso del personal de apoyo no detiene el acceso a las operaciones o procesos que se manejan en la institución, de igual manera el personal de recepción no detiene el acceso a los procesos u operaciones, la falta de recursos como alimento, agua y combustible no detienen el acceso, por tanto, contabilizando los ítems de la tabla 3.29 se tiene el valor numérico para la continuidad de **LC_{Ct}=7.**

No repudio

Enumerar y probar el uso o las deficiencias de los monitores y sensores para identificar correctamente y registrar el acceso o las interacciones con los activos para obtener pruebas específicas que cuestionen el repudio, documentar la profundidad de la interacción que es registrada. En la tabla 3.30 se muestran los datos obtenidos para el no repudio dentro de La UTN.

TABLA 0.30 Elaboración del No Repudio dentro del canal Físico

No Repudio	
Técnica:	**Observación, Ingeniería social**
Objetivo:	**UTN**
Uso de sensores para identificar el acceso (Anexo 2)	**1.-** Uso de cámaras de video vigilancia
	2.- Monitores para cámaras de seguridad

Fuente: Elaboración propia

La manera de identificar y registrar el acceso no autorizado a un área física se realiza mediante el uso de cámaras de seguridad y el uso de monitores como se visualiza en el anexo 2, por tanto, sumando el valor numérico de la tabla 3.30 se obtiene un valor numérico de **LC_{NR}=2.**

Confidencialidad

Enumerar y probar el uso o las deficiencias de todas las señales, la comunicación física y los elementos transportados entre los procesos internos y externos usando códigos del personal, lenguaje indescifrable, interacciones personales "silenciosas" o "cercanas" para promover la confidencialidad de la comunicación únicamente a aquellos con la clasificación de seguridad adecuada para esa comunicación. En la tabla 3.31 se muestran los datos obtenidos para la confidencialidad.

TABLA 0.31 Elaboración de la Confidencialidad dentro del canal Físico

Confidencialidad	
Técnica:	**Observación e Ingeniería social**
Objetivo:	**UTN**
Confidencialidad de la comunicación física	códigos del personal lenguaje indescifrable **1.-** interacciones personales

Fuente: Elaboración propia

En base a técnicas de observación e ingeniería social, se verificó que para la comunicación fisica y promover la confidencialidad entre el personal autorizado se utiliza las interaciones personales por medio de espacios fisicos como las oficinas o cualquier lugar a puerta cerrada, por tanto el valor numerico para la confidencialidad es **$LC_{cf}=1$.**

Privacidad

Enumerar y probar el uso o las deficiencias de todas las interacciones dentro del alcance utilizando paquetes no marcados o no videntes o etiquetadas, las interacciones "silenciosas" o de "cuarto cerrado", y dentro de cuartos elegidos al azar para ocultar o proteger la privacidad de la interacción y solo a aquellos con la debida autorización de seguridad para ese proceso o activo. En la tabla 3.32 se muestran los datos obtenidos para la privacidad.

TABLA 0.32 Elaboración de la Privacidad dentro del canal Físico

Privacidad	
Técnica:	**Observación**
Objetivo:	**UTN**
Personal autorizado	Paquetes no etiquetados Espacio físico abierto **1.-** Espacio físico cerrado

Fuente: Elaboración propia

En base a técnica de observación se determina que la comunicación verbal de carácter institucional más eficiente y repetitiva en todos los departamentos u áreas se la realiza en espacios físicos cerrados, no se hace uso de paquetes no marcados o sellados entre el personal por dudosa procedencia y desconocimiento del contenido, por tanto, el valor numérico para la privacidad es de **LC_{Pr}=1.**

Integridad

- Enumerar y probar las insuficiencias en todas las señales y la comunicación entre los procesos y el personal mediante un proceso documentado, sellos, firmas, hash o marcas cifradas para proteger y asegurar que los activos no puedan ser cambiados, redirigidos o revertidos sin que las partes involucradas lo conozcan.
- Enumerar y probar las deficiencias en todos los procesos e interacciones con los activos en el transporte que utilizan procesos documentados, firmas, sellos, cinta de embalar, marcas, etiquetas, sensores o marcas cifradas para proteger y asegurar que los activos no puedan ser cambiados, redirigidos, o revertidos sin que las partes involucradas lo conozcan.
- Verificar que todos los medios de almacenamiento de información no estén en peligro debido a una descomposición natural, como el daño por calor o humedad, el desgaste por la luz solar directa o la degradación magnética.

En la tabla 3.33 se detallan los datos obtenidos para la integridad.

TABLA 0.33 Elaboración de la Integridad dentro del canal Físico

Integridad	
Técnica:	**Observación**
Objetivo:	**UTN**
Proceso operacional documentado	Comunicación entre procesos **1.-** Señales
Interacciones con los activos transportados	Equipos informáticos
Medios de almacenamiento de información	descomposición natural

Fuente: Elaboración propia

Existe insuficiencia en las señales dentro de un proceso operacional y para las interacciones con los activos transportados como son los equipos informáticos no se encontraron deficiencias debido a que utilizan su correcta documentación, y si un medio de almacenamiento de información sufrió un daño por descomposición natural es reemplazado enseguida por el personal autorizado, por tanto, el valor numérico para la integridad es de **LC_{It}=1.**

Alarma

Verificar y enumerar el uso de un sistema de advertencia localizado en todo el alcance, ingreso o mensaje para cada puerta de acceso en una situación sospechosa observada por el personal en caso de intentos de elusión, actividad fraudulenta, allanamiento, asegurarse de que los sensores/sistemas estén instalados según los estándares nacionales, regionales o internacionales y que se prueben regularmente para cubrir todos los puntos de acceso.

No existe un sistema de alerta en cada acceso que advierta una situación sospechosa como una actividad fraudulenta, allanamiento o un intento de elusión que alerte a todo el personal, por tanto, el valor numérico para este control es de **LC_{Al}=0.**

3.2.3 Limitaciones

Vulnerabilidad

Una vulnerabilidad puede ser tan simple como una puerta de vidrio, una puerta de metal corroída por el tiempo, una puerta que se puede sellar encajando monedas en la brecha entre esta y su marco, equipo electrónico no controlados contra plagas como hormigas o ratones, una unidad de CD de arranque en una PC, o un proceso que permita a un empleado tomar un cubo lo suficientemente grande como para ocultar o transportar activos fuera del alcance. En la tabla 3.34 se muestran los datos obtenidos para la vulnerabilidad.

TABLA 0.34 Elaboración de la Vulnerabilidad dentro del canal Físico

Vulnerabilidad	
Técnica:	**Observación**
Objetivo:	**UTN**
	1.- Se hace uso de puertas de cristal dentro de la UTN en las que se pueden quebrantar
	2.- El ingreso vehicular por las entradas principales de trabajadores como estudiantes puede ser suficiente para ocultar un activo de la institución

Vulnerabilidades encontradas (Anexo 2)	**3.-** Más de un laboratorio de computación de las facultades FICA, FACAE, FICAYA, FECYT y FCCSS se encuentran abiertos durante las horas laborales para dar acceso a personas que deseen ocupar las computadoras
	4.- Se otorga permisos de acceso en las entradas principales a personas particulares ajenas a la institución
	5.- Se puede eludir las paredes y mallas alrededor de la UTN

Fuente: Elaboración propia

Utilizando técnicas de observación se obtuvo los ítems marcados en la tabla 3.34, por tanto, sumando se tiene un valor numérico de **Lv=5.**

Debilidad

Una debilidad puede ser una cerradura de una puerta que se abre cuando una tarjeta se encaja entre ella y el marco de la puerta, un generador de respaldo sin combustible o un seguro que no cubre daños por inundación en una zona de inundación, debilidad o errores de los controles de clase A. En la tabla 3.35 se muestran los datos obtenidos para la Debilidad.

TABLA 0.35 Elaboración de la Debilidad dentro del canal Físico

Debilidad	
Técnica:	**Observación**
Objetivo:	**UTN**
Controles Clase A	**Fallas en los controles**
Indemnización	**1.-** El uso de señales de cuidado no se encuentran en todos los lugares
Continuidad	**2.-** La falta de recursos como agua y alimento en tiempo prolongado detiene el acceso

Fuente: Elaboración propia

Para el control de autenticación, resistencia y subyugación no se encontró fallas o errores, por tanto, sumando los ítems de la tabla anterior y aplicando la ecuación 5 se obtiene un valor numérico de:

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

$$L_w = 0 + 1 + 0 + 0 + 1$$

$$L_w = 2$$

Preocupación

Una preocupación puede ser un mecanismo de bloqueo de la puerta cuyos controles de operación y tipos de llaves son públicos, un generador de respaldo sin medidor de potencia o indicador de combustible, un proceso de equipo que no requiere que el empleado firme la salida de materiales cuando se recibe, o una alarma contra incendios que no sea lo suficientemente alta como para ser escuchada por los trabajadores de la maquinaria pesada que usan tapones para los oídos, se aplica a los controles de clase B. En la tabla 3.26 se muestran los datos obtenidos para la preocupación.

TABLA 0.36 Elaboración de la Preocupación dentro del canal Físico

Preocupación	
Técnica:	**Observación**
Objetivo:	**UTN**
Controles Clase B	**Fallas en los controles**
Confidencialidad	**1.-** Las interaciones personales por medio de las oficinas fisicas o cualquier lugar a puerta cerrada tiene inconvenientes debido a que cuando existe algún tipo de urgencia la interaccion no se realiza a puerta cerrada.

Fuente: Elaboración propia

Para los controles de clase B como son: no repudio, privacidad, integridad y alarma no se encontró errores o fallas, de tal manera que aplicando la ecuación 6 se obtiene el valor numérico de:

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

$$Lc = 0 + 1 + 0 + 0 + 0$$

$$Lc = 1$$

Exposición

Una exposición puede ser una ventana que permite visualizar activos y procesos o un medidor de potencia que muestra la cantidad de energía que utiliza un edificio y su fluctuación a lo largo del tiempo**.** En la tabla 3.37 se detallan los datos obtenidos para la exposición.

TABLA 0.37 Elaboración de la Exposición dentro del canal Físico

Exposición	
Técnica:	**Observación**
Objetivo:	**UTN**
Exposición física (Anexo 2)	**1.-** Los activos son visualizados a través de las ventanas transparentes dentro de la UTN **2.-** Los activos de laboratorios de computación de las facultades se encuentran expuestas a daños o hurtos **3.-** Los documentos son transportados internamente por el personal sin uso de sellos y firmas

Fuente: Elaboración propia

Contabilizando los ítems de la tabla 3.37 se obtiene un valor numérico para la exposición de **L_E=3**

Anomalía

Una anomalía puede ser aves muertas descubiertas en el techo de un edificio alrededor del equipo de comunicación. En la tabla 3.38 se muestran los datos obtenidos para la Anomalía.

TABLA 0.38 Elaboración de la Anomalía dentro del canal Físico

Anomalía	
Técnica:	**Observación**
Objetivo:	**UTN**
Anomalías	**1.-** Se hace uso de tarjetas de acceso para las puertas físicas de aulas por parte de estudiantes de la institución, la cual puede ser considerada como una exposición **2.-** Ingreso de personas con comida a laboratorios y aulas de clase en la institución **3.-** Algunos de los equipos de controles de acceso con tarjeta de las entradas a la universidad están apagados.

Fuente: Elaboración propia

Mencionado los ítems de la tabla anterior se obtiene un valor numérico para la anomalía de **L_A = 3.**

3.2.4 Aplicación del RAV

Para la aplicación del RAV se utilizó la hoja de cálculo propia de la metodología, la cual se encuentra disponible en su sitio oficial www.osstmm.com, los valores se consiguieron a través de técnicas de observación, Ingeniera social, reglamento de la institución y encuestas. En la tabla 3.39 se detallan los valores obtenidos para la prueba de seguridad física.

TABLA 0.39 Datos Obtenidos para el RAV del canal Físico

Datos Obtenidos para el RAV del Canal Físico (PHYSSEC)		
Ítems		**Valor Total**
Porosidad	Visibilidad	**(PV) = 16**
	Acceso	**(PA) = 4**
	Confianza	**(PT) = 1**
Controles	Autenticación	**(LCAu) = 9**
	Indemnización	**(LCID) = 6**
	Resistencia	**(LCRe) = 3**
	Subyugación	**(LCSu) = 0**
	Continuidad	**(LCCt) = 7**
	No repudio	**(LCNR) = 2**
	Confidencialidad	**(LCCf) = 1**
	Privacidad	**(LCPr) = 1**
	Integridad	**(LCIt) = 1**
	Alarma	**(LCAl) = 0**
Limitaciones	Exposición	**LE = 3**
	Vulnerabilidad	**LV = 5**
	Debilidad	**Lw = 2**
	Preocupación	**Lc = 1**
	Anomalía	**LA = 3**

Fuente: Elaboración propia

Análisis de resultados

La Medida de seguridad de la superficie de ataque para canal Físico se visualiza en la tabla 3.40.

TABLA 0.40 Calculadora RAV de OSSTMM 3, Prueba de Seguridad Físico

RAV Canal Físico

OSSTMM versión 3.0

Inserte en los espacios en blanco los valores numéricos para OPSEC, Controles y Limitaciones con los resultados de la prueba de seguridad. Visite OSSTMM 3 (www.osstmm.org) para más información

OPSEC	
Visibilidad	16
Acceso	4
Confianza	1
Total (Porosidad)	21

CONTROLES		
Clase A		Ausentes
Autenticación	9	12
Indemnización	6	15
Resistencia	3	18
Subyugación	0	21
Continuidad	7	14
Total Clase A	25	80
Clase B		Ausentes
No-Repudio	2	19
Confidencialidad	1	20
Privacidad	1	20
Integridad	1	20
Alarma	0	21
Total Clase B	5	100
		Ausentes Verdaderos
Total Controles	30	180
Cobertura Total	14,29%	85,71%

LIMITACIONES		Valor Numérico	Valor Total
Vulnerabilidad	5	9,571429	47,857143
Debilidad	2	4,809524	9,619048
Preocupación	1	5,761905	5,761905
Exposición	3	1,197279	3,591837
Anomalías	3	0,421769	1,265306
Total # Limitaciones	14		68,0952

OPSEC	11,038515
Controles Verdaderos	6,143292
Controles Completos	6,143292
Cobertura Verdadera A	23,81%
Cobertura Verdadera B	4,76%
Total Cobertura Verdadera	14,29%
Limitaciones	14,693273
Seguridad Δ	-19,59
Protección Verdadera	80,41

Seguridad Actual 80,45 ravs

Fuente: Elaboración propia

Los valores numéricos obtenidos dentro de este canal son rellenados automáticamente en la hoja de cálculo del RAV perteneciente a la metodología, los valores a rellenar son: valor total de OpSec, valor ausente y valor total del control de clase A y B, valores ausentes y total de Limitaciones, el RAV básicamente resta la porosidad y las limitaciones de los controles como lo indica la ecuación 1. Se resalta el valor numérico de la seguridad Δ enmarcado de color rojo lo que significa una carencia o insuficiencia del 19,59 de los controles adoptados, la cual indica que el área perimetral de la UTN y la información física se encuentra parcialmente vulnerable y expuesta a posibles atracos y sustracciones de activos.

R A V = CONTROLES VERDADEROS – POROSIDAD – LIMITACIONES

RAV = 6,1432 – 11,0385 – 14,6932

RAV = - 19,59

3.3 Pruebas de Seguridad Inalámbrica (SPECSEC)

En este canal se realiza la interacción del analista en un rango cercano al vector de ataque, para iniciar las pruebas de este canal de manera adecuada aplicando la metodología se debe empezar en regirse a las políticas de seguridad o la regulación legislativa que existe en la institución para el espectro electromagnético y similares en caso de no existir recurrir a la legislación contemplada a nivel nacional, (Pete Herzog, 2010).

“La auditoría informática es útil, pero no constituye una ciencia exacta, debe apoyarse en un conjunto de suposiciones” (Derrien, 2009, pág. 7), con este concepto para la elaboración del estudio se consideró las redes inalámbricas principales WUTN_Admin, WUTN_Estudiantes y Eduroam, se utilizó herramientas de Kali Linux y se aplicó encuestas hacia el responsable del área de redes y comunicaciones, en el anexo 3 se muestran los datos obtenidos para resolver este canal. Los literales o pasos a seguir son interpretados por el autor y director Pete Herzog de la metodología OSSTMM.

3.3.1 Porosidad

La porosidad reduce la separación entre una amenaza y un acceso para obtener este valor es necesario calcular el valor de la visibilidad, el acceso y la confianza.

Visibilidad

La visibilidad se considera como "presencia" y no se limita a la vista humana. Son pruebas de enumeración y verificación para la visibilidad del personal con el cual la interacción es posible a través de todos los canales. En la tabla 3.41 se muestran los datos obtenidos para la visibilidad.

TABLA 0.41 Elaboración de la Visibilidad dentro del canal Inalámbrico

Visibilidad		
Técnica:	**Herramientas Kali Linux, Observación y Encuesta**	
Interceptación (Localización)	Control de acceso	**1.-** Lector biométrico (hacia los servidores)
		2.- código pin (hacia los servidores)
	Seguridad Perimetral	**3.-** Cortafuegos (Firewalls)
Detección de frecuencias Wi-Fi	Frecuencias	**4.-** 2,4 GHZ
		5.- 5 GHz
Otras señales	Sistema RFID (Radio Frecuencia)	No se utiliza

Fuente: Elaboración propia

Mediante la herramienta aircrack-ng de Kali Linux se encontraron redes de 2,4 GHz y 5 GHz (anexo 3), se aplicó encuestas hacia el administrador de redes y comunicaciones para determinar la seguridad perimetral y mediante observación se determinó los controles de acceso, sumando los ítems de la tabla 3.41 se obtiene un valor numérico de Visibilidad de ***P*v= 5**

Acceso

Realizar pruebas para la enumeración de puntos de acceso al personal dentro del alcance, si bien el acceso al personal fuera del alcance es un escenario real y se usa a menudo para el robo de propiedad de información, el analista puede limitarse solamente a la interacción con el alcance para proteger los derechos de privacidad independientes del personal en su vida privada. En la tabla 3.42 se detallan los datos obtenidos para el acceso.

TABLA 0.42 Elaboración del Acceso dentro del canal Inalámbrico

Acceso	
Técnica:	**Encuesta**
Control de acceso lógico	**1.-** Los equipos informáticos para la red inalámbrica se encuentran con su configuración básica para un funcionamiento normal

Control de acceso físico	Los puntos de acceso (AP), no poseen protección física como encerramiento con caja de llave
	2.- Los puntos de acceso (AP) de la UTN durante todo el día se encuentran encendidos

Fuente: Elaboración propia

Los datos se obtuvieron a través de encuestas realizadas hacia el administrador de redes y comunicaciones, y se encuentran enmarcadas en los ítems en la tabla 3.42, por tanto, el valor numérico para el acceso es de $P_a = 2$.

Confianza

La confianza es cualquier interacción no autenticada con cualquiera de los destinos, realizar pruebas de confianza entre el personal en el que la confianza se refiere al acceso a la información o a la propiedad física sin necesidad de identificación o autenticación, en la tabla 3.43 se muestran los datos obtenidos para la confianza.

TABLA 0.43 Elaboración de la Confianza dentro del canal Inalámbrico

Confianza	
Técnica:	**Encuesta**
métodos de Autenticación	**1.-** Clave Compartida
	2.- Usuario y contraseña

Fuente: Elaboración propia

Los métodos de autenticación que genera confianza para el acceso hacia los AP son el uso de usuario y contraseñas, por tanto, el valor numérico para la confianza es de $P_T = 2$.

3.3.2 Controles

Los controles son un medio para controlar las amenazas y proteger la información.

Autenticación

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

Al realizar un escaneo de redes inalámbricas que existen en la UTN, se obtuvieron los siguientes datos que se muestra la tabla 3.44.

TABLA 0.44 Elaboración de la Autenticación dentro del canal Inalámbrico

Autenticación			
Técnica:	**Herramientas Kali Linux y Encuesta**		
Autenticación	**Cifrado en red inalámbrica (Anexo 3)**	WUTN.Docentes	**1.-** PSK
		WUTN.Admin	Ninguna
		Eduroam	**2.-** MGT
	Encriptación en red Inalámbrica (Anexo 3)	WUTN.Docentes	**3.-** WPA2
		WUTN.Admin	Abierta
		Eduroam	**3.-** WPA2
Autorización	**Red Inalámbrica**	Eduroam	**4.-** Se necesita credenciales de correo institucional y contraseña

Fuente: Elaboración propia

El valor numérico obtenido para la autenticación en base a los ítems de la tabla 3.44 es de $\boldsymbol{LCAu}$ **= 4** debido a que las redes inalámbricas WUTN.Docentes y Eduroam cuentan con encriptación y cifrado además que la red inalámbrica Eduroam requiere una autorización mediante correo electrónico institucional y contraseña.

Indemnización

Documentar y enumerar que los objetivos y servicios están protegidos contra el abuso o elusión de las políticas de los empleados, están asegurados contra robo o daños, o uso de responsabilidad y renuncias de permisos. En la tabla 3.45 se detallan los datos obtenidos para el control de Indemnización.

TABLA 0.45 Elaboración de la Indemnización dentro del canal Inalámbrico

Indemnización	
Técnica:	**Encuesta**
Equipos de Comunicación Inalámbricos	**1.-** Se encuentran protegidos contra hurtos o daños
	2.- El acuerdo de uso de responsabilidad por parte de empleados y usuarios es el uso de carnet de identificación visible
	3.- Cuando algún usuario u empleado incumple un acuerdo legal como un activo sustraído se reporta al personal de seguridad y a la autoridad jerárquica superior

Fuente: Elaboración propia

Sumando los ítems marcados en la tabla 3.45 se obtiene para el control de Indemnización un valor numérico de $\boldsymbol{LC}$**Id = 3**

Subyugación

Enumerar y poner a prueba las insuficiencias de todos los canales a utilizar o habilitar los controles que no estén activados de forma predeterminada. En la tabla 3.46 se muestran los datos obtenidos para la subyugación.

TABLA 0.46 Elaboración de la Subyugación dentro del canal Inalámbrico

Subyugación	
Técnica:	**Encuesta**
Controles	Se hace énfasis en su configuración básica para un funcionamiento normal
	1.- Se hace énfasis en los certificados de actualización de los equipos informáticos

Fuente: Elaboración propia

El control que se hace énfasis fuera de su configuración predeterminada de los equipos informáticos son los certificados de actualización, por tanto, el valor numérico para el control de subyugación es **LC_{Su}= 1**

Resistencia

Documentar el proceso que realizan los guardias para desconectar los canales debido a incumplimientos o preocupaciones de seguridad como un análisis de la brecha con la regulación y la política de seguridad.

Según el Estatuto Orgánico de la UTN, establece que: los bienes adquiridos no pueden salir del predio universitario sin autorización escrita del custodio a cargo (Legislación legal UTN, 2012).

1.- Cuando existen incumplimientos o preocupación de seguridad el personal de seguridad detiene a la persona o a las personas infractoras para luego ser tramitados y evaluados según la ley interna de la UTN.

por tanto, remarcando lo dicho anteriormente, el valor numérico para el control de resistencia es de $\boldsymbol{LCRe}$ **= 1.**

Continuidad

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. En la tabla 3.47 se muestran los datos obtenidos para la continuidad.

TABLA 0.47 Elaboración de la Continuidad dentro del canal Inalámbrico

Continuidad	
Técnica:	**Encuesta**
Equipos Informáticos	**1.-** El DDTI recibe apoyo del centro de transferencia y desarrollo tecnológico
Funcionamientos de equipos	**2.-** El tiempo en resolver el inconveniente es de menos de 7 días

Fuente: Elaboración propia

Al suscitarse problemas o inconvenientes con los equipos informáticos se recibe apoyo adecuado de otros departamentos y el tiempo de respuesta frente a un inconveniente se lo hace en el menor tiempo posible de manera eficiente. Por tanto, sumando los numerales de la continuidad se tiene un valor numérico de $\boldsymbol{LCCt}$ **= 2**

No repudio

Enumerar y probar el uso o las deficiencias de los daemons y sistemas para identificar y registrar adecuadamente el acceso o interacciones a la propiedad para tener una evidencia específica que permita resistir el repudio.

No existe ningún sistema especial que identifique y registre el acceso en los equipos inalámbricos de la UTN, por tanto, el valor numérico para este control es **LC_{NR} = 0**

Confidencialidad

Enumerar y examinar el uso de equipos para amortiguar las señales de transmisión electromagnética fuera de la organización y los controles en el lugar para asegurar y encriptar las transmisiones inalámbricas. En la tabla 3.48 se muestran los datos obtenidos para la confidencialidad.

TABLA 0.48 Elaboración de la Confidencialidad dentro del canal Inalámbrico

Confidencialidad	
Técnica:	**Encuesta**
Controles:	No se hace uso de ningún equipo para amortiguar la señal inalámbrica y evitar que esta salga de la institución
	1.- Se hace uso de la encriptación de la red inalámbrica

Fuente: Elaboración propia

Para este control se hace uso de la encriptación de la red inalámbrica, por tanto, marcando el ítem de la tabla anterior se tiene un valor numérico para la confidencialidad de **LC_{Cf} = 1.**

Privacidad

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.), En la tabla 3.49 se muestran los datos obtenidos para la privacidad.

TABLA 0.49 Elaboración de la Privacidad dentro del canal Inalámbrico

Privacidad	
Técnica:	**Encuesta**
Controles de acceso físico:	**1.-** Cámaras de vigilancia
	2.- Cerradura con llave
	3.- Personal de seguridad

Fuente: Elaboración propia

Existen controles de acceso público para proteger los AP de la UTN en las que se encuentran: las cámaras de seguridad, cerradura de las puertas externas con llave y por último para proteger estos activos se encuentra el personal de seguridad, por tanto, sumando los ítems de la tabla 3.49 se obtiene un valor numérico de $\mathbf{LC_{Pr} = 3}$

Integridad

Determinar que los datos sólo puedan ser consultados y modificados por aquellos que están autorizados y garantizar que el adecuado cifrado este en uso para garantizar la firma y la confidencialidad de las comunicaciones. En la tabla 3.50 se detallan los datos obtenidos para la Integridad.

TABLA 0.50 Elaboración de la Integridad dentro del canal Inalámbrico

Integridad	
Técnica:	**Encuesta**
Personal Autorizado	**1.-** Uso de contraseñas
Cifrado	**2.-** Uso de cifrado para la red inalámbrica

Fuente: Elaboración propia

Los datos pueden ser consultados y modificados por el personal autorizado mediante el uso de contraseñas, y se hace uso del cifrado en la red inalámbrica, por tanto, contabilizando los ítems de la tabla 3.50 se obtiene un valor numérico para el control de Integridad de $\mathbf{LC_{It}=2.}$

Alarma

Verificar y enumerar el uso de un sistema de alerta localizado 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. En la tabla 3.51 se detallan los datos obtenidos para el control de alarma.

TABLA 0.51 Elaboración de la Alarma dentro del canal Inalámbrico

Alarma	
Técnica:	**Encuesta y Observación**
Sistema de alerta	**1.-** Sistema de alarma
	2.- Software antivirus
	3.- Personal de seguridad
	4.- Mensajes o llamadas personales

Fuente: Elaboración propia

Para mitigar una actividad sospechosa existen sistemas de alerta tales como: Software antivirus, Sistema de alarma, personal de seguridad y el uso de mensajes o llamadas telefónicas personales, por tanto, contabilizando los ítems de la tabla 3.51 se obtiene un valor numérico para el control de alarma de **$LC_{AI} = 4$.**

3.3.3 Limitaciones

Son los agujeros, vulnerabilidades, debilidades y problemas para mantener esa separación entre un activo y una amenaza o para asegurar que los controles continúen funcionando correctamente, Las limitaciones se clasifican en cinco categorías vulnerabilidad, debilidad, preocupación, exposición y anomalía, las limitaciones se verifican siempre que sea posible (Pete Herzog, 2010).

Exposición

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

Los equipos inalámbricos son configurados para no interrumpir con otros dispositivos o maquinas además de no existir puntos de acceso en desuso, por tanto, el valor numérico para la exposición es **$L_E=0$.**

Vulnerabilidad

Una vulnerabilidad puede ser un hardware que puede ser sobrecargado y quemado por las versiones de mayor potencia en 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 AP inalámbrico cuando cae su conexión cerca de un horno microondas.

1.- Se encuentran vulnerabilidades en los AP debido a que estos poseen una configuración estándar por tanto pueden estar expuestos a un ataque informático.

Mencionado lo anterior el valor numérico para la vulnerabilidad es de **Lv=1**

Debilidad

Una debilidad de seguridad informática puede ser un punto de acceso inalámbrico con autenticación de usuario basada en direcciones MAC (que se pueden falsificar) o una tarjeta de seguridad RFID que ya no recibe señales y, por lo tanto, queda en "abierta" después de recibir una señal que procede de una fuente de alta potencia. En la 3.52 se muestran los datos obtenidos para la debilidad informática.

TABLA 0.52 Elaboración de la Debilidad dentro del canal Inalámbrico

Debilidad	
Técnica:	**Encuesta**
Controles de clase A	**Falla o Error**
Autenticación	La red inalámbrica WUTN.Admin es abierta pero no cuenta con acceso a internet
Subyugación	**1.-** Puede pasar desapercibido las actualizaciones de los AP debido a que existen varios AP en toda la Institución y estos requieren una actualización constante

Fuente: Elaboración propia

Se ha encontrado fallas o errores en los controles de subyugación debido a que existen varios AP en la UTN y estos deben ser actualizados constantemente para mantener un debido funcionamiento y mantener una correcta seguridad de la red, en los controles de autenticación, indemnización, resistencia y continuidad no se encontraron fallas o errores. Por tanto, el valor numérico para la debilidad aplicando la ecuación 5 se obtiene:

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

$$Lw = 0 + 0 + 0 + 1 + 0$$

$$Lw = 1$$

Preocupación

Una preocupación puede ser un punto de acceso inalámbrico que utiliza un cifrado de datos débil o un abridor de puertas por infrarrojos que no puede leer al remitente en la lluvia. En la tabla 3.53 se muestran los datos obtenidos para la preocupación.

TABLA 0.53 Elaboración de la Preocupación dentro del canal Inalámbrico

Preocupación	
Técnica:	**Encuesta**
Controles de clase B	**Falla o Error**
confidencialidad	**1.-** No se hace uso de ningún equipo para amortiguar la señal inalámbrica y evitar que esta salga de la institución
privacidad	**2.-** La cerradura con llave de las puertas del exterior de la UTN presenta inconvenientes debido que se puede falsear
integridad	**3.-** El uso de contraseñas para el acceso del personal autorizado hacia los equipos inalámbricos presenta inconvenientes debido a que puede existir divulgación de contraseñas

Fuente: Elaboración propia

En la tabla anterior se hace mención de las fallas encontrados en los controles de clase B como; no repudio y alarma, en las que no se encontró errores o fallas. Por tanto, aplicando la ecuación 6 y sumando las deficiencias de los controles de los ítems marcados en la tabla 3.53 se obtiene un valor numérico para la preocupación de:

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

$$Lc = 0 + 1 + 1 + 1 + 0$$

$$Lc = 3$$

Anomalía

Una anomalía puede ser una señal local que no se puede localizar correctamente ni hace ningún daño conocido. En la tabla 3.54 se muestran los datos obtenidos para la Anomalía.

TABLA 0.54 Elaboración de la Anomalía dentro del canal Físico

Anomalía	
Técnica:	**Encuesta**
Objetivo:	**UTN**
Anomalías	**1.-** Los SSID de las redes inalámbricas WUTN.Admin y WUTN.Docentes no han sido cambiados desde hace mucho tiempo debido a normas internas **2.-** Las contraseñas de la red inalámbrica WUTN.Docentes no hace cambiada desde hace varios meses

Fuente: Elaboración propia

Según los criterios anteriores se obtiene para la anomalía un valor numérico de **L_A=2**

3.3.4 Aplicación del RAV

Para la aplicación del RAV se utilizó la hoja de cálculo propia de la metodología, la cual se encuentra disponible en su sitio oficial www.osstmm.com, los valores se consiguieron a través de técnicas de encuestas y mediante herramientas de Kali Linux. En la tabla 3.55 se detallan los valores obtenidos para la prueba de seguridad inalámbrica.

TABLA 0.55 Datos Obtenidos para el RAV del canal Físico

Datos Obtenidos para el RAV del Canal Inalámbrica (SPECSEC)		
Ítems		**Valor Total**
Porosidad	Visibilidad	**(PV) = 5**
	Acceso	**(PA) = 2**
	Confianza	**(PT) = 2**
Controles	Autenticación	**(LCAu) = 4**
	Indemnización	**(LCID) = 3**
	Resistencia	**(LCRe) = 1**
	Subyugación	**(LCSu) = 1**
	Continuidad	**(LCCt) = 2**
	No repudio	**(LCNR) = 0**
	Confidencialidad	**(LCCf) = 1**
	Privacidad	**(LCPr) = 3**
	Integridad	**(LCIt) = 2**
	Alarma	**(LCAl) = 4**
Limitaciones	Exposición	**LE = 0**
	Vulnerabilidad	**LV = 1**
	Debilidad	**Lw = 1**

	Preocupación	**Lc = 3**
	Anomalía	**LA = 2**

Fuente: Elaboración propia

Análisis de resultados

La Medida de seguridad de la superficie de ataque para canal Inalámbrico se visualiza en la tabla 3.56.

TABLA 0.56 Calculadora RAV de OSSTMM 3, Prueba de Seguridad Inalámbrica

RAV Canal Inalámbrico

OSSTMM versión 3.0

Inserte en los espacios en blanco los valores numéricos para OPSEC, Controles y Limitaciones con los resultados de la prueba de seguridad. Visite OSSTMM 3 (www.osstmm.org) para más información

OPSEC

Visibilidad	5
Acceso	2
Confianza	2
Total (Porosidad)	9

CONTROLES

Clase A		Ausentes
Autenticación	4	5
Indemnización	3	6
Resistencia	1	8
Subyugación	1	8
Continuidad	2	7
Total Clase A	11	34

Clase B		Ausentes
No-Repudio	0	9
Confidencialidad	1	8
Privacidad	3	6
Integridad	2	7
Alarma	4	5
Total Clase B	10	35

		Ausentes Verdaderos
Total Controles	21	69
Cobertura Total	23,33%	76,67%

LIMITACIONES

		Valor Numérico	Valor Total
Vulnerabilidad	1	8,666667	8,666667
Debilidad	1	4,777778	4,777778
Preocupación	3	4,888889	14,666667
Exposición	0	1,151852	0,000000
Anomalías	2	0,725926	1,451852
Total # Limitaciones	7		29,5630

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

OPSEC	8,730399
Controles Verdaderos	5,402289
Controles Completos	5,402289
Cobertura Verdadera A	24,44%
Cobertura Verdadera B	22,22%
Total Cobertura Verdadera	23,33%
Limitaciones	12,047111
Seguridad Δ	-15,38
Protección Verdadera	84,62

Seguridad Actual 84,55 ravs

OSSTMM RAV - Creative Commons 3.0 Attribution-NonCommercial-NoDerivs 2011, ISECOM

Fuente: Elaboración propia

Los valores numéricos obtenidos dentro de este canal son rellenados automáticamente en la hoja de cálculo del RAV perteneciente a la metodología, los valores a rellenar son: valor total de OpSec, valor ausente y valor total del control de clase A y B, valores ausentes y total de Limitaciones, el RAV básicamente resta la porosidad y las limitaciones de los controles como lo indica la ecuación 1. Se resalta el valor numérico de la seguridad Δ enmarcado de color rojo lo que significa una carencia o insuficiencia de 15,38 de los controles adoptados, la cual indica que la red inalámbrica se encuentra parcialmente expuesta a posibles ataques informáticos.

R A V = CONTROLES VERDADEROS – POROSIDAD – LIMITACIONES

RAV = 5,4022 – 8,7303 – 12,0471

RAV = - 15,38

3.4 Prueba de Seguridad de las Redes de Datos (COMSEC)

Las pruebas para este canal requieren interacciones con los seguros operacionales de la red de comunicación de datos existentes utilizados para controlar el acceso a la propiedad, este canal cubre la implicación de los sistemas informáticos, principalmente las redes operativas dentro del alcance, si bien algunas organizaciones consideran esto simplemente como "pruebas de penetración", el verdadero objetivo de cumplimiento de las pruebas de seguridad en este canal es la interacción del sistema y las pruebas de calidad operativa con mediciones de distancias con el estándar de seguridad requerido descrito en la política de la empresa, regulaciones de la industria o la legislación regional, para este canal se requerirá que el analista tenga métodos para evitar la divulgación de las pruebas. (Pete Herzog, 2010).

“La auditoría informática es útil, pero no constituye una ciencia exacta, debe apoyarse en un conjunto de suposiciones” (Derrien, 2009, pág. 7), con este concepto para la elaboración del estudio se consideró recurrir a técnicas mediante encuestas hacia el encardo del área de redes y Comunicaciones y mediante herramientas de Kali Linux, en el anexo 4 se muestran los datos obtenidos para resolver este canal. Los literales o pasos a seguir son interpretados por el autor y director Pete Herzog de la metodología OSSTMM.

3.4.1 Porosidad

La porosidad reduce la separación entre una amenaza y un acceso, para obtener este valor es necesario calcular el valor de la visibilidad, el acceso y la confianza.

Visibilidad

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

- Identifique el perímetro del (de los) segmento(s) de la red de destino y el vector desde el cual serán examinados.

Para identificar el perimetro de la red de destino desde exterior hacia el interior y viceversa y siguiendo el procedemiento de autenticación a la red se utilizó el acceso a la pagina web de la institucion utilizando la herramienta Nmap de Kali Linux, en la figura 25 se muestra como resultado:

1.- direccion de red clase B publica (128.0.0.0 a 191.255.255.255).

2.- direccion de red clase B privada (172.16.0.0 a 172.31.255.255).

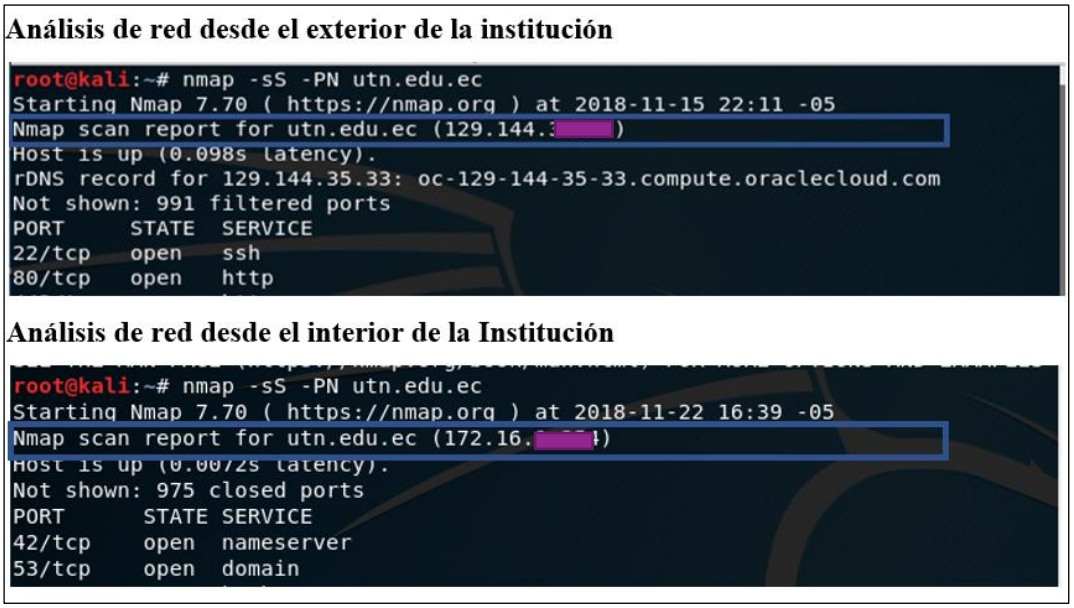


Fig. 25. Análisis de red del exterior y viceversa de la UTN, herramienta Nmap

Fuente: Elaboración propia

- Usar un sniffer de red para identificar protocolos que proceden de las respuestas de los servicios de red o peticiones aplicables. Por ejemplo, NetBIOS, ARP, BGP, NFS, OSPF, MPLS, RIPv2, etc.

Para realizar este paso se utilizó el sniffer de red wireshark que se muestra en la figura 26, y como resultado los protocolos que proceden de las respuestas de los servicios de red es el protocolo: **1.-** ARP y **2.-** RIPv2**.**

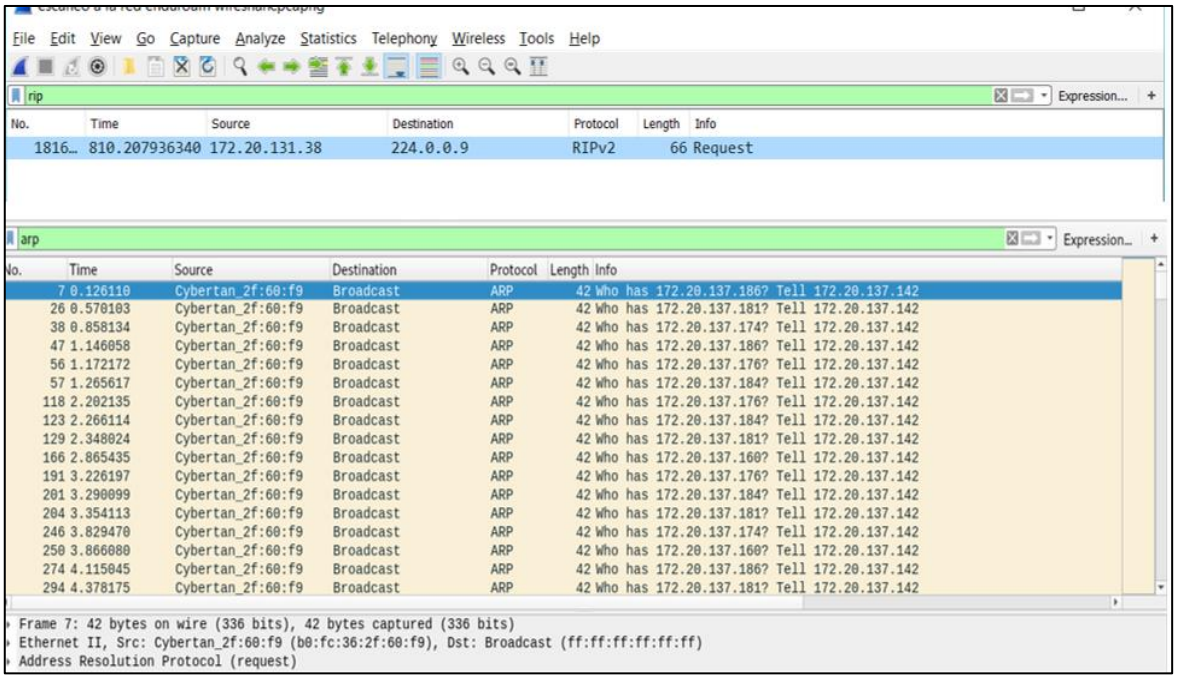


Fig. 26. Protocolos que proceden de las respuestas de los servicios de red, Wireshark

Fuente: Elaboración propia

- Consultar todos los nombres de los servidores y los nombres de los servidores del ISP o proveedor de hosting, si se encuentran disponibles, así como la capacidad para realizar transferencias de zona para determinar la existencia de todos los objetivos en la red y cualquier redundancia relacionada al balanceo de carga, almacenamiento en caché, proxy y hosting virtual.

En la figura 27 se muestra la información recopilada de los servidores encontrados a través de la página web oficial de la institución desde el exterior de la universidad con ayuda de la herramienta DNSrecon.

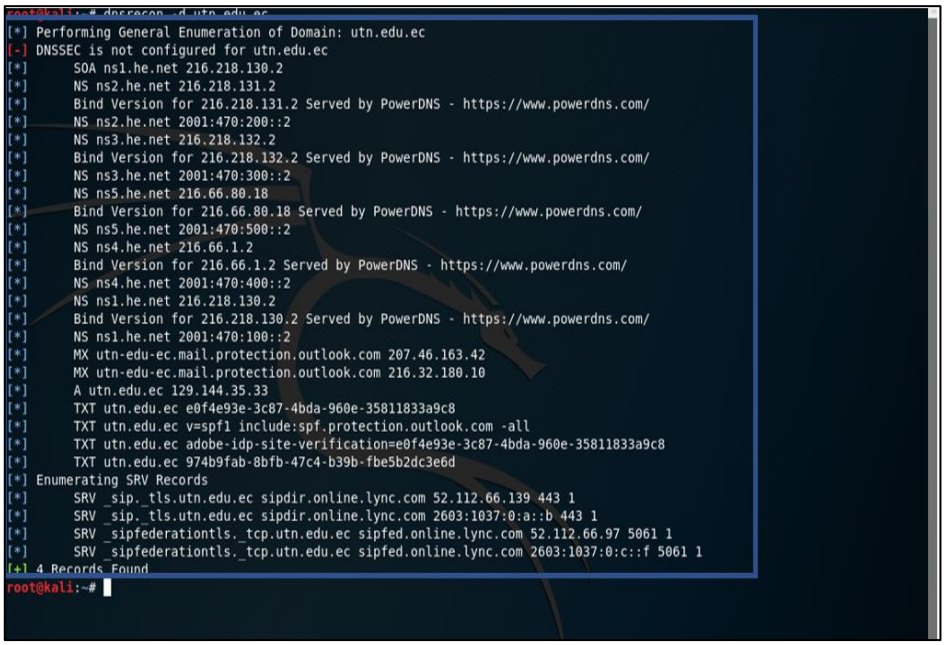


Fig. 27. Análisis de red desde el exterior hacia el interior, herramienta DNSRecon

Fuente: Elaboración propia

En la figura 28 y 29 se muestra la información recopilada de los servidores encontrados a través de la página web oficial de la institución desde la red de área local con ayuda de la herramienta DNSenum y Nmap respectivamente.

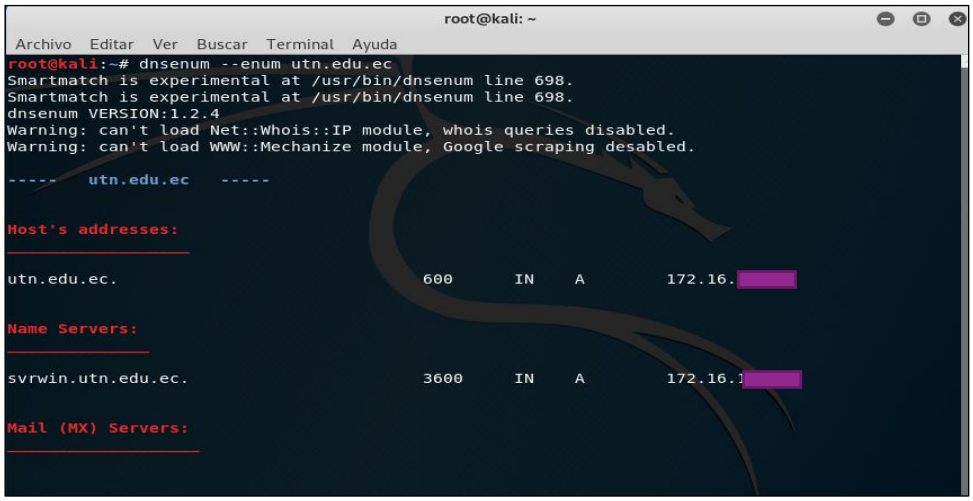


Fig. 28. Análisis de red desde la red local UTN, herramienta DNSenum

Fuente: Elaboración propia

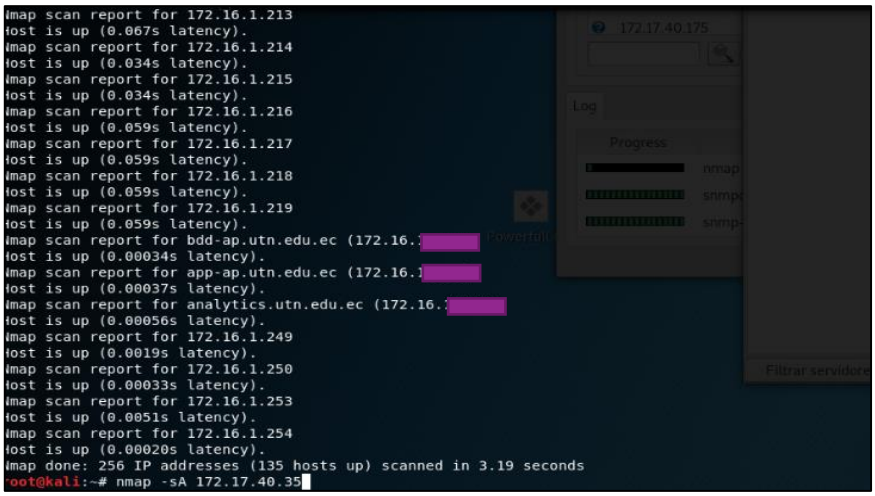


Fig. 29. Análisis de red desde la red local UTN, herramienta Nmap

Fuente: Elaboración propia

En la tabla 3.57 se visualizan los datos encontrados para esta sección.

TABLA 0.57 Datos Obtenidos de Servidores Disponibles

	Servidor	**IP**
1.- Servidor web	utn.edu.ec (exterior)	129.144.xxx.xxx
2.- Servidores de Alojamiento de DNS	ns1.he.net	216.218.xxx.xxx
	ns2.he.net	216.218.xxx.xxx
	ns3.he.net	216.218.xxx.xxx
	ns4.he.net	216.66.xxx.xxx
	svrwin.utn.edu.ec (interior)	172.16.xxx.xxx
	ns5.he.net	216.66.xxx.xxx
3.- Servidores de correo electrónico	utn-eduec.mail.protection.outlook.com	216.32.xxx.xxx
	utn-eduec.mail.protection.outlook.com	207.46.xxx.xxx
4.- Servidor de base de datos	bdd-ap.utn.edu.ec	172.16.xxx.xxx
5.- Servidor de aplicación móvil	app-ap.utn.edu.ec	172.16.xxx.xxx
6.- Servidor de Analíticas	Analitycs.utn.edu.ec	172.16.xxx.xxx

Fuente: Elaboración propia

La página web de la institución se aloja en la nube de Oracle.

No se encontraron datos relacionados al balanceo de carga y almacenamiento de cache.

- Verificar peticiones de difusión y las respuestas de todos los objetivos.

Para esta sección se utilizó la herramienta Wireshark en la figura 30 se puede ver algunas peticiones de difusión y respuestas de todos los objetivos en la UTN, estas son: **1.-** Multicast **2.-** Broadcast y **3.-** Unicast.

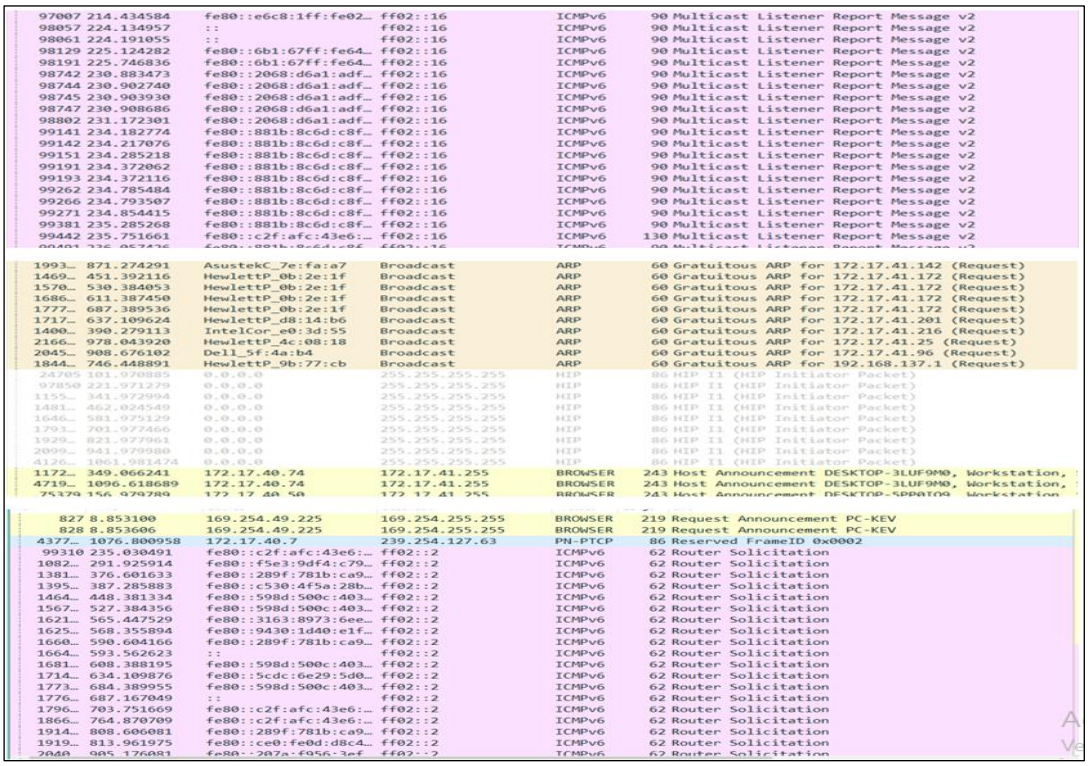


Fig. 30. Peticiones de difusión y respuestas, herramienta Wireshark

Fuente: Elaboración propia

- Verificar y examinar el uso de tráfico y los protocolos de enrutamiento de todos los objetivos.

Para esta sección se utilizo la herramienta wireshark en la figura 31 en la cuál se verifica que el protocolo que genera mas trafico es: **1.-** ARP y se resalta que dentro de la institución se maneja: **2.-**protocolos de enrutamiento para manejar la información.

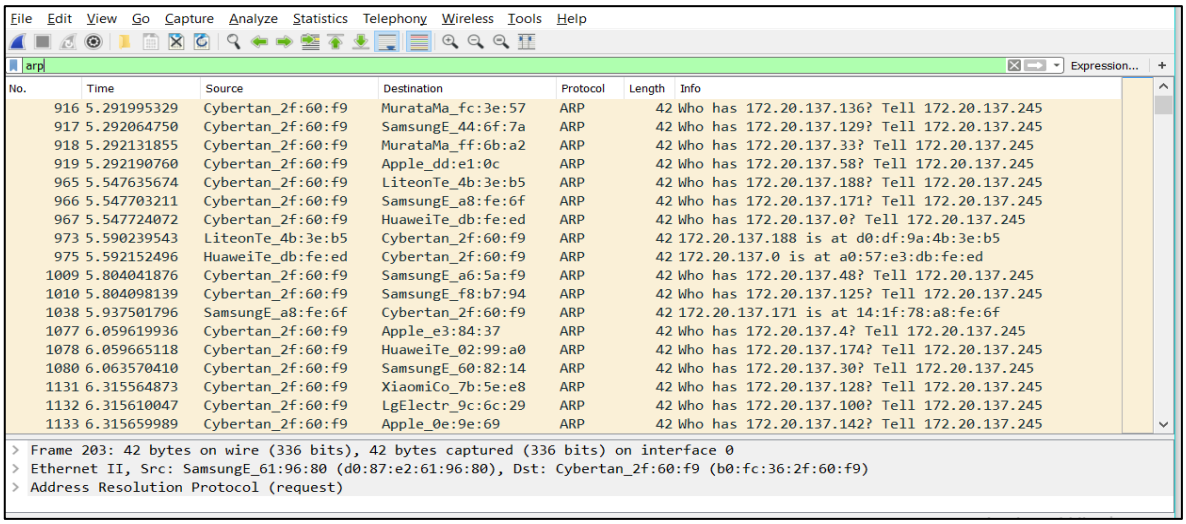


Fig. 31. Protocolos de enrutamiento, herramienta Wireshark

Fuente: Elaboración propia

- Verificar defectos y probables nombres de comunidades SNMP en uso están de acuerdo con el desarrollo práctico de todas las versiones de SNMP.

Para esta sección se utilizó la herramienta Nmap, donde no se encontró nombres de comunidades SNMP en la figura 32 el SNMP se encuentra en estado filtrado es decir que el filtrado puede provenir de un dispositivo de cortafuegos dedicado en la red, o por un cortafuegos instalada en el propio equipo.

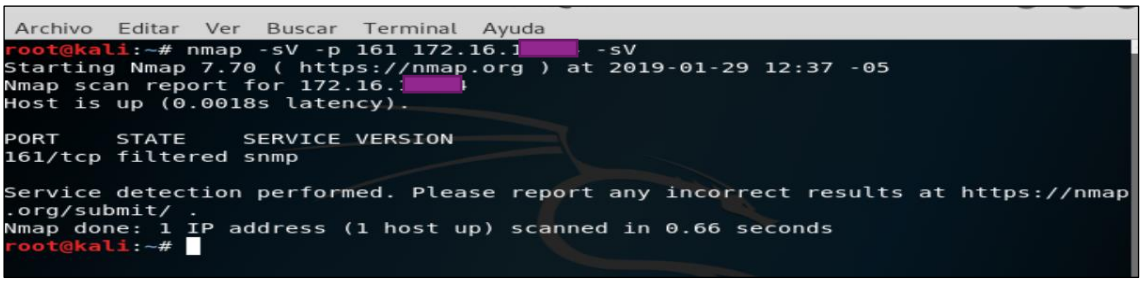


Fig. 32. Protocolos SNMP abiertos, herramienta NMAP

Fuente: Elaboración propia

- Verificar respuestas ICMP para los tipos de ICMP 0-255 y los códigos ICMP 0-2 de todos los objetivos.

En la figura 33 se muestran datos obtenidos para las respuestas del protocolo de mensajes de internet ICMP en todos los objetivos de a red de datos están ICMPv4 **1.-** echo ping reply **2.-** echo ping request con respuestas de direcciones IP internas y para el protocolo en IPv6 o

ICMPv6 existen respuestas como: **3.-** neighbor solicitation, **4.-** neighbor Advertisement, **5.-** Multicast listener report message v2, **6.-** Router solicitation, **7.-** Router Advertisement.

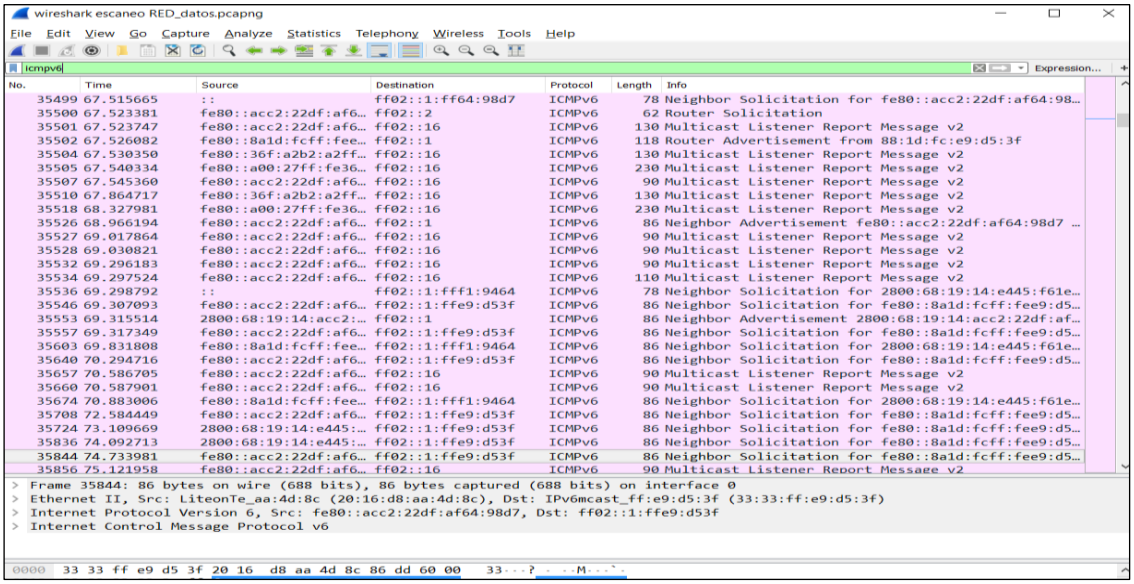


Fig. 33. Respuestas ICMP versión 4 y 6, herramienta Wireshark

Fuente: Elaboración propia

Contabilizando los ítems en los literales de la visibilidad se tiene un valor numérico de ***Pv* = 22**

Acceso

Efectuar pruebas para la enumeración de los principales puntos de acceso dentro del alcance.

- Solicitar servicios comunes conocidos los cuales utilizan UDP para las conexiones desde todas las direcciones.

Para esta seccion se utilizó la herramienta sparta figura 34 en donde se encontró que los servicios que utilizan UDP en estado abierto para las conexiones en todas las direcciones son: **1.-** Puerto 161 **SNMP** y **2.-** Puerto 137 **Netbios-ns.**

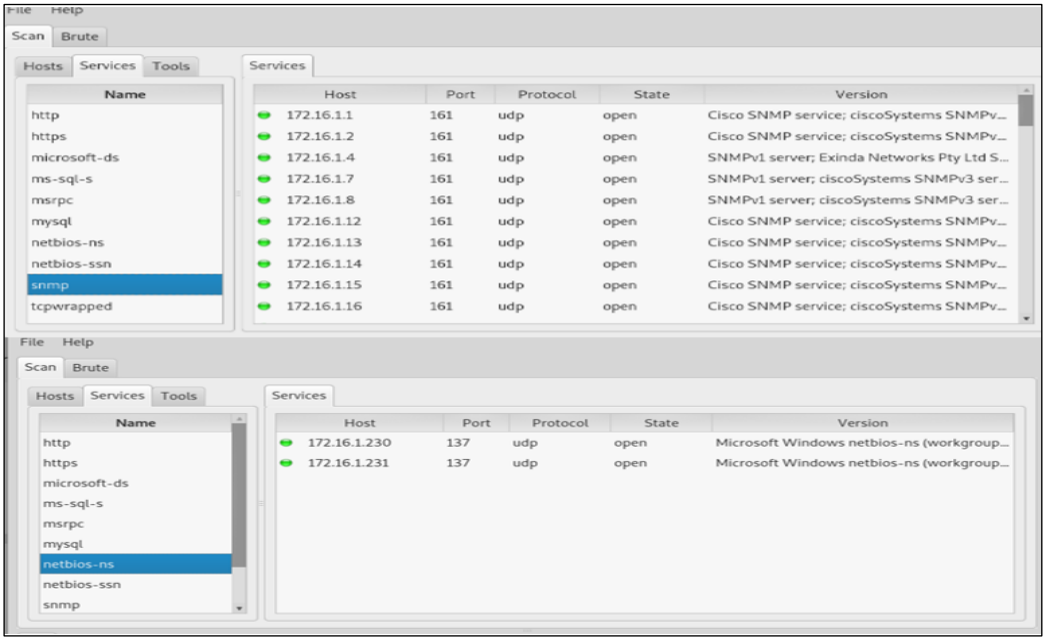


Fig. 34. Servicios que utilizan UDP, herramienta Sparta

Fuente: Elaboración propia

- Solicitar servicios comunes conocidos VPN, incluidos aquellos que utilizan IPSEC e IKE para conexiones desde todas las direcciones, (Pete Herzog, 2010).

En la institución no se hace uso del protocolo de intercambio de claves en internet (IKE) en la red de datos.

- 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.

En la figura 35 se muestran los servicios más comunes dentro de la institución, los servicios que se utilizan frecuentemente el protocolo TCP en la red son: **1.-**http, **2.-**microsoft-ds, **3.-**srpc, **4.-**netbios-ssn, **5.**-mysql, **6.-**ms-sql-s, **7.-**https, **8.-**postgresql, **9.**-tcpwrapped, **10.-**telnet.

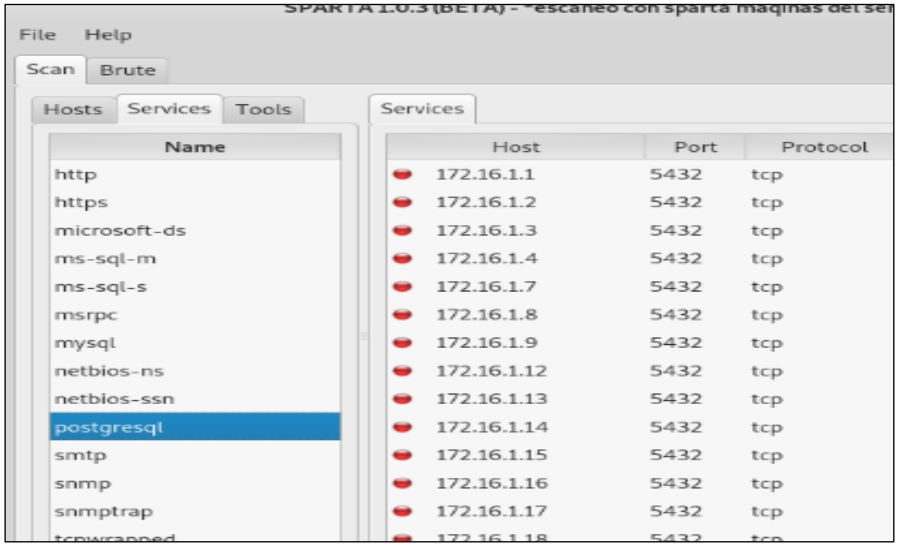


Fig. 35. Servicios que utilizan el protocolo TCP, herramienta Sparta

Fuente: Elaboración propia

- 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)

En la figura 36 se observan puertos abiertos de un servidor y puerto abiertos en la red de la UTN con ayuda de la herramienta Zenmap perteneciente a Nmap.

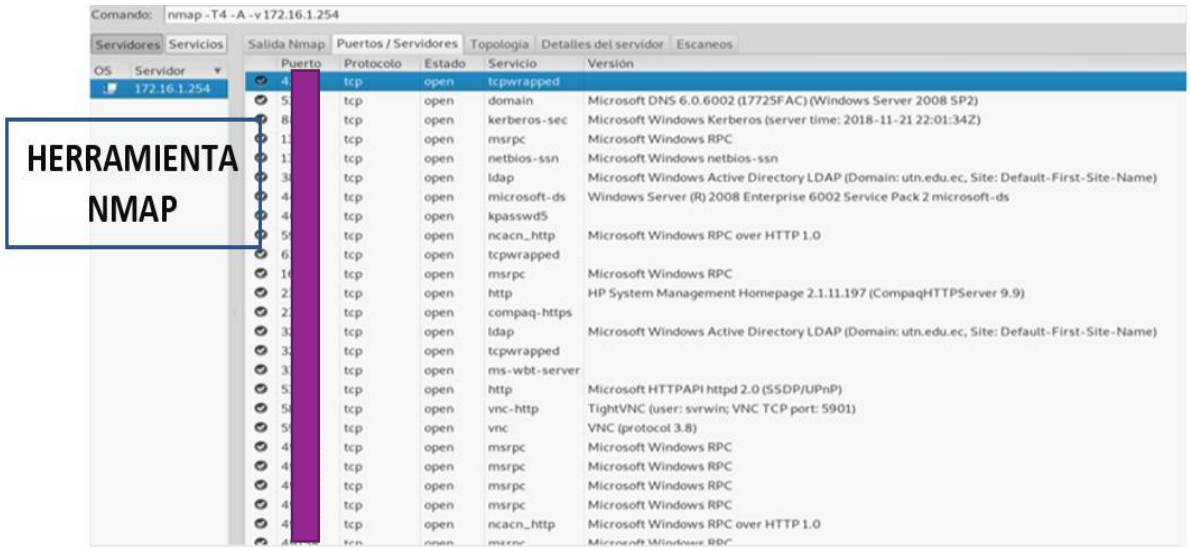


Fig. 36. Protocolos abiertos con herramienta Nmap

Fuente: Elaboración propia

En la tabla 3.58 se detallan los puertos que se encuentran abiertos.

TABLA 0.58 Datos Obtenidos de puertos abiertos, Herramienta Nmap

Número	Puerto	Protocolo	Servicio
1.-	13xx	udp	Microsoft Windows netbios-ns
2.-	16xx	udp	Snmpv1 server, cisco snmp service, snmpv3 server
3.-	8xx	tcp	switch telnetd
4.-	42xx	tcp	tcpwrapped
5.-	53xx	tcp	domain Microsoft DNS windows Server 2008 SP2
6.-	80xx	tcp	http
7.-	88xx	tcp	Microsoft windows kerberos
8.-	13xx	tcp	Microsoft Windows RPC
9.-	13xx	tcp	Microsoft Windows netbios-ssn
10.-	38xx	tcp	Microsoft Windows Active Directory
11.-	44xx	tcp	HP Integrated Lights-Out web interface 1.30
12.-	44xx	tcp	https
13.-	44xx	tcp	Microsoft-ds Microsoft windows server 2003 2008 2012
14.-	46xx	tcp	kpasswd5
15.-	59xx	tcp	Microsoft Windows RPC over HTTP 1.0
16.-	143xx	tcp	Microsoft SQL Server
17.-	168xx	tcp	Microsoft Windows RPC
18.-	230xx	tcp	HP System Management Homepage 2.1.11.197 (CompagHTTPServer 9.9)
19.-	238xx	tcp	compaq-https
20.-	326xx	tcp	Microsoft Windows Active Directory LDAP (Domain: utn.edu.ec)
21.-	326xx	tcp	tcpwrapped
22.-	330xx	tcp	MySQL
23.-	338xx	tcp	ms-w1A-server
24.-	535xx	tcp	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
25.-	580xx	tcp	TightVNC (user: svrwin; VNC TCP port: 5901)
26.-	590xx	tcp	VNC (protocol 3.8)
27.-	491xx	tcp	Microsoft Windows RPC
28.-	491xx	tcp	Microsoft Windows RPC
29.-	491xx	tcp	Microsoft Windows RPC

30.-	491xx	tcp	Microsoft Windows RPC
31.-	491xx	tcp	Microsoft Windows RPC over HTTP 1.0
32.-	491xx	tcp	Microsoft Windows RPC

Fuente: Elaboración propia

Sumando los ítems dentro los literales para el acceso se tiene un valor numérico de $\boldsymbol{P_A}$ **= 44.**

Confianza

Realizar pruebas de confianza entre los 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.

1.- La única manera de acceder a la información y propiedad física de la institución es la autorización y resolución por escrito por parte de las autoridades competentes hacia el DTI en donde se maneja toda la información, el valor numérico de confianza para esta sección es de $\boldsymbol{PT}$=**1**.

3.4.2 CONTROLES

Autenticación

- Enumerar el proceso de autenticación y documentar todos los privilegios descubiertos que se pueden usar para proporcionar acceso.

El proceso de autenticación cuando se hace uso de la red de datos es una **1.-** asignación de dirección DHCP y los privilegios a la información en los servidores de la institución por parte del personal autorizados consiste en **2.-** privilegios de escritura.

- Verificar el método para obtener una autorización adecuada para la autenticación.

Para obtener una adecuada autorización y hacer uso de la red de datos no es necesario obtener credenciales de acceso puesto que existen muchos puntos de acceso gratuito dentro de la institución, en caso de acceder a los servidores de la institución por parte del personal autorizado se requiere **1.-** Identificador y contraseña.

- Verificar el método para ser identificado correctamente y poder contar con la autenticación.

Al existir puntos de acceso gratuitos y asignación DCHP, la identificación de una dirección Ip es desapercibida.

- Verificar la solidez de la autenticación mediante el descifrado de contraseñas y volver a aplicar las contraseñas descubiertas a todos los puntos de acceso que requieren autenticación.

1.- Mediante fuerza bruta con la utilización de la herramienta aircrack-ng como lo muestra la figura 37 en donde se hizo un escaneo de redes inalámbricas y posteriormente capturar paquetes de la red WUTN.Docentes con cifrado WPA2 y luego se usó un diccionario de palabras gratuito en la internet, se descubrió la contraseña para la red mencionada.

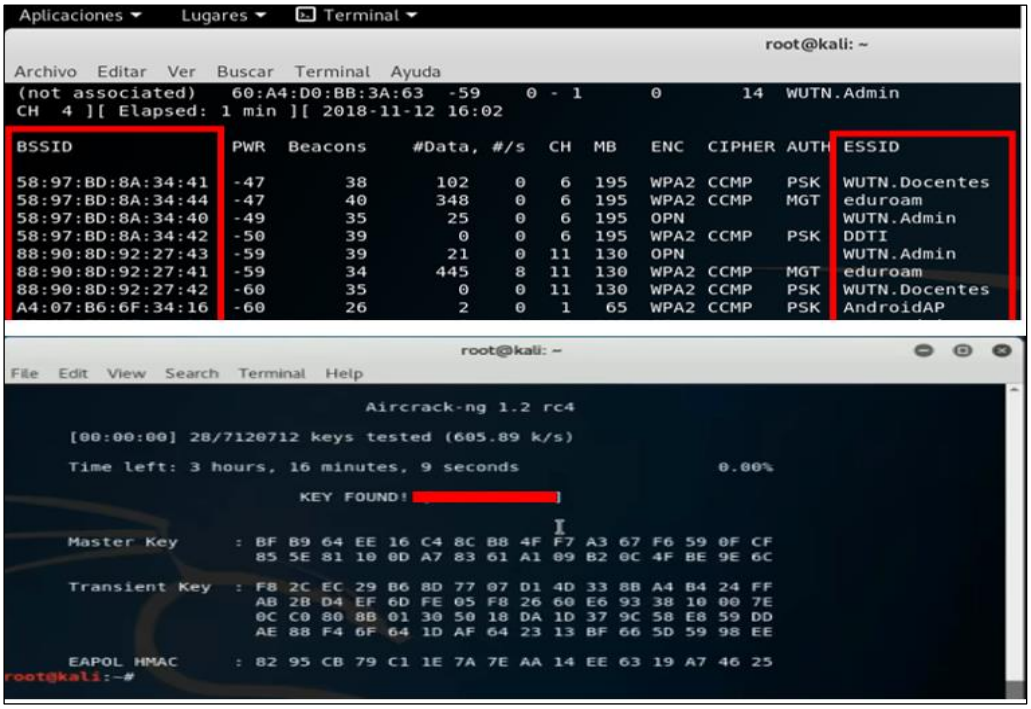


Fig. 37. Descifrando red utilizando la herramienta aircrack-ng

Fuente: Elaboración propia

Contabilizando los ítems en los literales del control de autenticación se tiene un valor numérico de $\boldsymbol{LCAu}$ **= 4.**

Indemnización

- Documentar y 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 usan responsabilidad.

Los objetivos que se encuentran protegidos contra daño o robo son **1.-** equipos informáticos pertenecientes a la institución como son: computadoras, routers, cables, etc.

- Verificar el efecto de las limitaciones de responsabilidad en la seguridad o medidas de seguridad.

1.- Las limitaciones que se presentan es que la información de los servidores se encuentra protegida sólo para personal autorizado, sin embargo, usuarios intenta acceder a ella sin previa autorización.

- Examinar el lenguaje de la póliza de seguro por limitaciones en los tipos de daños o activos.

La póliza de seguros que protegen a los empleados en caso de un incidente con los equipos informáticos es por **1.-** robos o daños no comprobables.

Contabilizando los ítems en los literales del control de indemnización se tiene un valor numérico de $\boldsymbol{LC}_{\mathbf{Id}}$ **= 3.**

Resistencia

- Verificar los puntos únicos de fallo (cuellos de botella) en la infraestructura donde el cambio o el fracaso pueden causar una interrupción del servicio, (Pete Herzog, 2010).

Dentro de la infraestructura de la red el punto que genera cuellos de botella son **1.-** Descontinuidad de actualización en software y **2.-**Descontinuidad de actualización en Hardware.

- Verificar el impacto al acceso del objetivo que causará un fallo del sistema o servicio.

El impacto al acceso de los objetivos que causa un posible fallo al sistema son **1.-** Des continuidad de actualización en software y **2.-** Bajo rendimiento de algunos equipos informáticos debido a que nuevos programas requieren más requisitos de sistema en hardware.

- Verificar los privilegios disponibles del acceso inducido por fallos.

En caso de falla en la red no se limitan los privilegios de acceso.

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

No se hace uso de privilegios de acceso en caso de fallas en la red.

Contabilizando los ítems en los literales del control de indemnización se tiene un valor numérico de $\boldsymbol{LCRe}$ **= 4.**

Subyugación

En una auditoría de redes de datos COMSEC, si un log-in puede hacerse en HTTP, así como en 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. En la tabla 3.59 se muestran los datos obtenidos para la subyugación.

TABLA 0.59 Elaboración de la Subyugación dentro del canal de Red de Datos

Subyugación	
Login en modo no seguro	**Login en modo seguro**
Portafolio de autoridades http://cloud1.utn.edu.ec/ords/f?p=215:LOGIN_DESKTOP::::::	**1.-** Quipux
Portafolio de directores http://cloud1.utn.edu.ec/ords/f?p=187:LOGIN_DESKTOP::::::	
Portafolio de dependencias http://cloud1.utn.edu.ec/ords/f?p=216:LOGIN_DESKTOP::::::	
Portafolio Docentes http://cloud1.utn.edu.ec:9073/ords/f?p=116:LOGIN_DESKTOP::::::	
Portafolio Estudiantes http://cloud1.utn.edu.ec:9071/ords/f?p=109:LOGIN::::::	
Portafolio Administrativos http://cloud1.utn.edu.ec/ords/f?p=108:LOGIN_DESKTOP::::::	
Portafolio resoluciones http://cloud1.utn.edu.ec/ords/f?p=172:LOGIN_DESKTOP::::::	

Fuente: Elaboración propia

Los sistemas que requieren un login de modo seguro en del protocolo HTTPS se encuentra el servicio web del sistema de gestión documental Quipux, por tanto, se tiene un valor numérico para la subyugación de **LC_{Su}=1.**

Continuidad

- Enumerar y probar las insuficiencias de todos los objetivos con respecto a los retrasos de acceso y los tiempos de respuesta del servicio a través de los sistemas de back-up o el cambio a canales alternativos.

En caso de suscitarse problemas o fallas en los servidores de la institución, no existen backups de respaldo para mitigar, cuando existe un problema con los equipos informáticos el **1.-** tiempo en resolverlo es en menos de 7 días.

- Verificar que los esquemas de bloqueo contra intrusos no puedan ser usados contra los usuarios válidos.

Existen cortafuegos implementados en hardware y en software, por tanto **1.-** se bloquea el acceso no autorizado de los usuarios hacia la red de forma automática.

Sumando los ítems marcados dentro del control de continuidad se tiene un valor numérico de $\boldsymbol{LCCt}$ **= 2.**

No repudio

- Enumerar y probar el uso o las deficiencias de los procesos y sistemas para identificar y registrar correctamente el acceso o las interacciones a la propiedad para obtener pruebas específicas que cuestionen el repudio.

- Verifique que todos los métodos de interacción se registren correctamente con la identificación adecuada.

- Identificar los métodos de identificación que derrotan el repudio.

Para identificar el acceso no autorizado hacia la red de la institución de forma lógica se hace uso de **1.-** registro de dirección IP, y para identificar el acceso de forma física no autorizada a los equipos de la red se hace de **2.-** cámaras de video vigilancia y **3.-** sistema de autenticación por el reloj biométrico. Sumando los ítems marcados se obtiene un valor numérico del control no repudio de **LC_{NR} = 3.**

Confidencialidad

- Enumerar todas las interacciones con los servicios dentro del alcance de las comunicaciones o activos transportados a través del canal mediante líneas seguras, cifrado, interacciones "silenciosas" o "cerradas" para proteger la confidencialidad de la propiedad de información entre las partes involucradas.

- Verificar los métodos aceptables utilizados para la confidencialidad.
- Probar la resistencia y el diseño del método de cifrado u ofuscación.

Para proteger la propiedad de la información entre las partes involucradas se hace uso de la **1.-** encriptación de los datos y se hace uso de la **2.-** confidencialidad de la información que se manipula, por tanto, para el control de la confidencialidad se obtiene un valor numérico de **LC_{Cf} = 2.**

Privacidad

- Enumerar los servicios dentro del alcance de las comunicaciones o los activos transportados mediante el uso de firmas específicas e individuales, identificación personal, interacciones personales "silenciosas" o de "habitaciones cerradas" para proteger la privacidad de la interacción y el proceso de proporcionar activos solo a aquellos dentro de la habilitación de seguridad adecuada, para ese proceso, comunicación o activo, (Pete Herzog, 2010). En la 3.60 se muestran los datos obtenidos para este literal.

TABLA 0.60 Elaboración de la Privacidad dentro del canal de Red de Datos

Privacidad	
Sistemas institucionales con identificación de usuario	**1.- Portafolio de autoridades** http://cloud1.utn.edu.ec/ords/f?p=215:LOGIN_DESKTOP::::::
	2.- Portafolio de directores http://cloud1.utn.edu.ec/ords/f?p=187:LOGIN_DESKTOP::::::
	3.- Portafolio de dependencias http://cloud1.utn.edu.ec/ords/f?p=216:LOGIN_DESKTOP::::::
	4.- Portafolio Docentes http://cloud1.utn.edu.ec:9073/ords/f?p=116:LOGIN_DESKTOP::::::
	5.- Portafolio Estudiantes

	http://cloud1.utn.edu.ec:9071/ords/f?p=109:LOGIN::::::
	6.- Portafolio Administrativos
	http://cloud1.utn.edu.ec/ords/f?p=108:LOGIN_DESKTOP::::::
	7.- Portafolio de Resoluciones
	http://cloud1.utn.edu.ec/ords/f?p=172:LOGIN_DESKTOP::::::

Fuente: Elaboración propia

Dentro de los sistemas propios de la institución con requerimiento de identificación personal se encuentran los mostrados en la tabla 3.60.

- Relacionar la información con los puertos TCP y UDP que no responden para determinar si la disponibilidad depende de un tipo de contacto o protocolo privado, (Pete Herzog, 2010). En la figura 38 se muestran los datos obtenidos para este literal.

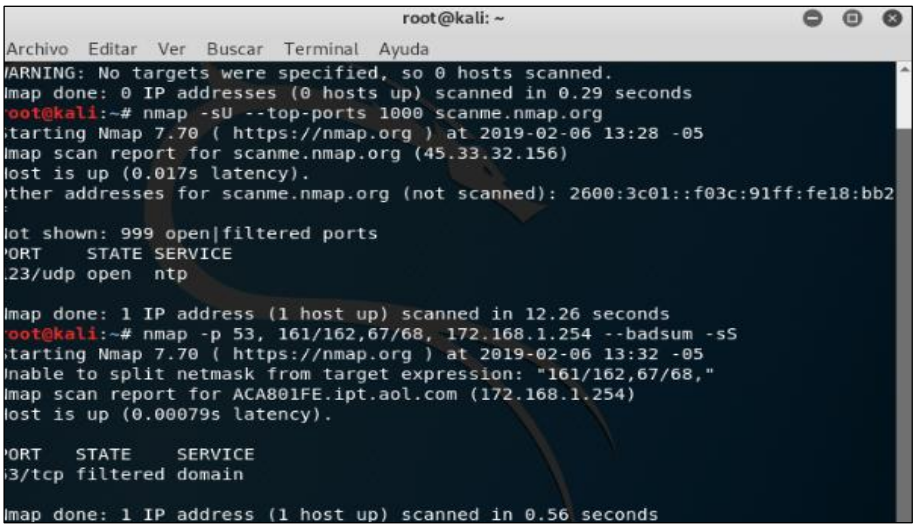


Fig. 38. Descifrando Red utilizando la herramienta aircrack-ng

Fuente: Elaboración propia

En la figura anterior se visualiza que existe puertos TCP y UDP que se encuentran filtrados, el escaneo se hizo mediante la herramienta nmap encontrando: **1.-** puerto filtrado. Sumando los ítems marcados dentro del control de privacidad se tiene un valor numérico de **LC_{Pr}=8.**

Integridad

Enumerar y probar las deficiencias de integridad cuando se utilice un proceso documentado, firmas, cifrado, hash o marcas para asegurar que el activo no pueda ser cambiado, redirigido o invertido sin que las partes involucradas lo conozcan.

En la institución no se manejan un servicio o programa que asegure la integridad de la información y que no sea cambiada o redirigida, por tanto, el valor numérico de este control es de **LC_{It}=0.**

Alarma

Verificar y enumerar la utilización de un sistema de alerta localizado en todo el alcance, registro, o un mensaje para cada Gateway de acceso a través de cada canal donde una situación sospechosa es observada por el personal, en caso de duda de elusión por parte de intrusos, ingeniería social, o una actividad fraudulenta. En la tabla 3.61 se muestran los datos obtenidos para el control de alarma.

TABLA 0.61 Elaboración de la Alarma dentro del canal de Red de Datos

Alarma	
Técnica:	**Encuesta**
Sistema de alerta	**1.-** Firewall en hardware
	2.- Software antivirus
	3.- Firewalls en software

Fuente: Elaboración propia

Para aminorar o detectar una actividad sospechosa existen sistemas de alerta en la red de datos tales como: Software antivirus, Firewalls en software en computadoras de trabajo y firewall en hardware dentro de topología de la red, por tanto, contabilizando los ítems de la tabla 3.61 se obtiene un valor numérico para este control de **LC_{AI} = 3.**

3.4.3 LIMITACIONES

Exposición

Una exposición puede ser una bandera descriptiva y válida sobre un servicio (las banderas de desinformación no son exposiciones) o una respuesta de eco ICMP de un host. En la figura 39 se muestran las respuestas para el protocolo ICMP.

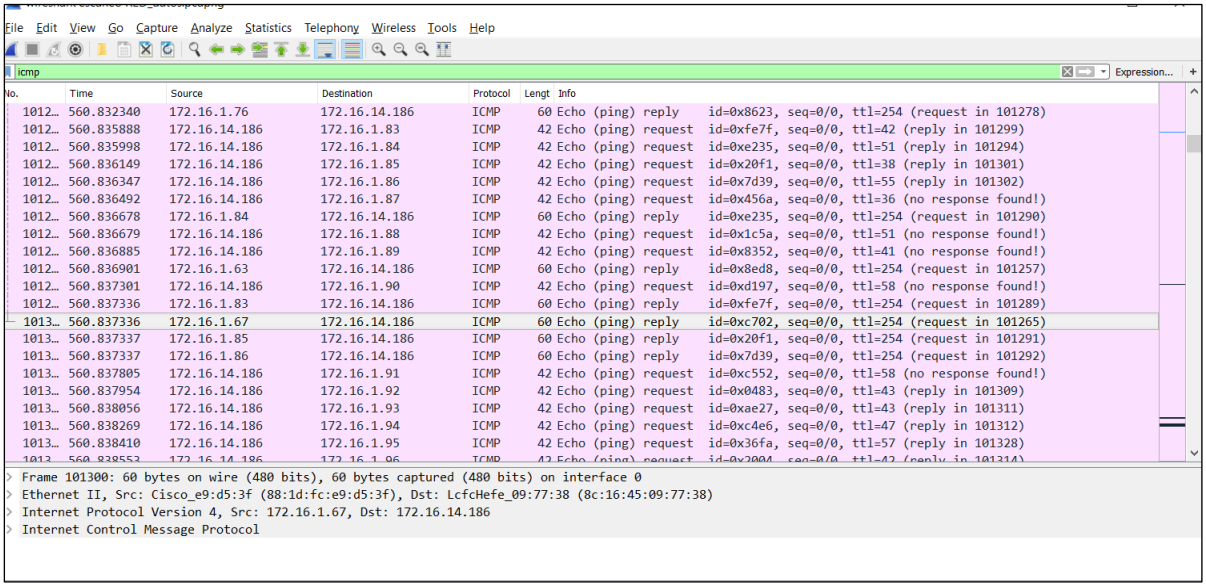


Fig. 39. Respuesta ICMP utilizando la herramienta wireshark

Fuente: Elaboración propia

Capturando paquetes mediante la herramienta wireshark se obtuvo que existen respuestas de eco ICMP de un host dentro de la red de la institución, por tanto, el valor numérico para la exposición es de **LE=1.**

Vulnerabilidad

Una vulnerabilidad puede ser una falla en el software que permite que un atacante sobrescriba el espacio de la memoria para obtener acceso, una falla de cálculo que permite a un atacante bloquear la CPU en un 100%, o un sistema operativo que permite que los datos suficientes sean copiados en el disco hasta que ya no pueda funcionar más.

Para el control de vulnerabilidad no se encontraron fallas debido que los sistemas operativos se encuentran actualizadas a la versión más reciente de Windows, además que cada computadora cuenta con su respectivo antivirus por tanto el valor numérico para la visibilidad es de **Lv=0**.

Debilidad

Una debilidad puede ser un inicio de sesión que permita intentos ilimitados o una granja de servidores web con DNS round-robin para el equilibrio de carga, sin embargo, cada sistema también tiene un nombre único para la vinculación directa, (Pete Herzog, 2010).

En la tabla 3.62 se muestran los datos obtenidos para la debilidad.

TABLA 0.62 Elaboración de la Debilidad dentro del canal Red de Datos

Debilidad	
Técnica:	**Encuesta**
Controles de clase A	**Falla o Error**
Autenticación	**1.-** Puntos de acceso gratuito
Resistencia	**2.-** Des continuidad de actualización en software
	3.- Des continuidad de actualización en hardware

Fuente: Elaboración propia

Se ha encontrado fallas o errores en las medidas de los controles de autenticación debido a que existen puntos acceso a internet gratuito dentro de la institución, en el control de resistencia se encontró fallas debido que no todos los equipos se encuentran actualizados a su misma versión y en las actualizaciones de hardware algunas computadoras no soportan los requerimientos de nuevas herramientas, para los controles de indemnización, subyugación y continuidad no se encontraron errores, por tanto, el valor numérico para la esta limitación y aplicando la ecuación 5 se obtiene:

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

$$Lw = 1 + 0 + 2 + 0 + 0$$

$$Lw = 3$$

Preocupación

Una preocupación puede ser el uso de certificados del servidor web generados localmente para HTTPS o archivos de registro que registran solo a los participantes en las operaciones y no a la fecha y hora correcta del registro de transacción. En la tabla 3.63 se muestran los datos obtenidos para la preocupación.

TABLA 0.63 Elaboración de la Preocupación dentro del de Red de Datos

Preocupación	
Técnica:	**Encuesta**
Controles de clase B	**Falla o Error**
confidencialidad	**1.-** No todo el personal autorizado hace uso de la encriptación de los datos

	2.- No todo el personal hace uso de una correcta confidencialidad de la información	
privacidad	**3.-** Portafolio de autoridades	Registro de manera no seguro
	4.- Portafolio de directores	Registro de manera no segura
	5.- Portafolio de dependencias	Registro de manera no segura
	6.- Portafolio de docentes	Registro de manera no segura
	7.- Portafolio de estudiantes	Registro de manera no segura
	8.- Portafolio de administrativos	Registro de manera no segura
	9.- Portafolio de resoluciones	Registro de manera no segura
Alarma	**10.-** Existen aplicaciones que saltan el control del software antivirus	
	11.- Existen aplicaciones que saltan el control del firewall de software	

Fuente: Elaboración propia

En la tabla 3.63 se hace mención de las fallas encontrados en los controles de clase B, en el control de privacidad se hace uso de acceso con credenciales de manera no segura es decir en http y no en https, en el control de alarma existen aplicaciones que pueden pasar desapercibidas por el firewall y el antivirus en las que la computadora de trabajo puede ser infectada por un virus malicioso. Para el control de no repudio e integridad no se encontraron errores o fallas por tanto, aplicando la ecuación 6 y sumando las deficiencias de los controles de los ítems marcados se obtiene un valor numérico para la preocupación de:

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

$$Lc = 0 + 2 + 7 + 0 + 2$$

$$Lc = 11$$

Anomalía

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

1.- Cuando no se tiene acceso a internet desde una computadora personal se desenchufa el cableado de internet para conectarla a la computadora personal y obtener acceso dentro de la institución.

2.- No todos los puntos de acceso por cable ethernet tienen acceso a internet.

3.- Navegación anónima a través de la red con aplicaciones dedicadas.

Sumando los ítems de la anomalía se tiene un valor numérico de **LA=3.**

3.4.4 Aplicación del RAV

Para la aplicación del RAV se utilizó la hoja de cálculo propia de la metodología, la cual se encuentra disponible en su sitio oficial www.osstmm.com, los valores se consiguieron a través de técnicas de encuestas, Observación y mediante herramientas de Kali Linux. En la tabla 3.64 se detallan los valores obtenidos para la prueba de seguridad de las Redes de Datos.

TABLA 0.64 Datos Obtenidos para el RAV del canal de Redes de Datos

Datos obtenidos para el RAV de las Redes de Datos (COMSEC)		
Ítems		**Valor Total**
Porosidad	Visibilidad	**(PV) = 22**
	Acceso	**(PA) = 44**
	Confianza	**(PT) = 1**
Controles	Autenticación	**(LCAu) = 4**
	Indemnización	**(LCID) = 3**
	Resistencia	**(LCRe) = 4**
	Subyugación	**(LCSu) = 1**
	Continuidad	**(LCCt) = 2**
	No repudio	**(LCNR) = 3**
	Confidencialidad	**(LCCf) = 2**
	Privacidad	**(LCPr) = 8**
	Integridad	**(LCIt) = 0**
	Alarma	**(LCAl) = 3**
Limitaciones	Exposición	**LE = 1**
	Vulnerabilidad	**LV = 0**
	Debilidad	**Lw = 3**
	Preocupación	**Lc = 11**
	Anomalía	**LA = 3**

Fuente: Elaboración propia

Análisis de resultados

La Medida de seguridad de la superficie de ataque para canal de las Redes de Datos se visualiza en la tabla 3.65.

TABLA 0.65 Calculadora RAV de OSSTMM 3, Prueba de Seguridad de las Redes de Datos

RAV Canal de Redes de Datos

OSSTMM versión 3.0

Inserte en los espacios en blanco los valores numéricos para OPSEC, Controles y Limitaciones con los resultados de la prueba de seguridad. Visite OSSTMM 3 (www.osstmm.org) para más información

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

OPSEC

Visibilidad	22
Acceso	44
Confianza	1
Total (Porosidad)	67

CONTROLES

Clase A		Ausentes
Autenticación	4	63
Indemnización	3	64
Resistencia	4	63
Subyugación	1	66
Continuidad	2	65
Total Clase A	14	321

Clase B		Ausentes
No-Repudio	3	64
Confidencialidad	2	65
Privacidad	8	59
Integridad	0	67
Alarma	3	64
Total Clase B	16	319

		Ausentes Verdaderos
Total Controles	30	640
Cobertura Total	4,48%	95,52%

LIMITACIONES

		Valor Numérico	Valor Total
Vulnerabilidad	0	10,552239	0,000000
Debilidad	3	5,791045	17,373134
Preocupación	11	5,761194	63,373134
Exposición	1	1,149922	1,149922
Anomalías	3	0,223212	0,669637
Total # Limitaciones	18		82,5658

OPSEC	14,639344
Controles Verdaderos	6,143292
Controles Completos	6,143292
Cobertura Verdadera A	4,18%
Cobertura Verdadera B	4,78%
Total Cobertura Verdadera	4,48%
Limitaciones	15,341737
Seguridad Δ	-23,84
Protección Verdadera	76,16

OSSTMM
www.osstmm.org
Open Source Security Testing Methodology Manual

Seguridad Actual 76,57 ravs

Fuente: Elaboración propia

Los valores numéricos obtenidos dentro de este canal son rellenados automáticamente en la hoja de cálculo del RAV perteneciente a la metodología, los valores a rellenar son: valor total de OpSec, valor ausente y valor total del control de clase A y B, valores ausentes y total de Limitaciones, el RAV básicamente resta la porosidad y las limitaciones de los controles como lo indica la ecuación 1. Se resalta el valor numérico de la seguridad Δ enmarcado de color rojo lo que significa una carencia o insuficiencia de 23,84 de los controles adoptados, la cual indica que la red de datos se encuentra parcialmente expuesta a posibles ataques informáticos.

R A V = CONTROLES VERDADEROS – POROSIDAD – LIMITACIONES

RAV = 6,1432 – 14,6393 – 15,3417

RAV = - 23,84

CAPÍTULO 4

Resultados

Después de haber realizado las pruebas de seguridad en cada uno de los canales a continuación se describen las debilidades y vulnerabilidades más importantes encontradas:

4.1 Canal humano

- En el DDTI se permite el ingreso de personal de otros departamentos u áreas no relacionadas con el entorno laboral, asimismo se permite el ingreso de personas que no ejercen actividad laboral dentro del departamento, como se detalla en la tabla 3.2. Para salvaguardar la información se debe crear un plan de capacitación continua al personal de la UTN en temas de seguridad de la información.
- Se comparte información del trabajo por cuentas de correo electrónico personal, además que el personal del DDTI asegura haber recibido información de dudosa procedencia por correo institucional.
- Mediante la herramienta de recopilación de datos maltego de Kali Linux como se muestra en la figura 24, se hizo seguimiento a un correo institucional de un trabajador y se evidenció información personal como sus redes sociales, imágenes, ubicación y números de teléfonos, es decir, la actividad que realiza en el internet.
- El registro de acceso es visible en áreas como laboratorios de computación de la UTN debido a que el registro se realiza en hojas físicas (anexo A) y quienes hacen usos de los equipos no se registran lo que lleva a problemas relacionados con hurtos o daños a los equipos.
- Existe manipulación total de computadoras de trabajo del personal de la UTN por parte de practicantes, esto puede ocasionar perdida de información confidencial.
- A diferencia de los trabajadores de la UTN los estudiantes de la institución aseguran que la información de la UTN no se encuentra totalmente segura (anexo A).

4.2 Canal físico

- Se pueden eludir las paredes y mallas alrededor de la UTN, igualmente se hace uso de puertas y ventanas de cristal sin protección dentro de la UTN en las que se pueden quebrantar (anexo B). Esto puede generar sustracciones, atracos, atentados, daños a los activos y al personal dentro de la institución.
- Los activos de los laboratorios de computación de las facultades se encuentran expuestas al público en general lo que puede ocasionar daños o hurtos a los equipos.

4.3 Red inalámbrica

- Actualmente, no se hace uso de algún sistema de control de acceso para los usuarios que ingresan a las redes inalámbricas de la UTN, pero si se hace uso de un método de autenticación, el cual consiste en una contraseña para las redes WUTN.Docentes y usuario y contraseña para eduroam como se detalla en la tabla 3.44.
- Existen 132 puntos de acceso en el campus universitario (anexo C); los que se encuentran encendidos las 24 horas durante todo el año, en los AP no se hace uso de ningún equipo para amortiguar la señal inalámbrica y evitar que esta salga del perímetro interno de la UTN, además estos cuentan con una configuración estándar, todo esto hace que se encuentren expuestos a posibles ataques informáticos.
- El SSID de la red inalámbrica WUTN.Admin y el SSID y contraseña de la red inalámbrica WUTN.Docentes no han sido cambiados desde hace varios meses esto representa problemas debido a que trabajadores o estudiantes que ya no tiene relación alguna con la institución aún puede acceder a dichas redes sin ninguna restricción desde su celular o computadora ocasionando tráfico en la red y posibles ataques informáticos.
- Con la suite aircrack-ng de Kali Linux y por búsqueda de fuerza bruta se descubrió contraseñas de las redes inalámbricas como se visualiza en la figura 37.

4.4 Redes de datos

- En caso de presentarse algún fallo en la red, no se limitan los privilegios de acceso y en caso de suscitarse un problema de configuración en la red el tiempo que tarda el personal encargado en resolverlo es en menos de 7 días.
- Si bien los equipos informáticos se encuentran actualizados en software protegiendo la seguridad, algunos equipos se encuentran obsoletos físicamente como los switch de Core de la facultada FICA que aún tienen interfaces de red Fast Ethernet ya que actualmente se maneja fibra óptica dentro de la UTN.
- No se limita el acceso a usuarios y personal autorizado cuando se accede de forma lógica a los servidores de la UTN, es decir que no existe un sistema de control de acceso hacia estos.
- Utilizando la herramienta nmap de Kali Linux se descubrió varios puertos tcp y udp en estado abierto en computadoras de trabajo y servidores de la UTN como se detalla en la tabla 3.58, esto provocaría una infiltración de un hacker a la red por medio de un puerto obteniendo un control total de una computadora o los mismos servidores.
- Existen puntos de acceso por cable ethernet gratuitos dentro de la institución y se maneja asignación de direcciones ip en DHCP (anexo D), y no se hace uso de algún

tipo de sistema de detección de intrusos en la red de datos, por tanto conlleva a un anonimato total de un equipo cuando este se conecte en la red de datos.

- Existe des continuidad de actualización en software y des continuidad de actualización en hardware, esto provoca demora de respuestas a los servicios de la intranet e internet.
- Se hace uso de control de acceso en páginas web pertenecientes a la UTN con login en modo no seguro es decir http como se muestra en la tabla 3.60, estas son: portafolio de autoridades, portafolio de directores, portafolio de dependencias, Portafolio de docentes, portafolio de estudiantes, portafolio de administrativos y portafolio de resoluciones, en la cual por medio de wireshark de Kali Linux se puede capturar los paquetes de datos de manera más eficaz y obtener las credenciales de acceso.

En la tabla 4.1 muestra los valores de evaluación de riesgo encontrados en cada canal sugerido por la metodología OSSTMM v3.

TABLA 4.1 Valores de evaluación de riesgo de los Canales Aplicados.

Nombre Canal	**Valores de Evaluación de Riesgo (RAV)**	
Descripción	**Situación Actual**	**Riesgo**
Canal Humano	78,76	21,40
Canal Físico	80,45	19,59
Canal Inalámbrico	84,55	15,38
Canal de Redes de Datos	76,57	23,84

Fuente: Elaboración propia

Los valores numéricos de la tabla 4.1 se obtuvieron aplicando la metodología OSSTMM v3, donde; la columna de situación actual indica el nivel de seguridad encontrado y la columna de riesgo indica el nivel de insuficiencia o la falta de controles por cada canal.

La medición de riesgo se realizó a través de la escala de Likert, la misma que tiene representación numérica de acuerdo con el estado encontrado en el estudio; tal como se muestra en la tabla 4.2.

TABLA 4.2 Representación numérica.

Nivel	Nivel de Riesgo (puntos)	Color
1	1 - 20	Muy Bajo
2	21 - 40	Bajo
3	41 - 60	Medio
4	61 - 80	Alto
5	81 - 100	Muy Alto

Fuente: Elaboración propia

De la tabla 4.2 se identifica una escala de cinco niveles con un rango de 20 puntos cada una dando un total de 100 puntos; donde el nivel 1 corresponde a un riesgo de seguridad muy bajo, el nivel 2 corresponde a un riesgo de seguridad bajo, el nivel 3 corresponde a un riesgo de seguridad medio, el nivel 4 corresponde a un riesgo de seguridad alto y el nivel 5 corresponde a un riesgo de seguridad muy alto.

Con los valores de la tabla 4.1 y la tabla 4.2 se realizó la medición de riesgo actual; como lo muestra la tabla 4.3.

TABLA 4.3 Escala Likert, Medición de Riesgo de los Canales Aplicados.

Nombre Canal	Nivel de Riesgo				
Descripción	**Muy Alto**	**Alto**	**Medio**	**Bajo**	**Muy Bajo**
Canal Humano				21,40	
Canal Físico					19,59
Canal Inalámbrico					15,38
Canal de Redes de Datos				23,84	

Fuente: Elaboración propia

En la tabla 4.2 se visualiza el nivel de riesgo y el valor total de insuficiencias de controles encontradas en los canales; se consideraron dos valores cuantitativos para el nivel de riesgo; siendo un valor de 100 a un riesgo muy alto y 0 a un riesgo muy bajo, por tanto se obtiene que el canal humano y canal de redes de datos se encuentran en un nivel de riesgo por encima del 20 puntos, si bien el riesgo es bajo se debe aplicar medidas de corrección debido a que por cada canal se maneja información delicada y confidencial. A diferencia del canal físico y canal inalámbrico con un nivel de riesgo muy bajo por lo que podemos deducir un nivel aceptable de seguridad.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- La metodología OSSTMM en su versión 3 con su uso en canales permite que las pruebas obtenidas sean beneficiosas tanto para el analista como para la organización ya que permite conocer datos más cercanos a la realidad de la infraestructura fisca y estructura lógica de la red, localizando un número mayor de vulnerabilidades para luego emplear métodos de corrección y prevención en el canal que lo requiera.
- La seguridad informática se encarga de asegurar la integridad, disponibilidad y privacidad de la información dentro de una organización.
- Mas allá de la seguridad que requiere la infraestructura de la red, el personal y estudiantes son el activo más valioso de la UTN, así mismo es la brecha más peligrosa en seguridad, se debe emplear más tiempo en formación y capacitación como prioridad antes de emplear seguridad en infraestructura.
- Después de haber realizado el análisis en los diferentes canales de la metodología con el uso de herramientas de Kali Linux se puede verificar que ninguna aplicación web o red es totalmente segura y libre de ataques.
- Kali Linux es un sistema operativo completo y robusto en pruebas de penetración y auditoría de seguridad. Dentro de este estudio utilizando Kali Linux con la metodología OSSTMM v3 se comprobó debilidades y vulnerabilidades que posee la infraestructura de la red.

Recomendaciones

- Se recomienda monitorear constantemente la red en busca de actividad anormal y sospechosa e implementar nuevas medidas para contrarrestar posibles ataques informáticos en la red y evitando altos costes en reparación de daños.
- La seguridad informática se tiene que considerar como una norma muy importante y de manejo delicado dentro de una organización o institución por lo que no debe aislarse de los demás procesos que se manejan en ella.
- Implementar sistemas de control de acceso o sistema de detección de nuevos usuarios que intentan acceder a la red de la institución.
- Se debe poner énfasis por el personal encargado de la infraestructura de la red en los servicios y puertos que no están en uso principalmente el de los servidores debido a

que un tercero los usaría como una ventana abierta y permitiría adueñarse de información delicada.

- Utilizar el sistema operativo Kali Linux como medida de precaución y prevención a ataques informáticos; debido a que es un sistema gratuito y robusto en temas de seguridad informática.

Referencias

Aguilera, P. (2011). *Redes seguras (Seguridad informática)*. Editex.

Agustín López López. (2011). estudio de metodologías para pruebas de penetración a sistemas informáticos.

Alamanni, M. (2015). *Kali Linux Wireless Penetration Testing Essentials*. Packt Publishing. Recuperado de https://books.google.com.ec/books?id=CrVJCgAAQBAJ

Aldo Valdez Alvarado. (2013). articulo caso de estudio OSSTMMv3. Recuperado de http://www.revistasbolivianas.org.bo/pdf/rits/n8/n8a13.pdf

Álvarez Marañón, G., & Pérez García, P. P. (2004). *Seguridad informática para empresas y particulares*. Madrid, SPAIN: McGraw-Hill España. Recuperado de http://ebookcentral.proquest.com/lib/utnortesp/detail.action?docID=3195263

Antonio Quina. (2015). SPARTA - Herramienta de prueba de penetración de infraestructura de red. Recuperado 9 de febrero de 2019, de http://sparta.secforce.com/

Arturo, B. G. G. (2015). Seguridad En Redes: CAPITULO 4. Recuperado 21 de abril de 2018, de http://redsecurityunad.blogspot.com/2015/05/capitulo-3-criptografia-leccion-11.html

Baca Urbina, G. (2016). *Introducción a la seguridad informática*. Distrito Federal, UNKNOWN: Grupo Editorial Patria. Recuperado de http://ebookcentral.proquest.com/lib/utnortesp/detail.action?docID=4849850

Barceló Ordinas, J. M., Íñigo Griera, J., & Llorente Viejo, S. (2008). *Protocolos y aplicaciones Internet*. Barcelona, SPAIN: Editorial UOC. Recuperado de http://ebookcentral.proquest.com/lib/utnortesp/detail.action?docID=3206994

Bigelow, S. J. (2003). *Localización de averías, reparación, mantenimiento y optimización de redes*. México, D.F., MEXICO: McGraw-Hill Interamericana. Recuperado de http://ebookcentral.proquest.com/lib/utnortesp/detail.action?docID=3194217

Bracho, C. L., & Cuzme, F. G. (2017). Auditoría de seguridad informática siguiendo la metodología OSSTMMv3: caso de estudio., 8.

Bracho, D., & Rincón, C. (2010). Modelo para la cuantificación del riesgo telemático en una organización, 81.

Calle, B., Elizabeth, S., Lascano, G., & Jeanett, E. (2010). Auditoría informática de la seguridad de la red física y lógica para el departamento de gestión informática y sistemas de la dirección provincial de salud de Pichincha (DPSP), 197.

Carmona Romera, G. (2011). *Sistema operativo, búsqueda de información: Internet/Intranet y correo-e (UF0319)*. Málaga, SPAIN: IC Editorial. Recuperado de http://ebookcentral.proquest.com/lib/utnortesp/detail.action?docID=3212107

CARPENTIER, J.-F. (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas*. Ediciones ENI.

Cerra Mariel. (2010). *200 respuestas de seguridad* (1a ed). USERSHOP. Recuperado de https://books.google.com.ec/books?id=WHCUYnQ2hz0C

Chicano Tejada, E. (2014). *Auditoría de seguridad informática (MF0487_3)*. Madrid, UNKNOWN: IC Editorial. Recuperado de http://ebookcentral.proquest.com/lib/utnortesp/detail.action?docID=4184005

Colobran Huguet, M., Arqués Soldevilla, J. M., & Marco Galindo, E. (2008). *Administración de sistemas operativos en red*. Barcelona, SPAIN: Editorial UOC. Recuperado de http://ebookcentral.proquest.com/lib/utnortesp/detail.action?docID=3206493

Costas Santos, J. (2014). *Seguridad y alta disponibilidad*. Madrid, SPAIN: RA-MA Editorial. Recuperado de http://ebookcentral.proquest.com/lib/utnortesp/detail.action?docID=3228975

Cristian Borghello. (2017, agosto 21). Estándar y guía de ejecución de Pentesting v1.0. Recuperado 20 de abril de 2018, de http://blog.segu-info.com.ar/2017/08/estandar-y-guia-de-ejecucion-de.html

Darín, J. R., & Academy, I. T. C. (2016). *Fundamentos de Redes Informáticas: 2ª Edición* (2da edición). CreateSpace Independent Publishing Platform. Recuperado de https://books.google.com.ec/books?id=gGTkDAAAQBAJ

Derrien, Y. (2009). *Técnicas de la auditoría informática*. Barcelona, SPAIN: Marcombo. Recuperado de http://ebookcentral.proquest.com/lib/utnortesp/detail.action?docID=3176647

Díaz Orueta, G., Alzórriz Armendáriz, I., & Sancristóbal Ruiz, E. (2014). *Procesos y herramientas para la seguridad de redes*. Madrid, SPAIN: UNED - Universidad Nacional de Educación a Distancia. Recuperado de http://ebookcentral.proquest.com/lib/utnortesp/detail.action?docID=3220062

Dirección General de Modernización Administrativa. (2012). Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método, 127.

DORDOIGNE, J. (2015). *Redes informáticas - Nociones fundamentales (5ª edición): (Protocolos, Arquitecturas, Redes inalámbricas, Virtualización, Seguridad, IP v6 ...)* (5ta edición). ENI. Recuperado de https://books.google.com.ec/books?id=Huwy1L0PEq8C

Freitas, V. D. (2009). Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar, 55.

Gerald Combs. (2018). Wireshark · Go Deep. Recuperado 2 de octubre de 2018, de https://www.wireshark.org/

Giménez Albacete, J. F. (2014). *Seguridad en equipos informáticos (MF0486_3)*. Madrid, UNKNOWN: IC Editorial. Recuperado de http://ebookcentral.proquest.com/lib/utnortesp/detail.action?docID=4184155

Gómez Beas, D. (2014). *Resolución de incidencias en redes telemáticas (UF1881)*. Madrid, SPAIN: IC Editorial. Recuperado de http://ebookcentral.proquest.com/lib/utnortesp/detail.action?docID=4310548

Gómez Vieites, Á. (2014). *Seguridad en equipos informáticos*. Madrid, SPAIN: RA-MA Editorial. Recuperado de http://ebookcentral.proquest.com/lib/utnortesp/detail.action?docID=3229330

González, A. C. (2003, noviembre 28). Administración de riesgos en tecnología informática - GestioPolis. Recuperado 24 de abril de 2018, de https://www.gestiopolis.com/administracion-de-riesgos-en-tecnologia-informatica/

Gutiérrez de Mesa, J. A., & Pagés Arévalo, C. (2008). *Planificación y gestión de proyectos informáticos*. Alcalá de Henares, SPAIN: Servicio de Publicaciones. Universidad de Alcalá. Recuperado de http://ebookcentral.proquest.com/lib/utnortesp/detail.action?docID=3176931

Héctor Jara y Federico G. Pacheco. (2012). *Ethical Hacking* (1ra edición). Buenos Aires: USERSHOP.

Henry Raúl González Brito. (2017, mayo 10). Metodología de Pruebas de Intrusión en la NIST SP 800-115. Recuperado 20 de abril de 2018, de https://henryraul.wordpress.com/2017/05/10/metodologia-de-pruebas-de-intrusion-en-la-nist-sp-800-115/

Heredero, C. de P., Agius, J. J. L. H., Romero, S. M. R., & Salgado, S. M. (2012). *Organización y transformación de los sistemas de información en la empresa*. ESIC Editorial.

Hertzog, R., & Mas, R. (2016). *El manual del Administrador de Debian*. Lulu.com.

Hurley, C., Rogers, R., Thornton, F., & Baker, B. (2007). *WarDriving and Wireless Penetration Testing*. Syngress.

ISECOM. (2015). ISECOM - Open Source Security Testing Methodology Manual (OSSTMM). Recuperado 25 de abril de 2018, de http://www.isecom.org/research/

Jalca, J. J. R., Castro, V. F. R., Menéndez, M. D. J. A., Quimiz, L. R. M., Anzúles, G. R. P., Pilay, Y. H. C., & Pin, Á. L. P. (2018). *REDES DE COMPUTADORAS*. 3Ciencias.

Jhon Diaz Moreno. (2013). Seguridad de la Información y Metodologías de Análisis de Riesgo: Analisis de Riesgos. Recuperado 25 de abril de 2018, de http://metodologiasderiesgo.blogspot.com/2014/12/analisis-de-riesgos.html

Jorge Domínguez Chávez. (2015). Figura 4: Proceso Octave y sus fases en la seguridad informática. Recuperado 25 de abril de 2018, de https://www.researchgate.net/figure/Figura-4-Proceso-Octave-y-sus-fases-en-la-seguridad-informatica_fig1_286371326

Kapczyński, A., Tkacz, E., & Rostanski, M. (2012). *Internet - Technical Developments and Applications 2*. Springer Science & Business Media.

Lago, K. R. (2017, diciembre 12). Metodologías para la auditoria de la seguridad. Recuperado 19 de abril de 2018, de https://www.linkedin.com/pulse/metodolog%C3%ADas-para-la-auditoria-de-seguridad-kevin-rodriguez-lago

López, P. A. (2011). *Introducción a la seguridad informática (Seguridad informática)*. Editex.

MARIA DEL PILAR ALEGRE RAMOS, & HURTADO, A. G.-C. (2011). *SEGURIDAD INFORMATICA ED.11 Paraninfo*. Editorial Paraninfo.

McClure, S., Scambray, J., & Kurtz, G. (2010). *Hackers 6: secretos y soluciones de seguridad en redes*. México, D.F., MEXICO: McGraw-Hill Interamericana. Recuperado de http://ebookcentral.proquest.com/lib/utnortesp/detail.action?docID=3191899

MediaWiki. (2011, febrero 22). The Penetration Testing Execution Standard. Recuperado 19 de abril de 2018, de http://www.pentest-standard.org/index.php/Main_Page

Medina, J. (2015). *Evaluación de Vulnerabilidades TIC*. SG6 CB.

Mike Kershaw. (s. f.). Kismet Wireless. Recuperado 22 de octubre de 2018, de https://www.kismetwireless.net/

MIRANDA, C. V. (2005). *Sistemas informáticos y redes locales* (1ra edición). España: Ediciones Paraninfo, S.A. Recuperado de https://books.google.com.ec/books?id=jWvPAgAAQBAJ

Molina Robles, F. J., & Polo Ortega, E. (2014). *Servicios en red*. Madrid, SPAIN: RA-MA Editorial. Recuperado de http://ebookcentral.proquest.com/lib/utnortesp/detail.action?docID=3229687

Moreno Pérez, J. C., & Santos González, M. (2014). *Sistemas informáticos y redes locales*. Madrid, SPAIN: RA-MA Editorial. Recuperado de http://ebookcentral.proquest.com/lib/utnortesp/detail.action?docID=3229362

Nmap: the Network Mapper - Free Security Scanner. (s. f.). Recuperado 20 de septiembre de 2018, de https://nmap.org/

offensive security. (2018). Our Most Advanced Penetration Testing Distribution, Ever. Recuperado 26 de mayo de 2018, de https://www.kali.org/

Orloff, J. T. (2009). *Ubuntu Linux: paso a paso*. México, D.F., MEXICO: McGraw-Hill Interamericana. Recuperado de http://ebookcentral.proquest.com/lib/utnortesp/detail.action?docID=3191879

Ortega, B., & Leonel, C. (2017). Auditoría de seguridad informática dirigida al gobierno autónomo descentralizado del cantón Mira basado en el estándar cobitv5, siguiendo la metodología osstmmv3. Recuperado de http://repositorio.utn.edu.ec/handle/123456789/6878

RAMOS, M. D. P. A., & HURTADO, A. G.-C. (2011). *SEGURIDAD INFORMATICA ED.11 Paraninfo*. Editorial Paraninfo.

RAULT, R., SCHALKWIJK, L., ACISSI, AGÉ, M., CROCFER, N., CROCFER, R., … LASSON, S. (2015). *Seguridad informática - Hacking Ético: Conocer el ataque para una mejor defensa (3ª edición)*. Ediciones ENI.

Legislación legal UTN. (2012). Código de ética UTN. (pág. 10). Ibarra: UTN.

Legislación legal UTN. (2012). Reglamento Custodio de Bienes . (pág. 7). Ibarra: UTN.

Legislación legal UTN. (2012). Reglamento Infracciones Sanciones. (pág. 5). Ibarra: UTN.

LOTAIP. (2004). LEY ORGANICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN. (pág. 13). Quito: LOTAIP.

Roa Buendía, J. F. (2013). *Seguridad informática*. Madrid, SPAIN: McGraw-Hill España. Recuperado de http://ebookcentral.proquest.com/lib/utnortesp/detail.action?docID=3211239

Roman, O. (2017, febrero 28). Auditoria de Seguridad, Auditoria de Vulnerabilidades, Pentest o Hacking Etcio. Recuperado 26 de abril de 2018, de https://medium.com/@ingoroman/auditoria-de-seguridad-auditoria-de-vulnerabilidades-pentest-o-hacking-etcio-c45f0186f908

Romero, C. (2010). *Servicios en Red*. Editorial Paraninfo.

Santoyo, R. L. (2015). TRABAJO FIN DE GRADO, 61.

Sanz Mercado, P. (2008). *Seguridad en linux: guía práctica*. Madrid, SPAIN: Editorial Universidad Autónoma de Madrid. Recuperado de http://ebookcentral.proquest.com/lib/utnortesp/detail.action?docID=3218549

Scambray, J., & McClure, S. (2009). *Hackers en Windows: secretos y soluciones de seguridad en Windows (3a Ed.)*. México, D.F., MEXICO: McGraw-Hill Interamericana. Recuperado de http://ebookcentral.proquest.com/lib/utnortesp/detail.action?docID=3191943

Shah, S., & Soyinka, W. (2007). *Manual de administración de Linux*. México, D.F., MEXICO: McGraw-Hill Interamericana. Recuperado de http://ebookcentral.proquest.com/lib/utnortesp/detail.action?docID=3191942

Simpson, M. T. (2012). *Hands-On Ethical Hacking and Network Defense*. Cengage Learning.

Solé Almagro, D. (2015). *Administración y auditoría de los servicios de mensajería electrónica (UF1274)*. Madrid, SPAIN: IC Editorial. Recuperado de http://ebookcentral.proquest.com/lib/utnortesp/detail.action?docID=4310534

Thomas Otreppe. (s. f.). Aircrack-ng. Recuperado 22 de octubre de 2018, de https://www.aircrack-ng.org/

Touhill, G. J., & Touhill, C. J. (2014). *Cybersecurity for Executives: A Practical Guide*. Wiley.

Vieites, Á. G. (2014). *Enciclopedia de la Seguridad Informática. 2ª edición* (2da edisión). Madrid, SPAIN: Grupo Editorial RA-MA. Recuperado de https://books.google.com.ec/books?id=Bq8-DwAAQBAJ

Walker, M. (2016). *CEH Certified Ethical Hacker All-in-One Exam Guide, Third Edition*. McGraw Hill Professional.

Pete Herzog. (2010). *Manual de la Metodología Abierta de Testeo de Seguridad.* USA, New York: ISECOM.

ANEXOS

En la siguiente tabla se muestra el tiempo aproximado de duración de las pruebas en cada tarea o ítem especifico por canal de acuerdo con la metodología OSSTMM en su versión 3.

Nro.	Nombre de tarea	Duración	MES 1				MES 2				MES 2			
	Tema: APLICACIÓN DE LA METODOLOGIA OSSTMM PARA LA SEGURIDAD DE LA RED INALÁMBRICA DE LA UNIVERSIDAD TÉCNICA DEL NORTE MEDIANTE HERRAMIENTAS DE KALI LINUX.	**días**												
1	APLICACIÓN METODOLOGÍA OSSTMM	73 días												
2	1. Canal humano	15 días												
3	1.1 Porosidad	3 días												
4	1.2 Controles	9 días												
5	1.3 Limitaciones	3 días												
6	2. Canal Físico	15 días												
7	2.1 Porosidad	3 días												
8	2.2 Controles	9 días												
9	2.3 Limitaciones	2 días												
10	3. Canal Inalámbrico	21 días												
11	3.1 Porosidad	4 días												
12	3.2 Controles	12 días												
13	3.3 Limitaciones	5 días												
14	4. Canal de Redes de Datos	22 días												
15	4.1 Porosidad	4 días												
16	4.2 Controles	14 días												
17	4.3 Limitaciones	4 días												

Fuente: Elaboración propia

Anexo A. Pruebas de Seguridad Humana (HUMSEC)

Encuestas

Personal del Departamento de Desarrollo Tecnológico e Informático (DTI), y responsables de los laboratorios de las Facultades: FICA, FECYT, FACAE, FICAYA, FCCSS.

1.- ¿Usted comparte las contraseñas de acceso de su computadora de trabajo y aplicaciones con otras personas?

2.- ¿Alguna vez ha notado que la información de su computadora de trabajo ha sido total o parcialmente modificada?

3.- Cuando comparte información institucional, ¿está totalmente segura/o de que la información la recibió la persona a la que iba dirigida?

4.- ¿Cree usted que la información de la UTN se encuentra totalmente segura?

5.- ¿Hace uso de los términos "cifrado de datos", “encriptación” en la información que manipula?

6.- ¿Comparte información de su trabajo por una cuenta de correo electrónico personal como Hotmail, Gmail, u otros?

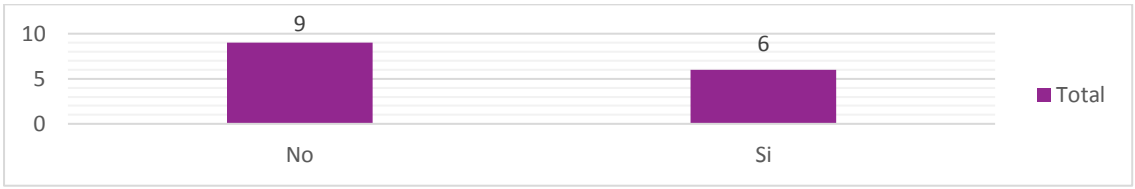
7.- ¿Conoce si su computadora de trabajo puede ser manipulado de manera remota?

8.- ¿Cree que los activos transportados por el personal de la UTN es un método confiable?

9.- ¿Su computadora de trabajo alguna vez ha sido utilizada por otra persona?

10.- ¿Existen tipos de autenticación obligatorios a las áreas restringidas de la UTN?

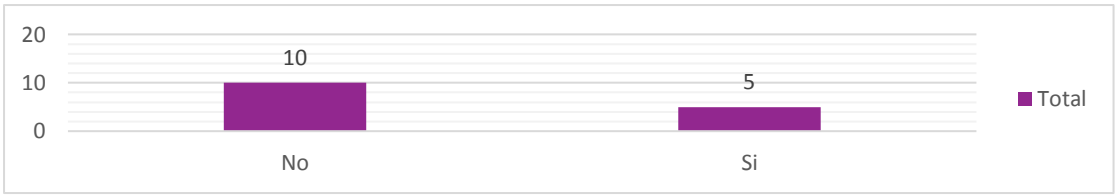
11.- ¿Alguna vez se le ha perdido algún dispositivo de almacenamiento con información de su trabajo?



12.- ¿A compartido información personal e institucional a personas de otros departamentos vía telefónica?

13.- ¿Para interactuar con el personal de recepción se necesita registro o autenticación?

14.- ¿Para interactuar con el personal de recepción se necesita tener permiso de la autoridad respectiva?



15.- ¿Existen políticas a seguir en caso de que otra persona utilice su computadora de trabajo?

16.- ¿La ausencia del Personal de apoyo se relaciona con permisos u obligaciones de la institución?

17.- ¿La ausencia del Personal de apoyo causa inconvenientes laborales?

18.- ¿El registro de acceso se encuentra expuesto a la vista de las personas?

19.- ¿Los activos informáticos de la UTN cuando son transportados hacen uso de firmas y sellos eficientes?

20.- ¿Las comunicaciones verbales que se realizan entre el personal son confiables y autorizadas?

21.- ¿La información que le llega al correo institucional provienen de correos confiables?

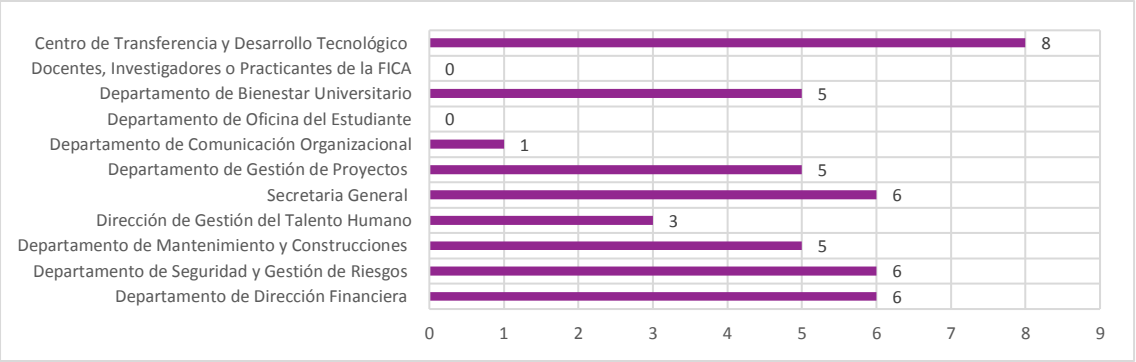
22.- ¿Alguna vez a recibido información de dudosa procedencia?

23.- ¿Hace uso de un software especial de alarma para la detección de información no confiable?

24.- ¿Usa su computador personal institucional fuera de su puesto de trabajo?

25.- Que áreas están autorizadas a acceder sin autenticación hacia el Departamento de Desarrollo Tecnológico e Informático (DTI).

La pregunta se realizó al personal del DTTI

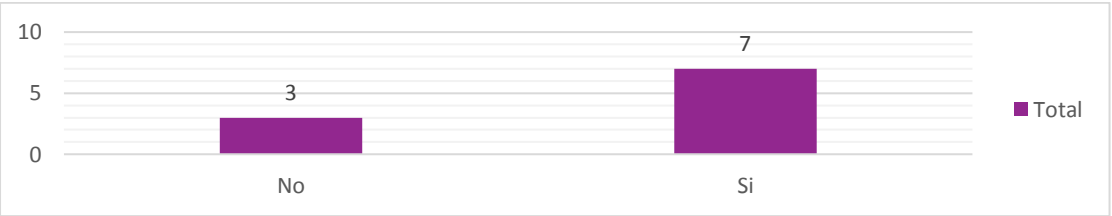


Encuesta Dirigida a:

Estudiantes de la Universidad Técnica del Norte

1.- ¿Cree usted que la información de la UTN se encuentra totalmente segura?

2.- Cuando comparte información de su computadora dentro de la institución, ¿está totalmente segura/o de que la información la recibió la persona a la que iba dirigida?



3.- ¿Alguna vez ha notado que la información de su computadora de trabajo ha sido total o parcialmente modificada al conectarla a la red institucional?

4.- ¿Usted comparte las contraseñas de acceso de su computadora de trabajo y aplicaciones con otras personas en la institución?

5.- ¿Conoce sobre los términos "cifrado de datos", “encriptación” y hace uso de ellos?

6.- ¿Sabe si su computadora puede ser manipulado de manera remota, es decir que no exista la necesidad de que una persona este físicamente interactuando con su computadora?

7.- ¿Utiliza dispositivos de almacenamiento extraíbles para compartir información dentro de la Institución?

8.- ¿Alguna vez se le ha perdido algún dispositivo de almacenamiento con información de sus trabajos en la Institución?

9.- ¿A compartido información personal e institucional con el personal de la UTN vía telefónica?

10.- ¿Para interactuar con el personal de recepción dentro de la UTN necesita registrarse por un medio de autenticación?

11.- ¿Para interactuar con el personal de recepción necesita tener una autorización de la autoridad respectiva?

12.- ¿Cree Usted que los activos transportados a través del personal autorizado de la UTN es un método confiable y seguro?

13.- ¿las comunicaciones verbales de carácter Institucional que Usted realiza son eficientes y seguras?

14.- ¿Hace uso de un sistema de alarma en su computadora basada en él envió y recepción de mensajes?

15.- ¿El sistema de acceso implementado en las entradas de la universidad es un método seguro y confiable?

16.- ¿Ha ingresado alguna vez al Departamento de Desarrollo Tecnológico e Informático (DDTI) sin necesidad de una autorización por escrito u otro tipo de identificación personal?

17.- ¿Alguna vez a obtenido información personal o credenciales de acceso de un docente, estudiante u otro trabajador de la institución?

18.- Al insertar un medio extraible en una computadora de la Institución y luego en su computadora. ¿Alguna vez se le ha mostrado alertas de riesgos informático?

19.- Cuándo hace uso de los laboratorios de Computación, ¿Usted se registra?

20.- ¿Cuándo se registra, la información proporcionada está expuesta a la vista de las personas que frecuentan al laboratorio de computación?

La pregunta fue llenada por 4 personas que utilizaron los laboratorios y se registraron

En la siguiente tabla se muestra el directorio del personal DDTI

Art. 7 de la Ley Orgánica de Transparencia y Acceso a la Información Pública - LOTAIP								
El directorio completo de Dirección de Desarrollo Tecnológico e Informático (DDTI)								
No.	**Apellidos y Nombres de los servidores y servidoras**	**Puesto Institucional**	**Unidad a la que pertenece**	**Dirección institucional**	**Ciudad en la que labora**	**Teléfono institucional**	**Extensión telefónica**	**Correo Electrónico institucional**
1	CARLOZAMA CHICAIZA MARCO JAVIER	ANALISTA DE SISTEMAS 2	DIRECCIÓN DE DESARROLLO TECNOLÓGICO E INFORMÁTICO	AV. 17 DE JULIO 5-21 Y GRAL JOSE MARIA CORDOBA	IBARRA	062997800	7051	mjcarlozama@utn.edu.ec
2	CARRION ORTIZ EDISON MARCELO	ASISTENTE DE REDES Y COMUNICACIONES	DIRECCIÓN DE DESARROLLO TECNOLÓGICO E INFORMÁTICO	AV. 17 DE JULIO 5-21 Y GRAL JOSE MARIA CORDOBA	IBARRA	062997800	7053	emcarrion@utn.edu.ec
3	CHAMORRO SANGOQUIZA MAYRA ISABEL	ANALISTA DE SISTEMAS 2	DIRECCIÓN DE DESARROLLO TECNOLÓGICO E INFORMÁTICO	AV. 17 DE JULIO 5-21 Y GRAL JOSE MARIA CORDOBA	IBARRA	062997800	7041	michamorros@utn.edu.ec
4	CHAVEZ GUAMIALAMA LENIN XAVIER	ANALISTA DE SISTEMAS 1	DIRECCIÓN DE DESARROLLO TECNOLÓGICO E INFORMÁTICO	AV. 17 DE JULIO 5-21 Y GRAL JOSE MARIA CORDOBA	IBARRA	062997800	7044	lxchavez@utn.edu.ec
5	ENRIQUEZ HUACA EVELIN GUADALUPE	ANALISTA DE SISTEMAS 2	DIRECCIÓN DE DESARROLLO TECNOLÓGICO E INFORMÁTICO	AV. 17 DE JULIO 5-21 Y GRAL JOSE MARIA CORDOBA	IBARRA	062997800	7046	egenriquez@utn.edu.ec
6	GARCIA PINCHAO JUAN CARLOS	ANALISTA DE SISTEMAS 3 / DIRECTOR ENCARGADO	DIRECCIÓN DE DESARROLLO TECNOLÓGICO E INFORMÁTICO	AV. 17 DE JULIO 5-21 Y GRAL JOSE MARIA CORDOBA	IBARRA	062997800	7040	jcgarcia@utn.edu.ec
7	GUERRA MORALES EDWIN VINICIO	ANALISTA DE REDES Y COMUNICACIONES 1	DIRECCIÓN DE DESARROLLO TECNOLÓGICO E INFORMÁTICO	AV. 17 DE JULIO 5-21 Y GRAL JOSE MARIA CORDOBA	IBARRA	062997800	7052	vinicio.guerra@utn.edu.ec
8	LOPEZ NARVAEZ IRVING VLADIMIR	ASISTENTE DE SISTEMAS INFORMATICOS	DIRECCIÓN DE DESARROLLO TECNOLÓGICO E INFORMÁTICO	AV. 17 DE JULIO 5-21 Y GRAL JOSE MARIA CORDOBA	IBARRA	062997800	7041	ivlopez@utn.edu.ec
9	RIVERA BELTRAN MARIA FERNANDA	ANALISTA DE SISTEMAS 1	DIRECCIÓN DE DESARROLLO TECNOLÓGICO E INFORMÁTICO	AV. 17 DE JULIO 5-21 Y GRAL JOSE MARIA CORDOBA	IBARRA	062997800	7043	mfrivera@utn.edu.ec
10	RODRIGUEZ JACOME JUAN CARLOS	ANALISTA DE SISTEMAS 3	DIRECCIÓN DE DESARROLLO TECNOLÓGICO E INFORMÁTICO	AV. 17 DE JULIO 5-21 Y GRAL JOSE MARIA CORDOBA	IBARRA	062997800	7050	jcrodriguez@utn.edu.ec
11	ROSERO PINEDA JUANA MARIA NARCISA	ANALISTA DE SISTEMAS 1	DIRECCIÓN DE DESARROLLO TECNOLÓGICO E INFORMÁTICO	AV. 17 DE JULIO 5-21 Y GRAL JOSE MARIA CORDOBA	IBARRA	062997800	7048	jrosero@utn.edu.ec
12	TIXILIMA ALVEAR SAYELI ELIZABETH	ANALISTA DE SISTEMAS 1	DIRECCIÓN DE DESARROLLO TECNOLÓGICO E INFORMÁTICO	AV. 17 DE JULIO 5-21 Y GRAL JOSE MARIA CORDOBA	IBARRA	062997800	7042	setixilima@utn.edu.ec

13	TORRES AZA ESTEFANIA GRACIELA	ANALISTA DE REDES Y COMUNICACIONES 1	DIRECCIÓN DE DESARROLLO TECNOLÓGICO E INFORMÁTICO	AV. 17 DE JULIO 5-21 Y GRAL JOSE MARIA CORDOBA	IBARRA	062997800	7054	egtorres@utn.edu.ec
14	YARUSCUAN MORALES KLEBER VINICIO	ANALISTA DE SISTEMAS 1	DIRECCIÓN DE DESARROLLO TECNOLÓGICO E INFORMÁTICO	AV. 17 DE JULIO 5-21 Y GRAL JOSE MARIA CORDOBA	IBARRA	062997800	7049	kvyaruscuanm@utn.edu.ec
15	AGUILAR BUITRON LUIS ROLANDO	ANALISTA DE SISTEMAS 2	DIRECCIÓN DE DESARROLLO TECNOLÓGICO E INFORMÁTICO	AV. 17 DE JULIO 5-21 Y GRAL JOSE MARIA CORDOBA	IBARRA	062997800	7045	lraguilar@utn.edu.ec
16	BEDON TORRES SAMIA DEL ROCIO	SECRETARIA DE DESPACHO	DIRECCIÓN DE DESARROLLO TECNOLÓGICO E INFORMÁTICO	AV. 17 DE JULIO 5-21 Y GRAL JOSE MARIA CORDOBA	IBARRA	062997800	7041	sbedon@utn.edu.ec
17	CARDENAS ROSERO GABRIELA ELIZABETH	ASISTENTE DE SISTEMAS INFORMATICOS	DIRECCIÓN DE DESARROLLO TECNOLÓGICO E INFORMÁTICO	AV. 17 DE JULIO 5-21 Y GRAL JOSE MARIA CORDOBA	IBARRA	062997800	7047	gecardenas@utn.edu.ec

Fuente: Elaboración propia

Fotos

Acceso por Biométrico hacia el DDTI

Fuente: Elaboración propia

Registro en Hojas

Fuente: Elaboración propia

Sistema de alarma en la UTN

Fuente: Elaboración propia

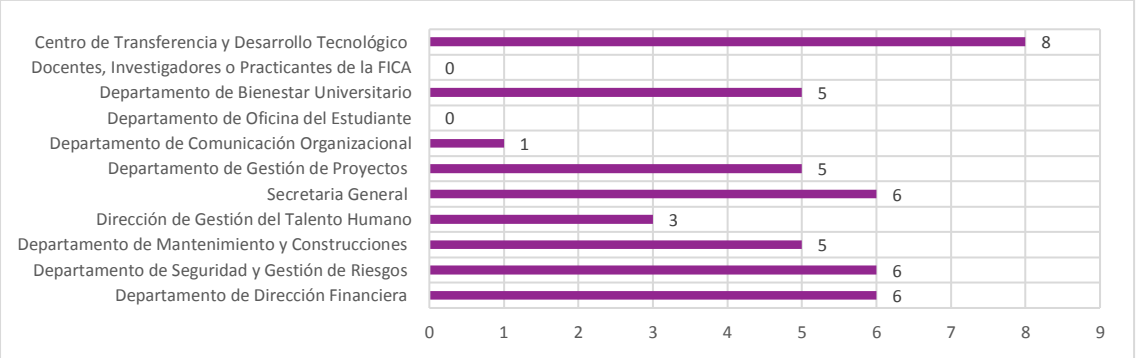
Anexo B. Pruebas de seguridad física (PHYSSEC)

Encuesta Dirigida a:

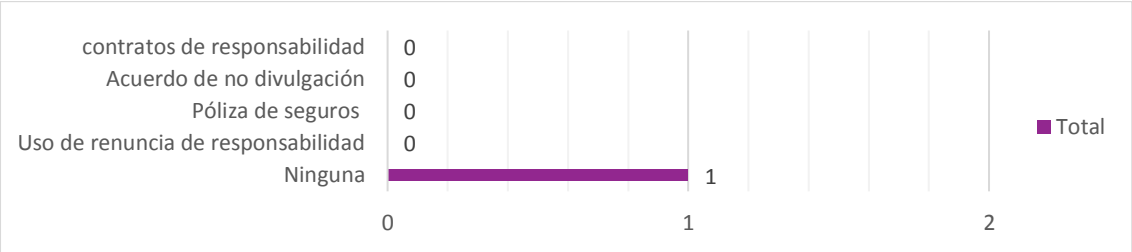
Dirigente del área de redes y Sistemas.

1.- Que áreas están autorizadas a acceder sin autenticación hacia el Departamento de Desarrollo Tecnológico e Informático (DTI).

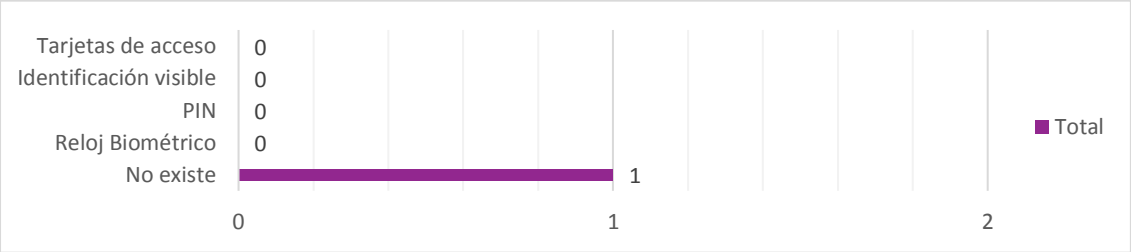
La pregunta fue realizada dentro del canal humano y se realizó al personal del DTTI



2.- Se hace uso de políticas como:



3.- Existe divulgación o duplicación de los controles de acceso por:



4.- ¿La ausencia del Personal de apoyo causa inconvenientes laborales?

La pregunta fue realizada dentro del canal humano

5.- La falta de recursos no prolongadas como: agua, luz eléctrica, combustible, alimento. ¿Detiene el acceso físico y las operaciones que se manejan?

6.- En caso de una amenaza de alerta alta como: incendio, sismo, etc. ¿Se Detiene el acceso físico y las operaciones que se manejan?

7.- ¿Los activos informáticos de la UTN cuando son transportados hacen uso de firmas y sellos eficientes?

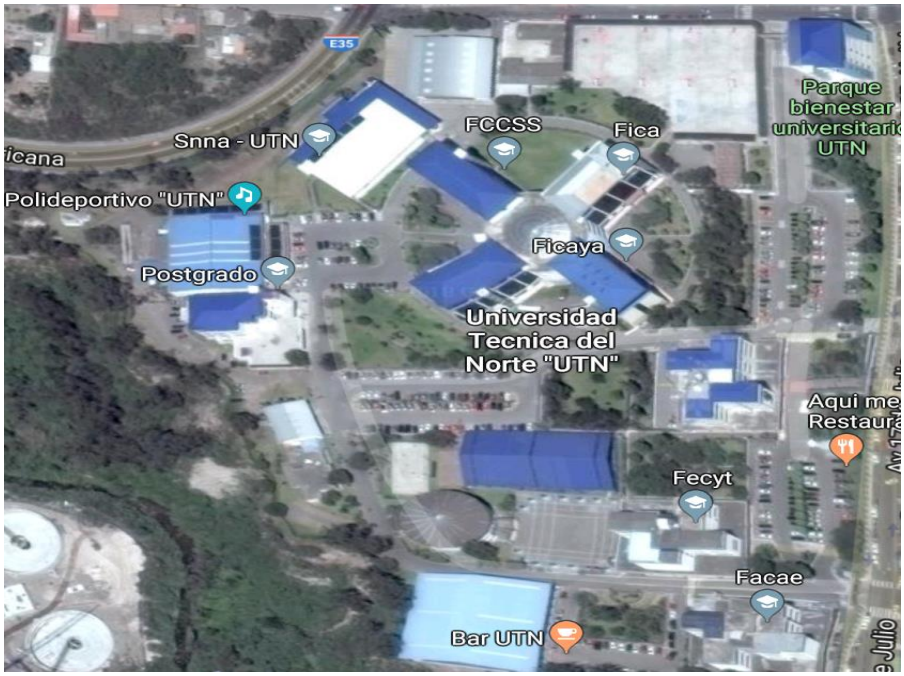
La pregunta fue realizada dentro del canal humano

8.- ¿Las comunicaciones verbales que se realizan entre el personal son confiables y autorizadas?

La pregunta fue realizada dentro del canal humano

Fotos

Perímetro del alcance Interno de la UTN



Fuente: Google Maps

Señalética vehicular y peatonal dentro de la UTN

Fuente: Elaboración Propia

Señales de advertencia y aviso de área dentro de la UTN

Fuente: Elaboración Propia

Cámaras y monitores de video vigilancia dentro de la UTN

Fuente: Elaboración Propia

Puertas y ventanas de cristal y sin protección dentro de la UTN

Fuente: Elaboración Propia

Vallas y Mallas que se pueden eludir en la UTN

Fuente: Elaboración Propia

Falta de señales dentro de la UTN

Fuente: Elaboración Propia

Control de acceso apagado en entrada principal a la UTN

Fuente: Elaboración Propia

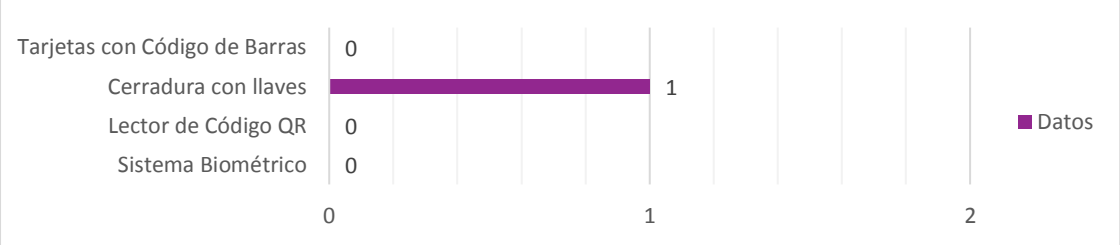
Anexo C. Pruebas de Seguridad Inalámbrica (SPECSEC)

Encuesta Dirigida a:

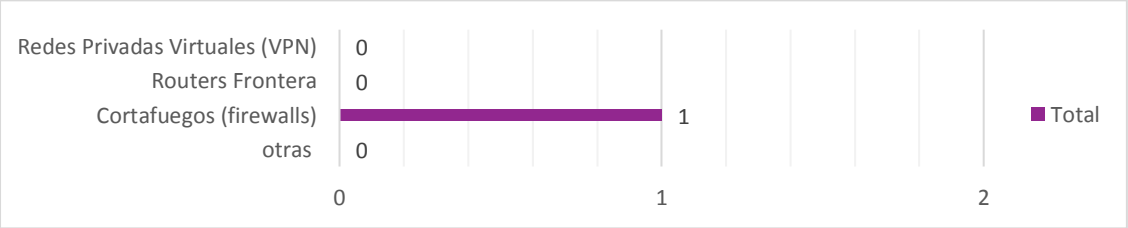
Dirigente del área de redes y Sistemas.

1.- ¿Qué tipos de mecanismos de seguridad existen para regular el acceso hacia los equipos inalámbricos en la UTN?

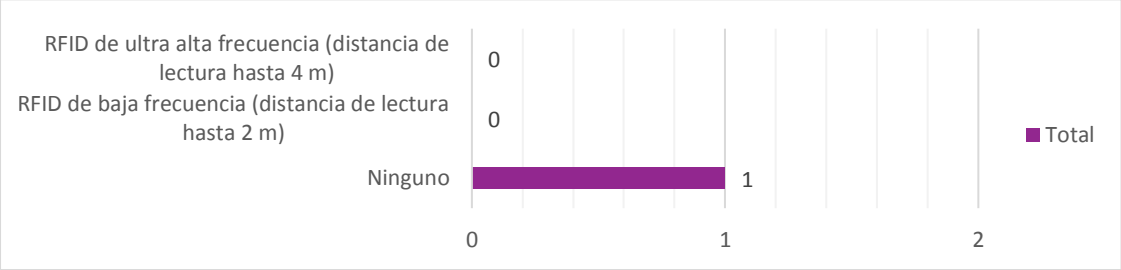
2.- ¿Qué tipos de mecanismos de seguridad existen para regular el acceso hacia los equipos inalámbricos en la UTN?



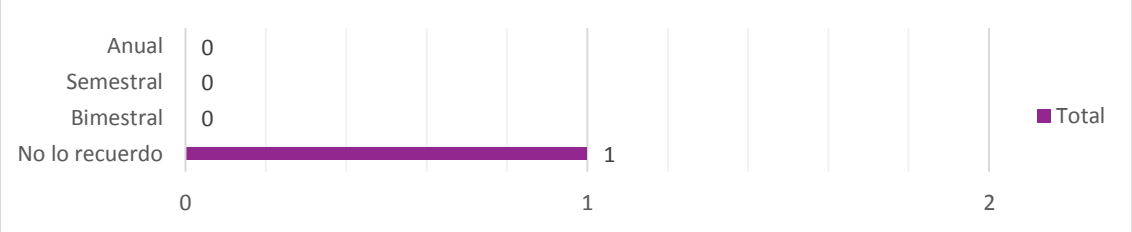
3.- ¿Existe algún elemento de seguridad perimetral que protejan contra ataques informáticos hacia la red inalámbrica?



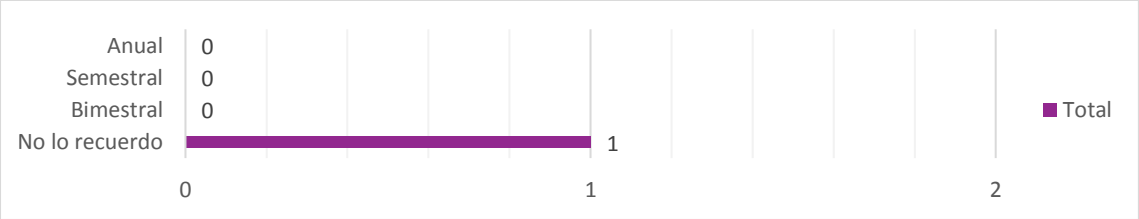
4.- ¿Se hace uso de algún tipo de sistema RFID (Radio Frecuencia), o algún otro tipo de sistema inalámbrico?



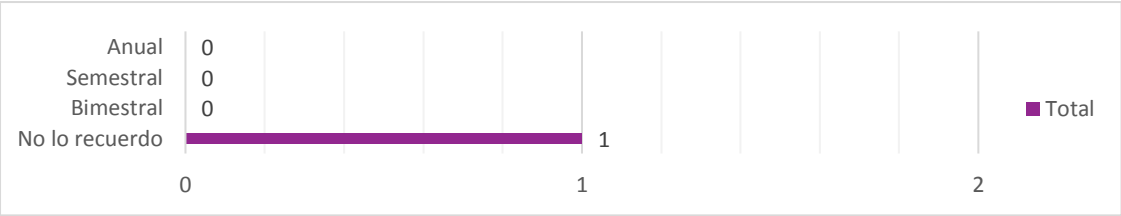
5.- ¿Con que frecuencia de tiempo se cambia el SSID de la red inalámbrica?



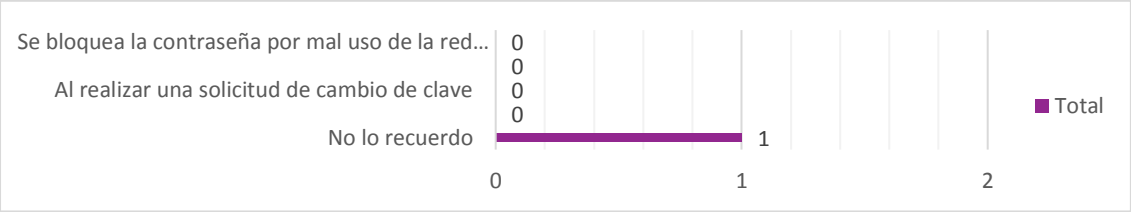
6.- ¿Con que frecuencia de tiempo se cambia la contraseña de la red inalámbrica WUTN_Admin?



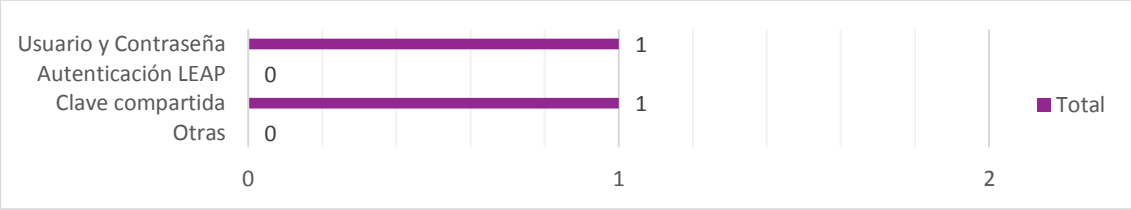
7.- ¿Con que frecuencia de tiempo se cambia la contraseña de la red inalámbrica WUTN_Docentes?



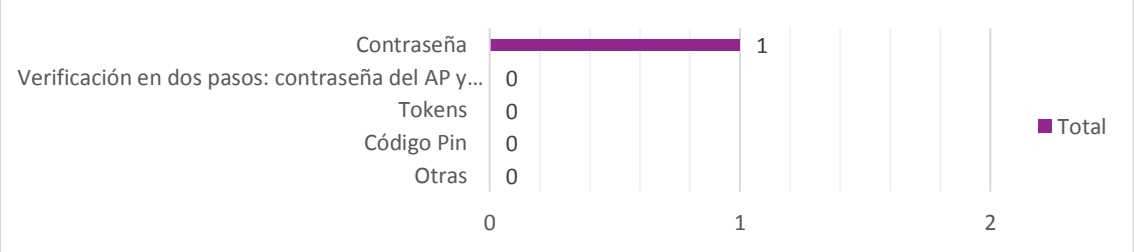
8.- ¿Con que frecuencia de tiempo se cambia la contraseña de la red inalámbrica Eduroam?



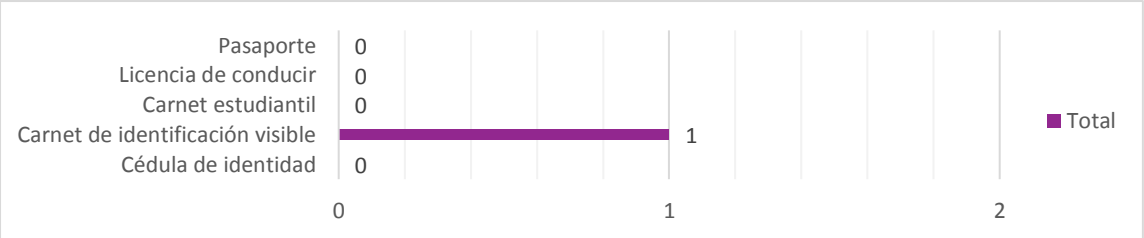
9.- ¿Qué tipo de método de autenticación existe para conectarse a los AP inalámbricos de la UTN?



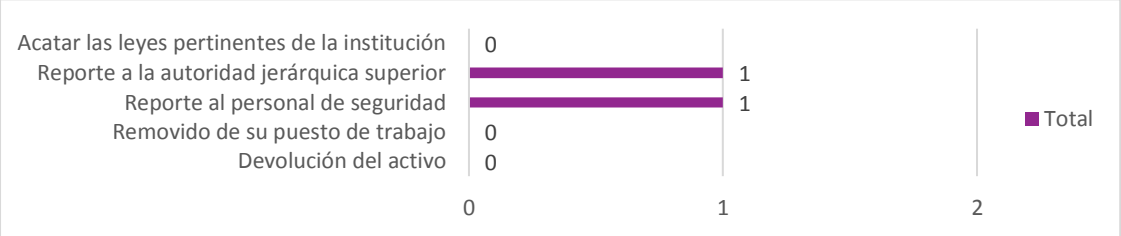
10.- ¿Existe algún método único de autenticación por parte del personal autorizado para entrar en los AP inalámbricos de la UTN?



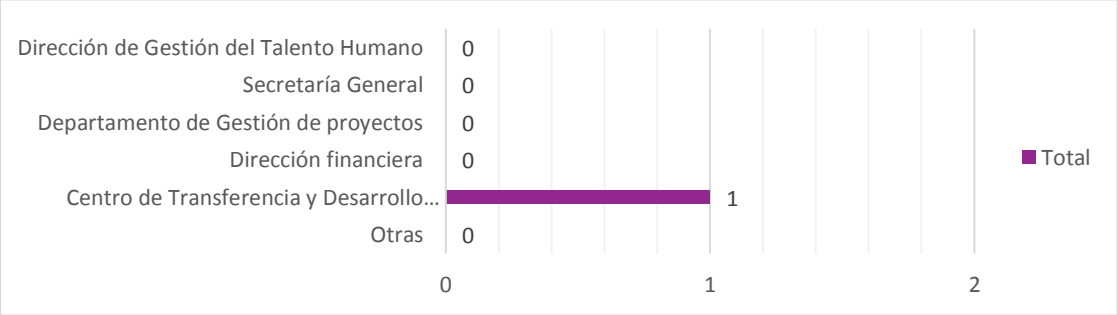
11.- ¿Qué documento habilita como acuerdo de uso de responsabilidad por parte de empleados y usuarios cuándo se hace uso de los equipos inalámbricos de la UTN?



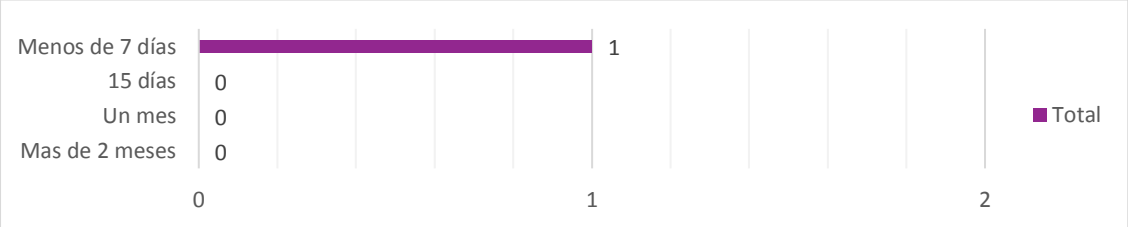
12.- ¿Cuál es el procedimiento a seguir cuando algún usuario u empleado incumple con un acuerdo legal, si un activo es sustraído o tiene un virus malicioso?



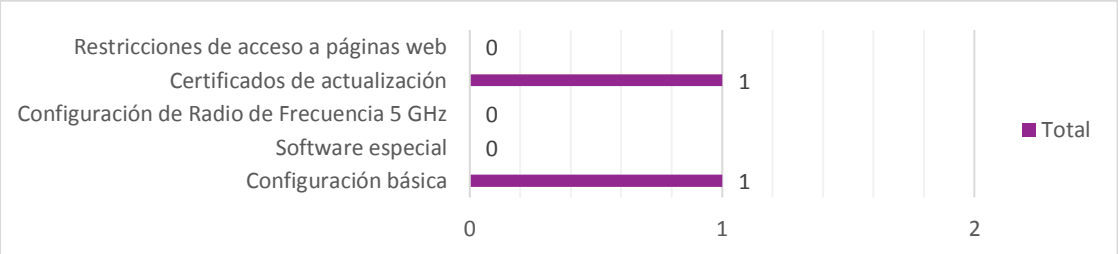
13.- Cuando existe algún problema con los equipos inalámbricos de la UTN. ¿El DDTI recibe apoyo de otras áreas o departamentos cuáles son?



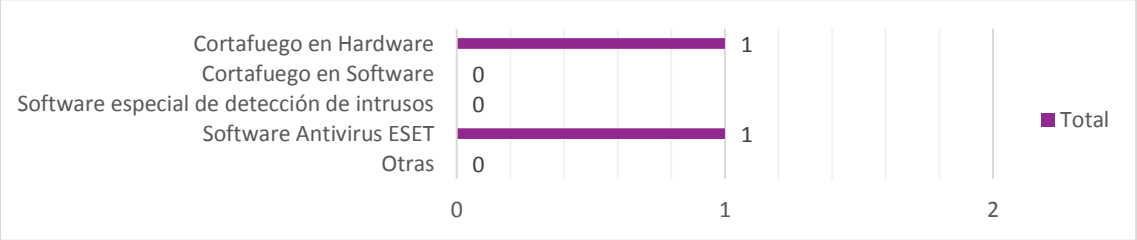
14.- Cuando existe algún problema con los equipos inalámbricos de la UTN. ¿Cuánto tiempo se tarda en resolverlo?



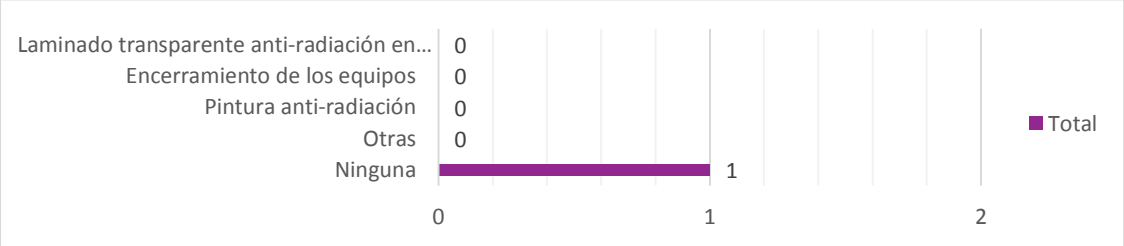
15.- ¿Cuándo se instala un Equipo Informático para la red inalámbrica a qué tipo de controles se hace énfasis en su configuración?



16.- ¿Se hace uso de algún sistema de alerta para evitar actividad fraudulenta, ingeniería social o ingresos no autorizados a los equipos inalámbricos de la UTN?



17.- ¿Se hace uso de algún tipo de dispositivo electrónico o método que permita amortiguar las señales de transmisión inalámbrica evitando que la señal viaje a lugares no deseados?



18.- ¿Se hace uso de un horno microondas?

19.- ¿Existe algún AP inalámbrico que acepte señal de terceros en lugar de la prevista?

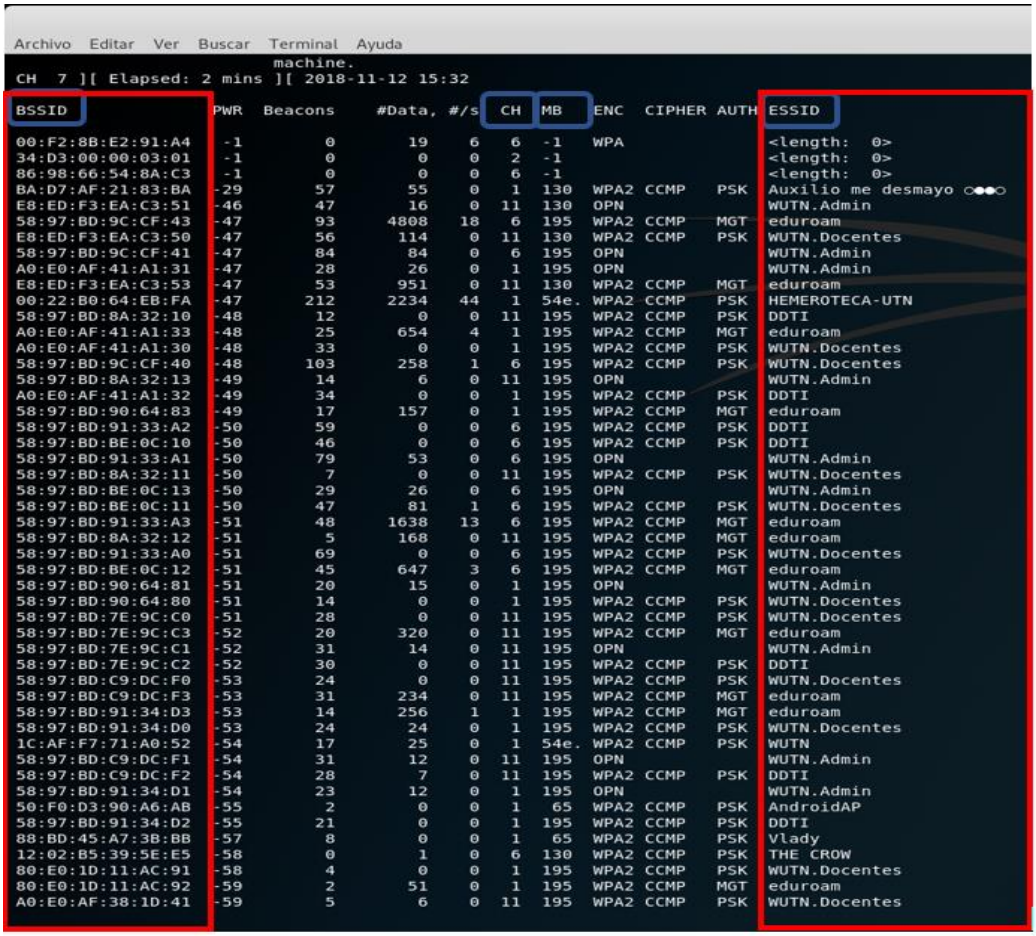
20.- ¿Se apagan los Puntos de Acceso inalámbricos cuando no se hace uso de ellos?

21.- ¿Existen equipos informáticos inalámbricos en su área de trabajo que no estén recibiendo la señal o que estén en desuso?

22.- ¿El personal está capacitado en prevención de riesgos informáticos?

Fotos

Escaneo de redes con Aircrack-ng dentro de la UTN



```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
                machine.
CH  7 ][ Elapsed: 2 mins ][ 2018-11-12 15:32

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:F2:8B:E2:91:A4  -1        0       19    6   6  -1   WPA                <length:  0>
34:D3:00:00:03:01  -1        0        0    0   2  -1                      <length:  0>
86:98:66:54:8A:C3  -1        0        0    0   6  -1                      <length:  0>
BA:D7:AF:21:83:BA  -29       57       55    0   1  130  WPA2 CCMP   PSK  Auxilio me desmayo
E8:ED:F3:EA:C3:51  -46       47       16    0  11  130  OPN                WUTN.Admin
58:97:BD:9C:CF:43  -47       93     4808   18   6  195  WPA2 CCMP   MGT  eduroam
E8:ED:F3:EA:C3:50  -47       56      114    0  11  130  WPA2 CCMP   PSK  WUTN.Docentes
58:97:BD:9C:CF:41  -47       84       84    0   6  195  OPN                WUTN.Admin
A0:E0:AF:41:A1:31  -47       28       26    0   1  195  OPN                WUTN.Admin
E8:ED:F3:EA:C3:53  -47       53      951    0  11  130  WPA2 CCMP   MGT  eduroam
00:22:B0:64:EB:FA  -47      212     2234   44   1  54e. WPA2 CCMP   PSK  HEMEROTECA-UTN
58:97:BD:8A:32:10  -48       12        0    0  11  195  WPA2 CCMP   PSK  DDTI
A0:E0:AF:41:A1:33  -48       25      654    4   1  195  WPA2 CCMP   MGT  eduroam
A0:E0:AF:41:A1:30  -48       33        0    0   1  195  WPA2 CCMP   PSK  WUTN.Docentes
58:97:BD:9C:CF:40  -48      103      258    1   6  195  WPA2 CCMP   PSK  WUTN.Docentes
58:97:BD:8A:32:13  -49       14        6    0  11  195  OPN                WUTN.Admin
A0:E0:AF:41:A1:32  -49       34        0    0   1  195  WPA2 CCMP   PSK  DDTI
58:97:BD:90:64:83  -49       17      157    0   1  195  WPA2 CCMP   MGT  eduroam
58:97:BD:91:33:A2  -50       59        0    0   6  195  WPA2 CCMP   PSK  DDTI
58:97:BD:BE:0C:10  -50       46        0    0   6  195  WPA2 CCMP   PSK  DDTI
58:97:BD:91:33:A1  -50       79       53    0   6  195  OPN                WUTN.Admin
58:97:BD:8A:32:11  -50        7        0    0  11  195  WPA2 CCMP   PSK  WUTN.Docentes
58:97:BD:BE:0C:13  -50       29       26    0   6  195  OPN                WUTN.Admin
58:97:BD:BE:0C:11  -50       47       81    1   6  195  WPA2 CCMP   PSK  WUTN.Docentes
58:97:BD:91:33:A3  -51       48     1638   13   6  195  WPA2 CCMP   MGT  eduroam
58:97:BD:8A:32:12  -51        5      168    0  11  195  WPA2 CCMP   MGT  eduroam
58:97:BD:91:33:A0  -51       69        0    0   6  195  WPA2 CCMP   PSK  WUTN.Docentes
58:97:BD:BE:0C:12  -51       45      647    3   6  195  WPA2 CCMP   MGT  eduroam
58:97:BD:90:64:81  -51       20       15    0   1  195  OPN                WUTN.Admin
58:97:BD:90:64:80  -51       14        0    0   1  195  WPA2 CCMP   PSK  WUTN.Docentes
58:97:BD:7E:9C:C0  -51       28        0    0  11  195  WPA2 CCMP   PSK  WUTN.Docentes
58:97:BD:7E:9C:C3  -52       20      320    0  11  195  WPA2 CCMP   MGT  eduroam
58:97:BD:7E:9C:C1  -52       31       14    0  11  195  OPN                WUTN.Admin
58:97:BD:7E:9C:C2  -52       30        0    0  11  195  WPA2 CCMP   PSK  DDTI
58:97:BD:C9:DC:F0  -53       24        0    0  11  195  WPA2 CCMP   PSK  WUTN.Docentes
58:97:BD:C9:DC:F3  -53       31      234    0  11  195  WPA2 CCMP   MGT  eduroam
58:97:BD:91:34:D3  -53       14      256    1   1  195  WPA2 CCMP   MGT  eduroam
58:97:BD:91:34:D0  -53       24       24    0   1  195  WPA2 CCMP   PSK  WUTN.Docentes
1C:AF:F7:71:A0:52  -54       17       25    0   1  54e. WPA2 CCMP   PSK  WUTN
58:97:BD:C9:DC:F1  -54       31       12    0  11  195  OPN                WUTN.Admin
58:97:BD:C9:DC:F2  -54       28        7    0  11  195  WPA2 CCMP   PSK  DDTI
58:97:BD:91:34:D1  -54       23       12    0   1  195  OPN                WUTN.Admin
50:F0:D3:90:A6:AB  -55        2        0    0   1   65  WPA2 CCMP   PSK  AndroidAP
58:97:BD:91:34:D2  -55       21        0    0   1  195  WPA2 CCMP   PSK  DDTI
88:BD:45:A7:3B:BB  -57        8        0    0   1   65  WPA2 CCMP   PSK  Vlady
12:02:B5:39:5E:E5  -58        0        1    0   6  130  WPA2 CCMP   PSK  THE CROW
80:E0:1D:11:AC:91  -58        4        0    0   1  195  WPA2 CCMP   PSK  WUTN.Docentes
80:E0:1D:11:AC:92  -59        2       51    0   1  195  WPA2 CCMP   MGT  eduroam
A0:E0:AF:38:1D:41  -59        5        6    0  11  195  WPA2 CCMP   PSK  WUTN.Docentes
```

Fuente: Elaboración propia

En donde BSSID es la dirección MAC del punto de acceso, CH es el número de canal, MB es la velocidad máxima soportada por el Punto de Acceso, ESSID es el nombre de identificación de la red.

En la siguiente tabla se detalla la distribución de los AP en el campus universitario

FACAE	AP-FACAE-PB-C	PLANTA BAJA CENTRO	CISCO
	AP-FACAE-PB-D	PLANTA BAJA DERECHA	CISCO
	AP-FACAE-PB-I	PLANTA BAJA IZQUIERDA	CISCO
	AP-FACAE-PA1-I	PRIMER PISO IZQUIERDA	CISCO
	AP-FACAE-PA1-D	PRIMER PISO DERECHA	CISCO
	AP-FACAE-PA2-I	SEGUNDO PISO IZQUIERDA	CISCO
	AP-FACAE-PA2-D	SEGUNDO PISO DERECHA	CISCO
	AP-FACAE-PA3-I	TERCER PISO IZQUIERDA	CISCO
	AP-FACAE-PA3-D	TERCER PISO DERECHA	CISCO
	AP-FACAE-PA4	CUARTO PISO	CISCO

FECYT	AP-FECYT-PB-I	PLANTA BAJA IZQUIERDA	CISCO
	AP-FECYT-PB-D	PLANTA BAJA DERECHA	CISCO
	AP-FECYT-PA1-I	PRIMER PISO IZQUIERDA	CISCO
	AP-FECYT-PA1-D	PRIMER PISO DERECHA	CISCO
	AP-FECYT-PA2-I	SEGUNDO PISO IZQUIERDA	CISCO
	AP-FECYT-PA2-D	SEGUNDO PISO DERECHA	CISCO
	AP-FECYT-PA3-I	TERCER PISO IZQUIERDA	CISCO
	AP-FECYT-PA3-D	TERCER PISO DERECHA	CISCO
	AP-FECYT-PA4	CUARTO PISO	CISCO

FICAYA	AP-FICAYA-PB-I	PLANTA BAJA IZQUIERDA	CISCO
	AP-FICAYA-PB-D	PLANTA BAJA DERECHA	CISCO
	AP-FICAYA-PA1-I	PRIMER PISO IZQUIERDA	CISCO
	AP-FICAYA-PA1-D	PRIMER PISO DERECHA	CISCO
	AP-FICAYA-PA2-I	SEGUNDO PISO IZQUIERDA	CISCO
	AP-FICAYA-PA2-D	SEGUNDO PISO DERECHA	CISCO
	AP-FICAYA-PA3-I	TERCER PISO IZQUIERDA	CISCO
	AP-FICAYA-PA3-D	TERCER PISO DERECHA	CISCO
	AP-FICAYA-PA4	CUARTO PISO	CISCO

FCCSS	AP-FCCSS-PB-I	PLANTA BAJA IZQUIERDA	CISCO
	AP-FCCSS-PB-D	PLANTA BAJA DERECHA	CISCO
	AP-FCCSS-PA1-I	PRIMER PISO IZQUIERDA	CISCO
	AP-FCCSS-PA1-D	PRIMER PISO DERECHA	CISCO
	AP-FCCSS-PA2-I	SEGUNDO PISO IZQUIERDA	CISCO
	AP-FCCSS-PA2-D	SEGUNDO PISO DERECHA	CISCO
	AP-FCCSS-PA3-I	TERCER PISO IZQUIERDA	CISCO
	AP-FCCSS-PA3-D	TERCER PISO DERECHA	CISCO
	AP-FCCSS-PA4-I	CUARTO PISO DERECHA	CISCO

FICA	AP-FICA-PB-D	PLANTA BAJA DERECHA	CISCO
	AP-FICA-PA1-I	PRIMER PISO IZQUIERDA	CISCO
	AP-FICA-PA2-D	SEGUNDO PISO DERECHA	CISCO
	AP-FICA-PA3-I	TERCER PISO IZQUIERDA	CISCO
	AP-FICA-PA4-I	CUARTO PISO IZQUIERDA	CISCO
	AP-FICA-PA4-D	CUARTO PISO DERECHA	CISCO

POSTGRADO	AP-POSTGRADO-AU-I	PLANTA BAJA AUDITORIO IZQ	CISCO
	AP-POSTGRADO-AU-D	PLANTA BAJA AUDITORIO DER	CISCO
	AP-POSTGRADO-PB-CUBI	PLANTA BAJA CUBICULOS	CISCO
	AP-POSTGRADO-PB-PASILLO	PLANTA BAJA PASILLO	CISCO
	AP-POSTGRADO-PA1-I	PRIMER PISO IZQUIERDA	CISCO
	AP-POSTGRADO-PA1-D	PRIMER PISO DERECHA	CISCO
	AP-POSTGRADO-PA2-I	SEGUNDO PISO IZQUIERDA	CISCO
	AP-POSTGRADO-PA2-D	SEGUNDO PISO DERECHA	CISCO

CAI	AP-CAI-PB-I	PLANTA BAJA IZQUIERDA	CISCO
	AP-CAI-PB-D	PLANTA BAJA DERECHA	CISCO

	AP-CAI-PA1-I	PRIMER PISO IZQUIERDA	CISCO
	AP-CAI-PA1-D	PRIMER PISO DERECHA	CISCO
	AP-CAI-PA2-I	SEGUNDO PISO IZQUIERDA	CISCO
	AP-CAI-PA2-D	SEGUNDO PISO DERECHA	CISCO
	AP-CAI-PA3-I	TERCER PISO IZQUIERDA	CISCO
	AP-CAI-PA3-D	TERCER PISO DERECHA	CISCO
	AP-CAI-PA4-I	CUARTO PISO IZQUIERDA	CISCO
	AP-CAI-PA4-D	CUARTO PISO DERECHA	CISCO
POLIDEPORTIVO	AP-POLIDEPORTIVO-PB	POLIDEPORTIVO PLANTA BAJA	CISCO
	AP-POLIDEPORTIVO-PA1	OFICINAS PRIMER PISO	CISCO
	AP-POLIDEPORTIVO-DANZA	POLIDEPORTIVO AULA DANZA	CISCO
	AP-POLIDEPORTIVO-SNNA	OFICINAS SNNA	CISCO
	AP-POLIDEPORTIVO-CB-I	CANCHA IZQUIERDA	
	AP-POLIDEPORTIVO-CB-D	CANCHA DERECHA	CISCO
BIBLIOTECA	AP-BIBLIOTECA-PB	PLANTA BAJA	CISCO
	AP-BIBLIOTECA-PA1-I	PRIMER PISO IZQUIERDA	CISCO
	AP-BIBLIOTECA-PA1-D	PRIMER PISO DERECHA	CISCO
	AP-BIBLIOTECA-PA1-H	PRIMER PISO HEMEROTECA	CISCO
	AP-BIBLIOTECA-PA2	SEGUNDO PISO	CISCO
	AP-BIBLIOTECA-PA2-R	SEGUNDO PISO RECTORADO	CISCO
	AP-BIBLIOTECA-PA3-R	TERCER PISO RACK	CISCO
	AP-BIBLIOTECA-PA3-A	TERCER PISO ASCENSOR	CISCO
	AP-BIBLIOTECA-PA3-G	TERCER PISO GRADAS	CISCO

EXTERIOR	AP-EXTERIOR-FACAE-PARQUE	FACAE EXTERIOR PARQUE	CISCO
	ANTENA		CISCO
	AP-EXTERIOR-FACAE-GRADAS	FACAE EXTERIOR GRADAS	CISCO
	ANTENA		CISCO
	AP-EXTERIOR-FACAE-PARQUEADERO	FACAE EXTERIOR PARQUEADERO	CISCO
	ANTENA		CISCO
	AP-EXTERIOR-FECYT	FECYT EXTERIOR PARQUE	CISCO
	ANTENA		CISCO
	AP-EXTERIOR-AUDITORIO-PLAZA	AUDITORIO EXTERIOR PLAZA	CISCO
	ANTENA		CISCO
	AP-EXTERIOR-AUDITORIO-CANCHAS	AUDITORIO EXTERIOR CANCHAS	CISCO
	ANTENA		CISCO
	AP-EXTERIOR-CENTRAL	PLANTA CENTRAL EXTERIOR	CISCO
	ANTENA		CISCO
	AP-EXTERIOR-POST-PARQUE	POSTGRADO EXTERIOR PARQUE	CISCO
	ANTENA		CISCO
	AP-EXTERIOR-POST-PISCINA	POSTGRADO EXTERIOR PISCINA	CISCO
	ANTENA		CISCO
	AP-EXTERIOR-CAI/FICAYA	CAI/FICAYA EXTERIOR	CISCO
	ANTENA		CISCO
	AP-EXTERIOR-FICA/FICAYA	FICA/FICAYA EXTERIOR	CISCO
	ANTENA		CISCO
	AP-EXTERIOR-FICA/FCCSS	FICA/FCCSS EXTERIOR	CISCO
	ANTENA		CISCO
	AP-EXTERIOR-PISCINA	PISCINA EXTERIOR	CISCO
	ANTENA		CISCO

BIENESTAR	AP-BIENESTAR-PB-I	PLANTA BAJA IZQUIERDA	CISCO
	AP-BIENESTAR-PB-D	PLANTA BAJA DERECHA	CISCO
	AP-BIENESTAR-PA1-I	PRIMER PISO IZQUIERDA	CISCO
	AP-BIENESTAR-PA1-D	PRIMER PISO DERECHA	CISCO
	AP-BIENESTAR-PA2-I	SEGUNDO PISO IZQUIERDA	CISCO
	AP-BIENESTAR-PA2-D	SEGUNDO PISO DERECHA	CISCO
	AP-BIENESTAR-PA3-I	TERCER PISO IZQUIERDA	CISCO
	AP-BIENESTAR-PA3-D	TERCER PISO DERECHA	CISCO

	AP-EXTERIOR-FICA	FICA EXTERIOR	CISCO
	ANTENA		CISCO
	AP-EXTERIOR-ENTRADA-NORTE-I	ENTRADA NORTE CANCHAS	CISCO
	ANTENA		CISCO
	AP-EXTERIOR-ENTRADA-NORTE-D	ENTRADA NORTE BIENESTAR	CISCO
	ANTENA		CISCO
	AP-EXTERIOR-HSVP		CISCO
	AP-EXTERIOR-PARQUE-HSVP		CISCO

PLANTA CENTRAL	AP-CENTRAL-PB-I-AB	PLANTA BAJA IZQUIERDA ALMACEN BODEGA	CISCO
	AP-CENTRAL-PB-I-V	PLANTA BAJA IZQUIERDA VINCULACIÓN	CISCO
	AP-CENTRAL-PB-DDTI	PLANTA BAJA DDTI	CISCO
	AP-CENTRAL-PA1-VAC	PRIMER PISO VICERRECTORADO ACADÉMICO	CISCO
	AP-CENTRAL-PA1-R	PRIMER PISO RECTORADO	CISCO
	AP-CENTRAL-PA1-VAD	PRIMER PISO VICERRECTORADO ADMINISTRATIVO	CISCO
	AP-CENTRAL-PA2-I-JM	SEGUNDO PISO IZQUIERDA JOSE MARTÍ	CISCO
	AP-CENTRAL-PA2-D	SEGUNDO PISO DERECHA	CISCO
	AP-CENTRAL-PA2-I-P	SEGUNDO PISO IZQUIERDA PLANEAMIENTO	CISCO
	AP-CENTRAL-PA3-I	TERCER PISO IZQUIERDA	CISCO
	AP-CENTRAL-PA3-D	TERCER PISO DERECHA	CISCO
	AP-CENTRAL-PA4-I	CUARTO PISO IZQUIERDA	CISCO
	AP-CENTRAL-PA4-D	CUARTO PISO DERECHA	CISCO
	AP-1	DDTI	CISCO

HSVP	AP-HSVP-PB-I	CISCO	AIR CAP3702I-A-K9
	AP-HSVP-PA1-I-LAT	CISCO	AIR CAP3702I-A-K9
	AP-HSVP-PA1-D	CISCO	AIR CAP3702I-A-K9
	AP-HSVP-PA-D	CISCO	AIR CAP3702I-A-K9
	AP-HSVP-PA1-I	CISCO	AIR CAP3702I-A-K9
	AP-HPASILLO-D2	CISCO	AIR CAP3702I-A-K9
	AP-HPASILLO-D1	CISCO	AIR CAP3702I-A-K9
	AP-HSVP-AUDITORIO-D	CISCO	AIR CAP3702I-A-K9
	AP-HPASILLO-I	CISCO	AIR CAP3702I-A-K9
	AP-SALON-DERECHA	CISCO	AIR CAP3702I-A-K9

ELECTRICIDAD	AP-ELECTRICIDAD-PASILLO	AULAS PASILLO	CISCO
	AP-ELECTRICIDAD-MECANICA	MECÁNICA	CISCO

	AP-AUDITORIO-I	AUDITORIO IZQUIERDA	CISCO

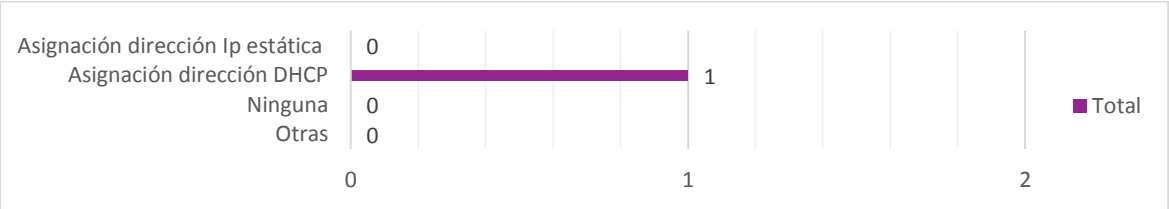
GIMNASIO	AP-GIMNASIO-PA1	PRIMER PISO	CISCO	AUDITORIO	AP-AUDITORIO-D	AUDITORIO DERECHA	CISCO
				PISCINA	AP-PISCINA-INTERIOR	INTERIOR	CISCO

Anexo D. Prueba de Seguridad de Redes de Datos (COMSEC)

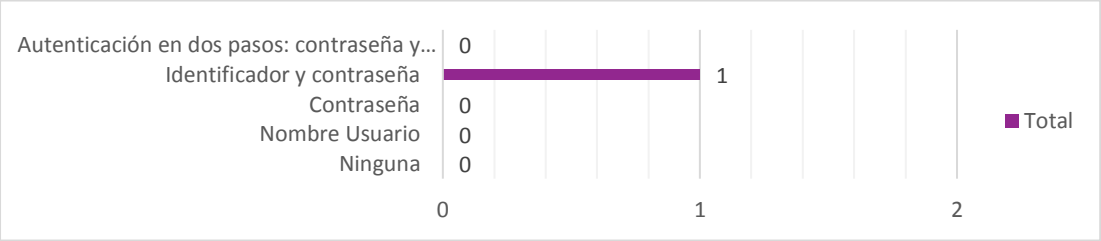
Encuesta Dirigida a:

Dirigente del área de redes y Sistemas.

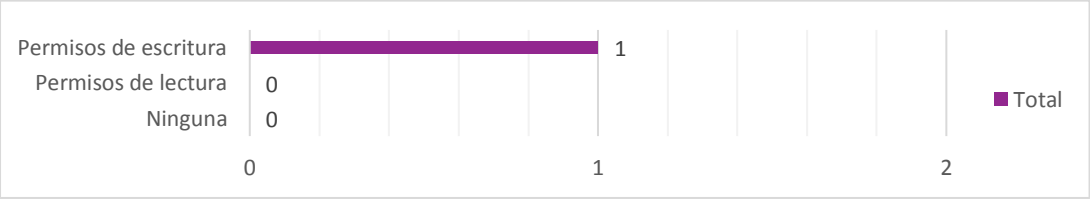
1.- ¿De qué manera acceden los equipos informáticos para hacer uso de la red de datos de la UTN?



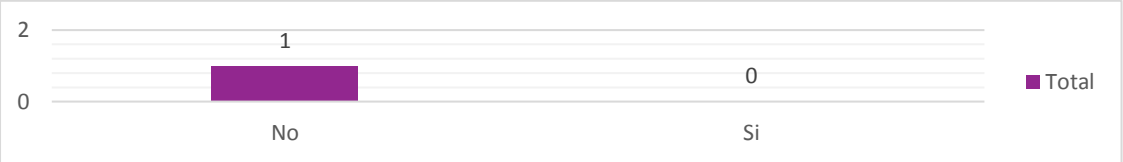
2.- ¿Cuál es el proceso de autenticación a seguir para acceder a la información de los servidores de la UTN por parte del personal autorizado?



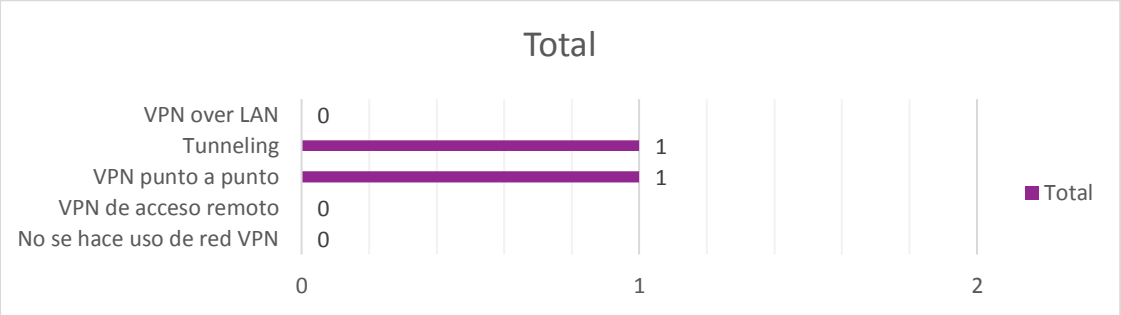
3.- ¿Qué privilegios conceden los servidores al acceder a la información de la UTN por parte del personal autorizado?



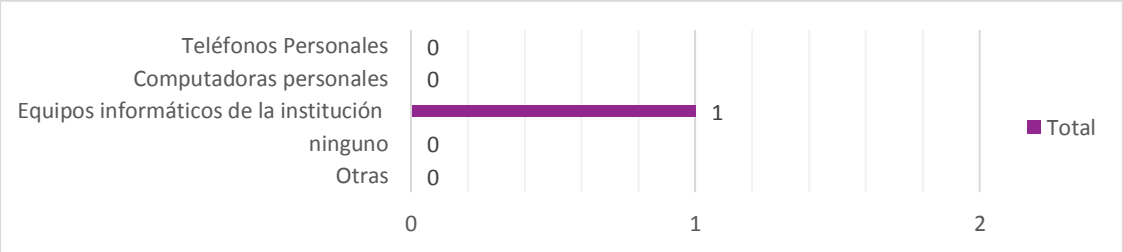
4.- ¿Se hace uso del protocolo de intercambio de claves en Internet (IKE) en la Red de Datos?



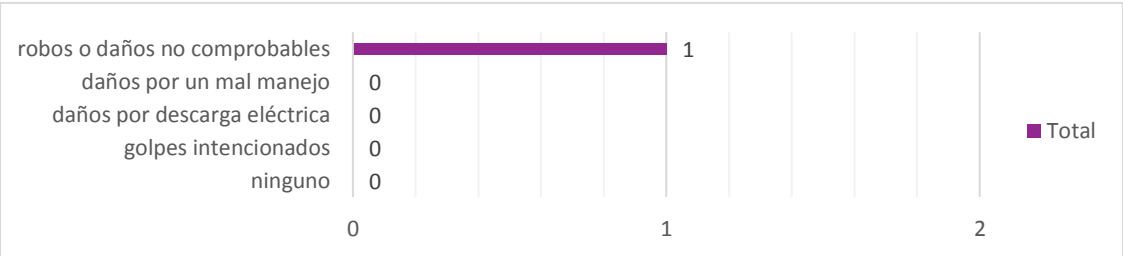
5.- ¿Qué tipo de red privada virtual (VPN) se utiliza en la institución?



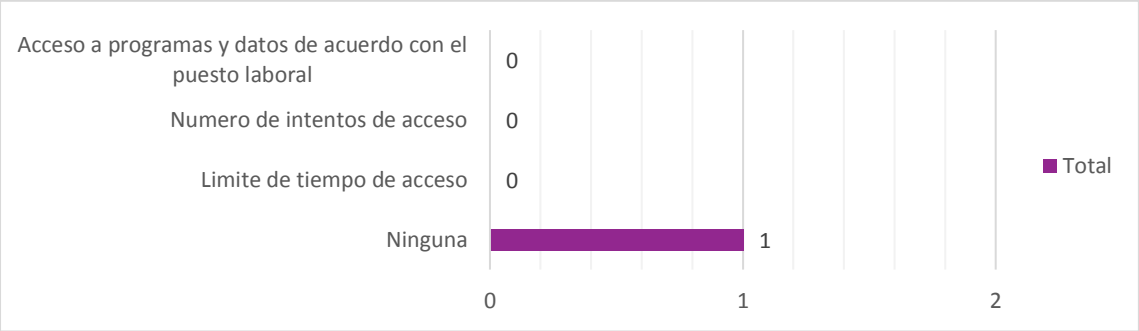
6.- ¿Qué equipos de comunicaciones se encuentran protegidos contra robos o daños?



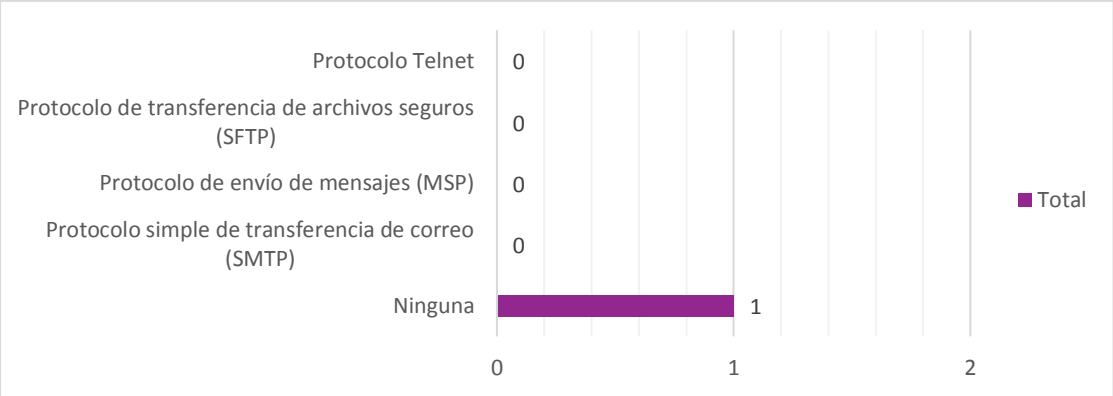
7.- La póliza de seguros que protege a los empleados en caso de un incidente con los equipos informáticos en el trabajo son:



8.- Cuando se accede a los servidores de la UTN de forma lógica se limita a:

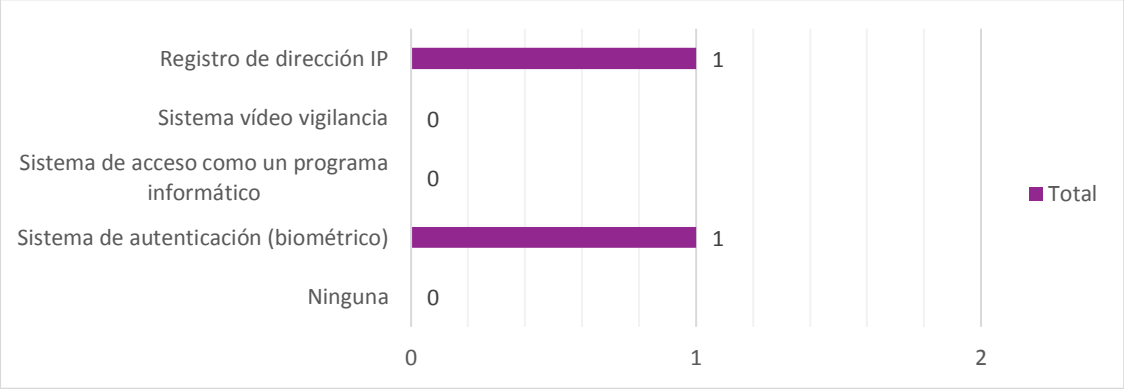


9.- ¿Se obliga al personal de la UTN a hacer uso de un tipo de protocolo o puerto en especial para la comunicación? Como:

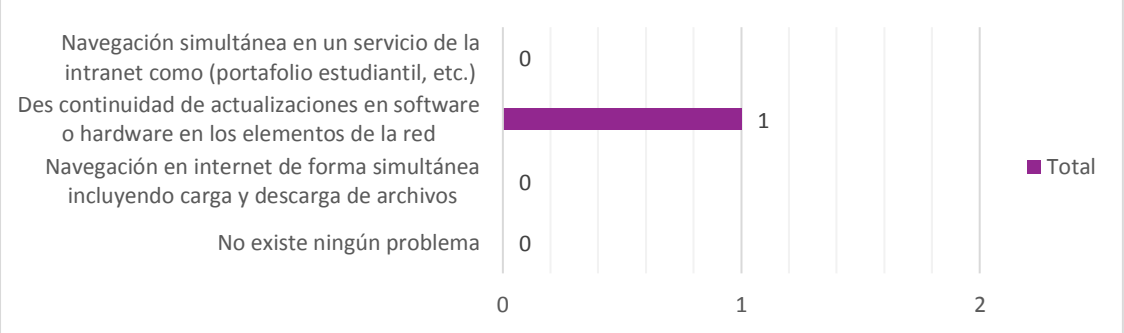


10.- En caso de daños en los servidores ¿Existen backups de respaldo para mitigar?

11.- ¿Qué tipos de sistemas existen para identificar el acceso no autorizado hacia la red de datos de forma física y lógica?



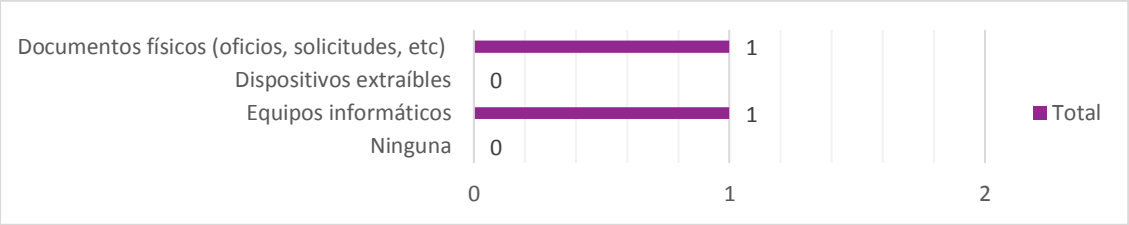
12.- Los cuellos de botella en la red se generan por:



13.- ¿Se hace uso de algún método para la confidencialidad de la información?

14.- En caso de suscitarse algún tipo de fallo con la red. ¿Se limitan los privilegios de acceso?

15.- ¿Qué elementos son introducidos y retirados de forma autorizada del DDTI?



Fotos

Puntos de acceso gratuitos de internet por cable dentro de la UTN

Fuente: Elaboración Propia