UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

"AUDITORÍA DE SEGURIDAD INFORMÁTICA EN LA RED INTERNA DE LA UNIVERIDAD TÉCNICA DEL NORTE SEGÚN LA METODOLOGÍA OFFENSIVE SECURITY PROFESSIONAL TRAINING AND TOOLS FOR SECURITY SPECIALISTS Y PLANTEAMIENTO DE POLÍTICAS DE SEGURIDAD BASADAS EN LA NORMA ISO/IEC 27001"

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

AUTOR: MARCELO WLADIMIR LEÓN GUDIÑO

DIRECTOR: ING. FABIÁN GEOVANNY CUZME RODRÍGUEZ

IBARRA-ECUADOR

2017

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

BIBLIOTECA UNIVERSITARIA

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

1.- IDENTIFICACIÓN DE LA OBRA

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

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

DATOS DEL CONTACTO	
Cédula de Identidad	100363671-7
Apellidos y Nombres	León Gudiño Marcelo Wladimir
Dirección	Juan de Salinas – Eugenio Borrero Casa 14
E-mail	mwleong@utn.edu.ec
Teléfono Fijo	062603310
Teléfono Móvil	0991329677
DATOS DE LA OBRA	

Título	"AUDITORÍA DE SEGURIDAD INFORMÁTICA EN LA RED INTERNA DE LA UNIVERIDAD TÉCNICA DEL NORTE SEGÚN LA METODOLOGÍA OFFENSIVE SECURITY PROFESSIONAL TRAINING AND TOOLS FOR SECURITY SPECIALISTS Y PLANTEAMIENTO DE POLÍTICAS DE SEGURIDAD BASADAS EN LA NORMA ISO/IEC 27001"
Autor	León Gudiño Marcelo Wladimir
Fecha	05 de junio del 2017
Programa	Pregrado
Título por el que se aspira:	Ingeniero en Electrónica y Redes de Comunicación
Director	Ing. Fabián Geovanny Cuzme Rodríguez

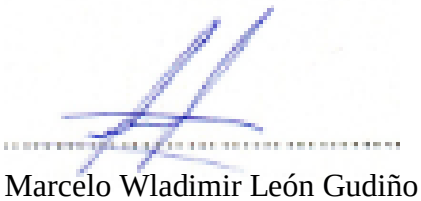
2.- AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, MARCELO WLADIMIR LEÓN GUDIÑO, con cédula de identidad Nro. 100363671-7, en calidad de autor y titular de los derechos patrimoniales del trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad de material y como apoyo a la educación, investigación y extensión, en concordancia con la ley de Educación Superior artículo 144.

3.- CONSTANCIAS

El auto 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 titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad Técnica del Norte en caso de reclamación por parte de terceros.

Ibarra, al 05 día del mes de junio del 2017



Marcelo Wladimir León Gudiño

100363671-7

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

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

Yo, MARCELO WLADIMIR LEÓN GUDIÑO, con cédula de identidad Nro. 100363671-7, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor del trabajo de grado denominado: "AUDITORÍA DE SEGURIDAD INFORMÁTICA EN LA RED INTERNA DE LA UNIVERIDAD TÉCNICA DEL NORTE SEGÚN LA METODOLOGÍA OFFENSIVE SECURITY PROFESSIONAL TRAINING AND TOOLS FOR SECURITY SPECIALISTS Y PLANTEAMIENTO DE POLÍTICAS DE SEGURIDAD BASADAS EN LA NORMA ISO/IEC 27001", que ha sido desarrollado para optar el título de Ingeniería en Electrónica y Redes de Comunicación, en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos concedidos anteriormente. En mi condición de autor me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

Ibarra, al 05 día del mes de junio del 2017

Marcelo Wladimir León Gudiño

100363671-7

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DECLARACIÓN

Yo, Marcelo Wladimir León Gudiño, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; y que éste no ha sido previamente presentado para ningún grado o calificación profesional.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Técnica del Norte, según lo establecido por las Leyes de Propiedad Intelectual, Reglamentos y Normatividad vigente de la Universidad Técnica del Norte

Marcelo Wladimir León Gudiño

100363671-7

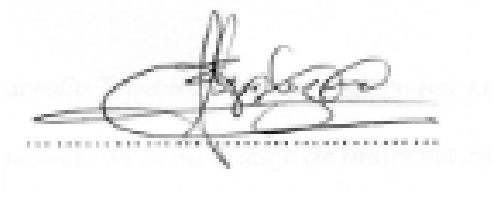
UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

Certifico que la Tesis "AUDITORÍA DE SEGURIDAD INFORMÁTICA EN LA RED INTERNA DE LA UNIVERIDAD TÉCNICA DEL NORTE SEGÚN LA METODOLOGÍA OFFENSIVE SECURITY PROFESSIONAL TRAINING AND TOOLS FOR SECURITY SPECIALISTS Y PLANTEAMIENTO DE POLÍTICAS DE SEGURIDAD BASADAS EN LA NORMA ISO/IEC 27001" ha sido realizada en su totalidad por el señor: MARCELO WLADIMIR LEÓN GUDIÑO portador de la cédula de identidad N° 100363671-7; previo a la obtención del Título de Ingeniero en Electrónica y Redes de Comunicación, bajo mi supervisión.

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



Ing. Fabián Geovanny Cuzme Rodríguez.

Cédula:131152701-2

Director de Tesis

AGRADECIMIENTO

En el presente proyecto agradezco a mi familia por haberme dado todo el apoyo en mi etapa estudiantil y ayudarme en el cumplimiento de mis objetivos.

A mi director de trabajo de grado, Ing. Fabián Cuzme por su esfuerzo y dedicación, quien con su experiencia y conocimiento supo guiarme en la terminación de este proyecto.

A la Universidad Técnica del Norte y la Facultad de Ingeniería en Ciencias Aplicadas, por haberme brindado las herramientas necesarias y base de conocimientos para el cumplimiento de mis años de estudio y formación profesional.

Al Departamento de Desarrollo Tecnológico e Informático por la confianza de sus dirigentes al permitir el desarrollo e implantación de mi trabajo de titulación en sus instalaciones.

Marcelo León

DEDICATORIA

Dedico este proyecto a mis padres Marcelo León Díaz y Susana Gudiño Román, a mis hermanas Susana, Gabriela y María Belén que son mi inspiración y un motivo para siempre seguir adelante y luchar por mis metas. A toda mi familia que siempre ha estado apoyándome en mis estudios.

Marcelo León

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

La implementación de medidas de seguridad en las instituciones es de suma importancia, debido a que en la actualidad existe la posibilidad de innumerables ataques cibernéticos. La seguridad en redes es un área fundamental dentro de las empresas; consiste en políticas adoptadas para prevenir y monitorear el acceso no autorizado, mal uso, denegación de servicios y equipos, sin embargo, poco se toma en cuenta. El mecanismo más adecuado para mejorar los niveles de seguridad en un sistema es la elaboración de auditorías informáticas en las redes institucionales, mismas que den paso a técnicas de control de funcionamiento, medidas de protección y análisis de riesgo.

La infraestructura de la red interna de la Universidad Técnica del Norte cuenta con equipamiento para brindar seguridad; el problema está en no tener políticas y procesos de seguridad que garanticen la integridad de la información y de los equipos. Anteriormente se ha registrado innumerables ataques a la red interna y sus aplicaciones, esto lo realizan personas sin ética que buscan vulnerabilidades en la red para realizar malas acciones queriendo indisponer los servicios informáticos. El portal Web de la institución es el principal objetivo de los atacantes, ya que es la aplicación con mayor cantidad de usuarios y cantidad de información en su base de datos.

En este contexto se realizó una auditoría de seguridad informática en la red interna de la casona universitaria mediante la metodología Offensive Security para buscar vulnerabilidades en la infraestructura de red, con la finalidad de elaborar políticas y procesos de protección en base a la norma ISO 27001; y con la retroalimentación del proceso de intrusión garantizar las soluciones propuestas, brindando una red mucho más confiable para el uso cotidiano y siempre la vanguardia.

ABSTRACT

The implementation of security measures in institutions is of the utmost importance, because at present there is the possibility of innumerable cyber-attacks. Network security is a fundamental area within companies; Consists of policies adopted to prevent and monitor unauthorized access, misuse, denial of services and equipment, however, little is taken into account. The most appropriate mechanism to improve the levels of security in a system is the elaboration of computer audits in institutional networks, giving rise to techniques for operational control, protection measures and risk analysis.

The infrastructure of the internal network of Universidad Técnica del Norte has equipment to provide security; The problem is not having security policies and processes that guarantee the integrity of information and equipment. Previously there have been countless attacks on the internal network and its applications, this is done by unethical people who look for vulnerabilities in the network to perform bad actions wanting to disrupt IT services. The Web portal of the institution is the main objective of the attackers, since it is the application with greater amount of users and amount of information in its database.

In this context, a computer security audit was carried out in the internal network of the university house through the Offensive Security methodology to search for vulnerabilities in the network infrastructure, with the purpose of elaborating policies and protection processes based on ISO 27001; And with the feedback of the intrusion process ensure the proposed solutions, providing a much more reliable network for everyday use and always the vanguard.

PRESENTACIÓN

El presente trabajo titulado "AUDITORÍA DE SEGURIDAD INFORMÁTICA EN LA RED INTERNA DE LA UNIVERIDAD TÉCNICA DEL NORTE SEGÚN LA METODOLOGÍA OFFENSIVE SECURITY PROFESSIONAL TRAINING AND TOOLS FOR SECURITY SPECIALISTS Y PLANTEAMIENTO DE POLÍTICAS DE SEGURIDAD BASADAS EN LA NORMA ISO/IEC 27001", se encuentra compuesto de los capítulos siguientes:

CAPÍTULO I: Antecedentes, En este capítulo se plantea el tema de estudio, el problema que se propone solucionar, los Objetivos (General y Específicos) planteados, el alcance del proyecto y la respectiva justificación, todo esto como antecedentes para la elaboración del presente proyecto.

CAPÍTULO II: Fundamento Teórico, Previo a la realización de la auditoria de seguridad informática se tiene la fundamentación teórica, se aborda temas de legislación de delitos informáticos Nacional e Internacional, conceptos básicos de seguridad informática y Ethical Hacking, teoría acerca de auditoría informática, fundamentos de la metodología y la norma que se va utilizar en la auditoría informática.

CAPÍTULO III: Aplicación de la metodología para la auditoría informática, En este capítulo se determinará la cantidad y tipos de ataques que se utilizará para la auditoria informática

en la red interna de la Universidad Técnica del Norte según la metodología OFFENSIVE SECURITY Professional Training and Tools for Security Specialists.

CAPÍTULO IV: Elaboración de Políticas de Seguridad, En este capítulo se recopilará toda la información de la auditoria informática que se efectuará en la red interna de la Universidad Técnica del Norte, para luego proceder a la elaboración de políticas y procesos de seguridad según la norma ISO/IEC 27001.

CAPÍTULO V: Implementación de las políticas de seguridad y pruebas de funcionamiento, En este capítulo se implementará soluciones a las vulnerabilidades encontradas por medio de políticas de seguridad según la norma ISO/IEC 27001, y se dejará como propuesta a la Universidad que se realice la certificación de un ente Internacional. También se realizará pruebas de funcionamiento en las cuales se demostrará la confiabilidad de la infraestructura de la red interna y los servicios de Internet.

Capítulo 1. Antecedentes.

El presente capítulo manifiesta de manera breve la necesidad de realizar una auditoría informática en la red interna de la Universidad Técnica del Norte, con la finalidad de mejorar la seguridad de la red, reconociendo el problema y brindado una solución detallada mediante la implementación de políticas de seguridad para los servicios de Internet, también se especifica en detalle las soluciones que se deben tomar ante cualquier incidente informático.

1.1. Tema.

Auditoría de seguridad informática en la red interna de la Universidad Técnica del Norte según la metodología OFFENSIVE SECURITY Professional Training and Tools for Security Specialists y planteamiento de políticas de seguridad basadas en la norma ISO/IEC 27001.

1.2. Problema.

En el último reporte por parte de la Fiscalía General del Estado acerca de delitos informáticos dice que desde el 10 de agosto del 2014 que entró en vigencia el Código Orgánico Integral Penal (COIP), se han reportado delitos como suplantación de identidad, espionaje, fraude, entre otros. En el departamento de tecnología y desarrollo informático (DDTI) se han reportado problemas de seguridad, como de acceso a personas no autorizadas a la red y denegación de los servicios afectando a la disponibilidad de los sistemas como es el caso del servidor web que se encuentra de acceso público.

La infraestructura de la red interna de la Universidad Técnica del Norte utiliza el Firewall Cisco ASA 5520, segmentación de red e IPS para la seguridad; pero no existen políticas de seguridad que garanticen la integridad de la información y de los equipos, se ha registrado innumerables ataques a la red interna en este centro de estudios por parte de personas sin ética que buscan vulnerabilidades en la red para realizar malas acciones queriendo neutralizar los servicios informáticos. Las fechas de matrículas es donde mayor cantidad de intrusiones tienen las aplicaciones debido a las caídas constantes de los servicios como por ejemplo la página Web de la Universidad, por tal motivo se requiere aplicar políticas de seguridad que aseguren la información y los servicios ante ataques informáticos y dar confiabilidad a los usuarios.

Se propone realizar una auditoría de seguridad informática en la red interna de la Universidad Técnica del Norte para buscar vulnerabilidades en la infraestructura de red con la finalidad de determinar políticas de seguridad necesarias; y mediante una retroalimentación del proceso de intrusión garantizará que las soluciones propuestas darán una red mucho más confiable de uso cotidiano.

1.3. Objetivos.

1.3.1. Objetivo general.

Realizar una auditoría informática en la infraestructura de la red interna de la Universidad Técnica del Norte utilizando la metodología OFFENSIVE SECURITY Professional Training and Tools for Security Specialists y la norma ISO/IEC 27001 para asegurar la integridad de la información mediante el planteamiento de políticas de seguridad.

1.3.2. Objetivos específicos.

Fundamentar teóricamente conceptos base acerca de legislación sobre delitos informáticos, la metodología de ataque Offensive Security y la norma ISO/IEC 27001 que se utilizarán durante el desarrollo del proyecto.

Analizar la situación actual de la infraestructura de la red interna, los equipos y el funcionamiento de los servicios DNS y WEB.

Aplicar la metodología OFFENSIVE SECURITY Professional Training and Tools for Security Specialists a la infraestructura de la red mediante un cierto número y tipo de ataques para la ejecución del test de penetración.

Implementar políticas de seguridad basado en la norma ISO/IEC 27001 para dar soluciones a las vulnerabilidades detectadas durante el proceso de intrusión a la red y servicios de internet.

Realizar pruebas de testing de intrusión con software libre para validar la implementación de las políticas de seguridad planteadas.

1.4. Alcance.

El presente proyecto de titulación consiste en implementar políticas de seguridad para la red interna de la Universidad Técnica del Norte que trabajan con los protocolos IPV4 e IPV6, esto se realizó mediante la utilización de una metodología de ataques y normas de seguridad acorde a los requerimientos del problema que tiene el servidor WEB con su respectivo DNS, y a su vez

poder reducir las vulnerabilidades de la red y brindar protecciones ante amenazas internas y externas.

Se analizó información acerca de legislación sobre delitos informáticos, la metodología de ataque Offensive Security para determinar objetivos de ataque dentro de la red y buscar vulnerabilidades en la infraestructura y la norma ISO/IEC 27001para la elaboración de políticas de seguridad para solventar los problemas de ataques que tiene la Universidad.

Se realizó un levantamiento de información de la situación actual de la infraestructura de la red interna, el equipamiento físico y lógico para conocer el sistema de seguridad tanto de hardware como de software que cuentan los servidores WEB y DNS; aquí se abordará las especificaciones y características de la red y los servicios.

Por otra parte se realizó un test de penetración a la red de servidores que están en internet, específicamente a los servicios de DNS y WEB que manejan los protocolos IPV4 e IPv6, aplicando la metodología OFFENSIVE SECURITY Professional Training and Tools for Security Specialists, para así determinar las vulnerabilidades que tienen el actual sistema de seguridad; esto se determinará mediante software libre de testeo de intrusiones para realizar pruebas de penetración y auditorias de seguridad.

Como siguiente paso se plantea políticas de seguridad basado en la norma ISO/IEC 27001, capaz de solventar las vulnerabilidades encontradas en el test de penetración a la infraestructura de red, buscando soluciones que reduzcan las falencias para que la UTN brinde servicios más seguros y de calidad evitando ataques internos y externos.

Una vez implementado las políticas de seguridad se realizó una nueva auditoría mediante pruebas de testing de intrusión para validar y garantizar las soluciones propuestas teniendo una red confiable de uso cotidiano.

1.5. Justificación.

La Universidad Técnica del Norte que en la actualidad posee una red de servicios de internet en IPV4 y algunos en IPV6, los cuales contienen gran cantidad de información para el personal administrativo, docente y estudiantil; esta infraestructura se encuentra vulnerable para que hackers informáticos sin ética profesional incurran en un delito, si bien es cierto la seguridad debe enmarcarse a nivel de toda la infraestructura tecnológica que tiene la UTN. El presente proyecto pretende dar un punto de partida en algunos de los servicios que han presentado mayor vulnerabilidad; dejando apertura a nuevas investigaciones que complementen a la que se realizó.

La auditoría informática se ejecuta aplicando la metodología OFFENSIVE SECURITY Professional Training and Tools for Security Specialists, la cual consiste en explotar las vulnerabilidades mediante pruebas de penetración, buscar soluciones a los errores encontrados y verificar que el problema se ha resuelto mediante un nuevo test; por otro lado se planteará políticas de seguridad tomando como base a la norma ISO/IEC 27001 que es un sistema de gestión de seguridad de la información que verifica independientemente que los riesgos de la organización estén correctamente identificados, evaluados y gestionados.

El presente proyecto tiene el compromiso ante la sociedad de cumplir con el “derecho al valor jurídico de los mensajes de datos y documentos escritos”, expuesta en (La Ley de Comercio

Electrónico, Firmas Electrónicas y Mensajes de Datos, 2002), y al derecho de la "conservación de los mensajes de datos", expuestas en el artículo 2 y 8 respectivamente. Debido a las vulnerabilidades de la información el Código Orgánico Integral Penal en el artículo 230 nos dice "La Interceptación ilegal de datos será sancionada con pena privativa de libertad de tres a cinco años" (COIP, 2015); las pruebas de penetración o más conocidas como auditorias informáticas nos sirven para buscar falencias en las redes de datos para que de alguna manera se reduzcan los delitos informativos.

El proyecto busca garantizar la seguridad, confidencialidad e integridad de la información que se encuentra en la infraestructura de la red interna de la Universidad, de esta manera se protegerá a diferentes ataques internos y externos para la casona universitaria. Este proyecto es un aporte significativo para que las áreas de trabajo mantengan un sistema seguro; de manera personal permite aumentar el conocimiento para la formación profesional en la carrera de Ingeniería Electrónica y redes de Comunicación en el campo de la seguridad informática.

Capítulo 2. Justificación Teórica.

En este capítulo se desarrolla el fundamento teórico que sirve para la elaboración del proyecto de titulación. Se analiza conceptos básicos acerca de la seguridad de datos, así como las plataformas y herramientas que sirven para realizar una auditoria informática. Mediante la guía de la norma ISO/IEC 27001 y la aplicación de la metodología OFENSIVE SECURITY respetando las normativas del COIP, la Ley de Comercio electrónico, entre otras.

2.1. Delitos Informáticos en el Ecuador.

El incremento de usuarios en la Internet por parte de entes empresariales hace que el riesgo de perder información crítica sea mayor, por tal motivo se requiere proteger y controlar el acceso a los sistemas. Cada año se incrementan los delitos informáticos, la Fiscalía General del Estado registró 626 denuncias de este tipo desde el 10 de agosto del 2014 hasta el 31 de mayo del 2015 cuando entró en vigencia el Código Orgánico Integral Penal (COIP), el cual se encarga de tipificar esta clase de transgresiones. (Fiscalía General del Estado, 2015)

2.2. Conceptos Básicos de Seguridad en Redes.

Es importante conocer varios términos que sirven de base para conceptualizar el tema de seguridad en las redes; los conceptos que involucran al desarrollo de una red segura corresponden a: activos que se van a proteger, los servicios de seguridad y las bases de seguridad.

2.2.1. Activos.

En términos tecnológicos, los activos: “Son los recursos que pertenecen al propio sistema de información o qué están relacionados con este”. (Aguilera, 2010)

2.2.1.1. ¿Qué son los datos?

En una organización los datos: “Constituyen el núcleo de toda organización, hasta el punto que se tiende a considerar que el resto de los activos están al servicio de la protección de datos”. (Aguilera, 2010)

2.2.1.2. ¿Qué es la información?

Se puede decir que de los datos sale la información, definiendo el término sería: “La información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente”. (Carlos Andrés Gil, 2008)

2.2.1.3. Software.

Según Aguilera (2010) se considera software a lo que está constituido por sistemas operativos y a las aplicaciones instaladas en los sistemas, encargadas de gestionar y transformar los datos al fin que estén establecidos.

2.2.1.4. Hardware.

La palabra hardware se refiere a todos los equipos que contienen al software, permitiendo su funcionamiento y que a su vez sirven de almacenamiento para la información del sistema.

2.2.1.5. Recurso humano.

Se conoce como recurso humano al conjunto de trabajadores que forman parte de una organización y a quienes cumplen con una lista de tareas y actividades específicas en una determinada área.

2.2.2. Servicios de seguridad.

La seguridad de la información se sustenta en 3 criterios fundamentales, que son los siguientes:

Confidencialidad. - Este criterio hace referencia a la privacidad de la información, la cual debe estar debidamente protegida de personas no autorizadas.

Integridad. - Se refiere a la capacidad de proteger la información ante alteraciones por parte de personas no autorizadas, con la finalidad de asegurar la consistencia de los datos que pueden ser externos o internos.

Disponibilidad. - Este término hace relación a que los sistemas tanto en hardware como en software puedan recuperarse ante un incidente y continuar con la producción en el menor tiempo posible.

Autenticación. - El sistema debe ser capaz de identificar a un usuario para que pueda acceder a él y poder tener acceso a la información o servicio requerido. La autenticación puede ser exigida antes, durante o al final de acceder a los datos.

No repudio. - Este servicio de seguridad: "consiste en no poder negar haber emitido una información que sí se emitió, y en no poder negar su recepción cuando sí ha sido recibida". Esto se puede dar en el origen cuando el emisor no puede negar el envío, o en el destino cuando el receptor no puede negar que recibió. (Aguilera, 2010)

2.2.3. Bases de la seguridad.

En la norma ISO 27001 que hace referencia en ISACA (2010) se tiene las siguientes bases de la Seguridad:

Prevención. - Es un proceso continuo de mejoramiento de la seguridad dentro de una organización.

Detección. – Consiste en la identificación oportuna de los ataques.

Respuesta. – Engloba las acciones a emprender cuando se origina una intrusión. Lo más común dentro de una organización es tener un plan de respuesta ante ataques informáticos y un plan de seguridad. (ISACA, 2010)

2.3. 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.

2.3.1. Definición de Hacker.

Este término ante la sociedad está mal interpretado, por lo general se piensa que es una persona que comete delitos informáticos, pero esto no es así, la verdadera definición es la siguiente:

"Una persona que se complace en tener una comprensión íntima del funcionamiento interno de un sistema, ordenadores y redes de ordenadores en especial. El término está mal dicho en un contexto peyorativo, donde "cracker" sería el término correcto". (Malkin G. , 1993)

2.3.2. Definición de Ethical Hacker.

Es un hacker experto considerado un analista de sistemas informáticos bien intencionado, una persona que tiene una visión clara del funcionamiento tanto en hardware y software; y que con esta información puede detectar las falencias de una aplicación con el objetivo de mejorar la seguridad de la organización ante ataques informáticos. (Rojas, 2014)

2.3.3. Pen Test.

Consiste en la realización de ciertas pruebas a los sistemas informáticos, para así identificar vulnerabilidades y el riesgo existente en la infraestructura de la red. Cuando un hacker está ejecutando un pen test el objetivo es acceder de un sistema a otro hasta llegar a su destino; proceso en el que se va escalando privilegios. (Allen Harper, 2015)

2.3.3.1. Tipos de Ataques.

En el artículo científico de Ramos (2008) menciona los siguientes tipos de ataques que se puede realizar en un Test de Penetración:

Acceso. - Este ataque consiste en acceder a sistemas no autorizados, la finalidad es vulnerar las barreras de defensa.

Modificación. - En este caso el atacante busca alterar la información, con el objetivo de afectar la integridad de la información.

Denegación de Servicio. - Es uno de los ataques más usados por personas mal intencionadas, consiste en que el atacante imposibilite los servicios que se encuentran en producción.

Refutación. - Este ataque consiste en rechazar el acceso de usuarios a los sistemas informáticos, tiene el propósito de bloquear el contacto entre servicio y persona. (Ramos, 2008)

2.3.3.2. Tipos de Pen Test.

El artículo de Ramos (2008) indica que el Pen Test se enfoca en lo siguiente:

Pruebas de penetración con objetivo. - Se realiza el test en secciones específicas de los sistemas informáticos críticos.

Pruebas de penetración sin objetivo. - El enfoque es global, es decir, se examina todos los componentes del sistema.

Pruebas de penetración a ciegas. - En este caso se utiliza información pública disponible.

Pruebas de penetración informadas. - Aquí se usa información privada la cual es dada por los dueños con el objetivo de simular ataques internos.

Pruebas de penetración externas. - Son ataques fuera de la red para probar la seguridad perimetral en la organización.

Pruebas de penetración internas. - Estas se realizan dentro de la red de la institución con el objeto de evaluar políticas internas de seguridad.

A su vez se tiene tres modalidades en los test de penetración, que son los siguientes:

Black-box. - En este caso el auditor no tiene conocimiento de los sistemas, el cliente solo proporciona el nombre de la organización para que realice el ataque, simulando una posible intrusión externa.

White-box. - El auditor en este punto tiene conocimientos detallados del sistema, este caso sirve para simular ataques provenientes de personas que tengan información del sistema.

Gray-box. - El auditor tiene acceso limitado al sistema, la idea es encontrar problemas que puedan ser aprovechados por empleados internos. (Ramos, 2008)

2.4. Auditoría.

Auditoría se refiere a: "la actividad para determinar, por medio de la investigación, la adecuación de los procedimientos establecidos, instrucciones, especificaciones, codificaciones y estándares u otros requisitos, la adhesión a los mismos y la eficiencia de su implantación" (Baudes, 2002), la cual nos ayuda a identificar la situación en la que se encuentra una organización, es decir, que calidad de servicio existe.

2.4.1. Auditoría informática.

Es la técnica para evaluar la seguridad informática en una empresa; comprende un examen metódico con la finalidad de mejorar la rentabilidad, seguridad y la eficacia del sistema. Requiere una metodología establecida, determinar fechas precisas y la realización por parte de una persona extraña al servicio informático.

2.4.1.1. Objetivos auditoría interna.

- Revisión y evaluación de controles contables, financieros y operativos.

- Determinación de la utilidad de políticas, planes y procedimientos, así como su nivel de cumplimiento.
- Custodia y contabilización de activo.
- Examen de la fiabilidad de datos.
- Divulgación de políticas y procedimientos establecidos.
- Información exacta a la gerencia.

2.4.1.2. Objetivos auditoría externa.

- Obtención de elementos de juicio fundamentados en la naturaleza de los hechos examinados.
- Medición de la magnitud de un error ya conocido, detección de errores supuestos o confirmación de la ausencia de errores.
- Propuesta de sugerencias, en tono constructivo, para ayudar a la gerencia.
- Detección de los hechos importantes ocurridos tras el cierre del ejercicio.
- Control de las actividades de investigación y desarrollo.

2.4.2. Importancia de una auditoría informática.

Con el avance de la tecnología en las comunicaciones, se ha incrementado los ciberdelitos y la información cada día es más vulnerable. La finalidad de realizar una auditoria informática es determinar errores y fallos en el sistema de una organización, adicionalmente con esto se busca evaluar los sistemas para mejorarlos y tener mayor eficiencia y eficacia en la organización. (Baudes, 2002)

2.5. Offensive Security.

Actualmente se tiene varias metodologías a disposición para realizar una auditoría informática, sin embargo, se eligió la metodología OFFENSIVE SECURITY porque esta permite validar las soluciones propuestas por el auditor.

En el sitio Web de Isaza (2013) se define a OFFENSIVE SECURITY como una metodología a nivel mundial que permite realizar pruebas de intrusión y estudios sobre la seguridad informática. Se fundamenta principalmente en estudiar la seguridad ofensiva para explotar las vulnerabilidades. Como principales ventajas tiene:

- Explotación en plataformas reales.
- Es netamente intrusivo.
- Los resultados no se basan en estadísticas generadas por herramientas, sino en los resultados del pen test.

En la Figura 1 se tiene las siguientes etapas de la metodología Offensive Security:

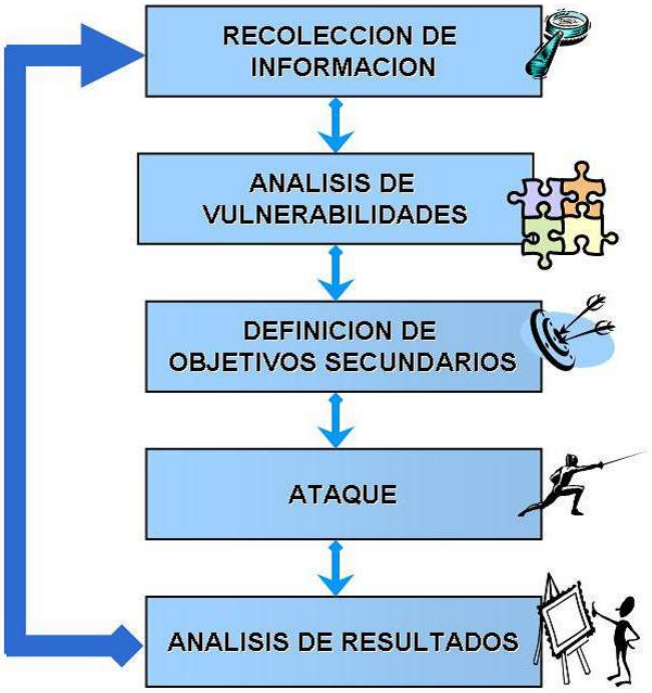


Figura 1. Etapas de la Metodología Offensive Security.
Fuente: Recuperado de https://seguridadinformaticahoy.blogspot.com/2013/02/metodologias-y-herramientas-de-ethical.html

Etapa 1: Recolección de información.

En esta etapa se identifica los objetivos que se van atacar partiendo de dos posibles escenarios:

- Pruebas ciegas, es decir, no se tiene información del cliente.
- Pruebas con información, esto es cuando el cliente proporciona cierta información al auditor.

Etapa 2: Análisis de Vulnerabilidades.

Esta fase consiste en determinar problemas de seguridad en los objetivos fijados en la primera fase. Puede realizarse de manera manual o automática por medio de software de auditoría, esto depende de la organización, una vez que se detecta las vulnerabilidades del sistema se identifica la estrategia con la cual se realizará el pent testing.

Etapa 3: Definición de objetivos.

Finalizando la segunda etapa los objetivos tienden a ser más precisos, aumentando la probabilidad de que los ataques sean exitosos. Para poder determinar el riesgo real que existe en el sistema, es necesario tener en cuenta objetivos secundarios que puedan servir de medio para llegar hasta los objetivos principales, a esto se conocer como escalar privilegios.

Etapa 4: Ataque.

Se ejecuta los ataques a los objetivos seleccionados en la anterior etapa, usando las vulnerabilidades encontradas. Aquí se prueba la existencia real de problemas de seguridad del sistema. Durante la ejecución de las intrusiones, es posible que surjan nuevas vulnerabilidades que no se detectaron antes, las cuales serán tomadas en cuenta dentro de esta misma fase.

Etapa 5: Análisis de Resultados.

En esta fase se analiza los resultados de los ataques, se toma en cuenta si se logró mejorar la seguridad del sistema, caso contrario, se repite el ciclo o se finaliza las pruebas y se realiza el último paso.

Análisis Final y Documentación.

Se debe realizar un informe detallado que abarque los resultados obtenidos durante la ejecución del pen test con el correspondiente análisis de la información y las respectivas soluciones ante los problemas de seguridad encontrados.

Adicionalmente se incluye:

- Aspectos positivos encontrados en el sistema.
- Aspectos en los que se puede mejorar el sistema. (Isaza, 2013)

2.6. La ISO (Intertational for Standardization).

La ISO (International Organization for Standardization), es una organización mundial de normalización que tiene alrededor de 160 países, los cuales manejan alrededor de 19000 estándares publicados desde su creación.

La finalidad de las Normas Internacionales de la ISO es proporcionar herramientas para que se trabaje en el mundo real, en campos como la salud y la seguridad, entre otros. Las normas

aseguran que los productos y servicios sean seguros, confiables y de buena calidad; para una institución son herramientas que sirven para aumentar la productividad y ayudar al desarrollo de l misma. (Collazos Balaguer, 2013)

2.6.1. Norma ISO/IEC 27001.

La norma está vigente desde el año 2013, específicamente se enfoca en Sistemas de Gestión de la Seguridad de la Información (SGSI); determina 130 requisitos para que se encuentre avalado, como se visualiza en la Tabla 1.

La estructura de la ISO 27001 básicamente tiene dos etapas como se muestra en la Figura 2, las cuales son una guía para la elaboración e implementación de las políticas de seguridad.

Figura 2. Estructura de ISO 27001
Fuente: Recuperado de https://advisera.com/27001academy/es/que-es-iso-27001/

Por otra parte, la norma se basa en cumplir con el SGSI que tiene como principio la (CIA), que es ofrecer Confidencialidad, Integridad y Disponibilidad de la información, buscando con ello la confianza entre organización y el cliente. (ISO, 2013)

Tabla 1 Norma ISO 27001

#	CLÁUSULAS	APARTADOS
0	Introducción	
1	Alcance	
2	Referencias normativas	
3	Términos y definiciones	
4	Contexto de la organización	4.1 Compresión de la organización y su contexto. 4.2 Comprensión de las necesidades y expectativas de las partes interesadas. 4.3 Determinación del alcance del sistema de gestión de continuidad de negocios. 4.4 Sistema de Gestión de Continuidad de Negocios
5	Liderazgo	5.1 Liderazgo y compromiso 5.2 Compromiso gerencial 5.3 Política 5.4 Roles, responsabilidades y autoridades de la organización.
6	Planificación	6.1 Acciones para atender los riesgos y las oportunidades. 6.2 Objetivos de continuidad de negocios y planes para lograrlos.

7	Soporte	7.1 Recursos 7.2 Competencia 7.3 Concientización 7.4 Comunicación 7.5 Información a documentar
8	Operación	8.1 Planificación y control operacional. 8.2 Análisis de impactos en los negocios y valuación de riesgos. 8.3 Estrategia de continuidad de negocios y planes para lograrlos. Establecimiento e implementación de los procedimientos de continuidad de negocios. 8.4 Establecimiento e implementación de los procedimientos de continuidad de negocios. 8.5 Ejercicios y pruebas.
9	Evaluación del desempeño	9.1 Monitoreo, medición, análisis y evaluación 9.2 Auditoría Interna. 9.3 Revisión gerencial.
10	Mejoramiento	10.1 No conformidades y acciones correctivas. 10.2 Mejoramiento continuo.

Fuente: Norma ISO/IEC 27001

2.6.1.1. Implementación de la ISO/IEC 27001.

Para implementar la norma ISO/IEC 27001 es necesario seguir las siguientes fases:

Fase 1.- Definición del alcance (scope) y los límites de SGSI.

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

Fase 2.- Definición de la política de la seguridad.

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

Fase 3.- Identificación de los activos de la empresa y sus riesgos asociados. ¿Dónde están las debilidades? ¿Qué amenazas hay que tener en cuenta?

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

Fase 4.- Control de riesgos.

En esta fase es necesario realizar las siguientes preguntas: ¿Qué riesgos se corren? y ¿son asumibles?

Fase 5.- Fijación de controles y objetivos.

En esta fase se termina los objetivos de control que debemos tener para la seguridad de la empresa.

Fase 6.- Definición de la Declaración de Aplicabilidad, la conocida SOA (Statement of Applicability), de la norma ISO/IEC 27001.

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

2.6.2. Sistema de gestión de la seguridad de la información.

En esta sección se define, se explica para qué sirve y cómo se implementa un SGSI; además de los sistemas de gestión que se pueden integrar.

2.6.2.1. Definición de SGSI.

SGSI es la abreviatura correspondiente a Sistema de Gestión de la Seguridad de la Información. Consiste en la preservación de la confidencialidad, integridad y disponibilidad de los datos de una red.

2.6.2.2.¿Para qué sirve un SGSI?

Puesto que toda información es susceptible de amenazas, aprovechando cualquier vulnerabilidad que tenga el sistema, se puede someter a los activos críticos de la información a diversos delitos informáticos, por ejemplo: fraude, espionaje, sabotaje o vandalismo.

El nivel de protección en una red que se puede alcanzar por medios técnicos es limitado, por ello es indispensable que el SGSI lo complemente por medio de procedimientos adecuados y la planificación e implementación de controles de seguridad basados en la evaluación de riesgos para poder medir su eficacia.

2.6.2.3. ¿Cómo se implementa un SGSI?

Para la implementación de un SGSI en base a la ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de calidad.

- Plan (planificar): establecer el SGSI.
- Do (hacer): Implementar y utilizar el SGSI.
- Check (verificar): monitorizar y revisar el SGSI.
- Act (actuar): mantener y mejorar el SGSI.
- Definir el alcance del SGSI en términos de la organización, de localización, activos y tecnologías.
- Definir una política de seguridad que: incluya el marco general y los objetivos de seguridad de la información de la organización; requerimientos legales relativos a

la seguridad de la información, evaluación de riesgos, gestión de riesgos, y por último sea aprobada por la dirección.

2.6.2.4. Sistemas de gestión que se integran al SGSI.

Los sistemas de gestión que se integran al SGSI son estándares internacionales de sistemas de gestión, tanto para, la calidad de gestión (ISO 9001), para el impacto ambiental (ISO 14001), en el caso de la prevención de riesgos laborales (OHSAS 18001), y el estándar para la gestión de seguridad de la información (ISO 27001).

2.6.3. Metodologías de análisis de riesgo.

La Norma ISO/IEC 27001 no establece métodos a seguir para el análisis de riesgos, por lo cual para el desarrollo del presente trabajo se ha realizado una comparación entre las metodologías de análisis y gestión de riesgos de los sistemas de información.

2.6.3.1.Magerit.

El análisis de riesgos bajo las directrices de la metodología Magerit proporciona al usuario una herramienta completa, por medio de una estructura sistemática en la que se ofrece todo lo necesario para analizar las contingencias derivadas del uso de tecnologías de la información y comunicación con el objetivo de descubrir cuáles son los posibles riesgos a los que está expuesta la seguridad de la institución y gestionarlos por medio de un exhaustivo control.

Objetivos de Magerit.

- Concientizar a los responsables de la información dentro de las organizaciones sobre la existencia de riesgos y la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento oportuno de riesgos.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda cada caso. (Ministerio de Obras Públicas, 2012)

Software Pilar.

Según Ortiz Beltrán (2015):

"Cada activo sometido al análisis de riesgos involucra gran cantidad de datos, conforme el procedimiento continúa y se aumenta la cantidad de activos el volumen total del proyecto adquiere un gran tamaño y gestionar toda aquella información se torna difícil, por tal razón se utiliza el software PILAR". (p. 36)

PILAR llamado así por sus siglas (procedimiento informático lógico para el análisis de riesgos) es un programa acoplado a los requerimientos de Magerit que se utiliza para análisis de riesgos.

2.6.3.2.Norma ISO 27005.

La Norma ISO 27005 es un estándar internacional que se fundamenta en la gestión de riesgos de seguridad de la información apoyando los requisitos del sistema de gestión de seguridad según la norma ISO 27001; la intención es aplicar un análisis de riesgos que se pueda aplicar en cualquier organización. (Ramirez, 2013)

2.6.3.3. Metodología Octave.

Octave (Operationally Critical Threat, Asset and Vulnerability Evaluation) es una metodología de análisis de riesgos para la seguridad de TI, con la finalidad de que la organización dirija y gestione evaluaciones de riesgos para tomar decisiones en base a los riesgos y a su vez proteger los activos claves de la información para finalmente comunicar de manera efectiva la información clave. (ISACA, 2010)

2.6.3.4. Metodología BAA.

La metodología de análisis de riesgo BAA, trae como beneficios para el atacante, la accesibilidad y la anonimidad. Además, ésta permite realizar una clasificación de los datos personales en función de las variables anteriores, con la finalidad de ponderar el riesgo e identificar la información en orden de prioridad para tener en cuenta las necesidades de protección más relevantes. (INAI, 2014)

Tabla 2 Metodologías de análisis de riesgo.

DETALLE	MAGERIT	ISO 27005	OCTAVE	BAA
Características principales.	-Concientiza a los responsables de la organización de la necesidad de gestionar los riesgos. -Ofrece un método sistemático para analizar los riesgos con el uso de las TIC. -Prepara a la organización para ser evaluada según corresponda el caso.	-Directrices para la ejecución del análisis de riesgo. -Nació para apoyar la tarea del SGSI. -Apoya a los conceptos expuestos en la norma ISO 27001.	-Construye perfiles de amenazas según los activos. -Identifica las vulnerabilidades de la infraestructura. -Desarrolla planes y estrategias de seguridad.	-Beneficio para el atacante: los datos personales de mayor beneficio son los que tienen más riesgo de ser atacados. -Accesibilidad del atacante: son datos de fácil acceso con mayor riesgo de ser atacados. -Anonimidad del atacante: datos que representan anonimidad es probable que sea atacado.
Fases de Método de Análisis de Riesgo.	-Identifica a los activos. -Identifica las amenazas. -Determina las salvaguardas que están dispuestas y qué tan eficaces son ante amenazas. -Estima el impacto sobre el activo. -Estima el riesgo.	-Alcance -Normativas de referencia. -Términos y directrices. -Estructura. -Antecedentes. Visión del progreso de gestión de riesgos de seguridad de la información.	-Visión organizativa, se refiere a la construcción de activos en perfil de amenazas. -Visión tecnológica, se refiere a la identificación de vulnerabilidades. -Desarrollo de estrategias del plan de seguridad.	-Identificación y clasificación de datos personales. -Análisis de riesgos de datos personales. -Identificación de medidas de seguridad. -Optimización de los niveles de riesgo. -Inventario de datos y sistemas de tratamiento.

		-Establecimiento del contexto. -Evaluación de riesgos. -Tratamiento de riesgo. -Aceptación del riesgo. -Comunicación del riesgo. -Monitorización y revisión del riesgo.	-Análisis y evaluación.	
Ámbito de aplicación.	Se puede aplicar al Gobierno, Organismos, Compañías Grandes, PYME, Compañías Comerciales y no Comerciales. Ofrece una aplicación para el análisis de riesgos y su gestión llamada PILAR (Proceso informático lógico para el análisis de gestión de negocios), esta herramienta es libre.	Puede aplicar en cualquier organización pública o sociedades, organizaciones no lucrativas, agencias públicas, ONGs o bien la entidad que gestione un SGSI. La intención es manejar los riesgos que pueden comprometer la seguridad de la información.	Usa como herramientas una aplicación llamada OCTAVE Automated Tool. Aplica a PYME, para pequeñas y medianas empresas.	Se puede aplicar a cualquier tipo de empresa que tenga información crítica. Usa como base la norma ISO 27002.
Ventajas	-Es metódica, es decir, de fácil comprensión.	-Identifica necesidades de la organización y	-Aplica criterios (atributos y resultados)	-Esta metodología se basa en el tratamiento de los datos personales.

	-Los activos son identificados. -Busca cumplir con: disponibilidad, autenticidad, integridad y trazabilidad. -Comprende los procesos de análisis y gestión de riesgos, mediante un método cuantitativo y cualitativo. -Soporta herramientas EAR, PILAR y normas ISO.	requisitos para su seguridad. -Ayuda a crear los SGSI. -Aborda riesgos de manera eficaz y oportuna según lo necesite. -Integridad para todas las actividades de gestión de seguridad.	compatibles con OCTAVE. -Involucra a todo el personal de la organización. -Es de las más completas ya que involucra en el modelo análisis de riesgos: procesos, activos, recursos, vulnerabilidades, amenazas y salvaguardas.	-Se fundamenta con la norma ISO 27002. -Identifica el riesgo por el tipo de dato. -Optimiza los niveles de riesgo. -Se utiliza listas de control y patrones de control para tomar medidas de seguridad.
Desventajas	-No toma en cuenta el principio de no repudio de la información. -No analiza vulnerabilidades. -No incluye recomendación de controles dentro del análisis de riesgos, sino en gestión y evaluación. -La estimación del impacto se ejecuta en el proceso de gestión y evaluación de riesgos.	No recomienda una metodología concreta, depende de factores que se vaya a implementar.	-Aplicable solo en PYME, pequeña y mediana empresa. -No es compatibles con estándares.	-No tiene como herramientas un software, todo es en base de cálculos cuantitativos y cualitativos; mediante la utilización de tablas para representar el riesgo.

Fuente**:** Recuperado de http://es.slideshare.net/abbyramirez89/anlisis-comparativo-50183515

En la Tabla 2 se realiza la comparación de metodologías de análisis de riegos para tomar una decisión en cuanto a la utilización de una de ellas; esto dependerá de la que mejor se adapte a la norma ISO 27001 y a los requerimientos de la institución.

2.7. Legislación del Ecuador Relacionadas con Delitos Informáticos.

En el Ecuador existen varias leyes y sanciones relacionadas a los delitos informáticos, en esta sección se detalla lo correspondiente a las sanciones por vulnerar la red interna y los servicios de una página WEB con su respectivo DNS. Entre estas se encuentran:

- Constitución de la República del Ecuador.
- Ley Orgánica de Transparencia y Acceso a la Información Pública. (Lotaip)
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
- Ley de Propiedad Intelectual.
- Ley Especial de Telecomunicaciones.
- Ley de Control Constitucional. (Reglamento Habeas Data)
- Ley Orgánica de Comunicación.
- Código Orgánico Integral Penal. (COIP)

2.7.1. Constitución de la República del Ecuador.

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

la existencia del Ecuador y quienes han de gobernar. En ella se estipula los principios por los cuales han sido creadas todas las leyes incluyendo las mencionadas en esta sección. (Asamblea Nacional del Ecuador, 2008)

2.7.2. Ley Orgánica de Transparencia y Acceso a la Información Pública.

La Ley Orgánica de Transparencia y Acceso a la Información Pública en el Registro Oficial Suplemento 337 del 18 de mayo del 2004 se basa en los artículos 18,91 y 92 de nuestra Constitución que garantizan el derecho de los ciudadanos a buscar, recibir, intercambiar, producir o difundir información con responsabilidad sobre sí misma, o sobre sus bienes existente en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas.

Mediante esta ley la ciudadanía puede conocer lo que sucede en el país, cuáles son las decisiones adoptadas, quién las toma, porqué causas, etc. Además, facilita el control de los recursos, la rendición de cuentas, la fiscalización de recursos públicos, es decir, fomenta una sociedad más democrática. (Asamblea Nacional del Ecuador, 2008)

2.7.3. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

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

“Art. 1.- Objeto de la ley. - Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas”.

“Art. 4.- Propiedad intelectual. - Los mensajes de datos serán sometidos a las leyes, reglamentos y acuerdos internacionales relativos a la propiedad intelectual”.

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

“Art. 8.- Conservación de los mensajes de datos. - Toda información sometida a esta Ley, podrá ser conservada; este requisito quedará cumplido mediante el archivo del mensaje de datos, siempre que se reúnan las siguientes condiciones”:

Que la información que contenga sea accesible para su posterior consulta;

Que sea conservado con el formato en el que se haya generado, enviado o recibido, o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida;

Que se conserve todo dato que permita determinar el origen, el destino del mensaje, la fecha y hora en que fue creado, generado, procesado, enviado, recibido y archivado; y,

Que se garantice su integridad por el tiempo que se establezca en el reglamento a esta ley.

Toda persona podrá cumplir con la conservación de mensajes de datos, usando los servicios de terceros, siempre que se cumplan las condiciones mencionadas en este artículo.

La información que tenga por única finalidad facilitar el envío o recepción del mensaje de datos, no será obligatorio el cumplimiento de lo establecido en los literales anteriores.

"Art. 9.- Protección de datos. - Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros".

La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.

No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.

"Art. 10.- Procedencia e identidad de un mensaje de datos. - Salvo prueba en caso contrario se entenderá que un mensaje de datos proviene de quien lo envía y, autoriza a quien lo recibe, para actuar conforme al contenido del mismo, cuando de su verificación exista concordancia entre la identificación del emisor y su firma electrónica, excepto en los siguientes casos":

Si se hubiere dado aviso que el mensaje de datos no proviene de quien consta como emisor; en este caso, el aviso se lo hará antes de que la persona que lo recibe actúe conforme a dicho mensaje. En caso contrario, quien conste como emisor deberá justificar plenamente que el mensaje de datos no se inició por orden suya o que el mismo fue alterado; y,

Si el destinatario no hubiere efectuado diligentemente las verificaciones correspondientes o hizo caso omiso de su resultado. (Asamblea Nacional del Ecuador, 2008)

2.7.4. Ley de Propiedad Intelectual.

La Ley de Propiedad Intelectual publicada en el Registro Oficial No 320 del 19 de mayo de 1998 considera la protección de las creaciones intelectuales como un derecho fundamental de los ecuatorianos fomentando así la libre competencia y el desarrollo tecnológico y económico del país.

Esta ley fue creada para proteger las invenciones en todos los campos de la tecnología, programas de ordenador, obras audiovisuales, obras arquitectónicas, obras de artes plásticas, entre otras, mediante la concesión de patentes de invención o de procedimientos siempre y cuando la adquisición sea legal.

Los autores de las creaciones intelectuales pueden acogerse a la no divulgación de la información, misma que puede referirse a las características o finalidades de los productos; a los métodos o procesos de producción; la configuración y composición precisas de sus elementos; o, a los medios o formas de distribución o comercialización de productos o prestación de servicios.

Se protege la información no divulgada relacionada con los secretos comerciales, industriales o cualquier otro tipo de información confidencial contra su adquisición, utilización o divulgación no autorizada del titular.

Según el artículo 83 de la presente ley también se considera como “Información no divulgada el conocimiento tecnológico integrado por procedimientos de fabricación y producción en general; y, el conocimiento relativo al empleo y aplicación de técnicas

industriales resultantes del conocimiento, experiencia o habilidad intelectual, que guarde una persona con carácter confidencial".

Según los artículos 3 y 346 de la presente ley, el IEPI es un organismo con autonomía administrativa, económica, financiera, operativa y patrimonio propio que posee la facultad para velar por el cumplimiento y respeto de los principios establecidos en esta ley, el respeto de los derechos de propiedad intelectual, promover y fomentar la creación intelectual en todos los campos de la producción, así como la difusión de los conocimientos tecnológicos dentro de los sectores culturales y productivos; y establecer medidas preventivas que pongan en riesgo la propiedad intelectual y la libre competencia. (Asamblea Nacional del Ecuador, 2008)

2.7.5. Ley Especial de Telecomunicaciones.

La Ley Especial de Telecomunicaciones fue publicada en el Registro Oficial No 770 del 30 de agosto de 1995, en la que se declara a los servicios de telecomunicaciones como un sector estratégico y de gran importancia para el desarrollo del país, por lo que es necesaria la creación de un marco legal que regule y gestione la prestación de los servicios radioeléctricos y de telecomunicaciones.

Esta ley regula en todo el territorio nacional la instalación y operación de los sistemas de transmisión y recepción de información video, voz y datos a través de cualquier tipo de medio de transmisión sea misma electromagnéticos, medios ópticos, radioeléctricos entre otros.

Mediante esta ley se establece el control de los servicios de telecomunicaciones portadores y finales, declara que los servicios públicos tienen la prioridad en la obtención de títulos habilitantes y asignación de frecuencia. El CONATEL es el organismo que protege y promueve la libre competencia, control en la prestación de servicios de las diferentes empresas y fomentar la interconexión de los diferentes prestadores de servicios.

Según el artículo 22 de la presente ley se define como un Servicio Universal a la obligación de extender el acceso de un conjunto definido de servicios de telecomunicaciones a todos los habitantes del territorio nacional; si los prestadores de servicios no establecen proyectos de Servicio Universal, los fondos del FODETEL financiarán dichos proyectos. (Asamblea Nacional del Ecuador, 2008)

2.7.6. Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional.

La ley orgánica de garantías jurisdiccionales y control constitucional fue publicada en el Registro Oficial No 52 del 22 de octubre del 2009.

En la Constitución Política de la República del Ecuador en su artículo 92 establece la acción de hábeas data como un derecho de los ciudadanos "a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico."

FODETEL: Fondo para el Desarrollo de las Telecomunicaciones en Áreas Rurales y Urbano-Marginales.

Según los artículos 1, 6 y 74 del presente reglamento, esta ley tiene la misión de regular la jurisdicción constitucional para garantizar los derechos establecidos en la Constitución y la inviolabilidad de los tratados internacionales en materia de derechos humanos y medio ambiente; como también garantizar la unidad y coherencia del ordenamiento jurídico a través de la identificación y la eliminación de las incompatibilidades normativas, por razones de fondo o de forma. (Asamblea Nacional del Ecuador, 2008)

2.7.7. Ley Orgánica de Comunicación.

La ley orgánica de comunicación fue publicada en el registro oficial No 22 el 25 de junio del 2013 cuyas facultades corresponden el desarrollar, proteger y regular el derecho a todo tipo de información u opinión de las personas ecuatorianas, extranjeras y compatriotas residentes en el exterior a través de los medios de comunicación social en base a la correcta explotación de las tecnologías de información.

El derecho al acceso universal a las tecnologías de la información y comunicación se expresa en el artículo 35 en el que se confiere a todas las personas el derecho al acceso, la capacitación y uso de las tecnologías de información y comunicación para potenciar el disfrute de sus derechos y oportunidades de desarrollo. (Asamblea Nacional del Ecuador, 2008)

2.7.8. Código Orgánico Integral Penal.

El Código Penal es un instrumento del Estado para sancionar o imponer penas a quienes se hallaron culpables en la materialización de un delito tipificado en la ley, el

antiguo código ha sido modificado por varias leyes entre las que constan la ley de comercio electrónico, firmas electrónicas y mensajes de datos publicada en el Registro Oficial Suplemento No. 577 de 17 de abril de 2002.

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

"No son aplicables estas normas para la persona que divulgue grabaciones de audio y video en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley".

Si bien es cierto una página web es de uso público, el acceso a los servidores está totalmente restringido, es decir si una persona accede al servidor WEB o DNS de una institución sin contar con el consentimiento del administrador o sin tener la autorización legal a la información contenida en algún soporte informático, está cometiendo un delito informático.

"Artículo 188.- Aprovechamiento ilícito de servicios públicos.- La persona que altere los sistemas de control o aparatos contadores para aprovecharse de los servicios públicos de energía eléctrica, agua, derivados de hidrocarburos, gas natural, gas licuado de petróleo o de telecomunicaciones, en beneficio propio o de terceros, o efectúen conexiones directas, destruyan, perforen o manipulen las instalaciones de transporte,

comunicación o acceso a los mencionados servicios, será sancionada con pena privativa de libertad de seis meses a dos años".

"La pena máxima prevista se impondrá a la o al servidor público que permita o facilite la comisión de la infracción".

"La persona que ofrezca, preste o comercialice servicios públicos de luz eléctrica, telecomunicaciones o agua potable sin estar legalmente facultada, mediante concesión, autorización, licencia, permiso, convenios, registros o cualquier otra forma de contratación administrativa, será sancionada con pena privativa de libertad de uno a tres años".

De acuerdo con este artículo del COIP alterar o usar un servicio público para beneficio propio o de terceros es un delito, en el caso de que un atacante altere el sistema de control de los servidores y lo use para darse publicidad o comercialice servicios ajenos a la institución, y lo realice por este medio de telecomunicaciones que es la página WEB.

"Artículo 190.- Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años".

"La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia o violación de seguridades electrónicas, informáticas u otras semejantes".

Obtener claves secretas o encriptadas que sirven de acceso para un sistema de telecomunicaciones, y a su vez usarlas para desactivar estos dispositivos es considerado un delito según el COIP.

"Artículo 212.- Suplantación de identidad. - La persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa libertad de uno a tres años".

Suplantar la identidad de un administrador de red o de algún servidor especifico y utilice esto para beneficio propio o de terceros viene a ser un delito informático según lo que nos dices este artículo del COIP.

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

"Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años".

La revelación de información contenida en una base de datos es un delito muy grave, ya que va en contra de la confidencialidad de la información, este es un derecho que debe prevalecer, por lo tanto, toda base de datos debe estar debidamente protegida ante ataques informáticos.

"**Artículo 230.- Interceptación ilegal de datos. -** Será sancionada con pena privativa de libertad de tres a cinco años":

"La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible".

"La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder".

"La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares".

"La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior".

Este artículo se refiere al delito de interceptación de datos, es permitido entrar a un sistema de telecomunicaciones solamente con una orden judicial, de igual manera es considerado un delito robar o clonar algún sistema y comercializarlo, como también producir herramientas y dispositivos para realizar robos informáticos.

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

Con igual pena será sancionada la persona que:

"Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo".

"Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general".

"Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de la libertad".

La integridad de la información es un derecho que todos, el uso mal intencionado que buscan destruir o alterar equipos donde se contenga datos informáticos se considera también como un delito tipificado.

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

Los sistemas informáticos por lo general son privados, el acceso no consentido a estos sistemas es considerado un delito de acuerdo con este artículo ya que existen graves riesgos hacia los datos en ellos contenidos.

"Articulo 500.- Contenido Digital. - El contenido digital es todo acto informático que representa hechos, información o conceptos de la realidad, almacenados, procesados

o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí".

En la investigación se seguirán las siguientes reglas:

"El análisis, valoración, recuperación y presentación del contenido digital almacenado en dispositivos o sistemas informáticos se realizará a través de técnicas digitales forenses".

"Cuando el contenido digital se encuentra almacenado en sistemas y memorias volátiles o equipos tecnológicos que formen parte de la infraestructura crítica del sector público o privado, se realizará su recolección, en el lugar y en tiempo real, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido".

"Cuando el contenido digital se encuentre almacenado en medios no volátiles, se realizará su recolección, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido".

"Cuando se recolecte cualquier medio físico que almacene, procese o transmita contenido digital durante una investigación, registro o allanamiento, se deberá identificar e inventariar cada objeto individualmente, se fijará su ubicación física con fotografías y un plano del lugar, se protegerá a través de técnicas digitales forenses y se trasladará

mediante cadena de custodia a un centro de acopio especializado para este efecto". (Asamblea Nacional del Ecuador, 2008)

2.8. Legislación Internacional Relacionadas con Delitos Informáticos.

Con respecto a la Legislación Relacionada con Delitos Informáticos existen organismos internacionales que tienen un consenso político-jurídico de los problemas derivados al mal uso que se tiene con los ordenadores, esto ha dado lugar a que, en algunos casos, ciertos países modifiquen sus derechos penales. Entre estos organismos se encuentran:

- Organización Mundial de Comercio. (OMC)
- Organización de Cooperación y Desarrollo Económico. (OCDE)
- Organización de las Naciones Unidas. (ONU)
- Organización Mundial de la Propiedad Intelectual. (OMPI)

2.8.1. Organización Mundial de Comercio.

Ecuador es miembro de la OMC desde el 21 de enero de 1996. En la Segunda Conferencia Ministerial, celebrada en mayo de 1998, los ministros reconocen la expansión del comercio electrónico mundial, creando nuevas oportunidades de comercio. Para esto se estableció un programa de trabajo sobre el comercio electrónico, el mismo que fue adoptado en septiembre de 1998. El Consejo General encarga la aplicación a la OMC y los ministros examinan el programa en las Conferencia Ministeriales de la OMC.

El Consejo General estableció un programa de trabajo amplio con respecto al comercio electrónico mundial. En el programa de trabajo de Comercio electrónico se establece que: “Exclusivamente a los efectos del programa de trabajo, y sin perjuicio de sus resultados se entiende con la expresión ´comercio electrónico´ la producción, distribución, comercialización, o venta o entrega de bienes y servicios por medios electrónicos”. Los órganos de la OMC son:

El consejo del Comercio de Servicios. - Examina el trato de comercio electrónico en el marco jurídico del AGCS e informa al respecto.

El Consejo del Comercio de Mercancías. - Examina aspectos del comercio electrónico pertinentes a las disposiciones del GATT de 1994, acuerdos comerciales multilaterales del anexo 1ª de acuerdo sobre la OMC y al programa de trabajo aprobado, e informa al respecto.

El Consejo de los ADPIC. - Examina lo referente a la propiedad intelectual que se planten en relación con el comercio electrónico e informa al respecto.

El Comité de Comercio y Desarrollo. - Examina las consecuencias del comercio electrónico para el desarrollo e informa al respecto, teniendo en cuenta las necesidades económicas, financieras y desarrollo de los países. (Organización Mundial de Comercio, 2013)

Durante el Programa de Trabajo sobre el Comercio Electrónico se tuvo varias Conferencias Ministeriales luego de la realizada en Ginebra de 1998, entre estas están:

- Conferencia Ministerial de Ginebra de 1998.
- Conferencia Ministerial de Doha 2001.
- Conferencia Ministerial de Hong Kong de 2005.
- Conferencia Ministerial de Ginebra de 2009.
- Conferencia Ministerial de Ginebra de 2011.
- Conferencia Ministerial de Bali de 2013.

2.8.2. Organización de Cooperación y Desarrollo Económico.

La organización para la Cooperación y el Desarrollo Económico fundada en 1961 agrupa a 35 países miembros, Ecuador no está en la lista. En el año 1983 esta organización inició un estudio para aplicar y armonizar las leyes penales, con la finalidad de luchar contra el uso indebido de los programas de computación de carácter internacional.

En 1986 la OCDE publicó un informe de Delitos Informáticos que como temas fundamentales tiene: el análisis de las normas jurídicas, normas legislativas vigentes y propuestas de reforma en cuanto a leyes penales. En 1992 se elaboró normas para los sistemas de información, con el propósito de brindar bases para que los Estados y el sector privado puedan implementar un marco de seguridad en los sistemas de información. (Organización de Cooperación y Desarrollo Económico, 1992)

2.8.3. Organización de las Naciones Unidas.

La ONU fue fundada el 24 de octubre de 1945 en San Francisco, Estados Unidos. Ecuador es miembro de la Organización de las Naciones Unidas desde el 21 de diciembre de 1945.

Con el fin de tratar los problemas y desafíos relacionados con la seguridad y los delitos informáticos, el Consejo Económico y Social de las Naciones Unidas (ECOSOC), con la ayuda del Departamento de Asuntos Económicos y Sociales (DAES) y la colaboración de la Unión Internacional de Telecomunicaciones (UIT), buscan concienciar a nivel político internacional el panorama de la situación actual y los desafíos con respecto a la seguridad cibernética, identificar políticas prácticas alrededor del mundo para crear una cultura de seguridad informática, y examinar propuestas para dar una solución al incremento de delitos informáticos.

CNUMI ha llegado a ser reconocida como el órgano jurídico central del sistema de las Naciones Unidas en el ámbito del derecho mercantil internacional. Tiene como metas modernizar y armonizar las reglas del comercio internacional.

El grupo de Trabajo IV desde 1997 hasta la fecha ha realizado varios trabajos acerca del Comercio Electrónico, se tiene programada la siguiente reunión del 24 al 28 de abril de 2017 en Nueva York, en las resoluciones de la última reunión desde el 31 de octubre al 4 de noviembre de 2016 en Viena, se trató el tema de una ley modelo sobre los documentos transmisibles electrónicos. (Organización de las Naciones Unidas, 2017)

2.8.4. Organización Mundial de la Propiedad Intelectual.

La Organización Mundial de la Propiedad Intelectual es un organismo especializado de las Naciones Unidas creado en 1967 en Estocolmo, es el foro mundial en lo que atañe a servicios, políticas, información y cooperación en materia de Propiedad Intelectual; el Ecuador se adhirió desde 1988 a este organismo.

Esta organización maneja una base de datos llamada WIPO Lex que da acceso a la legislación de propiedad intelectual de los miembros de la (OMPI), la Organización Mundial del Comercio (OMC) y las Naciones Unidas (ONU). También tiene información sobre tratados relacionados a la Propiedad Intelectual (PI) administrados por organizaciones multilaterales y regionales y tratados bilaterales que incluyen disposiciones de PI. (Organización Mundial de la Propiedad Intelectual, 2016)

Capítulo 3. Aplicación de la metodología para la auditoría informática.

En este capítulo se determina la cantidad y tipos de ataques que se utilizan para la auditoria informática en la red interna de la Universidad Técnica del Norte según la metodología OFFENSIVE SECURITY Professional Training and Tools for Security Specialists que hace referencia a la Figura 1 del subtema Offensive Security.

3.1. Recolección de información.

En esta etapa se identifica los objetivos que se van atacar y los diferentes escenarios que poder ocurrir:

- Pruebas ciegas, es decir no se tiene información del cliente.
- Pruebas con información, es cuando el cliente proporciona cierta información al auditor.

3.1.1. Pruebas a ciegas.

En las pruebas a ciegas, debido a que no existe información del objetivo; como primer paso se debe utilizar la información pública mediante motores de búsqueda como: google, bing, yahoo, entre otros.

3.1.1.1.Búsqueda en Google.

La utilización del Internet es la mejor herramienta al momento de obtener información, el buscador de google está a disposición de usuarios de cualquier parte del mundo; de esta manera se obtuvo el dominio de nuestro objetivo que es el Portal Web de la Universidad Técnica del Norte, como se muestra en la Figura 3.

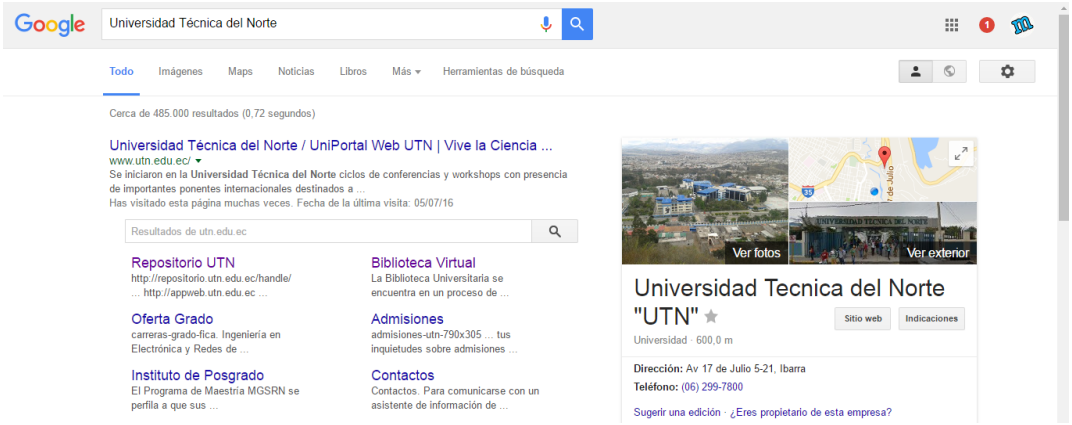


Figura 3. Búsqueda del dominio.
Fuente: Recuperado de https://www.google.com.ec/webhp?sourceid=chromeinstant&ion=1&espv=2&ie=UTF-8#q=Universidad+T%C3%A9cnica+del+Norte

3.1.1.2.Ubicación geográfica.

Existen varios mecanismos para la obtención de la ubicación geográfica, pero la más sencilla y práctica es utilizar la herramienta Google Maps. Como resultado se tiene la ubicación de la Universidad Técnica del Norte dada entre la Av. 17 de Julio y la calle General José María Córdova como se puede visualizar en la Figura 4.

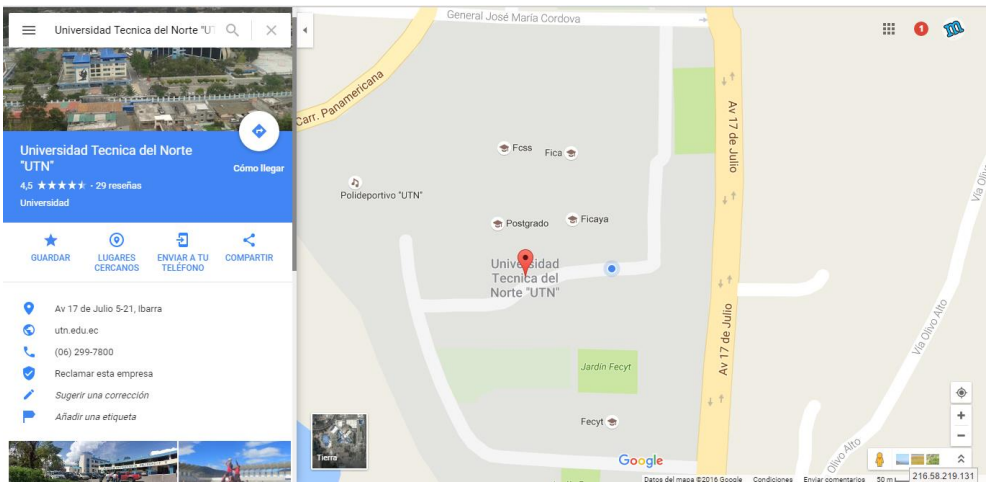


Figura 4. Ubicación Geográfica de la UTN.
Fuente: Recuperado de https://www.google.com.ec/maps/place/Universidad+Tecnica+del+Norte+%22UTN%22/@0.3589737,-78.1172485,15z/data=!4m5!3m4!1s0x0:0xc97eab5c0f6a095e!8m2!3d0.3581583!4d-78.1115408

3.1.1.3.Obtención de la Ip pública.

Desde cualquier ordenador con acceso a internet o que se encuentre en la red Universitaria se puede obtener la dirección pública del portal web de la Universidad Técnica del Norte, mediante el comando nslookup www.utn.edu.ec como muestra la Figura 5 en el "Símbolo del Sistema de Windows".

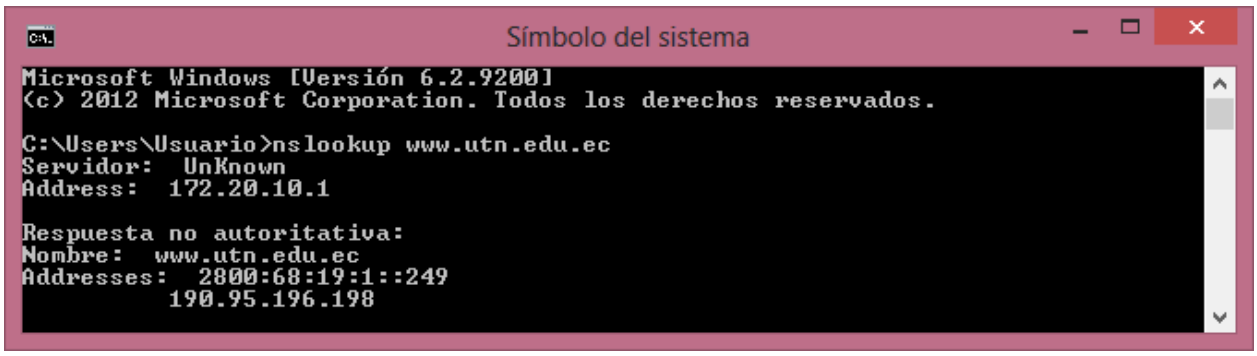


Figura 5. IP Pública del portal Web.
Fuente: Símbolo del Sistema de Windows para la obtención de IP pública.

Otra manera de obtener esta información es con el comando ping www.utn.edu.ec como se muestra en la Figura 6; en el caso de obtenerse una respuesta positiva con el dominio utilizado, se confirma que la dirección IP es verídica y es del portal web de la Universidad Técnica del Norte.

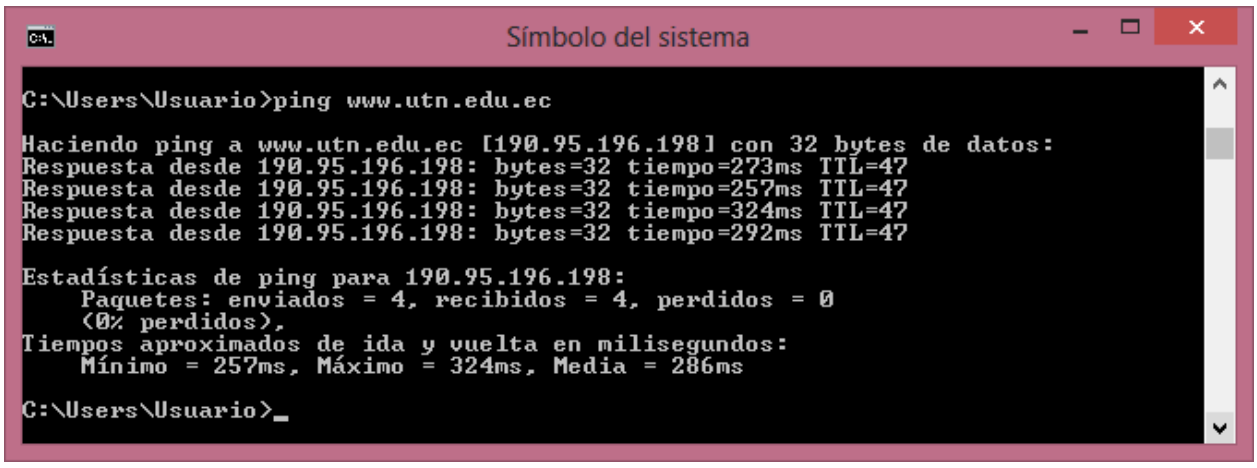


Figura 6. Comando ping.

Fuente: Símbolo del Sistema de Windows utilizando el comando ping.

El comando tracert www.utn.edu.ec es más complejo en cuanto permite visualizar los saltos que se tiene que realizar para llegar al destino que es el dominio del portal web. En la Figura 7 se muestra el proceso que se da en el ordenador para acceder desde fuera de la red.

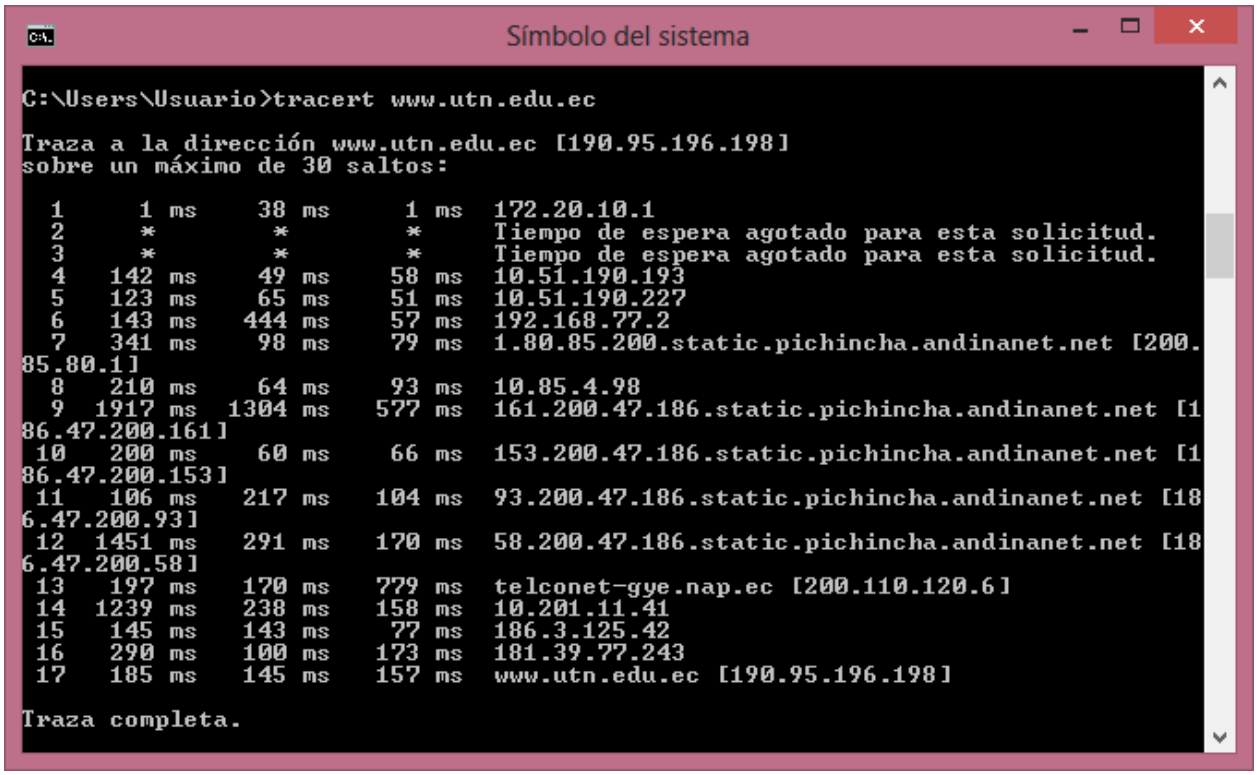


Figura 7. Comando Tracert.
Fuente: Símbolo del Sistema de Windows utilizando el comando tracert

3.1.1.4.Obtención del proveedor de Internet.

En la Figura 8 se muestra cómo se puede acceder a la información de cualquier dominio por medio del sitio web www.whoishostingthis.com. En esta página se puede obtener datos del host que en este caso es CEDIA y el proveedor para el ancho de banda que es Telconet, además de otra información pública. Hay que tener en cuenta que esta

no es la única manera de obtener dicha información dado que se puede utilizar otras herramientas y páginas.

Figura 8. Información del proveedor de Internet.
Fuente: http://www.whoishostingthis.com/?q=utn.edu.ec

La información más importante que se encontró en este sitio web es el tipo de servidor que tienen, un Apache/2.2.15 que está alojado en un servidor WEB con sistema operativo CENTOS, mediante consulta en Google, se identifica que CENTOS 6.3 es un sistema fácil de vulnerar, por lo tanto, se deduce que es poco probable que se esté utilizando mencionada versión de sistema operativo. Esta información se puede verificar en la Figura 9.

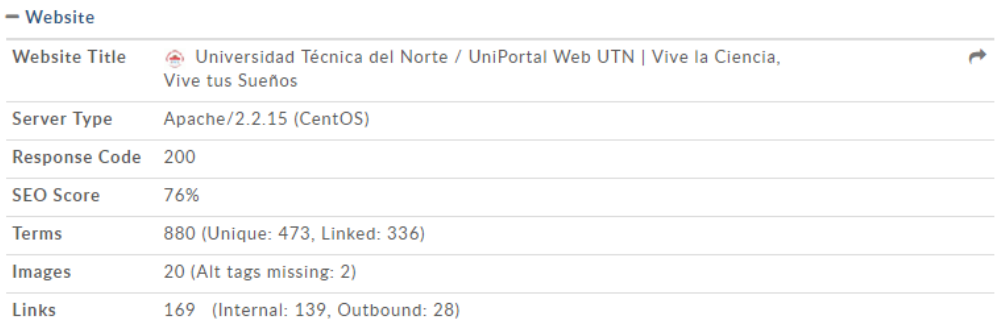


Figura 9. Información del Website de la UTN.
Fuente: Recuperado de http://whois.domaintools.com/utn.edu.ec

En la Tabla 3 se tiene información general de autoridades de la Universidad Técnica del Norte y empleados del departamento tecnológico, esta información puede no ser actualizada, pero permite determinar el sistema organizacional de la institución a breves rasgos.

Tabla 3. Contactos de autoridades y encargados del Departamento de Informática.

NOMBRE	CARGO	CORREO ELECTRÓNICO	CONTACTO
Miguel Naranjo Toro	Rector	rector@utn.edu.ec	+00.59362997800
Ing. Vinicio Guerra Morales	Administrador	admin@utn.edu.ec	+00.59362997800
Ing. Javier Torres Bolaños	Técnico	soporte@utn.edu.ec	+00.59362997800
Dra. Francisca Mafla	Facturación	soporte@utn.edu.ec	+00.59362997800

Fuente: Recuperado de http://whois.domaintools.com/utn.edu.ec

3.1.1.5.Análisis del dominio.

En la Figura 10 se puede observar información del DNS records, misma que contiene datos sobre el hostname, los dominios, los tipos de registros, el número de actualizaciones (TTL) y las direcciones (Content) donde se encuentran los DNS.

Los parámetros y registros del tipo de dominio son los siguientes:

Los registros SOA. - Tienen host origen, correo electrónico, número de serie, tiempo de actualización, tiempo de reintento, tiempo de caducidad y tiempo de vida.

Registro NS. - Significa Name Server, define el servidor de nombres de ese dominio.

Registro MX. - Es de intercambio de correo. Este indica que host se encarga del procesamiento del correo electrónico.

Registro A.- Significa Address, asocia los nombres del host a direcciones IP dentro de una zona.

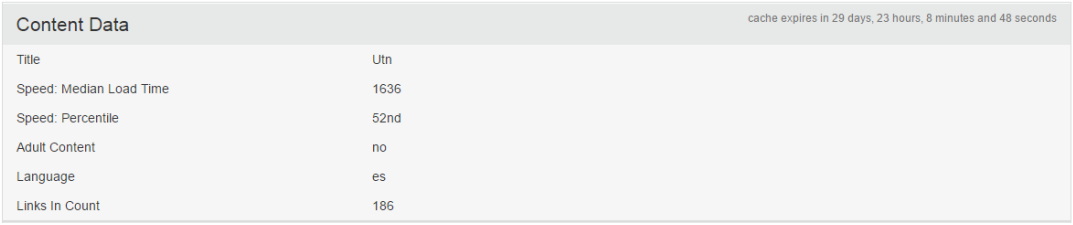
Registro CNAME. - Se conoce como alias, se utiliza para apuntar a un único host más de un nombre, así se simplifican procesos como albergar simultáneamente un servidor web y otro FTP en un mismo equipo.

DNS Records for utn.edu.ec

Hostname	Type	TTL	Priority	Content
utn.edu.ec	SOA	28799		ns1.telconet.net abuse@telconet.net 2015091515 10800 3600 2419200 900
utn.edu.ec	NS	28799		ns2.telconet.net
utn.edu.ec	NS	28799		ns3.telconet.net
utn.edu.ec	NS	28799		ns1.telconet.net
utn.edu.ec	A	86399		190.95.196.198
utn.edu.ec	MX	86399	0	utn-edu-ec.mail.protection.outlook.com
www.utn.edu.ec	A	30743		190.95.196.198
www.utn.edu.ec	AAAA	28799		2800:68:19:1::249

Figura 10. DNS Records de la UTN.
Fuente: Recuperado de https://who.is/website-information/utn.edu.ec

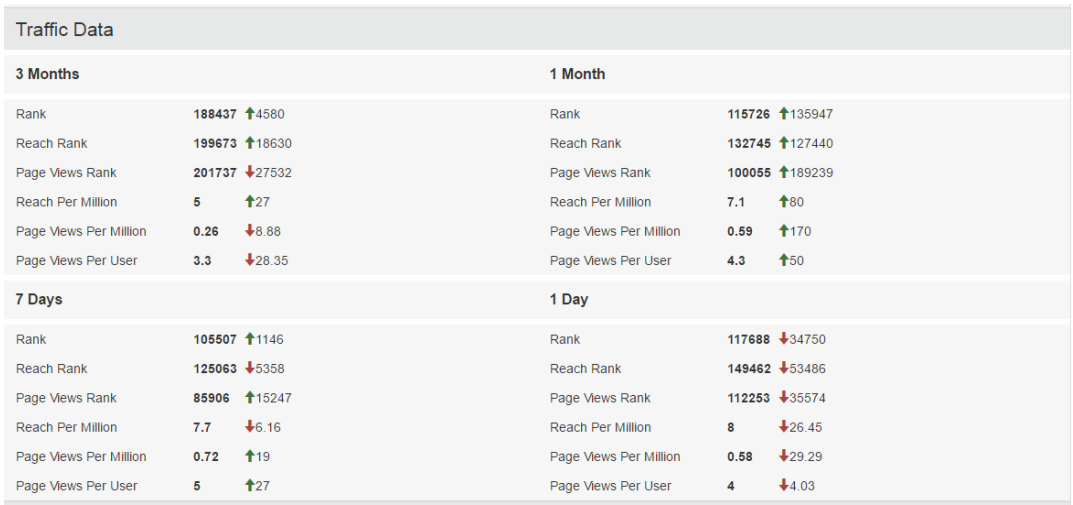
En los datos que muestra la Figura 11 hay información acerca de las velocidades que maneja el sitio web de la universidad. Además, se especifica el tipo de información, en este caso no es de pornografía, el lenguaje es español y tiene 186 enlaces.



Content Data	cache expires in 29 days, 23 hours, 8 minutes and 48 seconds
Title	Utn
Speed: Median Load Time	1636
Speed: Percentile	52nd
Adult Content	no
Language	es
Links In Count	186

Figura 11. Contenido de los datos.
Fuente: Recuperado de https://who.is/website-information/utn.edu.ec

El análisis de tráfico de datos que muestra la Figura 12 del sitio web es muy extenso en cuanto a información. Tiene como referencia los tres últimos meses y los siete últimos días de conexión; también analiza el tráfico de un mes y de un día de los usuarios conectados. Con esta información se tiene la concurrencia de los usuarios y que tan importante es el portal WEB.



Traffic Data					
3 Months			**1 Month**		
Rank	**188437**	↑4580	Rank	**115726**	↑135947
Reach Rank	**199673**	↑18630	Reach Rank	**132745**	↑127440
Page Views Rank	**201737**	↓27532	Page Views Rank	**100055**	↑189239
Reach Per Million	**5**	↑27	Reach Per Million	**7.1**	↑80
Page Views Per Million	**0.26**	↓8.88	Page Views Per Million	**0.59**	↑170
Page Views Per User	**3.3**	↓28.35	Page Views Per User	**4.3**	↑50
7 Days			**1 Day**		
Rank	**105507**	↑1146	Rank	**117688**	↓34750
Reach Rank	**125063**	↓5358	Reach Rank	**149462**	↓53486
Page Views Rank	**85906**	↑15247	Page Views Rank	**112253**	↓35574
Reach Per Million	**7.7**	↓6.16	Reach Per Million	**8**	↓26.45
Page Views Per Million	**0.72**	↑19	Page Views Per Million	**0.58**	↓29.29
Page Views Per User	**5**	↑27	Page Views Per User	**4**	↓4.03

Figura 12. Tráfico de los datos.
Fuente: Recuperado https://who.is/website-information/utn.edu.ec

El tráfico de datos que maneja el sitio web está medido en porcentajes como muestra la Figura 13; se visualiza que el dominio principal y los enlaces tienen cierto grado de disponibilidad para los usuarios, dichos datos corresponden a 1 y siete meses.

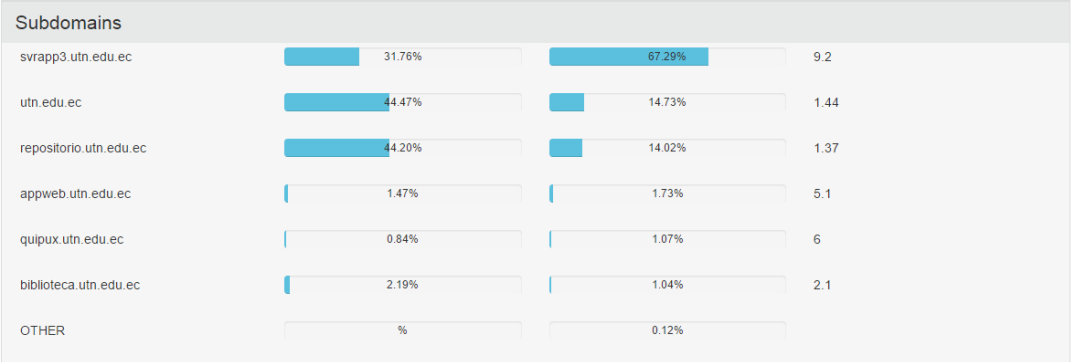


Figura 13. Porcentajes de tráfico de datos.
Fuente: Recuperado de https://who.is/website-information/utn.edu.ec

3.1.1.6.Análisis de pruebas a ciegas.

Durante el análisis de pruebas se obtuvo información de la ubicación geográfica de la institución; esta información es útil para efectuar ataques dentro de la red. También se obtuvo datos específicos como la obtención del dominio del portal web y su dirección IP pública en IPv4 e Ipv6, con estos datos es factible emprender una intrusión al portal web.

3.1.2. Pruebas con información.

En las pruebas con información se necesita del personal del área tecnológica; se debe hacer un análisis de situación actual, conocer la infraestructura y los equipos de la red interna, para luego realizar un análisis de riegos.

3.1.2.1.Análisis de situación actual.

La Universidad Técnica del Norte forma parte de la Red Nacional de Investigación y Educación del Ecuador CEDIA, quien le asigna el recurso 2800:68:19: :/48 en IPv6 y

190.95.216.x/26 IPv4, esta asignación de direcciones llega a la red de la institución por medio de la infraestructura del proveedor de servicios Telconet y un equipo de borde.

El equipo de borde tiene configurado doble pila, esto quiere decir que se puede trabajar en ambos protocolos de internet (ipv4/ipv6); una limitación de este dispositivo de red es que no tiene injerencia, pero si acceso directo como usuario. Por este motivo la institución tiene otro equipo entre el borde de red y el dispositivo de administración y control de la red universitaria (ASA 5520), el switch cisco 3750 está configurado en doble pila y enrutamiento estático para conectarse entre ambos extremos de red.

El comando de la ruta estática es el siguiente:

(X.X.X)#ip route 190.95.196.x 255.255.x.x 190.95.196.x

3.1.2.2.Topología lógica de red de datos UTN.

El servidor WEB y DNS se encuentra en el edificio central, en la Dirección de Desarrollo Tecnológico e Informático de la institución, estos equipos trabajan conjuntamente con otros servicios de internet y equipos de Telecomunicaciones que se conectan con el resto de facultades y dependencias universitarias; esto se muestra en la Figura 14.

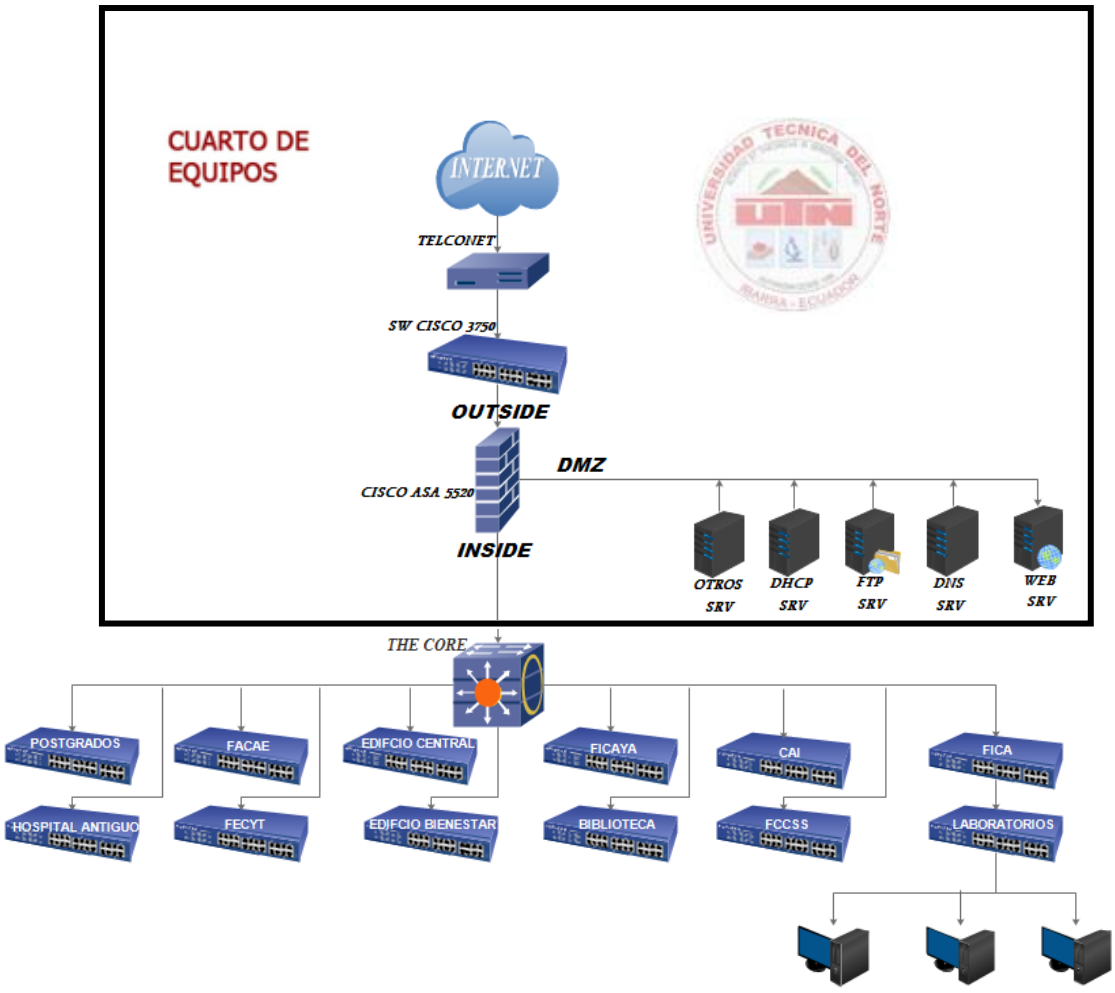


Figura 14. Topologia de la red Interna UTN.
Fuente: Recuperado de Dirección de Desarrollo tecnológico e informático.

3.1.2.3.Cuarto de Equipos.

El cuarto de equipos principal de la Universidad Técnica de Norte se encuentra ubicado en el interior de la Dirección de Desarrollo tecnológico e informático, se tiene equipos de telecomunicaciones en otros edificios, pero el que más interesa para la auditoría es el equipamiento principal de la infraestructura de la red interna, el cual se muestra en la Tabla 4.

Tabla 4. Descripción de los equipos de la red interna de la UTN.

EQUIPO	DESCRIPCIÓN
Cisco ASA 5520 Series	Es un equipo que sirve para controlar la red, aporta seguridad, con alta disponibilidad. Tiene capacidad IPSec, SSL VPN y Firewall.
Exinda 4761	Es un sistema de monitoreo de tráfico, calidad de servicio, aceleración de tráfico y de fácil gestión.
Nexus 5548	Es un equipo de conmutación de computación tradicional, virtualizado, unificado y de alto rendimiento (HPC).
Swicht The Core Catalys 4510R + E / 4500 +E Series	Este Switch es el primer Cisco Supervisor Engine Catalyst para proporcionar ancho de banda de 48 Gbps sin bloqueo por ranura y NetFlow.
Switch Cisco 4503 Series	Este switch reduce el tiempo de inactividad de la red, por sus fuentes de alimentación redundantes e intercambiables en caliente.
Cisco 3800 Series	Es un router con interfaces WAN, tarjetas de interfaz de voz WAN y módulos de integración avanzada.
Switch Cisco 3750	Es un conmutador Fast Ethernet de Capa 3 compatible con la tecnología Cisco EnergyWise, que ayuda a reducir el consumo de energía.
Cisco Media 7800	Es un equipo que permite aplicaciones de alta disponibilidad de alojamiento para acoger las aplicaciones dentro del sistema de Comunicaciones Unificadas de Cisco.
Proliant BL460c G1	Es un servidor que se gestiona mediante HPE OneView, una plataforma convergente que acelera la entrega de servicios TI.
Cisco Lan Controller	Es un dispositivo que sirve para controlar la asociación o la autenticación de clientes.

Fuente: Recuperado de http://www.cisco.com/cisco/web/support/

3.1.2.4.Características de Equipo Servidor

El Servidor Blade Hp Proliant BL460c es un equipo que tiene la capacidad de soportar tanto el protocolo IPv4 como el IPv6. Además, contiene una serie de cuchillas

disponibles para albergar varios servidores, también este equipo tiene soporte para poder operar sobre Windows, Linux y NetWare. A continuación, se tiene la Figura 15 que muestra el servidor físico donde está alojado los servicios de Web y Dns.

Figura 15. Servidor Blade Hp Proliant BL460c G8.
Fuente: Recuperado de: https://www.hpe.com/h20195/v2/GetPDF.aspx/4AA3-9690ENW.pdf

Es importante para un atacante informático conocer con detalles los equipos que se intenta vulnerar para luego detectar las falencias propias del equipo, por ello se realiza la Tabla 5 la cual posee las características más importantes de este servidor,

Tabla 5. Características del Servidor Blade Hp Proliant BL460c G1.

Característica	**Descripción**
Procesador	® 5300 procesadores de secuencia Hasta dos Quad-Core Intel® Xeon, tolera máximo dos procesadores de doble núcleo Intel ® Xeon ® 5100 o 5000.
Memoria	Hasta 32 GB de memoria, con el apoyo de los módulos DIMM (8) ranuras de PC2-5300 búfer completo a 667 MHz Soporte de memoria ECC avanzada.
Controlador de almacenamiento	Tiene integrado HP Smart Array E200i controlador RAID con 64 MB de caché (con batería opcional para respaldo caché de escritura con un actualizar a 128 MB de caché (BBWC)). Soporta RAID 0,1

Soporte de controlador interno	Hasta 2 unidades de disco duro de conexión en caliente (SFF) SAS o SATA pequeño factor de forma Controlador de red:
Soporte Mezzanine	Dos (2) ranuras de expansión de E / S adicionales a través de tarjeta intermedia. Soporta hasta (2) tarjetas intermedias Doble puerto de canal de fibra Mezzanine (4 Gb) opciones para conectividad SAN (Elección de Emulex o QLogic).
Soporte USB interno	Un (1) conector interno USB 2.0 para dispositivos clave de seguridad y llaves de unidad USB
Administración	Integrated Lights-Out 2 (iLO 2) Standard Hoja Edición (incluye KVM virtual y consola remota gráfica).

Fuente: Recuperado de http://www8.hp.com/h20195/v2/getpdf.aspx/c04110908.pdf?ver=7

3.1.2.5. Recurso para el Servidor Web y Dns.

Cada uno de los servicios que se encuentran en producción tienen diferentes características, esto depende de la necesidad del servicio y las limitaciones existentes para que el servidor trabaje a su mayor capacidad. Se tiene el siguiente recurso en la Tabla 6:

Tabla 6. Recurso para el servidor WEB y DNS.

DETALLE	WEB	DNS
Chasis	HP C7000	HP C7000
Cuchilla	HP ProLiant BL 460 C Gen 8	HP ProLiant BL 460 C Gen 1
Capacidad Memoria RAM	65Gb	8 Gb
Memoria Ram Asignada	56Gb	4 Gb
Capacidad Disco	220Gb	146Gb
Disco Asignado	56Gb	50Gb
Procesador	2 Xeon 1.4	2 Xeon 1.4
Número de procesor	E5-2670 v2	E5-2670 v2

Frecuencia del procesador	2.50 GHz	2.50 GHz
Sistema Operativo	Centos 6.7	Windows Server 2008

Fuente: Información entregada por la Dirección de Desarrollo Tecnológico e Informático.

La arquitectura del Portal está diseñada y desarrollado sobre Wordpress un CMS de código open source en PHP, la base de datos está en MySql, cada micro sitio dispone de una base para mantener disponibilidad de datos, es decir no existe conflicto de datos. Todo el CMS Wordpress y la BDD MySql están en el mismo equipo, la arquitectura de Hardware esta virtualizada en VMWARE ESXI 5.5 donde se aloja el servidor web.

El Hardware del servidor DNS esta virtualizado en VMWARE ESXI 5.5 dónde se tiene la máquina virtual, adicionalmente se tiene el servicio de Active Directory para el control de los usuarios de la red de la Universidad Técnica del Norte.

3.1.2.6.Análisis de riesgos.

El análisis de riesgos consiste en estudiar las posibles amenazas y probables sucesos no deseados y los daños que podrían sucitarse, en este caso, se realizó la audiotría al departamento de tecnología informática mediante la herramienta MSAT 4.0 (Microsoft Security Assessment Tool que se basa en la norma ISO/IEC 27005.

Esta herramienta analiza cuatro áreas especificas con preguntas claves a los administradores de la red y las aplicaciones, se tiene un análisis en la Infraestructura, las Aplicaciones, las Operaciones y al Personal. Se tiene un ejemplo de las preguntas en la Figura 16.

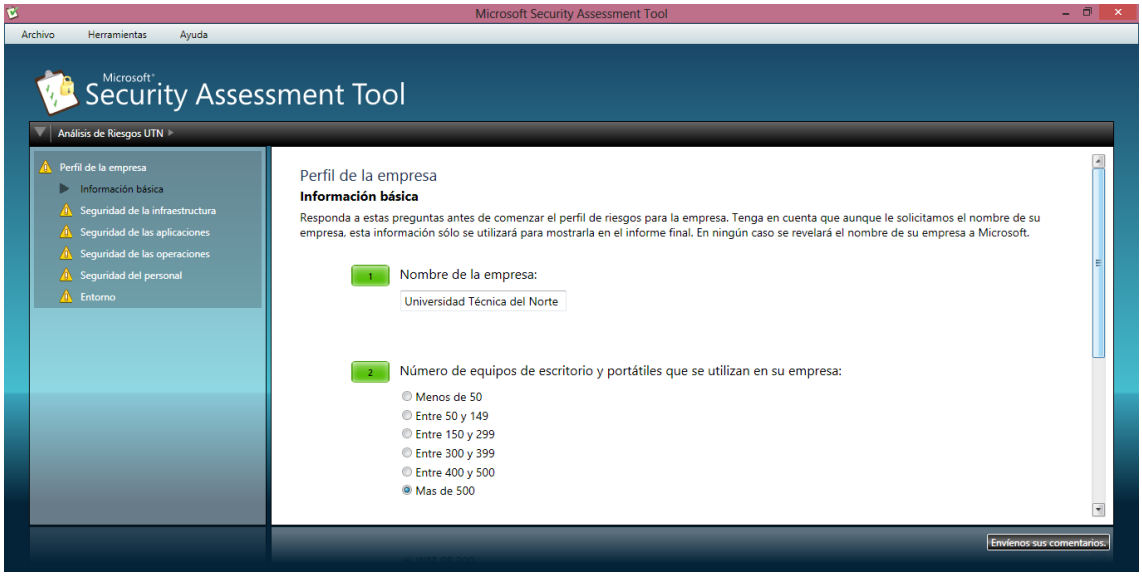


Figura 16. Información básica MSAT.
Fuente: Captura del software Microsoft Security Assessment Tool.

Una vez finalizada la entrevista a los admnisitradores con el software MSAT se presentan los siguientes resultados mediante un informe detallado de lo más relevante en cuando a seguridad informática. A continuacion se tiene la Figura 17 donde se detallan los resultados.

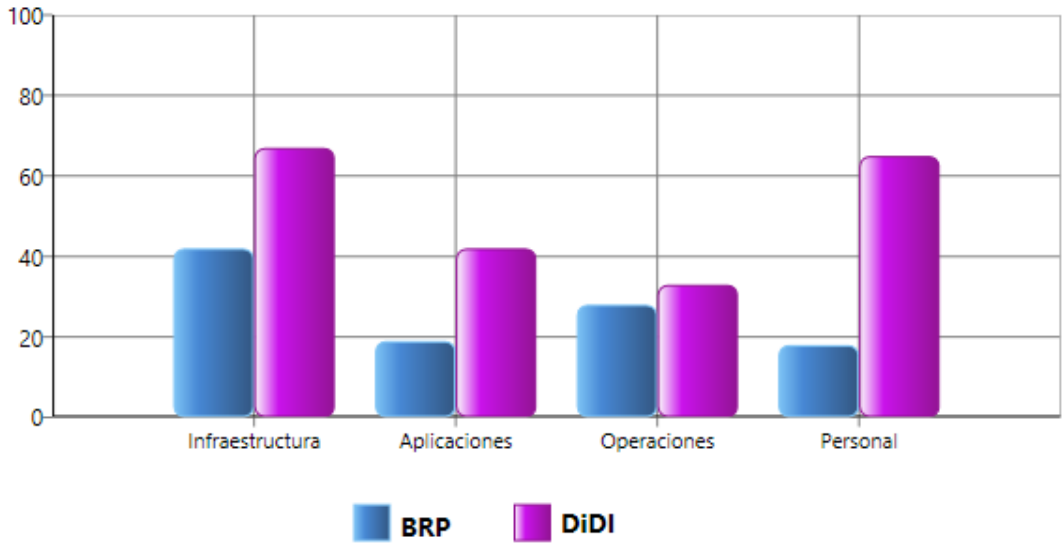


Figura 17. Resultados del análisis de riesgos.
Fuente: Captura del software Microsoft Security Assessment Tool.

Interpretación de gráficos.

La puntuación del BRP va de 0 a 100. Una puntuación más alta representa mayor riesgo al que está expuesta la institución en esta área de análisis. Es importante conocer que una puntuación de 0 no es posible; toda organización conlleva un nivel de riesgo, además hay riesgos comerciales que no se puede mitigar directamente.

Perfil de riesgos para la empresa (BRP): Medida del riesgo al que está expuesta una organización, según el entorno y el sector en que opera.

AoAS: Áreas de análisis que son: la infraestructura, las aplicaciones, operaciones y el personal.

DiDI también tiene una puntuación de 0 a 100. Una puntuación más alta significa un entorno donde se ha tomado más medidas para implementar estrategias de DiD en el área de análisis específica. La puntuación DiDI no indica la eficacia general de la seguridad ni siquiera la cantidad de recursos para la misma, sino que cuantifica la estrategia global que se utiliza para defender el entorno.

Índice de defensa en profundidad (DiDi): Medida de las defensas de seguridad utilizadas en el personal, los procesos y la tecnología para contribuir a reducir los riesgos identificados en una organización.

En principio, una puntuación baja de BRP y alta del DidI parecería un buen resultado, pero no siempre es así. Está fuera del ámbito de la presente autoevaluación tener en cuenta todos los factores. Una disparidad significativa entre la puntuación del

BRP y la del Didi para un área de análisis específica significa que se recomienda una revisión del área. Cuando se analice los resultados, es importante tener en cuenta las puntuaciones individuales, tanto de BRP como de DiDi, y cómo se relacionan entre sí. Un entorno estable probablemente tendría como resultado puntuaciones iguales en todas las áreas. Disparidades entre las puntuaciones DiDi son un indicio de una estrategia general de seguridad concentrada en una sola técnica de mitigación. Si la estrategia de seguridad no abarca al personal, los procesos ni la tecnología, el entorno estará expuesto a un mayor riesgo de ataque.

3.1.2.7. Madurez de la seguridad.

La madurez de la seguridad incluye los controles físicos y técnicos, la competencia técnica de los recursos informáticos, las directivas, los procesos y las prácticas sostenibles. Esta se mide únicamente a través de la capacidad de la organización para utilizar las herramientas disponibles de manera eficaz.

a) **Básica. -** Algunas medidas eficaces de seguridad utilizadas como primer escudo protector, respuesta de operaciones e incidentes aún mu**y** reactiva.
b) **Estándar. -** Capas múltiples de defensa utilizadas para respaldar una estrategia definida.
c) **Optimizada. -** Protección efectiva de los asuntos de forma correcta y garantía de la utilización del mantenimiento de las mejores prácticas recomendadas.

3.1.2.8.Resultados Generales del Análisis de Riesgos.

De acuerdo con las respuestas acerca de la evaluación de riesgos a cargo del personal de la DDTI, se tiene las siguientes medidas de defensa que se han calificado de la siguiente forma.

- Cumple las mejores prácticas recomendadas.
- Necesita mejorar.
- Carencias severas.

Áreas de análisis	Distribución de defensa de riesgos	Madurez de la seguridad
Personal	●	●
Operaciones	●	●
Aplicaciones	●	●
Infraestructura	●	●

Figura 18. Nivel de riesgo.
Fuente: Captura del software Microsoft Security Assessment Tool.

3.1.2.9. Tarjeta de puntuación en el análisis de riesgos.

En la tarjeta de puntuación se tiene un análisis de riesgos más minucioso, se representa mediante colores como en los resultados generales del Análisis de Riesgos; pero en este caso se lo hace con todos los parámetros que se evaluó conjuntamente con los administradores de la DDTI.

En el análisis general de las cuatro áreas evaluadas como se muestra en la Tabla 7, se tiene que la sección de Infraestructura y Personal enfrenta problemas leves de seguridad, pero se puede mejorar; en el caso de la sección de Aplicaciones y Operaciones existen carencias severas de seguridad.

Tabla 7. Análisis Generales de las 4 áreas evaluadas.

Infraestructura	
Aplicaciones	
Operaciones	
Personal	

Fuente: Captura del software Microsoft Security Assessment Tool.

Infraestructura.

Dentro del análisis de la infraestructura se analiza la defensa de perímetro, los mecanismos de autenticación y que tipo de gestión y control se maneja en la red.

En la Tabla 8 se hace un análisis de riesgos mejor detallado, en este caso se analiza la defensa del perímetro, esta se encuentra con problemas leves de seguridad para lo cual se puede instalar antivirus actualizados en los ordenadores y servidores, además se debe tomar medidas de seguridad en cuanto al acceso remoto e implementar un sistema de detección de intrusiones (IDS).

Tabla 8. Defensa del perímetro.

Defensa del perímetro	
Reglas y filtros de cortafuegos	
Antivirus	
Antivirus – Equipos de escritorio	
Antivirus – Servidores	
Acceso remoto	

Segmentación	
Sistema de detección de intrusiones (IDS)	
Inalámbrico	

Fuente: Captura del software Microsoft Security Assessment Tool.

La siguiente sección es la de autenticación, la Tabla 9 muestra que se tiene carencias severas en cuanto a la autenticación de los usuarios administrativos y directivas de contraseñas de las cuentas de acceso remoto, para los demás parámetros existe seguridad, pero se puede mejorar.

Tabla 9. Autenticación.

Autenticación	
Usuarios administrativos	
Usuarios internos	
Usuarios de acceso remoto	
Directivas de contraseñas	
Directivas de contraseñas – Cuenta administrador	
Directicas de contraseñas – Cuenta de usuario	
Directivas de contraseñas – Cuenta de acceso remoto	
Cuentas inactivas	

Fuente: Captura del software Microsoft Security Assessment Tool.

En el apartado de Gestión y control como se muestra en la Tabla 10, se puede reconocer que existe mayor seguridad con respecto a las otras secciones de seguridad, pero se puede mejorar.

Tabla 10. Gestión y control.

Gestión y control	
Informes sobre incidentes y respuesta	
Creación Segura	
Seguridad Física	

Fuente: Captura del software Microsoft Security Assessment Tool.

Aplicaciones.

Se refiere a los servicios que tiene la universidad, en esta área MSAT analiza la implementación y uso, el diseño de las aplicaciones y el almacenamiento y comunicaciones de datos, la Tabla 11 a continuación detalla esta información.

La primera sección que se analiza es la implementación y uso de las aplicaciones como se muestra en la Tabla 11; en este punto se tiene que tomar medidas correctivas urgentes ya que existen problemas severos en la seguridad.

Tabla 11. Implementación y uso de las aplicaciones.

Implementación y uso	
Equilibrio de carga	
Clústeres	
Aplicación y recuperación de datos	

Fabricante de software independiente (ISV)	
Desarrollo internamente	
Vulnerabilidades	

Fuente: Captura del software Microsoft Security Assessment Tool.

En cuanto al diseño de las aplicaciones existen algunos problemas severos que se tienen que mejorar, como es el caso de autorización y control de acceso, y la metodología de desarrollo de seguridad de software como se muestra en la Tabla 12.

Tabla 12. Diseño de aplicaciones.

Diseño de aplicaciones	
Autenticación	
Directivas de contraseñas	
Autorización y control de acceso	
Registro	
Validación de datos de entrada	
Metodologías de desarrollo de seguridad de software	

Fuente: Captura del software Microsoft Security Assessment Tool.

En la sección de almacenamiento y comunicaciones de datos de las aplicaciones hay problemas severos en cuanto al cifrado como se muestra en la Tabla 13, por lo que se deben tomar acciones para remediar dicho problema.

Tabla 13. Almacenamiento y comunicaciones de datos en las aplicaciones.

Almacenamiento y comunicaciones de datos	
Cifrado	
Cifrado – Algoritmo	

Fuente: Captura del software Microsoft Security Assessment Tool.

Operaciones.

Este apartado trata sobre las medidas técnicas en cuanto a la organización de los trabajadores de la dirección de desarrollo tecnológico e informativo.

Lo que muestra la Tabla 14 es el análisis del entorno de las operaciones, en esta es posible observar problemas severos en todos los puntos investigados, por lo que es urgente tomar medidas correctivas para mejorar.

Tabla 14. Análisis del entorno de las operaciones.

Entorno	
Host de gestión	
Host de gestión – Servidores	
Host de gestión – Dispositivos de red	

Fuente: Captura del software Microsoft Security Assessment Tool.

La directiva de seguridad de las operaciones presenta problemas severos también a excepción de los protocolos y servicios, esto es lo que se visualiza en la Tabla 15.

Tabla 15. Directiva de seguridad de las Operaciones.

Directiva de seguridad	
Clasificación de datos	
Eliminación de datos	
Protocolos y servicios	
Uso aceptable	
Gestión de cuentas de usuarios	
Regulación	
Directiva de seguridad	

Fuente: Captura del software Microsoft Security Assessment Tool.

Según la Tabla 16 hay problemas severos en cuanto a la documentación de la red y la gestión de actualizaciones, los demás puntos tienen cierto grado de seguridad, pero se pueden mejorar.

Tabla 16. Gestión de actualizaciones y revisiones de las Operaciones.

Gestión de actualizaciones y revisiones	
Documentación de la red	
Flujo de datos de la aplicación	
Gestión de actualizaciones	

Gestión de cambios y configuración	

Fuente: Captura del software Microsoft Security Assessment Tool.

En las copias de seguridad y recuperación se puede identificar problemas severos en todos los puntos analizados con excepción de las copias de seguridad que tiene la institución. En el caso de restauración existen posibilidades de mejora. En consecuencia, es necesario dar prioridad a los puntos críticos de esta sección, todo esto se puede constatar en la Tabla 17.

Tabla 17. Copias de seguridad y recuperación de las Operaciones.

Copias de seguridad y recuperación	
Archivos de registro	
Planificación de recuperación ante desastres y reanudación de negocio	
Copias de seguridad	
Dispositivos de copia de seguridad	
Copias de seguriidad y restauración	

Fuente: Captura del software Microsoft Security Assessment Tool.

Personal.

Con relación al personal existen problemas en lo que concierne a requisitos, evaluaciones, directiva y procedimientos, y formación y conocimiento, esto se expone con más detalle en la Tabla 18.

Con respecto al análisis de riesgos en el personal hay resultados positivos puesto que existe cumplimiento en las diferentes medidas de seguridad, por lo tanto, no es prioritario tratar estos puntos, pero se aconseja tenerlos en cuenta y revisión continua.

Tabla 18. Análisis de riesgos del Personal.

Personal	
Requisitos y evaluaciones	
Requisitos de seguridad	
Evaluaciones de seguridad	
Directiva y procedimientos	
Comprobaciones del historial personal	
Directiva de recursos humanos	
Relaciones con terceros	
Formación y conocimiento	
Conocimiento de seguridad	
Formación sobre seguridad	

Fuente: Captura del software Microsoft Security Assessment Tool.

3.1.2.10. Análisis final de pruebas con información.

De los resultados anteriores en primera instancia es posible identificar secciones donde existen problemas severos de seguridad, por lo que hay que tomar las respectivas medidas correctivas urgentes. En segunda instancia existen problemas leves que se pueden trabajar y en algunos casos se verificó que la institución cuenta con niveles de seguridad muy altos; todos estos análisis sirven para la posterior elaboración e implementación de políticas y manuales de procedimientos de seguridad.

En este proyecto se plantea mejorar el área de Aplicaciones que es uno de los problemas más críticos que tiene la institución, y el de Infraestructura que representa un problema leve de seguridad.

3.2. Análisis de Vulnerabilidades.

Esta fase consiste en determinar problemas de seguridad en los objetivos determinados en la primera fase. Para esta etapa es posible utilizar herramientas de auditoría, esto depende de la organización, una vez que se detecta las vulnerabilidades del sistema se determina la estrategia con la cual se realizara el pent testing.

En consecuencia, se dio énfasis a los puntos críticos encontrados en la anterior fase, para esto se utilizó el sistema de Kali Linux y sus componentes, de ser el caso se utilizará otros sistemas.

3.2.1. Escaneo de Redes.

La metodología del escaneo consiste en verificar si el sistema está operante, si los puertos están abiertos o cerrados, hacer un Banner Grabbing, escanear vulnerabilidades y realizar el diseño de la red.

¿Qué se escanea?

Se debe escanear puertos de una computadora, puertos de un servidor, puertos de un dispositivo. Para ello el siguiente proceso:

- Identificar qué tipo de red se va a escanear: Interna, Externa, Remota.
- Identificar los servicios que están involucrados en el sistema.
- Identificar el uso exacto de un sistema específico.
- Utilizar correctamente el rango de escaneo.
- No se debe escanear un sistema sin autorización.
- Es necesario que el proceso sea debidamente documentado.

3.2.1.1.Descubrimiento con DNS.

Se divide en 3 tipos: Forward Lookup Bruteforce, Reverse Lookup Bruterforce y Transfers.

3.2.1.2.Lookup Bruteforce.

Mediante el comando host www.utn.edu.ec se determina la dirección pública de los servidores víctimas.

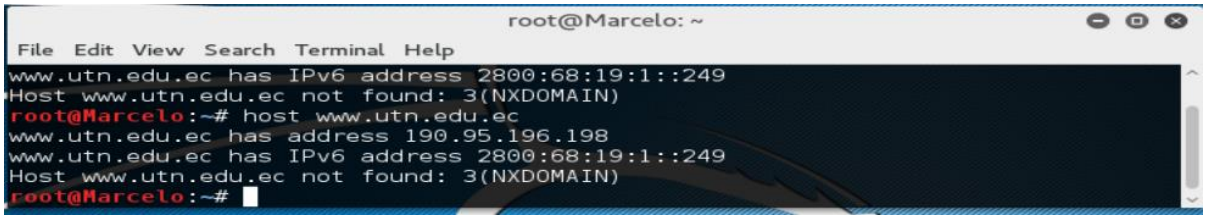


Figura 19. Lookup Bruteforce.
Fuente: Captura del sistema Kali Linux

Reverse Lookup Bruterforce.

Con el comando host 190.95.196.198 se determina el dominio de la dirección pública encontrada anteriormente.

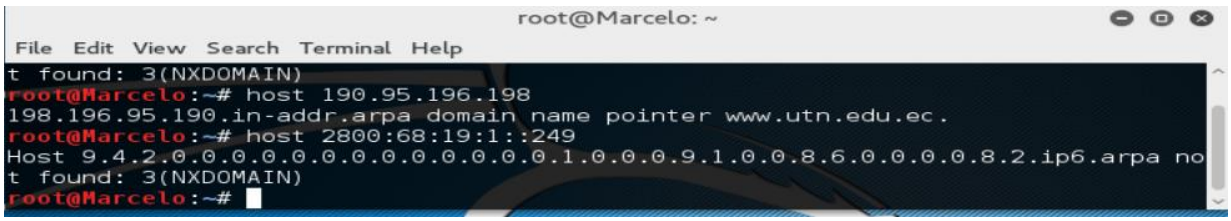


Figura 20. Reverse Lookup Bruterforce.
Fuente: Captura del sistema Kali Linux

Transfers.

Digitando el comando host -t ns utn.edu.ec se muestra los servidores del proveedor del servicio de internet.

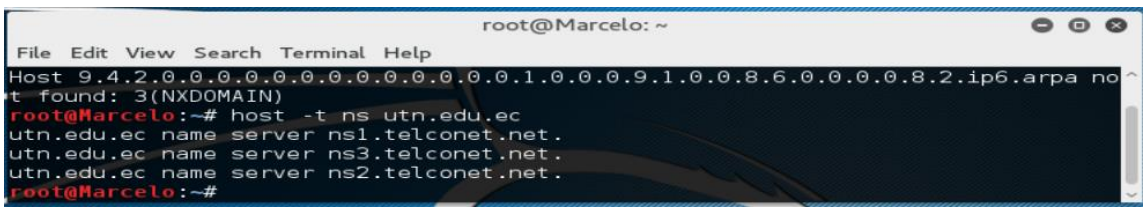


Figura 21. Transfers.
Fuente: Captura del sistema Kali Linux.

3.2.1.3. Fierce.

El comando fierce –dns utn.edu.ec permite visualizar los subdominios que tiene la página web con sus direcciones IP, esto sirve de información para llegar a obtener la dirección privada del servidor WEB. Se tiene que el servidor de DNS tiene la dirección 172.16.1.254 y un servidor ftp con la dirección 172.16.1.249 como datos más importantes.

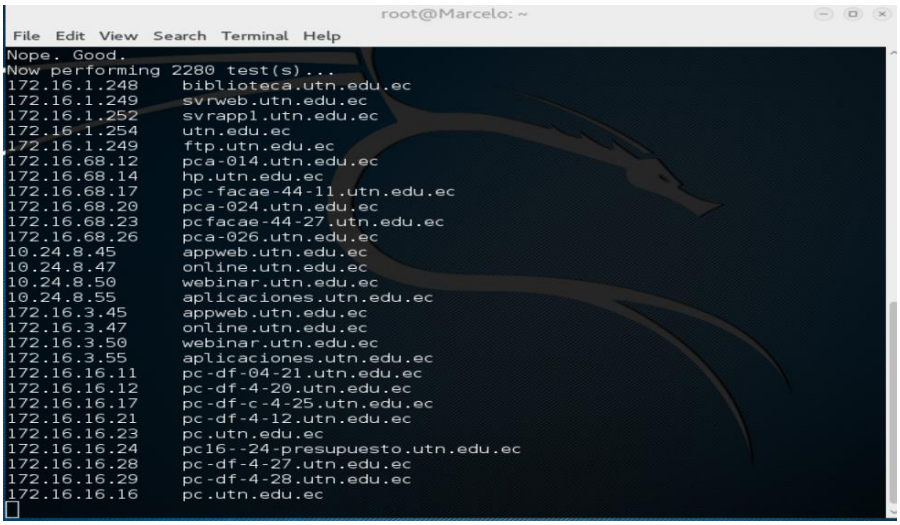


Figura 22. Fierce.
Fuente: Captura del sistema Kali Linux

3.2.1.4.Traceroute.

En la herramienta Kali Linux se realizó la traza, la cual permite visualizar los saltos para llegar hasta el dominio de la página web; para utilizar esta herramienta se tiene que entrar al terminal del sistema como usuario root, y digitamos scapy antes del comando traceroute www.utn.edu.ec que se muestra en la Figura 23.

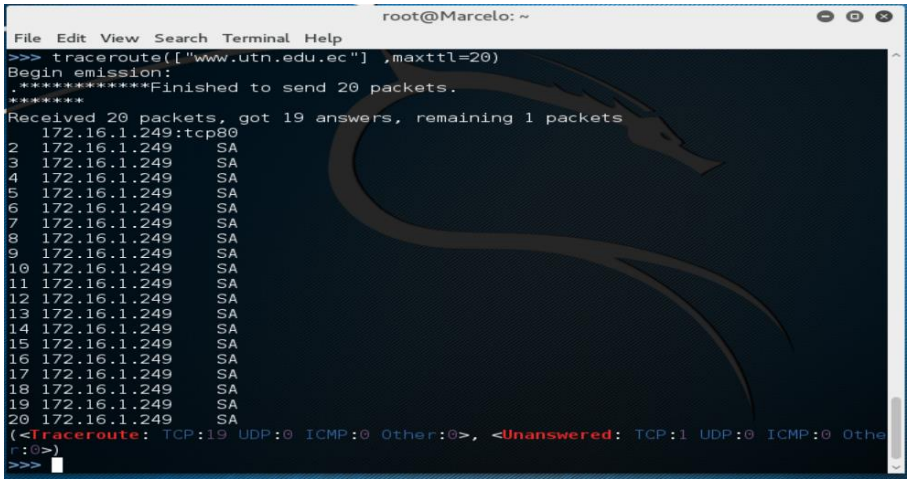


Figura 23. Traceroute.
Fuente: Captura del sistema Kali Linux

3.2.2. Enumeración.

Con este comando se confirma la dirección IP del servidor WEB que es 172.16.1.249.

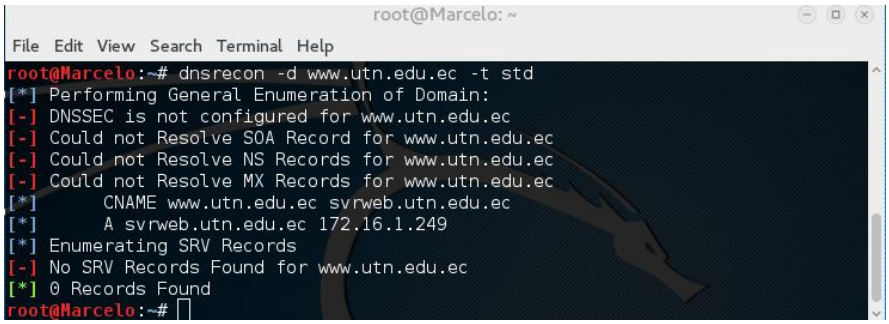


Figura 24. Comando enumeración.
Fuente: Captura del sistema Kali Linux.

3.2.3. Amenazas vulnerabilidades y riegos.

Mediante la siguiente tabla se hace un análisis de la red interna y el servicio del portal WEB en aspectos como amenazas, vulnerabilidades y riegos.

Tabla 19. Amenazas, vulnerabilidades y riesgos.

AMENAZAS	VULNERABILIDADES	RIESGOS
Limitado ancho de banda para el servicio del Portal WEB.	No tiene capacidad para tantos usuarios conectados.	Suspensión del servicio de portal WEB.
Redes inalámbricas sin protección de acceso.	Colapso en la red por exceso de usuarios.	Acceso de personas mal intencionadas.
Servidores con sistemas operativos antiguos.	Sistemas operativos con vulnerabilidades debido a que expiró su vida útil.	Fallas en el funcionamiento de los sistemas operativos, haciéndolos más vulnerables para los atacantes informáticos.
Escaneos de puertos abiertos en los servicios de internet.	Puertos innecesarios abiertos.	Acceso de atacantes por puertos abiertos innecesarios.
Varios servicios en un mismo equipo.	Aumenta la probabilidad de intentos para acceder a los servicios.	Acceder por cualquier servicio.
Escaneo de direcciones IP.	Descubrir las direcciones IP de los servicios de Internet.	Hacer ataques directos a las direcciones IP que no estén ocultas.
Accesos remotos.	Baja protección de los accesos remotos.	Atacantes que se conecten por este medio.

Fuente: Autor.

3.3. Definición de objetivos.

Finalizada la segunda etapa correspondiente a “análisis de vulnerabilidades”, los objetivos son más específicos, aumenta la probabilidad de que los ataques sean exitosos. Para poder determinar el riesgo real que existe en el sistema, es necesario tener en cuenta los objetivos secundarios que pueden servir de intermedio para llegar hasta los objetivos principales, a esto se conoce como escalar privilegios.

3.3.1. Objetivos Específicos.

Con la recolección de información y el análisis de vulnerabilidades en las fases anteriores de la metodología surgen objetivos más claros:

- Atacar al servidor WEB que al parecer trabaja con un Servidor FTP en el mismo equipo y dirección IP que es 172.16.1.249.
- Atacar al servidor DNS que al parecer trabaja con un Active Directory en el mismo equipo y dirección IP que es 172.16.1.254.

3.3.2. Objetivos Secundarios.

- Atacar a las redes inalámbricas que tiene la Universidad Técnica del Norte, para poder acceder a la red interna.
- Encontrar un punto de red que se encuentre visible y accesible para cualquier usuario, con la finalidad de acceder a la red interna por este medio.

3.3.2.1.Redes Inalámbricas.

Se encontró las siguientes redes inalámbricas a disposición para los usuarios de la institución educativa:

Figura 25. Redes Inalámbricas de la UTN.
Fuente: Captura de la señal de las redes inalámbricas cercanas.

El escaneo de redes inalámbricas se hizo en las proximidades del edificio principal, debido a que allí está el departamento de informática y las autoridades más importantes de la Universidad Técnica del Norte.

3.3.2.2.Redes Cableadas.

Dentro de las instalaciones de la Universidad se puede encontrar varios puntos de red en sitios donde existe ordenadores para buscar información pública, como por ejemplo, en la biblioteca de la institución se puede encontrar varias computadoras a disposición de los estudiantes para consultas y otros.

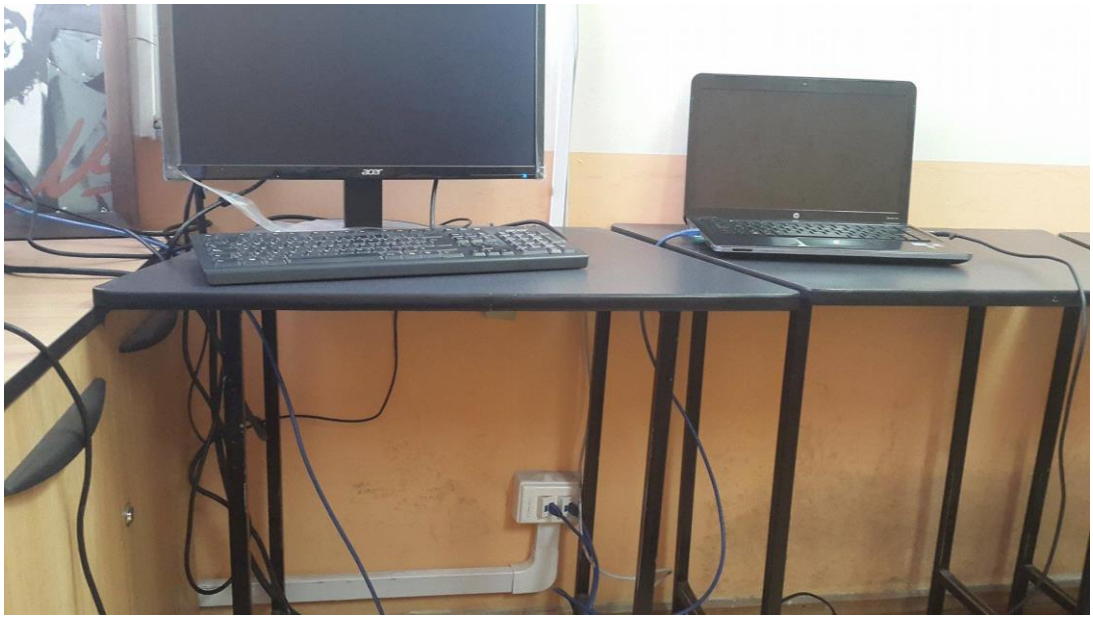


Figura 26. Computador de uso público de la UTN.
Fuente: Fotografía tomada en las instalaciones de la Universidad Técnica del Norte.

3.4. Ataque.

Se ejecuta los ataques a los objetivos seleccionados en la anterior etapa, usando las vulnerabilidades encontradas. Aquí se prueba la existencia real de problemas de seguridad del sistema. Durante la ejecución de los ataques, es posible que surjan nuevas vulnerabilidades que no se detectaron antes, las cuales son tomadas en cuenta dentro de esta misma fase.

3.4.1. Ataques Externos.

Se considera ataque externo el vulnerar la red local privada, desde un lugar fuera de la red de datos de la institución.

3.4.1.1.Escaneo de Puertos al Servidor Web

Se realizó un escaneo de puertos en el servidor WEB para determinar si existen puertos abiertos los cuales pueden ser utilizados para un acceso directo al servidor. Esto se hace directamente en la dirección privada obtenida en la etapa de análisis de vulnerabilidades donde ya se determinó esta IP.

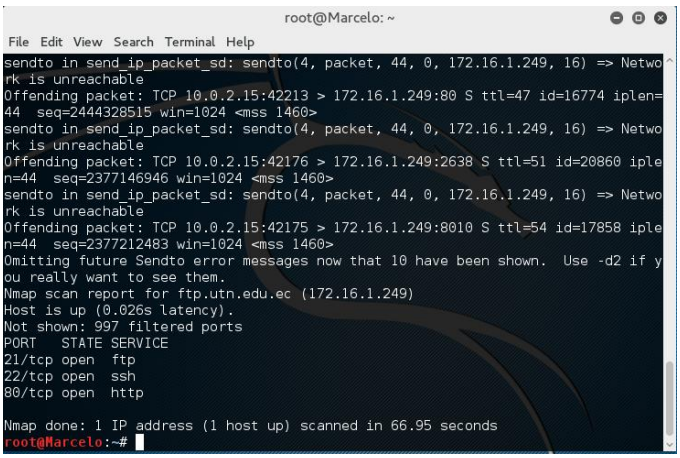


Figura 27.Escaneo de puertos abiertos servidor web.
Fuente: Captura del sistema operativo Kali Linux.

Como resultado se obtuvo que el servidor WEB tiene abiertos los puertos para la utilización de servicios ftp, ssh y http con los puertos 21, 22 y 80 respectivamente.

3.4.1.2.Escaneo de puertos al servidor DNS.

Se realizó un escaneo de puertos en el servidor DNS para determinar si existen puertos abiertos los cuales puedan ser utilizados para un acceso directo al servidor. Esto se hizo directamente en la dirección privada obtenida en la etapa de análisis de vulnerabilidades donde ya se determinó esta IP.

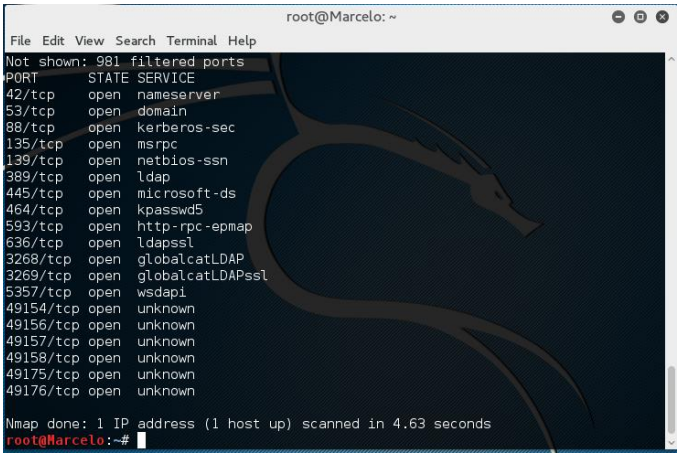


Figura 28. Escaneo de puertos abierdos del servidor dns.
Fuente: Captura del sistema operativo Kali Linux.

Se determinó mediante el escaneo que existen varios puertos abiertos entre ellos el 53, el cual pertenece al servicio de DNS.

3.4.1.3.Phishing

El término Phishing hace referencia a la suplantación, en este caso, se va a realizar la clonación del portal Web de la UTN.

Beef.

La BeEF es la abreviatura de The Browser Exploitation Framework; esta herramienta de pruebas de intrusión se centra en el navegador web. Para poder utilizar esta herramienta hay que ingresar al terminal de Kali Linux y digitar lo siguiente:

- # cd /usr/share/beef-xss/
- #./beef

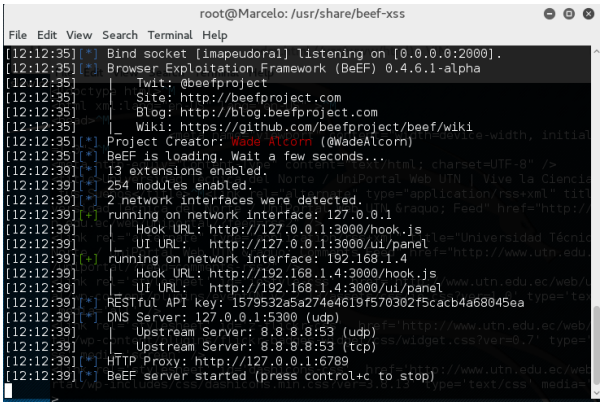


Figura 29. Ejecución Beef.
Fuente: Captura del sistema operativo Kali Linux.

Ahora es posible acceder de manera gráfica mediante cualquier navegador al BeEF con la dirección http://127.0.0.1:3000/ui/panel.

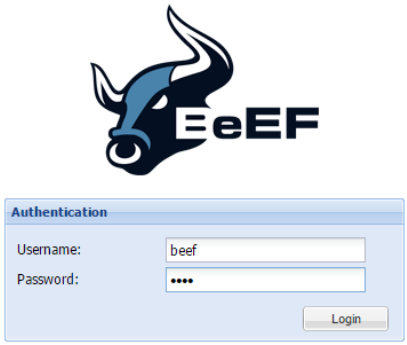


Figura 30. Interfaz de Beef.
Fuente: Software de navegación.

Una vez aquí se tiene acceso a la información de los usuarios que pasen por el sitio clonado. Lo ideal en este punto sería obtener las contraseñas de autenticación de los usuarios.

Phishing.

Comando para clonar un sitio WEB:

- #setoolkit
- Set>1
- Set>2
- Set>3
- Set>2
- Set>IP
- Set>http://www.utn.edu.ec

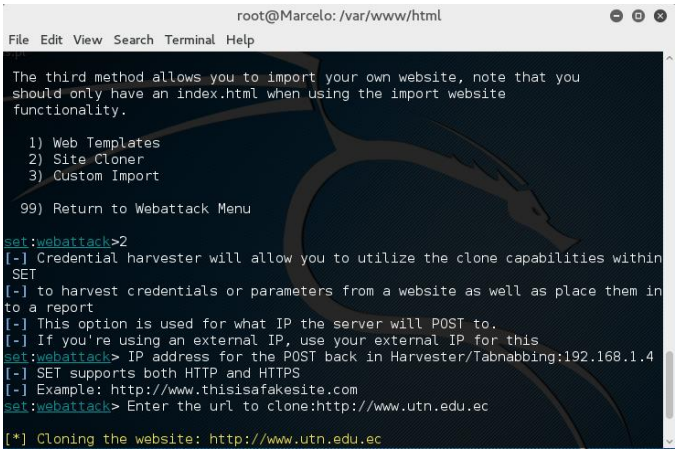


Figura 31. Proceso para clonar un sitio web.
Fuente: Captura del sistema operativo Kali Linux.

El código html se graba en la ubicación cd /var/www/html con el nombre index.html. Se puede comprobar también ingresando la dirección de Kali Linux en cualquier buscador.

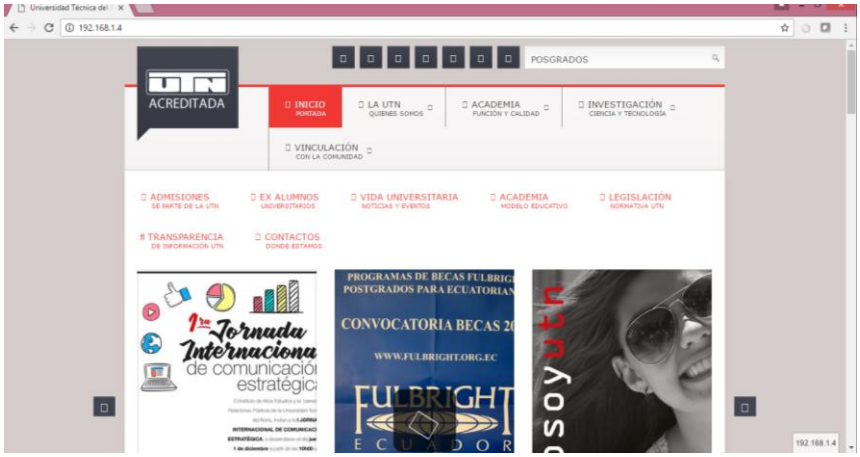


Figura 32. Portal web UTN falso.
Fuente: Software de navegación.

3.4.1.4.Extraer metadata.

Este ataque tiene la finalidad de extraer información que haya dentro del sitio Web. FOCA es una herramienta útil para ello puesto permite extraer la Metadata y analizar la misma; tiene varios parámetros que analiza como por ejemplo el dominio.

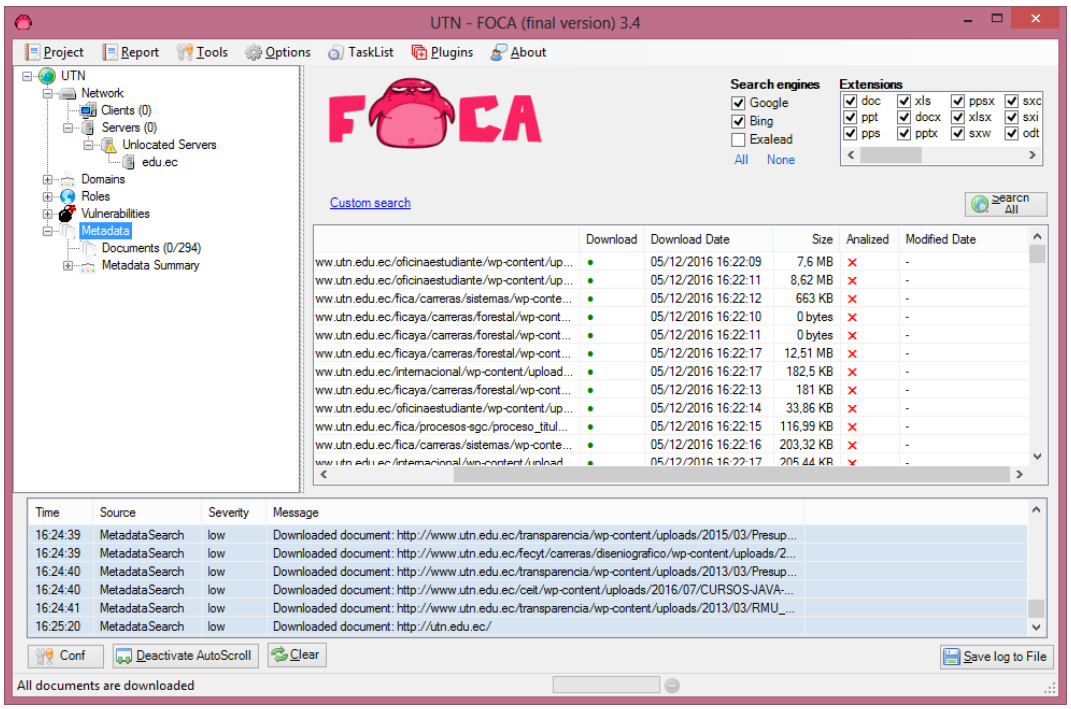


Figura 33. Extraer Metadata.
Fuente: Software FOCA.

Con esta herramienta se pudo encontrar información del personal de toda la universidad, como: impresoras, carpetas, usuarios, entre otros. Este software no detecta contraseñas.

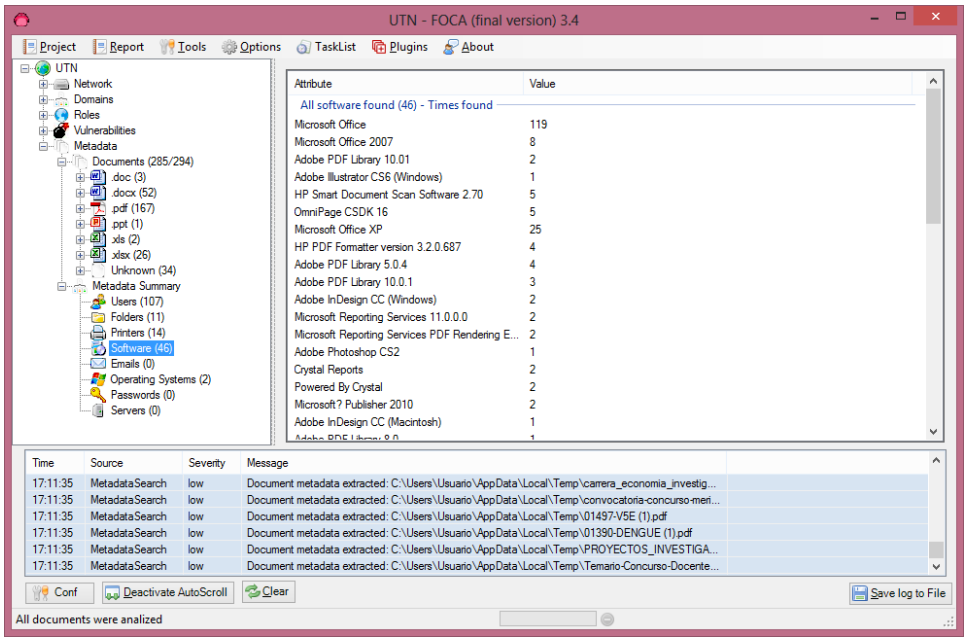


Figura 34. Información del Software Portal Web.
Fuente: Software FOCA.

En la Figura 35 mediante la herramienta FOCA se determina los usuarios del Portal Web de la UTN, dónde se muestra información relevante como la del administrador de la red y empleados del área de tecnología.

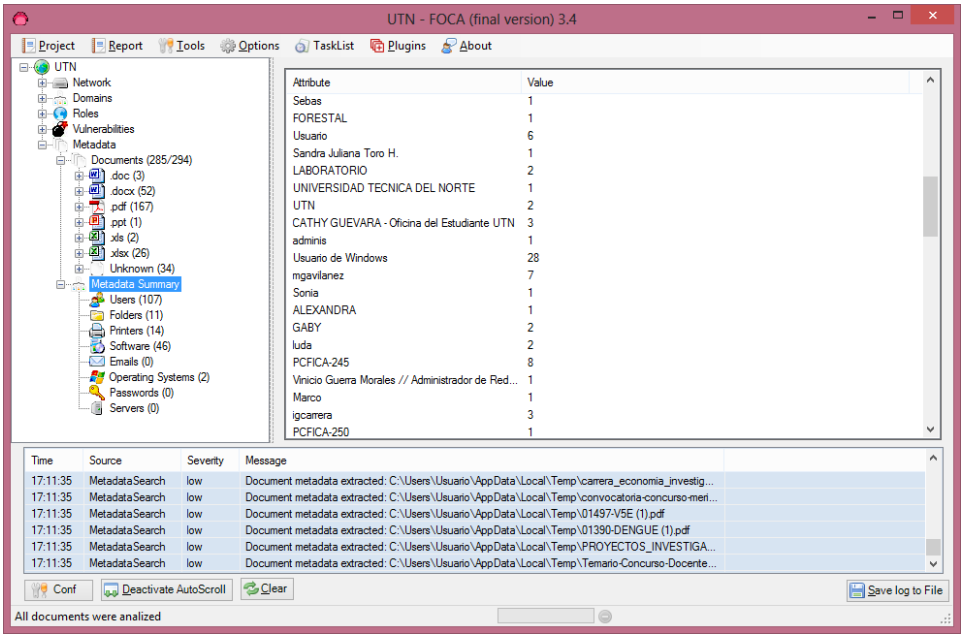


Figura 35. Usuarios del Portal Web UTN.
Fuente: Software FOCA.

3.4.1.5.Snooping.

DNS cache snooping es una técnica que permite conocer los nombres de dominio que ha resultado un servidor DNS. Permite al atacante averiguar qué dominios están resueltos por el servidor, y por consiguiente, cuáles no.

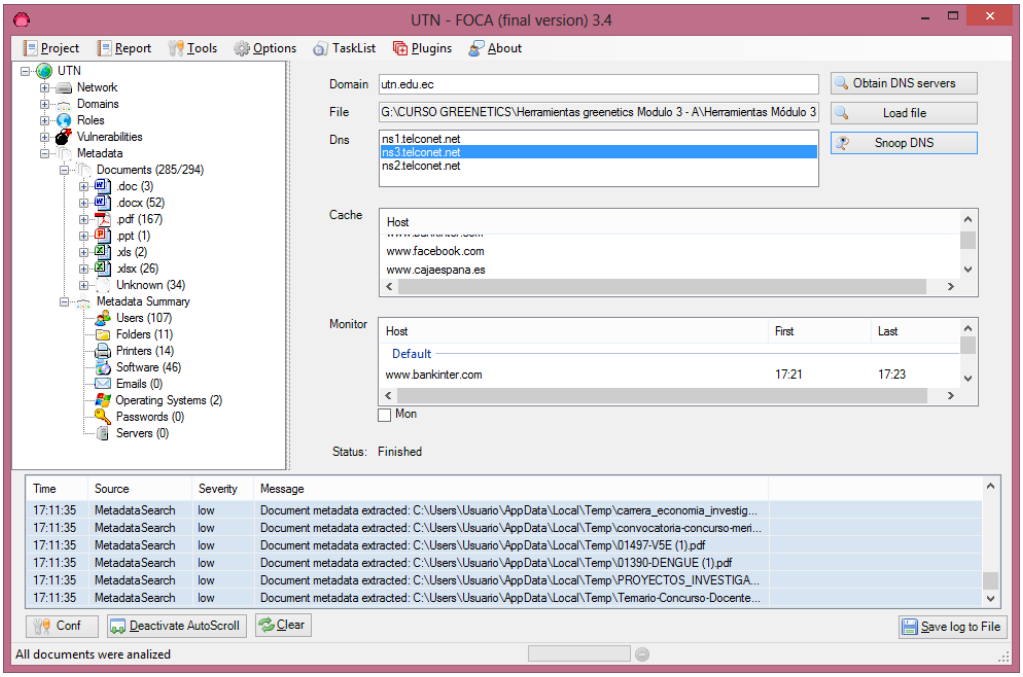


Figura 36. Ataque de Snooping.
Fuente: Software FOCA.

3.4.2. Ataques Internos.

Son considerados ataques internos los que se originan dentro de la red de datos de la institución, es decir, las intrusiones realizadas por medio de una conexión cableada o inalámbrica.

3.4.2.1.Ataque de autenticación con Winscp.

Este programa permite acceder de forma remota al servidor FTP. Dado que servidor FTP y servidor Web se encuentra en la misma cuchilla, es factible autenticarse por este medio.

Autenticación por medio de WinSCP.

Se ejecuta el programa instalado y se intenta autenticarse por ssh al servidor FTP; para ello se escribe la dirección del servidor y el puerto.

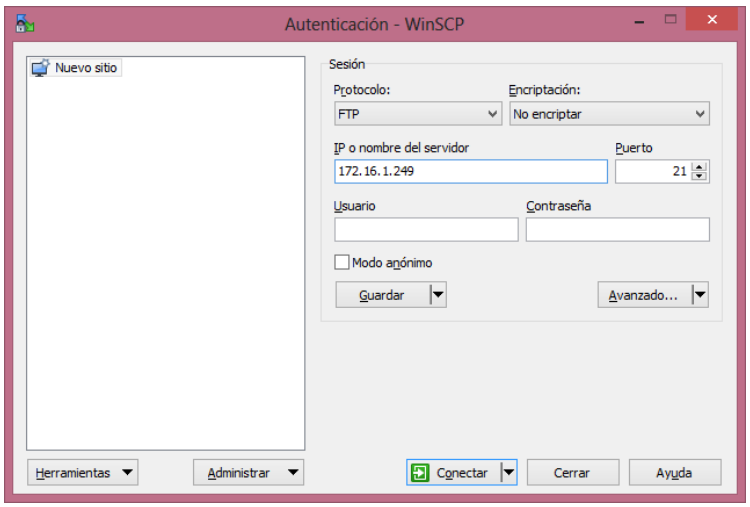


Figura 37. Autenticación WinSCP.
Fuente: Captura de Software WinSCP.

El siguiente paso es intentar acceder en modo root o administrador, utilizando claves por defecto y las contraseñas más utilizadas por administradores.

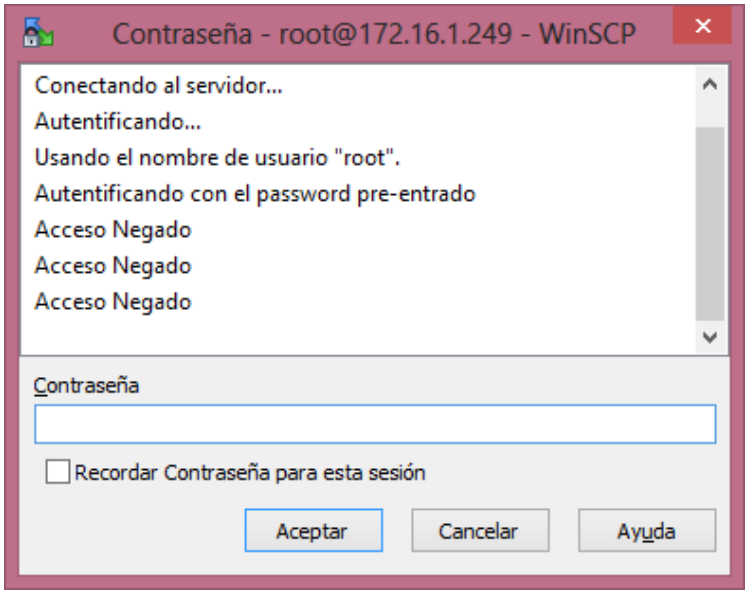


Figura 38. Intento fallido de ingreso al servidor FTP.
Fuente: Captura de Software WinSCP.

3.4.2.2.Ataque a la red Inalámbrica con Kali Linux.

Para acceder a la red inalámbrica se necesita de un ordenador que tenga instalado Kali Linux, sea de manera real o virtual, ya que este sistema cuenta con varias herramientas de auditoría informática, una de ellas es Linset, software que permite ingresar a la red inalámbrica rompiendo las contraseñas.

Figura 39. Linset.
Fuente: Kali Linux.

En la Figura 39 se muestra la interfaz de inicio del software, una vez aquí se elige la interfaz de red que se va utilizar para los paquetes, luego se elige el canal que se desea analizar para poder ver todas las redes conectadas, luego linset da la opción de escoger un punto de acceso falso. El siguiente paso es capturar un paquete y buscar el handshake, después viene la selección de un método para generar y capturar paquetes de handshake y obtener datos suficientes para generar una falsa autenticación en el AP, esto se hace hasta obtener un handshake funcional.

Con todo lo anterior, se puede montar la falsa red donde los usuarios deberán introducir sus contraseñas. Esto debe realizarse de la manera más fidedigna para que la suplantación sea totalmente efectiva.

3.4.2.3.Ataque a la red cableada

Ingresar a la red cableada es fácil, sólo se necesita conectarse a un punto de red y ejecutar los ataques informáticos. Una vez conectado en la red cableada se puede emplear el software sniffer para escuchar las comunicaciones entre ordenadores y otros equipos.

La herramienta para esta acción más conocida es Wireshark, que es un software gratuito que permite capturar paquetes de red en vivo a tiempo real, capaz de descifrar paquetes en función de su protocolo, cuya interfaz es muy interactiva y fácil de utilizar como se muestra en la Figura 40.

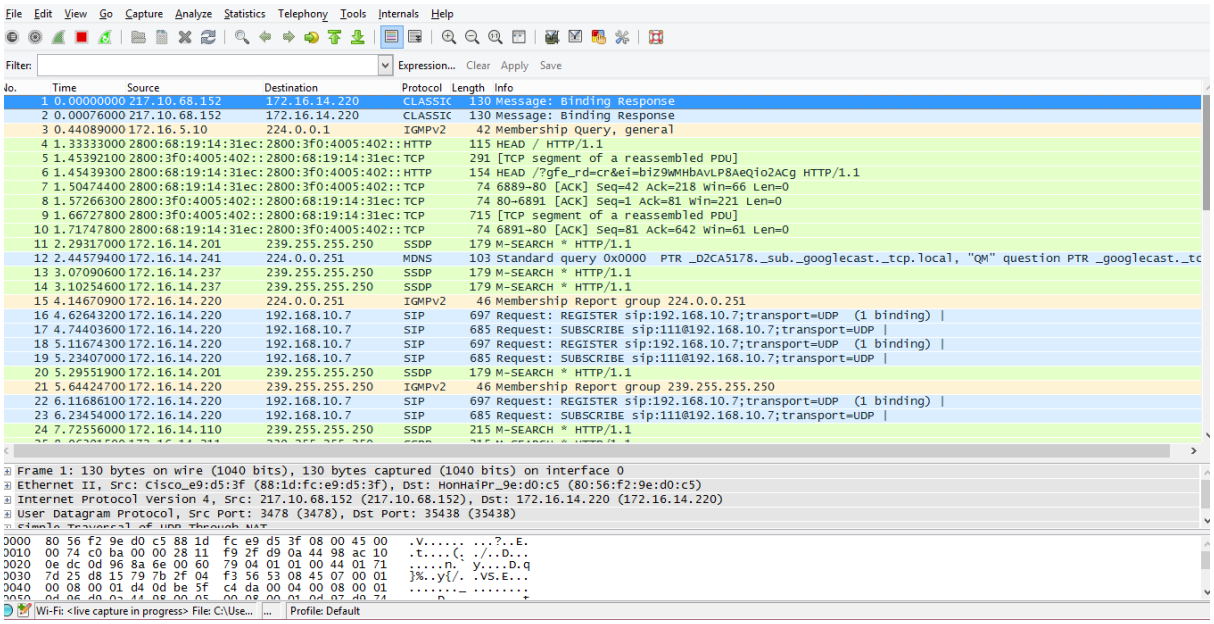


Figura 40. Análisis de paquetes mediante Wireshark.
Fuente: Captura de software Wireshark.

3.4.2.4.Ingeniería social.

La ingeniería social es considerada uno de los ataques más comunes y peligrosos, consiste en manipular a la víctima mediante una visita personal; el atacante busca sacarle información de manera sutil y poco sospechosa, esto requiere de un buen manejo de

habilidades sociales más que tecnológicas; pero puede ser muy efectiva, la clave del atacante es sobre todo hacer sentir bien a la víctima y ganarse su confianza.

Con este método de ataque se puede acceder a un punto de red, a una red inalámbrica, a servicios de la institución, a la infraestructura de la red; es decir, este ataque puede ser enfocado a cualquier área. Un ejemplo podría ser que el atacante se haga pasar por un estudiante o empleado de la institución, y en último caso por un visitante para acceder a su propósito, ya dentro de la red todo depende de la habilidad de este para ingresar a los sistemas más riesgosos.

3.4.2.5.Ataque de Fuerza Bruta.

Para ello se crea un diccionario mediante la herramienta Crunch propia de Kali Linux, para luego hacer el ataque con la herramienta Hydra, el proceso es el siguiente:

- Creación del diccionario con el comando crunch 1 5 abcdefghijklmnsopqrstuvwxyz > wordlist.txt
- Se elige el tamaño del archivo y se genera.

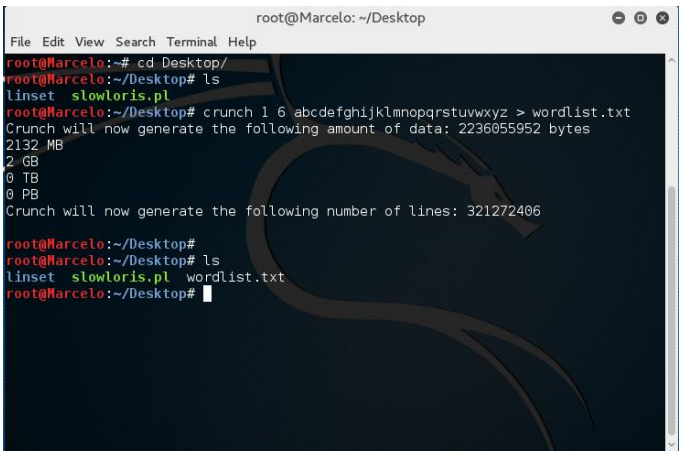


Figura 41. Creación del diccionario.
Fuente: Captura del sistema operativo Kali Linux.

EL siguiente paso es realizar el ataque con la ayuda de la herramienta Hydra, la cual conjuntamente trabaja con el diccionario creado anteriormente, el comando para la ejecución del ataque se observa en la Figura 42.

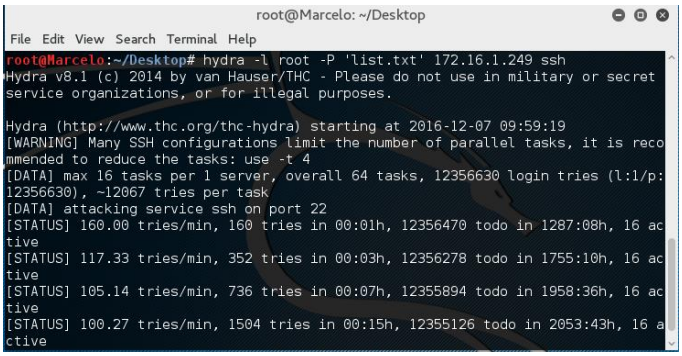


Figura 42. Ataque de Fuerza Bruta.
Fuente: Captura del sistema operativo Kali Linux.

Este comando hace que Hydra compare o intente autenticarse como usuario root con las posibles claves que están en el diccionario.

3.4.2.6.Ataque DDoS Servidor Web.

También se puede realizar un ataque por medio de denegación del servicio sea este DoS o DDoS. La diferencia entre DoS y DDoS, es que en el primero el ataque se realiza por un solo ordenador o persona y en el segundo el ataque es distribuido por dos o más personas, o dos o más bots (ordenadores zombies controlados por un atacante).

Hping3.- Es un mecanismo de ataque que genera paquetes y analiza el protocolo TCT/IP; herramienta que se utiliza para pruebas de firewall y redes.

Antes del ataque se midió la velocidad de conexión de los usuarios.

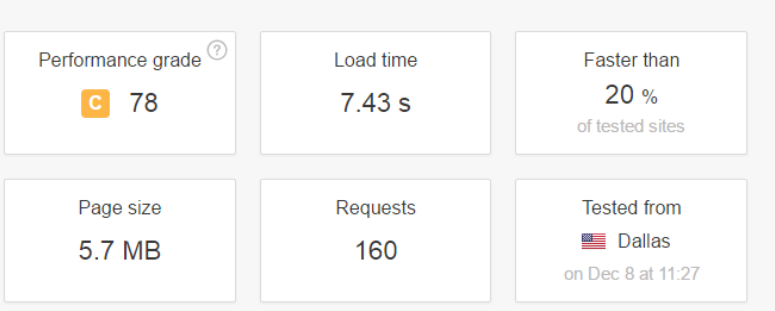


Figura 43. Tiempo de ingreso del portal web antes del ataque.
Fuente: Recuperado de https://tools.pingdom.com/#!/cuEjVc/http://www.utn.edu.ec

El tiempo de carga desde Dallas es 7.43 segundos.

Se ejecuta el ataque, pero antes es vital conocer en que consiste y cómo funciona el comando que se ejecuta en la Figura 44.

Hping3 nombre del ataque.

- -c 100000 número de paquetes que se envía.
- -d 120 tamaño del paquete.
- -s determina que solo son paquetes SYN.
- -w 64 tamaño de la ventana TCP.
- -p 80 el puerto destino para un servidor WEB.
- --flood modo de envío rápido, modo inundación.
- --rand-source para que las IPs de origen sean aleatorias.
- www.utn.edu.ec página víctima.

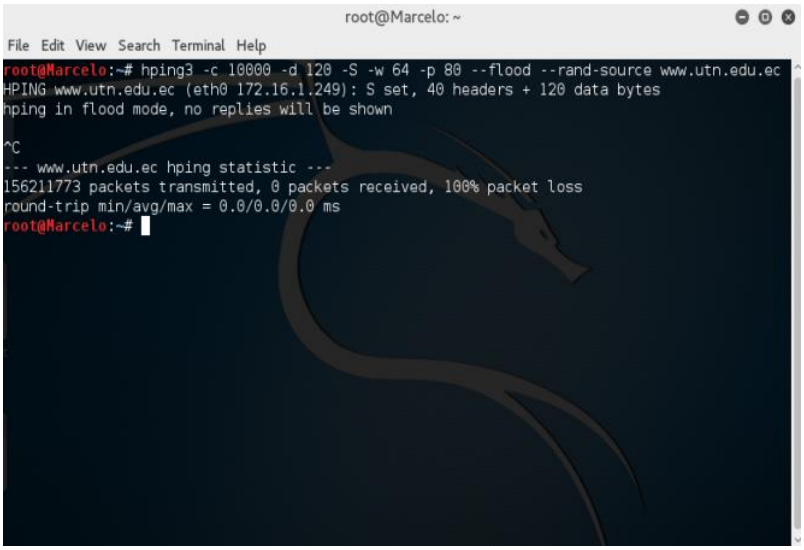


Figura 44. Ejecución del ataque hping3.
Fuente: Captura del sistema operativo Kali Linux.

Desde Dallas se intentó logear a la página WEB, se nota un insignificante cambio de velocidad, esto prueba que un solo atacante no puede dar de baja a la página WEB de la Universidad Técnica del Norte.

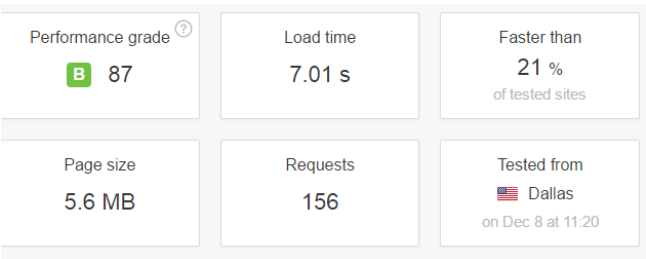


Figura 45. Tiempo de respuesta de la página web durante el ataque.
Fuente: Recuperado de https://tools.pingdom.com/#!/cuEjVc/http://www.utn.edu.ec

3.4.2.7.Ataque DDoS Servidor DNS.

De la misma manera se realiza un ataque DDoS al Servidor DNS, no se necesita la dirección IP, ya que también se puede realizar el ataque al dominio y al puerto 53 propio de un Servidor DNS.

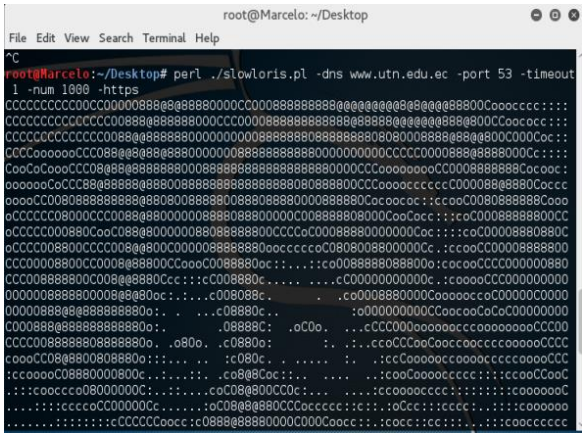


Figura 46. Ataque DoS al DNS
Fuente: Captura del sistema operativo Kali Linux.

A pesar de no ser un ataque tan fuerte, se bajó el servicio DNS mediante la inundación de peticiones como se muestra a continuación en la Figura 47, lo que hizo colapsar al servidor, y que este no reconozca ningún dominio. Cabe mencionar que cuando se dejó de ejecutar el ataque la página Web volvió a funcionar normalmente.

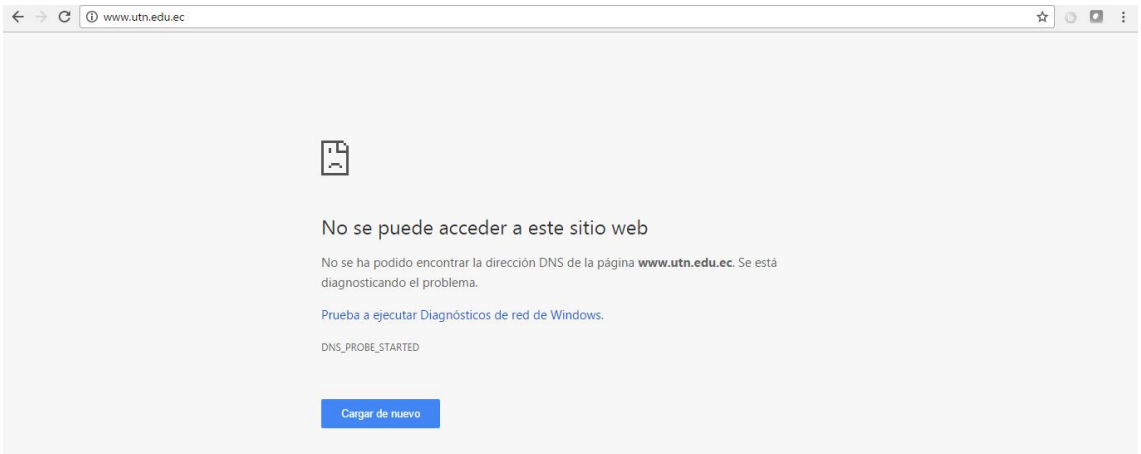


Figura 47. Resultado del Ataque.
Fuente: Captura del Navegador.

3.4.2.8. Dnschef

Esta herramienta permite conocer al servidor DNS que se encarga de traducir un dominio. Dnschef se convierte en dicho servidor DNS registrando la actividad que pasa por él y además posibilita la traducción de cualquier dominio a Ips.

En la Figura 48. Ip de los DNS.Figura 48 se muestra la Ip del servidor real y la dirección de defecto de Kali Linux que sirve para remplazar al DNS víctima, esto se realiza en el fichero cd /etc/resolv.conf.

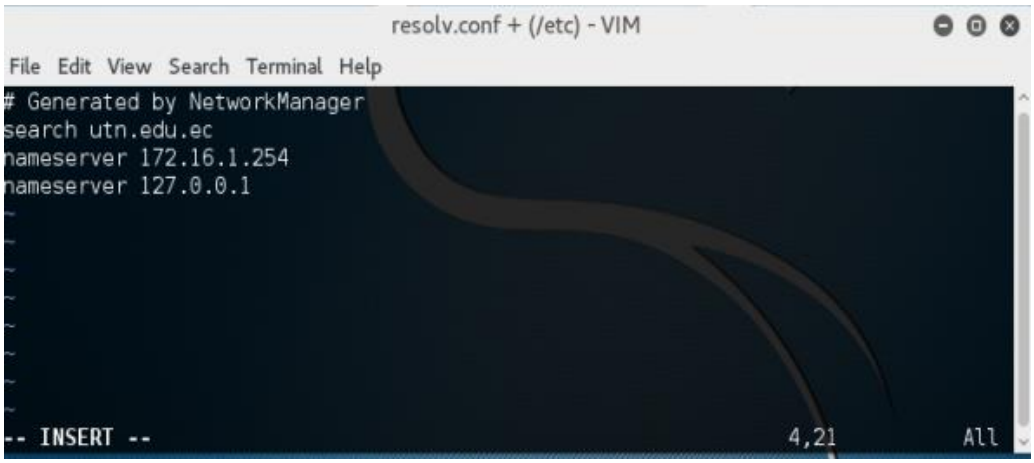


Figura 48. Ip de los DNS.
Fuente: Captura del sistema operativo Kali Linux.

Después de haber escrito las direcciones de los DNS, se ejecuta la herramienta dnschef con el comando que se muestra en la Figura 49, una vez ejecutado se puede realizar búsquedas en el dominio real.

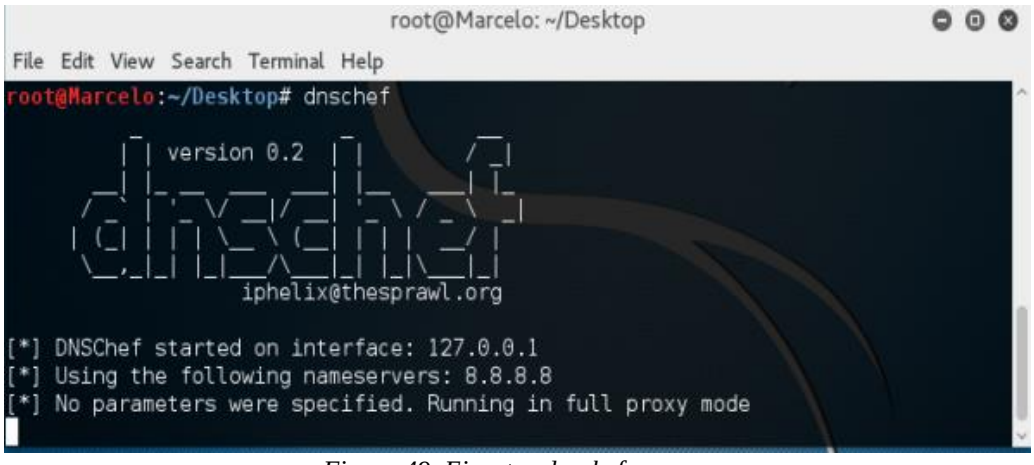


Figura 49. Ejecutar dnschef.
Fuente: Captura del sistema operativo Kali Linux

Una vez que esté ejecutándose dnschef hay que realizar algunas búsquedas para identificar los tipos de comunicación que tiene el servidor DNS de la Universidad Técnica del Norte, en la Figura 50 se utiliza comandos para descubrir algunos nameservers.

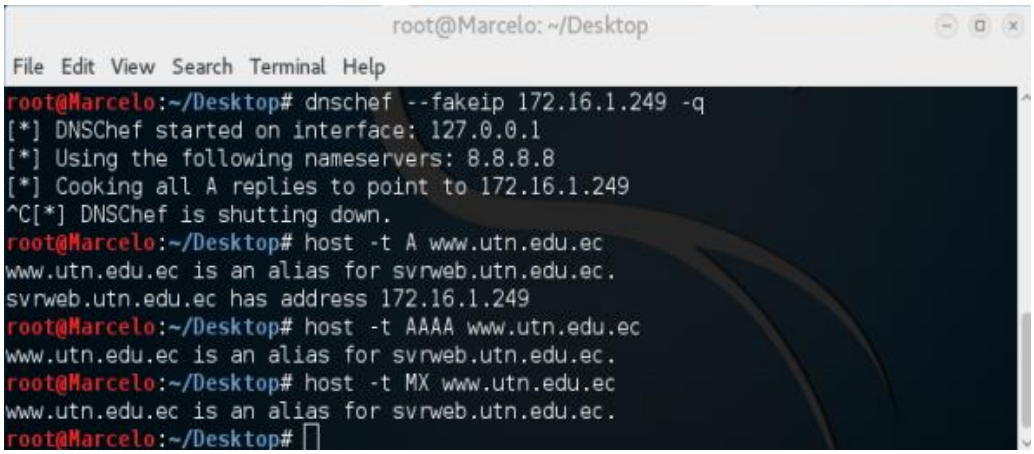


Figura 50. NameServers.
Fuente: Captura del sistema operativo Kali Linux.

3.5. Análisis de Resultados

En esta fase se analiza los resultados de los ataques. Una vez que se llega a esta etapa se debe tener en cuenta si la meta se alcanzó, que en este caso era mejorar el sistema de seguridad de la organización, caso contrario se repite el ciclo a la fase 1 que es la recolección de información o se finaliza las pruebas y se realiza el último paso.

Análisis Final y Documentación

Se debe realizar un informe detallado que abarque los resultados obtenidos durante la ejecución del pen testing con el respectivo análisis de la información obtenida y con las respectivas soluciones ante los problemas de seguridad encontrados.

Adicionalmente se incluye:

- Lo positivo que se encontró en el sistema.
- Aspectos en los que se puede mejorar el sistema (Isaza, 2013).

3.5.1. Análisis General de Resultados.

El mayor problema en la red interna es la facilidad de acceder a la red cableada o la inalámbrica, puesto se encontró redes libres y otras de fácil acceso.

Por parte de los servicios de internet evaluados se llegó a la conclusión de que se necesitan certificados digitales, como SSL/TLS y HTTPS; esta implementación aumentará la seguridad de estos servicios. En el proceso de escaneos se obtuvo abundante información útil para cualquier atacante, como, por ejemplo: puertos abiertos por defecto y direcciones IPs fácil de encontrar. Esto puede solucionarse mediante políticas de seguridad en el siguiente capítulo.

3.5.2. Lo negativo del sistema.

Después del análisis realizado se encontró las siguientes debilidades en el sistema:

- Hay una gran cantidad de archivos en la página WEB, lo que hace que la conexión no sea rápida.
- La página no cuenta con certificados digitales de un organismo autorizado, lo que existe es un certificado propio del administrador.
- El dominio principal es único, no tiene alias para acceder a la página lo que es un limitante al momento de que los usuarios quieran conectarse.

- El DNS tiene un problema interno ya que siempre hace el NAT dentro y fuera de la red, provocando lentitud de conexión en la red local.
- El servidor WEB tiene los puertos propios del servicio, lo que hace más fácil determinar su localización al igual que del servidor DNS.
- Tener conexiones remotas mediante SSH implica un riesgo, ya que es un medio idóneo para que cualquier atacante busque autenticarse a los servicios.
- Tener habilitado varios servicios en un equipo hace que el atacante tenga más opciones para ingresar al objetivo principal.

3.5.3. Lo positivo del sistema.

Después del análisis realizado se encontró las siguientes fortalezas en el sistema:

- El acceso directo al Servidor WEB tiene un alto grado de dificultad ya que no tiene muchos usuarios administradores y tiene contraseñas robustas. Para el caso del Domino se tiene seguridades ante ataques de DNS Snooping.
- La estabilidad de la página WEB ante ataques de DoS es aceptable ya que no hubo mucho cambio en la velocidad de conexión de los usuarios.

3.5.4. Aspectos que se puede mejorar.

Se tiene los siguientes aspectos a mejorar:

- Se sugiere separar los servicios de Internet que se encuentran en producción en diferentes equipos físicos.
- Implementar Políticas que obliguen un cambio periódico de las claves e incrementar la dificultad, que no solo incluya números y letras.
- Cuidar los accesos inalámbricos y cableados de la red interna; utilizar un mecanismo de autenticación.

3.5.5. Cuadro Resumen del Análisis de Resultados Obtenidos y Soluciones.

En la Tabla 20 se muestra los resultados obtenidos durante la realización de ataques informáticos en la red de datos universitaria, se utilizó herramientas de open source como Kali Linux, que es el sistema operativo con más herramientas para la realización de una auditoría informática; esto se realizó dentro y fuera de la institución, es decir se ejecutó ataques internos y externos.

Tabla 20. Resumen de los resultados obtenidos y planteamiento de soluciones.

ATAQUE	OBJETIVO	RESULTADO	SOLUCIÓN
Escaneo de Puertos	Servidor WEB	Se obtuvo los puertos abiertos del servidor.	Bloquear puertos innecesarios y cambiar los de defecto de ser posible.
Escaneo de Puertos	Servidor DNS	Se obtuvo los puertos abiertos del servidor.	Bloquear puertos innecesarios y cambiar los de defecto si es posible.
Phishing	Servidor WEB y DNS	Se hizo una página clon del servidor WEB.	Tener firmas digitales por organismos

			reguladores, SSL y HTTPS.
Extraer Metadata	Servidor WEB	Se extrajo todos los archivos que tiene la página WEB.	Información crítica no debe ser subida a la página WEB.
Snooping	Servidor DNS	Se obtuvo dominios resueltos por parte del Servidor DNS.	Borrar el caché DNS periódicamente, que no sean útiles.
Ataque de Autenticación con Winscp.	Servicio SSH	Se intentó acceder al servidor SSH con resultado negativo.	Cambiar periódicamente contraseñas con un igual o mayor grado de dificultad.
Ataque a la red Inalálmbrica	AP Inalámbrico	Se accedió a la red inalámbrica mediante el uso de la herramienta llinset.	Poner claves de autenticación para todos los AP e implementar algún tipo de control para el acceso.
Ataque a la red Cableada	Puntos de Red	Se accedió a la red cableada mediante un punto de red libre.	Implementar algún tipo de control de acceso.
Ataque de Fuerza Bruta	Servicio SSH	Se creó diccionarios para autenticarse por medio de este ataque.	Poner claves robustas y reducir usuarios.
Ataque DoS	Servidor WEB	Se utilizó un ataque Hping3.	Liberar espacio de la página WEB y mejorar el procesamiento.

Fuente: Autor.

Capítulo 4. Elaboración de Políticas de Seguridad.

En este capítulo se tiene como referencia a toda la información de la auditoria informática que se efectuó en la red interna de la Universidad Técnica del Norte, para luego proceder a la elaboración de políticas de seguridad según la norma ISO/IEC 27001.

4.1. Procedimiento para la elaboración de Políticas de Seguridad.

Según (Tools sf, 2015) el procedimiento para la elaboración de Políticas de Seguridad consiste en 7 pasos como se muestra en la Tabla 21:

Tabla 21. Procedimiento para la elaboración de políticas de seguridad.

Fase	Título	Descripción
1	Estudiar los requisitos.	Informarse acerca de una legislación que obligue incluir algún elemento específico (contratos de un cliente) y los requisitos de la norma ISO-27001.
2	Resultados del análisis de riesgos.	Los resultados determinarán los temas que se deben abordar en el documento.
3	Optimizar y alinear sus documentos.	Los documentos de Gestión de Seguridad de la Información basados en la ISO 27001.
4	Estructurar el documento.	La empresa tiene que definir un formato para todos sus documentos.
5	Redactar el documento.	El documento debe ser lo menos complejo y tiene que involucrar a los empleados.
6	Conseguir la aprobación del documento.	Debe aprobarse con la persona con suficiente poder en la organización.
7	Capacitación y concienciación de sus empleados.	Los empleados deben involucrarse en el proceso para recibir con el suficiente interés.

Fuente: Norma ISO 27001.

4.2. Procedimiento para implementar políticas de seguridad según la norma ISO 27001.

Obtener el apoyo de la dirección. – Este punto es muy importante para la implementación de las políticas de seguridad según la norma ISO 27001, ya que se debe contar con suficientes recursos humanos que trabajen en el proyecto y el suficiente apoyo económico.

Tomarlo como proyecto. - Debido a que la implementación de políticas de seguridad es un tema complejo que involucra diversas actividades, personas y demanda de mucho tiempo; se debe tomar con la responsabilidad del caso.

Definir el alcance. - Para una organización grande se puede implementar políticas de seguridad en un departamento o en alguna área de las comunicaciones; esto reduce el riesgo del proyecto.

Redactar una Política de SGSI. - No debe ser muy detallado, pero debe tener temas básicos de seguridad de la información de la institución; con el objetivo de mejorar la seguridad informática de la organización.

Definir la metodología de Evaluación de riesgos. - El objetivo de esto es definir reglas para identificar los activos, las vulnerabilidades, las amenazas, las consecuencias, las probabilidades y el nivel de riesgo.

Realizar la evaluación y el tratamiento de riesgos. - Se realiza un informe sobre la evaluación de riesgos que documente todos los pasos, con ello la aprobación de los riesgos residuales.

Redactar la Declaración de aplicabilidad. - Al finalizar el tratamiento de riesgos, se identificará qué controles del Anexo se necesita y cuáles no. La Declaración de aplicabilidad sirve para obtener la autorización de la dirección para implementar el SGSI.

Redactar el Plan de tratamiento del riesgo. - El objetivo es definir cómo se implementarán los controles de la Declaración de aplicabilidad, quién lo hará, cuándo, etc. Es un plan de implementación enfocado sobre los controles.

Determinar cómo medir la eficacia de los controles. - Se debe medir los objetivos logrados establecidos tanto para todo el SGSI como para la Declaración de aplicabilidad.

Implementación de controles y procedimientos obligatorios. - Generalmente se aplica nuevas tecnologías y nuevas conductas en la organización. Se debe implementar cuatro procedimientos obligatorios y los controles correspondientes del Anexo A.

- El procedimiento para el control de la documentación, debe definir quién es el responsable de aprobar y verificar los documentos, este procedimiento define cómo funcionará el flujo de documentos de la organización.

- El procedimiento para auditorías internas, define responsabilidades sobre la planificación y realización de auditorías, cómo se informan los resultados y sus registros.
- El procedimiento para medidas correctivas, define cómo se identifican los incumplimientos y sus causas, cuáles son las acciones necesarias, qué registros se llevan y cómo se revisa las medidas.
- El procedimiento para las medidas preventivas, se diferencia del anterior en que el objetivo es eliminar la causa del incumplimiento para que no se produzca. Debido a sus semejanzas se los puede unificar.

Implementar programas de capacitación y concienciación. - Se requiere que los empleados implementen todas las nuevas políticas y procedimientos, por lo tanto, se les debe explicar la importancia y la necesidad para luego capacitarlos.

Auditoría Interna. - Cuando los trabajadores no son conscientes de que están haciendo algo mal o no quieren que los descubran dañan a la organización, por eso la importancia de hacer auditorías internas para descubrir este tipo de cosas.

Medidas correctivas y preventivas. - El objetivo del sistema de gestión es corregir los errores o evitarlos. Para eso se realiza manuales de procedimientos correctivos y preventivos según la norma ISO 27001, es decir que se solucione y se controle.

4.3. Desarrollo de las políticas de seguridad.

Se propone elaborar políticas de seguridad para mejorar el sistema organizacional de la Dirección de Desarrollo Tecnológico e Informático, para esto a continuación se detallan los datos informativos para empezar su elaboración:

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD TÉCNICA DEL NORTE.
Título:	Planteamiento de Políticas de Seguridad basado en la norma ISO/IEC 27001 para la Dirección de Desarrollo Tecnológico e Informático de la Universidad Técnica del Norte.
Autor de la propuesta:	Sr. Marcelo León Gudiño.
Director de trabajo: **Co-Director de trabajo:**	Msc. Fabián Cuzme Rodríguez. Msc. Luis Suárez.
Beneficiario:	Dirección de Desarrollo Tecnológico e Informático de la Universidad Técnica del Norte.
Ubicación:	Avenida 17 de Julio, 5-21, y Gral. José María Córdova.
Tiempo estimado para desarrollar la propuesta:	Fecha de Inicio: diciembre del 2016, Fecha de finalización: enero 2017.
Equipo colaborador:	Funcionarios: Ing. Vinicio Guerra, Ing. Edison Carrión e Ing. Alex Guevara.

4.3.1. Objetivo.

Establecer lineamientos respecto a la Seguridad de la Información en la Universidad Técnica del Norte, con la finalidad de mejorar la organización en las áreas

de Infraestructura y Aplicaciones; mejorando así los servicios de la red tomando en cuenta criterios de confidencialidad, disponibilidad e integridad.

4.3.2. Alcance.

Se presenta a la Dirección de Desarrollo Tecnológico e Informático de la Universidad Técnica del Norte, las políticas desarrolladas en base a la norma ISO 27001; se tiene la elaboración de políticas para la seguridad considerando aspectos generales de organización y para la parte técnica se aborda las áreas de Infraestructura y Aplicaciones.

Para este proyecto de grado se tiene como alcance el desarrollo de las etapas de creación, aprobación e implementación de políticas de seguridad según la norma ISO 27001; y a su vez se considera todos los pasos de implementación de las mismas. De la misma manera la realización de manuales de procedimientos, estos se deben ejecutar ante cualquier tipo de ataque informático que surja en la institución, para ello se tomó en cuenta los procesos elementales según la norma ISO 27001.

Por último, las políticas y procedimientos se socializarán con la Dirección de Desarrollo Tecnológico e Informático de la Universidad Técnica del Norte, para su posterior revisión y aprobación.

4.3.3. Aplicabilidad.

En el documento se tiene todos los beneficiarios según lo determina la política, entre ellos se tiene los siguientes:

- La Dirección de Desarrollo Tecnológico e Informático.

- Administrador de la red.
- Administrador de aplicaciones.

4.3.4. Excepciones.

Este documento sirve como guía para la organización en cuanto a seguridad informática, dado el caso de que existan problemas que no consten en las soluciones de las políticas el Director de la Dirección de Desarrollo Tecnológico e Informático tiene la autoridad para decidir la solución del problema, de igual manera tiene la potestad de anular, modificar y actualizar el documento.

4.3.5. Políticas de Seguridad.

El manual de políticas de seguridad describe de manera detallada los objetivos de gestión de infraestructura y aplicaciones; que a su vez contiene: formato de políticas de la Universidad Técnica del Norte, firma de autor, firmas de revisión del encargado de la red interna y encargado del portal Web, y las fechas de revisiones.

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD TÉCNICA DEL NORTE
Elaborado por:	Marcelo León
Firma:	…….
Fecha de elaboración:	
Revisado por:	Ing. Vinicio Guerra Administrador de la Red
Firma:	…….
Revisado por:	Alex Guevara Administrador del Portal Web
Firma:	……
Fecha de revisión:	

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD TÉCNICA DEL NORTE
Control:	Política de Seguridad
Destinatario:	Dirección de Desarrollo Tecnológico e Informático

TÍTULO I.

POLÍTICAS DE SEGURIDAD PARA LA DIRECCIÓN DE DESARROLLO TECNOLÓGICO E INFORMÁTICO.

Capítulo 1.

Políticas de Seguridad Generales.

Art 1.- Este documento, "Políticas de seguridad en base a la norma ISO 27001", estable como se debe manejar la seguridad de la información en la gestión de infraestructura y aplicaciones.

Art 2.- Brindar una guía para los administradores de la red y encargados de las aplicaciones sobre políticas que deben cumplir para conservar los activos.

Art 3.- El director de TI es el responsable de que se haga cumplir las políticas y los procedimientos.

Art 4.- Revisar las políticas de seguridad considerando un periodo de 6 meses de acuerdo a las nuevas necesidades de la institución, con la finalidad de ser actualizadas de ser necesario.

Art 5.- Las políticas deben ser socializadas con todos los funcionarios que integran la Dirección de Desarrollo Tecnológico e Informático.

Capítulo 2.

Políticas Generales a los administradores.

Art. 6.- Cada vez que se necesite formatear los equipos del data center se debe hacer un respaldo de la información y de las configuraciones.

Art 7.- Todos los administradores deben cambiar las contraseñas de los equipos que se encuentran en el data center cada tres meses.

Art 8.- Las contraseñas deben ser mayores a 8 caracteres, de alto grado de dificultad, compuestas por letras minúsculas, mayúsculas, números y símbolos.

Art 9.- Los administradores no deben utilizar la misma contraseña en todos los equipos que tienen a su cargo, ni tampoco compartir estas contraseñas con personas que no están autorizadas o que son ajenas a la institución.

Art 10.- No abrir documentos adjuntos de dudosa procedencia, y tampoco hacer clic en enlaces de mensajes solicitados cuando no se conozca el origen de los mismos.

Art 11.- No proporcionar datos personales a desconocidos por teléfono o e-mail, sin antes validar el origen de la petición.

Capítulo 3.

Políticas de Seguridad para la Infraestructura.

Art. 12.- Todas las redes inalámbricas deben tener un sistema de autenticación para los usuarios.

Art 13.- Solo los equipos de computación de la UTN deben estar configurados para que puedan conectarse a la red cableada.

Art 14.- Se debe manejar sistemas de seguridad perimetral que permitan detectar intrusiones de personas a la institución, esto se realiza con la implementación de un sistema IDS.

Art 15.- Los servidores que se encuentran en producción en el data center deberán tener un sistema antivirus.

Art 16.- Todas las conexiones remotas del personal de la DDTI deben tomar las medidas de seguridad correspondientes, para esto se determina la utilización de VPNs y las directrices dadas en el Art. 8 para la creación de contraseñas.

Art 17.- La comunicación entre los equipos de telecomunicaciones del data center debe tener en cuenta la utilización de llaves públicas o métodos de encriptación de datos.

Capítulo 4.

Políticas de seguridad para las aplicaciones.

Art. 18.- Todas las aplicaciones deben tener las actualizaciones y parches correspondientes, con la finalidad de mejorar su funcionamiento.

Art 19.- Todos los puertos necesarios para el funcionamiento de los servicios del data center tienen que estar habilitados y los puertos que puedan ser perjudiciales en cuanto a seguridad deben ser cerrados.

Art 20.- Analizar la capacidad de los equipos en cuanto a la cantidad de aplicaciones que pueden soportar simultáneamente para que no exista sobrecarga o indisponibilidad del hardware donde corren los servicios.

Art 21.- Cuando exista la necesidad de adquirir software que no pueda ser desarrollado internamente, se deberá solicitar a proveedores externos debidamente certificados y con el aval del Director de la DDTI.

Art 22.- Toda modificación de las aplicaciones debe estar revisada y aprobada por el director de la DDTI, con la respectiva documentación de todo el proceso.

Art 23.- Las aplicaciones que se desarrollen internamente o se adquieran a proveedores deberán pasar por una auditoria de validación antes de ser implementadas dentro de la organización.

Art 24.- Todos los archivos críticos que se tienen en los servidores del data center de la DDTI deben estar cifrados.

Art 25.- El servidor donde está alojado el portal Web debe tener certificados digitales que validen la seguridad del sitio, y a su vez, habilitar el puerto seguro https.

4.4. Procedimiento de seguridad.

Un procedimiento de seguridad es la definición detallada de los pasos a ejecutar para llevar a cabo cualquier tarea. Mediante los procedimientos de seguridad se aplica las políticas de seguridad que se han aprobado en la institución.

4.5. Manual de Procedimientos de Seguridad.

Antes de implementarse un manual de procedimiento de seguridad debe estar previamente revisado y aprobado por los encargados del área tecnológica, como se tiene a continuación.

Se tiene algunos manuales de procedimientos para cumplir con la norma ISO 27001, los obligatorios para la certificación son: el manual de procedimientos para el control de la documentación, manual de procedimientos para auditoria interna, manual de procedimientos para medidas correctivas y manual de procedimientos para medidas preventivas; adicional a esto se tiene manuales de procedimientos técnicos para implementar cualquier tipo de seguridad.

	MANUAL DE PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD TÉCNICA DEL NORTE
Elaborado por:	Marcelo León
Firma:	…….
Fecha de elaboración:	
Revisado por:	Ing. Vinicio Guerra Administrador de la Red
Firma:	…….
Revisado por:	Ing. Alex Guevara Administrador del Portal Web
Firma:	……
Fecha de revisión:	

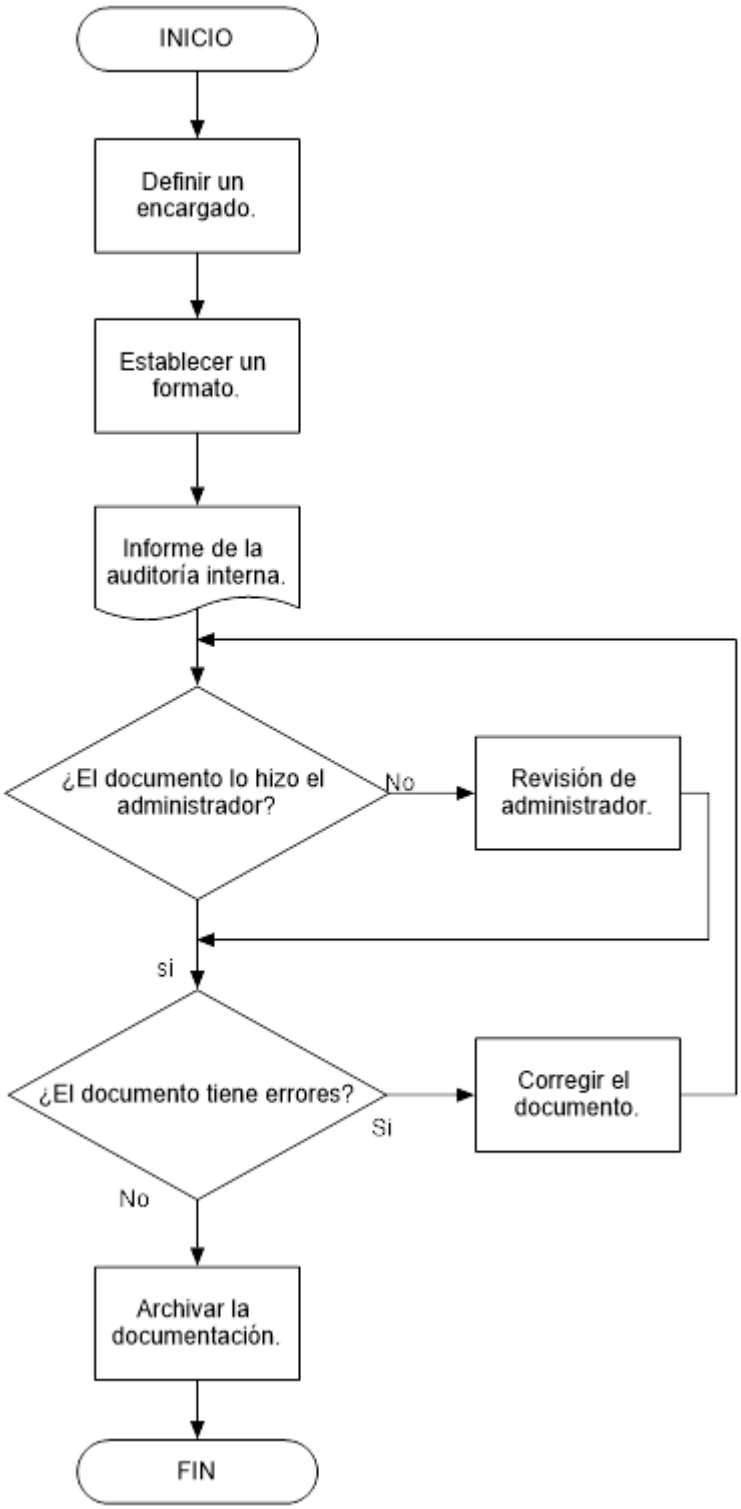
4.5.1. Manual de procedimientos para el control de la documentación.

	MANUAL DE PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD TÉCNICA DEL NORTE
Control:	Manual de Procedimientos de Seguridad.
Destinatario:	Dirección de Desarrollo Tecnológico e Informático
Nombre:	Procedimiento para el control de la documentación.
Objetivo:	Mejorar la organización de los administradores en cuanto a la seguridad de sus equipos y aplicaciones.

ACTIVIDAD	DESCRIPCIÓN
1	Definir quién es el encargado de aprobar y verificar los documentos, emitidos por todos los trabajadores de la DDTI.
2	Determinar un único formato para toda la documentación con respecto a la seguridad de la información.
3	Emitir un informe de alguna auditoria interna de seguridad en la red o cualquier otro documento, por parte de uno de los administradores de la DDTI.
3.1	En el caso que sea elaborado por un técnico o por una empresa externa a la organización debe ser revisado por el jefe del área.
3.2.	Si el documento es elaborado por el administrador se toma como válido y se procede a la revisión del encargado de la documentación,
4	Revisar y aprobar la documentación.

4.1.	En el caso de que se encuentre errores en el documento, el encargado tiene la obligación de emitir las observaciones y proceder a devolver el documento para que sea corregido.
4.2.	Si el documento cumple con todas las exigencias, el encargado debe aprobar y almacenar esta información con el debido proceso.
5	Archivar la información con su debido registro, es decir dónde se realizó la auditoría y las observaciones del caso.
6	FIN DEL PROCESO

Manual de procedimientos para el control de la documentación.



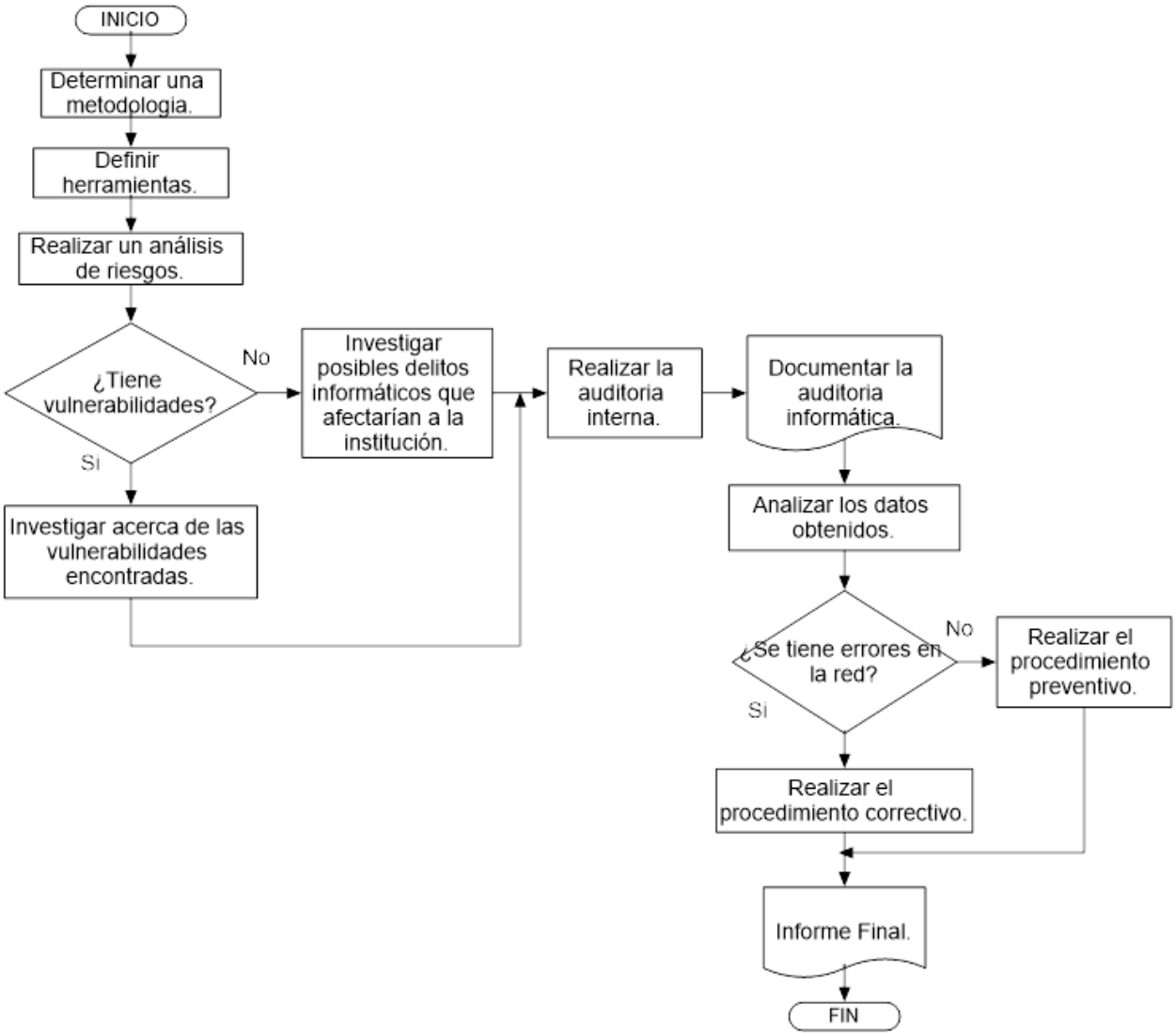
4.5.2. Manual de procedimientos para auditoria interna.

	MANUAL DE PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD TÉCNICA DEL NORTE
Control:	Manual de Procedimientos de Seguridad.
Destinatario:	Dirección de Desarrollo Tecnológico e Informático
Nombre:	Procedimiento para auditoría interna.
Objetivo:	Definir responsabilidades sobre la planificación y realización de auditorías.

ACTIVIDAD	DESCRIPCIÓN
1	Determinar una metodología para la auditoría interna de seguridad.
2	Definir el software que se va utilizar para realizar la auditoría interna de seguridad.
3	Realizar un previo análisis de riesgos para determinar las vulnerabilidades actuales del sistema, para posteriormente ser explotadas.
3.1.	En el caso que se tenga vulnerabilidades se las utiliza como punto de partida para evaluar las partes criticas del sistema.
3.2	Si en el análisis de riesgos se tiene resultados positivos, se debe investigar nuevos ataques e información acerca de delitos informáticos relacionados a lo que se tiene en la organización.
4	Realizar la auditoría informática en la red de datos de la organización.
5	Documentar todo el proceso de la auditoría interna.

6	Analizar los resultados obtenidos de la auditoría interna.
6.1.	En el caso de que se tenga errores en la red interna se debe realizar el procedimiento correctivo como nos dice el manual.
6.2.	Si la auditoría interna da resultados positivos, se procede a realizar el procedimiento preventivo como nos dice el manual, esto se ejecuta para no tener inconvenientes futuros.
7	Realizar un informe final de todo lo que se realizó en la auditoría interna para luego ser revisado y aprobado como se puede verificar en el manual de procedimientos para la documentación.
8	FIN DEL PROCESO.

Manual de procedimientos para la auditoría interna.



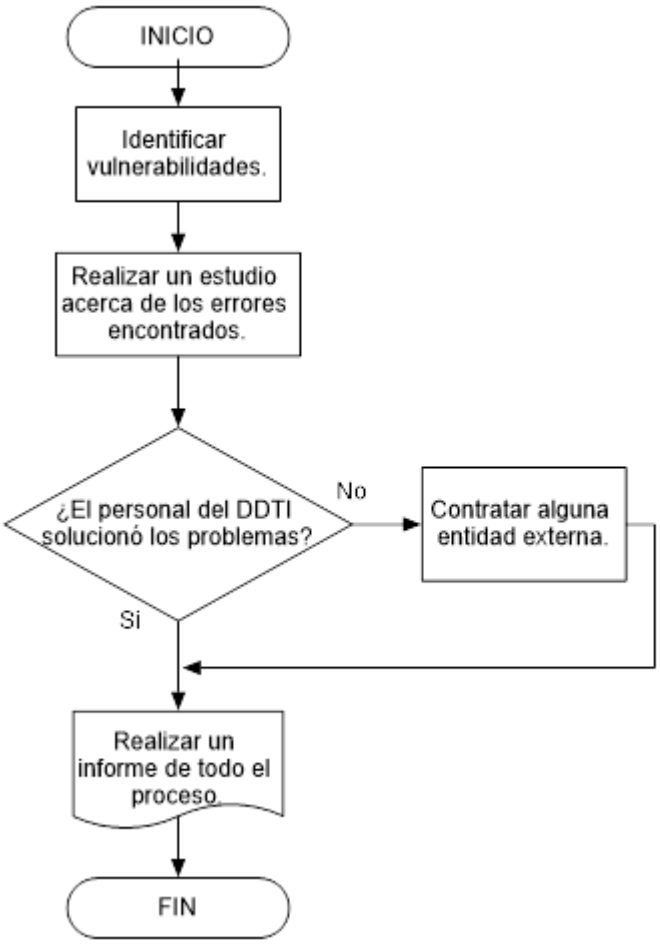
4.5.3. Manual de procedimiento para medidas correctivas.

	MANUAL DE PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD TÉCNICA DEL NORTE
Control:	Manual de Procedimientos de Seguridad.
Destinatario:	Dirección de Desarrollo Tecnológico e Informático
Nombre:	Procedimiento para medidas correctivas.
Objetivo:	Identificar incumplimientos y sus causas para realizar acciones necesarias y corregirlas.

ACTIVIDAD	DESCRIPCIÓN
1	Identificar las vulnerabilidades que se tiene en la red de datos o de alguna aplicación.
2	Investigar estas vulnerabilidades mediante un estudio minucioso para determinar las razones y el origen del problema.
3	Solucionar los problemas de seguridad.
3.1.	En el caso de que se necesite alguna entidad externa para resolver los problemas de seguridad, se debe tener en cuenta las seguridades correspondientes para el uso de los equipos y las configuraciones realizadas
3.1.1	Exigir un informe detallado a la entidad externa de todo lo que se hizo para luego revisarlo, y por último registrarlo dado el caso de que el problema se repita, y así no requerir de la entidad nuevamente.

3.2.	Si las soluciones provienen del personal de la DDTI se debe realizar un informe detallado de la solución y seguir los lineamientos del manual de procedimientos para la documentación.
4	FIN DEL PROCESO.

Manual de procedimientos para medidas correctivas.



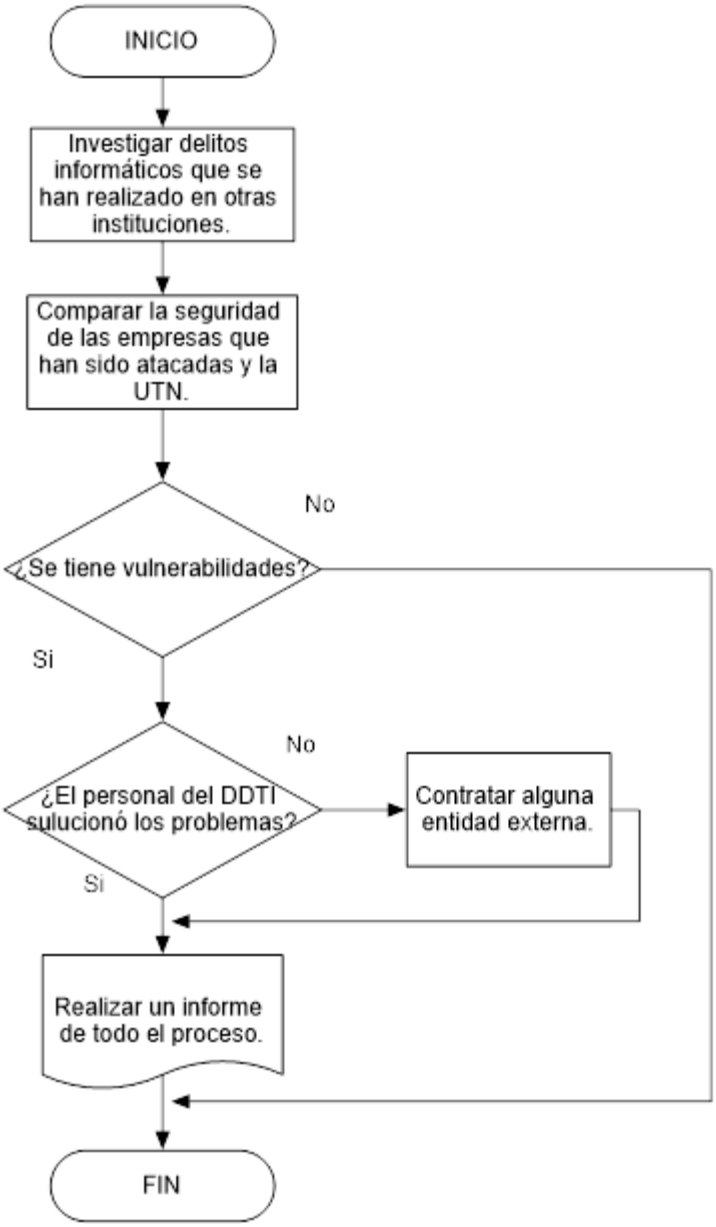
4.5.4. Manual de procedimientos para medidas preventivas.

	MANUAL DE PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD TÉCNICA DEL NORTE
Control:	Manual de Procedimientos de Seguridad.
Destinatario:	Dirección de Desarrollo Tecnológico e Informático
Nombre:	Procedimientos para medidas preventivas.
Objetivo:	Eliminar incumplimientos para que no se produzca algún error similar.

ACTIVIDAD	DESCRIPCIÓN
1	Investigar delitos informáticos en instituciones que cuenten con servicios similares a los de la UTN y los mecanismos que utilizaron los atacantes informáticos en dichas instituciones.
2	Comparar la seguridad que tienen las empresas que han sido atacadas, con la seguridad que tiene la UTN.
3	En el caso de que se tenga vulnerabilidades seguir con el procedimiento preventivo, caso contrario dar por terminado el proceso.
4	Solucionar los problemas de seguridad para evitar posibles ataques informáticos.
4.1.	En el caso de que se necesite de alguna entidad externa para que resuelva los problemas de seguridad, se debe tener en cuenta las seguridades correspondientes para el uso de los equipos y las configuraciones realizadas.
4.1.1	Exigir un informe detallado a la entidad externa de todo lo que se hizo para luego revisarlo, y por último, registrarlo dado el caso de

	que el problema se repita, y así no requerir de la entidad nuevamente.
4.2.	Si las soluciones provienen del personal de la DDTI se debe realizar un informe detallado de la solución y seguir los lineamientos del manual de procedimientos para la documentación.
5	FIN DEL PROCESO.

Manual de procedimientos para medidas preventivas.



4.5.5. Manual de procedimientos técnicos.

	MANUAL DE PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD TÉCNICA DEL NORTE
Control:	Manual de Procedimientos de Seguridad.
Destinatario:	Dirección de Desarrollo Tecnológico e Informático
Nombre:	Procedimientos para la obtención de certificados digitales.
Objetivo:	Implementar certificados digitales para mayor seguridad en las aplicaciones que se encuentran en la red.

ACTIVIDAD	DESCRIPCIÓN
1	Solicitar la autorización interna para la implementación de un certificado digital SSL/TLS.
2	Investigar qué organismos autorizados existen y escoger cuál es el que mejor se adapta a las necesidades de la institución.
3.	Realizar la solicitud para la obtención del certificado digital.
4.	Registrar a la institución con el organismo certificador.
5.	Realizar el depósito con el valor de la implementación del certificado digital.
6.	Instalación del certificado digital.
7	FIN DEL PROCESO.

Manual de procedimientos para la obtención de certificados digitales.

Capítulo 5. Implementación de las políticas de seguridad y pruebas de funcionamiento.

En este capítulo se detalla todo lo relacionado a la implementación de soluciones a las vulnerabilidades encontradas por medio de políticas de seguridad según la norma ISO/IEC 27001, y se presenta una propuesta a la Universidad para la realización de una certificación internacional en esta norma. También se realiza pruebas de funcionamiento en las cuales se demuestra la confiabilidad de la infraestructura de la red interna y los servicios de Internet.

5.1. Implementación de políticas de seguridad para la DDTI.

Una vez que se haya implementado las políticas de seguridad, se debe realizar pruebas de verificación antes de ejecutarlas en los equipos de producción. En este capítulo se muestra las pruebas de funcionamiento de las soluciones que se propone, para así demostrar el incremento de seguridad para la infraestructura y las aplicaciones, específicamente en los servicios de WEB y DNS.

5.2. Implementación de manuales de procedimientos de seguridad para la DDTI.

Una vez que los manuales de procedimientos han sido aprobados por el director de la DDTI se procede a la socialización y capacitación del personal que esté involucrado en las áreas en donde se propone dichas soluciones.

5.3. Soluciones a las vulnerabilidades propuestas en las políticas de seguridad.

Dado que en el desarrollo del proyecto se determinó vulnerabilidades críticas en los sistemas, se va realizar soluciones que mitiguen estos problemas. A continuación, se describen las soluciones planteadas para mejorar el sistema de seguridad de los equipos del data center de la DDTI.

5.3.1. Certificación Digital SSL/TLS.

La Certificación Digital TLS (Transport Layer Security) se encarga de dar seguridad en la capa de transporte, su antecesor SSL (Secure Sockets Layer) capa de puertos seguros es un protocolo que permite a las aplicaciones transmitir información de manera segura. Por medio de este se brindará mayor seguridad a todos los usuarios del portal Web de la UTN ante ataques de phishing o suplantación de identidad.

A continuación, el proceso de instalación de un certificado digital SSL/TLS en el sistema operativo Centos el cual es donde está alojado el servidor Web:

En este proceso se va utilizar un certificado auto-firmado. Dentro de las políticas de seguridad se tiene que se debe utilizar un certificado que sea válido, esto se deja de propuesta en la DDTI.

Instalación del certificado digital auto-firmado.

El primer paso es instalar el repositorio de mod_ssl con el siguiente comando:

```
#yum install mod_ssl
```

Se debe tener conexión a internet antes de ejecutar el comando, se debe verificar que se instaló correctamente todos los paquetes como se muestra en la Figura 51.

Figura 51. Instalación SSL/TLS.
Fuente: Captura del sistema operativo Centos.

Luego se crea una carpeta donde va estar el certificado digital, esto mediante el comando:

```
#mkdir /etc/httpd/ssl_certs
```

Se crea el certificado usando RSA:2048 bits, el estándar x.509 y que expire en 2 años, para ello se tiene el siguiente comando:

```
#openssl req -x509 -nodes -days 730 -newkey rsa:2048 -keyout /etc/httpd/ssl_certs/ieceit.org.key -out /etc/httpd/ssl_certs/ieceit.org.cert
```

Después de haber ingresado estos comandos, sale una ventana en la que se solicita datos del emisor del certificado: para quién, en qué país, en qué provincia y en qué ciudad, esto se observa en la Figura 52.

```
[root@localhost conf]# mkdir /etc/httpd/ssl_certs
[root@localhost conf]# openssl req -x509 -nodes -days 730 -newkey rsa:2048 -keyout /etc/httpd/ssl_certs/ieceit.org.key -out /etc/httpd/ssl_certs/ieceit.org.cert
Generating a 2048 bit RSA private key
.....................................................................+++
.....................+++
writing new private key to '/etc/httpd/ssl_certs/ieceit.org.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:EC
State or Province Name (full name) []:IMBABURA
Locality Name (eg, city) [Default City]:IBARRA
Organization Name (eg, company) [Default Company Ltd]:UNIVERSIDAD TECNICA DEL NORTE
Organizational Unit Name (eg, section) []:MARCELO LEON
Common Name (eg, your name or your server's hostname) []:UNIVERSIDAD TECNICA DEL NORTE
Email Address []:mwleong@utn.edu.ec
[root@localhost conf]#
```

Figura 52. Creación del Certificado SSL/TLS.
Fuente: Captura del sistema operativo Centos.

Después es necesario reemplazar este archivo /etc/httpd/conf.d/ssl.conf con lo siguiente:

```
SSLCertificateFile /etc/httpd/ssl_certs

SSLCertificateKeyFile /etc/httpd/ssl_certs
```

En la Figura 53 se tiene la ubicación exacta donde se digita lo expuesto anteriormente.

```
#   SSL Engine Switch:
#   Enable/Disable SSL for this virtual host.
SSLEngine on

#   SSL Protocol support:
# List the enable protocol levels with which clients will be able to
# connect.  Disable SSLv2 access by default:
SSLProtocol all -SSLv2

#   SSL Cipher Suite:
# List the ciphers that the client is permitted to negotiate.
# See the mod_ssl documentation for a complete list.
SSLCipherSuite DEFAULT:!EXP:!SSLv2:!DES:!IDEA:!SEED:+3DES

#   Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate.  If
# the certificate is encrypted, then you will be prompted for a
# pass phrase.  Note that a kill -HUP will prompt again.  A new
# certificate can be generated using the genkey(1) command.
#SSLCertificateFile /etc/pki/tls/certs/localhost.crt
SSLCertificateFile /etc/httpd/ssl_certs/ieceit.org.cert
```

Figura 53. SSL_Certs y TLS/certs.
Fuente: Captura del sistema operativo Centos.

Finalmente, hay que resetear el servidor con el comando:

```
#service restart httpd.
```

Otra posibilidad de tener un certificado digital SSL, en este caso de código libre, es realizar el siguiente procedimiento. Primero, se genera el openssl con el comando que se muestra en la Figura 54.

```
[root@localhost /]# cd root/
[root@localhost ~]# openssl genrsa -out ca.key 2048
Generating RSA private key, 2048 bit long modulus
.....................................................+++
.....................................+++
e is 65537 (0x10001)
[root@localhost ~]#
```

Figura 54. Open ssl Key.
Fuente: Captura del sistema operativo Centos.

Luego, se crea el certificado propio con cualquier dato como se puede observar en la Figura 55.

```
[root@localhost ~]# openssl req -new -key ca.key -out ca.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:EC
State or Province Name (full name) []:IMBABURA
Locality Name (eg, city) [Default City]:IBARRA
Organization Name (eg, company) [Default Company Ltd]:UNIVERSIDAD TECNICA DEL NORTE
Organizational Unit Name (eg, section) []:MARCELO LEON
Common Name (eg, your name or your server's hostname) []:UNIVERSIDAD TECNICA DEL NORTE
Email Address []:mwleong@utn.edu.ec

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:sslUTN
An optional company name []:DDTI
[root@localhost ~]#
```

Figura 55. Certificado SSL/TLS.
Fuente: Captura del sistema operativo Centos.

Una vez realizado lo anterior, se procede a la encriptación de los datos mediante el comando que se muestra en la Figura 56.

```
[root@localhost ~]# openssl x509 -req -days 365 -in ca.csr -signkey ca.key -out ca.crt
Signature ok
subject=/C=EC/ST=IMBABURA/L=IBARRA/O=UNIVERSIDAD TECNICA DEL NORTE /OU=MARCELO LEON/CN=UNIVERSIDAD TECNICA DEL NORTE/emailAddress=mwleong@utn.edu.ec
Getting Private key
[root@localhost ~]#
```

Figura 56. Habilitar SSL/TLS.
Fuente: Captura del sistema operativo Centos.

Después es necesario copiar los archivos generados a un nuevo fichero como se indica en la Figura 57.

```
[root@localhost ~]# cp ca.crt /etc/pki/tls/certs/
[root@localhost ~]# cp ca.key /etc/pki/tls/private/
[root@localhost ~]# cp ca.csr /etc/pki/tls/private/
[root@localhost ~]#
```

Figura 57. Cambio de archivo SSL/TLS.
Fuente: Captura del sistema operativo Centos.

Realizado esto, se debe añadir la nueva ubicación de estos ficheros en ssl.conf para que sean ejecutados.

```
#   Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate.  If
# the certificate is encrypted, then you will be prompted for a
# pass phrase.  Note that a kill -HUP will prompt again.  A new
# certificate can be generated using the genkey(1) command.
#SSLCertificateFile /etc/pki/tls/certs/localhost.crt
#SSLCertificateFile /etc/httpd/ssl_certs/ieceit.org.cert
SSLCertificateFile /etc/pki/tls/certs/ca.crt
SSLCertificateKeyFile /etc/pki/tls/private/ca.key
SSLCertificateChainFile /etc/pki/tls/certs/example.com.ca-bundle
```

Figura 58. Ubicación del Certificado SSL/TLS.
Fuente: Captura del sistema operativo Centos.

Por último, se habilita el puerto seguro 443 en las reglas del Firewall para que el servidor acepte las peticiones por este puerto; una vez hecho esto se resetea el servicio de iptables.

```
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type echo-request -j REJECT --reject-with icmp-host-prohibited
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 20 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 20 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 21 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 21 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 3306 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 3306 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 53 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 53 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 547 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 547 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 7 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 7 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j DROP
-A INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

Figura 59. Reglas del Firewall Puerto Seguro.
Fuente: Captura del sistema operativo Centos.

Lo ideal en cuanto a la certificación digital SSL/TLS es que sea adquirida por un ente autorizado, se deja como propuesta la adquisición del certificado de Neothek que posee las siguientes características:

Tabla 22. Comparación Certificados SSL/TLS.

Características	**AlphaSSL**	**DomainSSL**	**OraganizationSSL**	**WildcardSSL**	**EV SSL**
Precio-año	$ 24.00	$ 119.00	$ 175.00	$ 330.00	$ 530.00
Sello					
Candado					
Cifrado 2048 bits					
Funciona en dispositivos moóviles					
Tecnología SGC	X				

Comunicaciones Unificadas (SANs)	X				
Exchange 2007 UC	X	Autodiscover	Autodiscover	-	-
Garantía contra emisiones falsas	1000	10000	1.25 millones	1.25 millones	1.50 millones
Protección Anti-Phishing	X	Gratis	Gratis	Gratis	Gratis
Validación de compañía completa	X	X			
SiteLock	X	Gratis	Gratis	Gratis	Gratis
Soporta Sub-dominios ilimitado	-	-	-		-
Tiempo de emisión	5 minutos	5 minutos	3 días	3 días	7 días

Fuente: Recuperado de https://www.neothek.com/certificados-ssl/Ecuador/

Tomando en cuenta las características anteriores se recomienda realizar la adquisición a partir de la segunda propuesta, ya que el requerimiento básico es que el certificado digital sea Anti-Phishing, y sea para un solo dominio, esto queda a consideración de la DDTI.

5.3.2. Portal Web con seguridad HTTPS.

La finalidad de HTTPS es lograr conexiones más seguras en la www, de esta manera la información sensible se encuentra cifrada, en caso de que ciertos datos sean

interceptados, no obstante, presenta vulnerabilidades cuando se aplica a contenido estático públicamente disponible.

Para conseguir la página web segura, la URL debe comenzar con “https://”, y también se debe habilitar el puerto 443, una vez hecho esto HTTPS utilizará encriptación SSL y TLS. El protocolo HTTP opera en la capa de aplicación del modelo TCP/IP, pero el protocolo HTTPS trabaja en la subcapa inferior, codificando el mensaje HTTP en la transmisión y decodificando la información antes de que llegue para la recepción.

```
LoadModule ssl_module modules/mod_ssl.so

#
# When we also provide SSL we have to listen to the
# the HTTPS port in addition.
#
Listen 443

##
##  SSL Global Context
##
##  All SSL configuration in this context applies both to
##  the main server and all SSL-enabled virtual hosts.
##
```

Figura 60. Habilitar puerto seguro.
Fuente: Captura del sistema operativo Centos.

5.3.3. Implementación de un IDS con SNORT.

Se propone instalar un servidor IDS en la red de la Universidad Técnica del Norte, con la finalidad de tener un equipo que permita detectar ataques al Data Center que es el principal objetivo para los delitos informáticos. Este servidor permitirá detectar intrusiones vía direccionamiento, puertos de servicios e interfaces por dónde se realicen los ataques.

Es recomendable que el servidor IDS instalado funcione bajo el Sistema Operativo PfSense, el cual permite un entorno gráfico en todas sus herramientas, en el Anexo 4 se detalla la instalación de dicho sistema operativo.

Instalación y configuración de Snort.

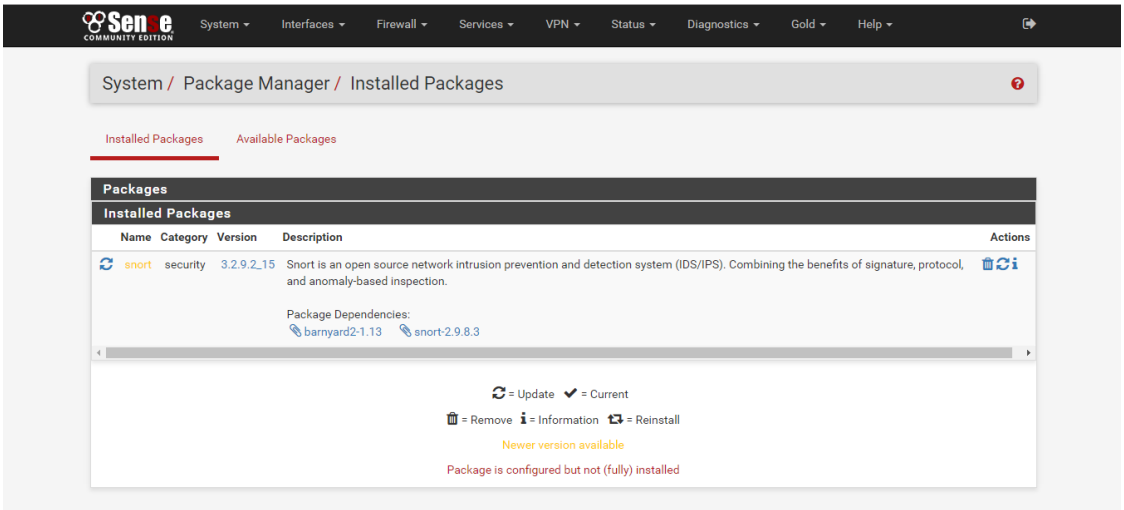


Figura 61. Descarga e instalación de Snort.
Fuente: Captura del sistema operativo PfSense.

Se crea una cuenta en SNORT completando la información requerida.

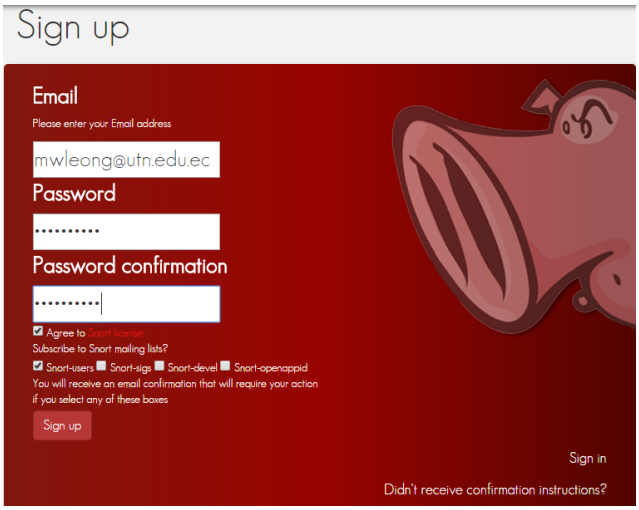


Figura 62. Creación de la cuenta Snort.
Fuente: Captura del servicio de Snort.

Contraseña: *******

Se ingresa el oinkcode como se muestra en la Figura 63:

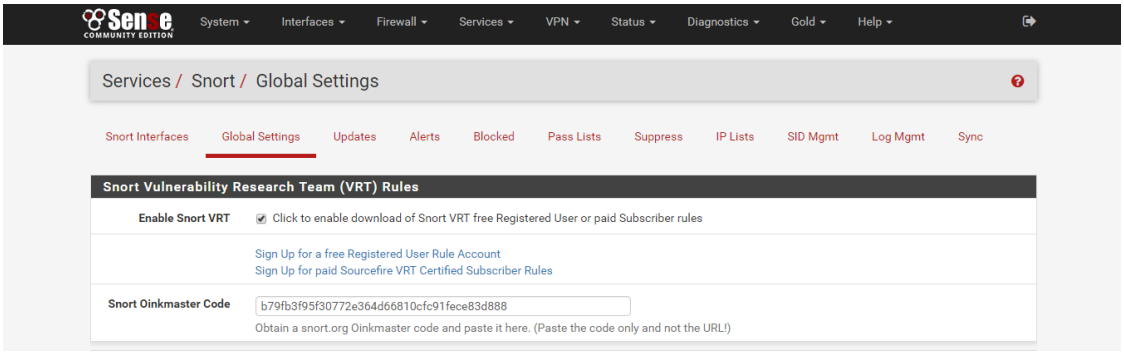


Figura 63. Oinkmaster Code.
Fuente: Captura del sistema operativo PfSense.

Adicionalmente, es necesario descargar otros paquetes de reglas correspondientes al servidor IDS como se indica en la Figura 64.

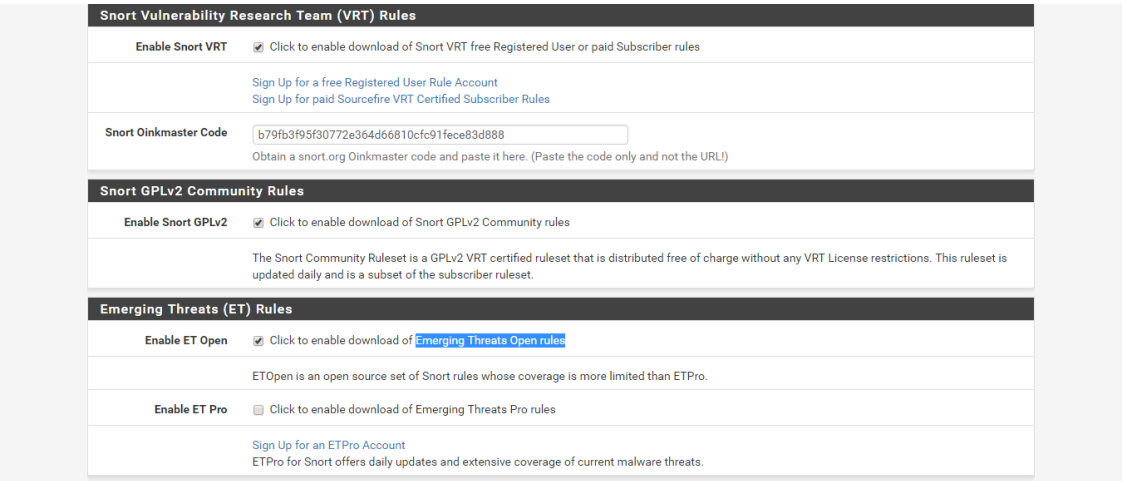


Figura 64. Community Rules.
Fuente: Captura del sistema operativo PfSense.

Realizado lo anterior, se procede a crear la interfaz dando clic en el botón add como se muestra en la Figura 65.

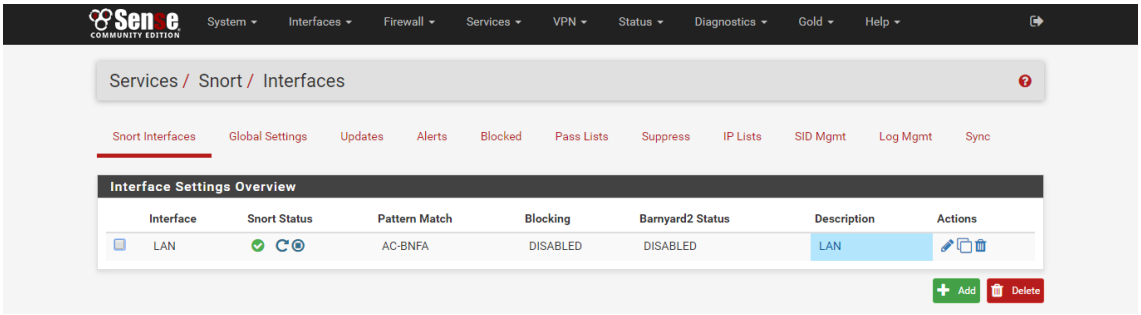


Figura 65. Interfaz dónde se van analizar el tráfico.
Fuente: Captura del sistema operativo PfSense.

Luego, se suben las reglas al servidor ingresando a Updates y seleccionando Update Rules como se ve en la Figura 66.

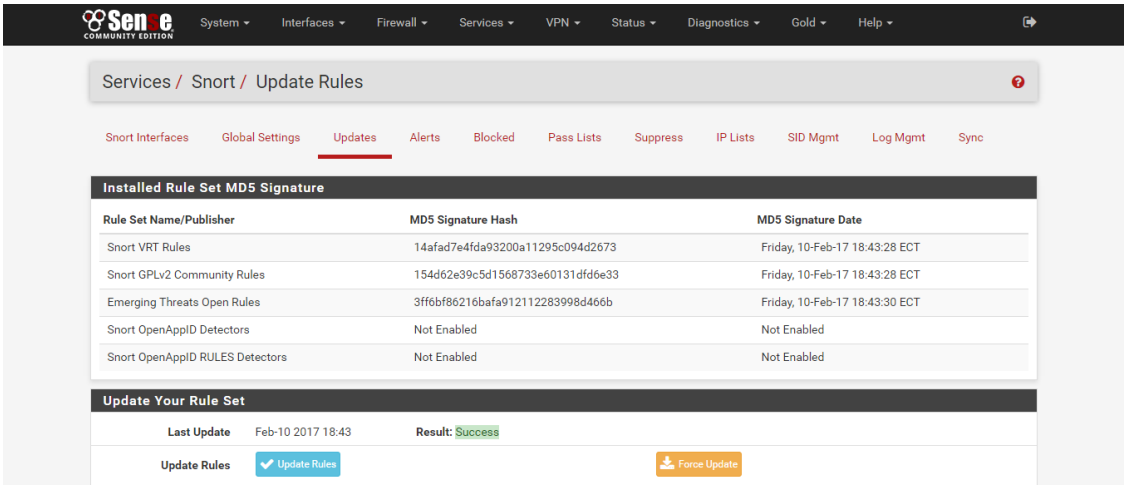


Figura 66. Update Rules.
Fuente: Captura del sistema operativo PfSense.

Una vez terminada la configuración de SNORT, hay que verificar su correcto funcionamiento para proceder a su utilización. La Figura 67 muestra el programa corriendo sin ningún error.

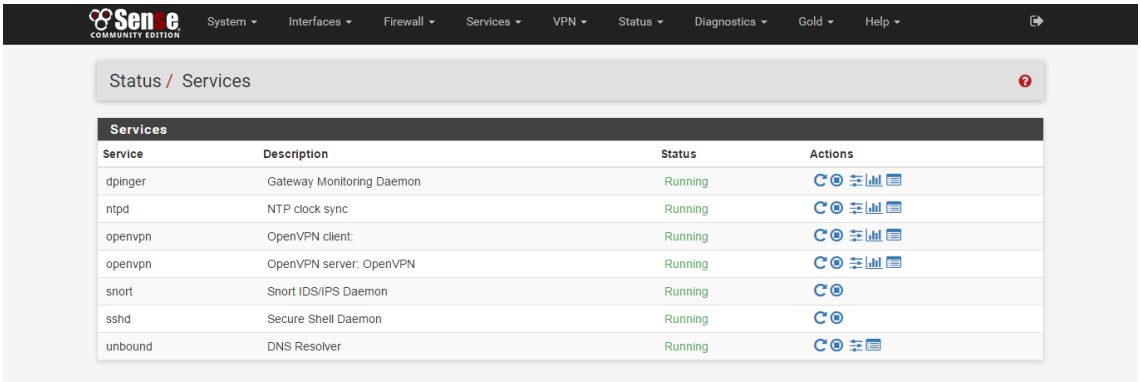


Figura 67. Snort Running.
Fuente: Captura del sistema operativo PfSense.

La Figura 68 permite observar la verificación de las alertas por las interfaces WAN y LAN durante la ejecución de un ataque controlado.

States

Interface	Protocol	Source (Original Source) -> Destination (Original Destination)	State	Packets	Bytes
WAN	icmp	192.168.10.20:28085 -> 172.16.14.1:28085	0:0	7.526 K / 0	206 KiB / 0 B
WAN	ipv6-icmp	fe80::2e0:4dff:fe33:78f2[28146] -> fe80::8a1d:fcff:fee9:d53f[28146]	NO_TRAFFIC:NO_TRAFFIC	3.763 K / 3.763 K	176 KiB / 176 KiB
WAN	tcp	172.16.14.240:47558 -> 172.16.14.235:80	FIN_WAIT_2:FIN_WAIT_2	8 / 14	850 B / 13 KiB
lo0	udp	172.16.14.235:42371 -> 172.16.14.235:1194	SINGLE:NO_TRAFFIC	4 / 0	280 B / 0 B
lo0	udp	172.16.14.235:42371 -> 172.16.14.235:1194	NO_TRAFFIC:SINGLE	4 / 0	280 B / 0 B
WAN	ipv6-icmp	fe80::8a1d:fcff:fee9:d53f -> fe80::2e0:4dff:fe33:78f2	NO_TRAFFIC:NO_TRAFFIC	1 / 1	72 B / 72 B
WAN	ipv6-icmp	fe80::2e0:4dff:fe33:78f2[49152] -> fe80::8a1d:fcff:fee9:d53f[49152]	NO_TRAFFIC:NO_TRAFFIC	1 / 1	64 B / 64 B
WAN	tcp	172.16.14.240:47568 -> 172.16.14.235:80	ESTABLISHED:ESTABLISHED	6 / 8	1 KiB / 6 KiB
WAN	tcp	172.16.14.240:47569 -> 172.16.14.235:80	FIN_WAIT_2:FIN_WAIT_2	4 / 3	172 B / 132 B
WAN	tcp	172.16.14.240:47570 -> 172.16.14.235:80	FIN_WAIT_2:FIN_WAIT_2	4 / 3	172 B / 132 B
WAN	tcp	172.16.14.240:47571 -> 172.16.14.235:80	FIN_WAIT_2:FIN_WAIT_2	4 / 3	172 B / 132 B

Figura 68. Alertas Snort.
Fuente: Captura del sistema operativo PfSense.

5.3.4. Instalación de antivirus en los servidores WEB y DNS.

La UTN cuenta con la licencia del antivirus Kaspersky para ordenadores, dados los resultados obtenidos en la investigación se propone implementar un antivirus en los

servidores ya que esta medida permitirá una mayor protección ante malware que pueda ser inyectado por medio de ataques informáticos.

Cabe recalcar que los equipos de estos servicios se encuentran en producción y atienden a gran cantidad de usuarios, por lo que se debe optimizar el procesamiento del mismo. Lo que se propone es que los administradores hagan un escaneo en todo el sistema, para que se identifique posible malware. Para la verificación y demostración de la importancia de un antivirus se realizó pruebas mediante un antivirus gratuito ClamAV.

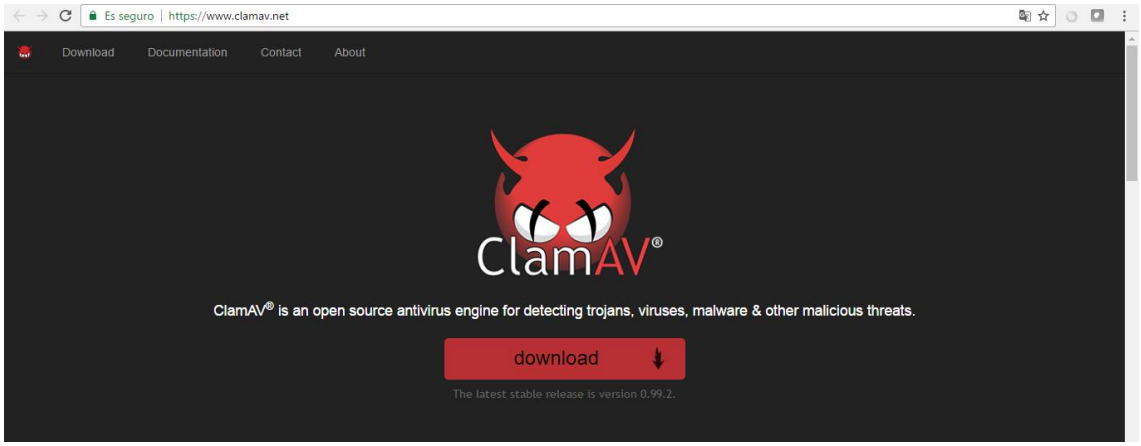


Figura 69. Download ClamAV.
Fuente: Recuperado de https://www.clamav.net/

ClamAV es un conjunto de herramientas antivirus open source (código fuente abierto) que tiene las siguientes características:

- Distribuido bajo los términos de la Licencia Pública General GNU.
- Cumple especificaciones de la familia POSIX (Portable Operating System Interface for UNIX o interfaz portable de sistema operático para Unix).
- Búsqueda rápida.
- Detecta más de 700 mil virus, gusanos, troyanos y otros programas maliciosos.

- Examina contenido de archivos ZIP, RAR, Tar, Gzip, Bzip2, MS OLE2, MS cabinet, MS CHM y MS SZDD.
- Explora archivos comprimidos UPX, FSG y Petite.
- Avanzada herramienta con soporte para firmas digitales y consultas sobre DNS.

Requerimientos lógicos necesarios.

Antes de ingresar a ClamAV, se recomienda crear previamente el grupo de usuarios correspondientes de la siguiente manera:

```
groupadd -r clamav
```

Luego, generar el usuario clamav:

```
useradd marcelo
```

Una vez efectuado lo anterior, se debe descargar el archivo:

```
wget -N http://www.alcancelibre.org/al/server/AL-Server.repo \ -o /etc/yum.repos.d/AL-Server.repo
```

Después, instalar el antivirus:

```
yum -y install clamav clamav-update
```

Una vez instalado el antivirus se requiere habilitar dos políticas para permitir un funcionamiento normal:

```
setsebool -P antivirus_use_jit 1

setsebool -P antivirus_can_scan_system 1
```

La política antivirus_use_jit permite utilizar el compilador JIT basado sobre LLVM para aumentar la capacidad de detección de virus. Mientras que la política antivirus_can_scan_system permite realizar la verificación del sistema de todos los archivos.

Para que Selinux permita el funcionamiento normal es necesario colocar el siguiente comando:

```
setsebool -P clamscan_disable_trans 1
```

Para que Selinux apruebe actualizar la base de datos de firmas digitales se ingresa el siguiente comando:

```
setsebool -P freshclam_disable_trans 1
```

Modo de Uso del antivirus.

Para revisar archivos sospechosos de estar infectados se coloca el consiguiente comando:

```
clamscan /Descargas/test.zip
```

Luego hay que generar un directorio para los archivos maliciosos, que estén en cuarentena por medio de:

```
mkdir -p /.clamav/virus
```

Para determinar que los archivos se envíen a cuarentena se escribe el siguiente comando:

```
clamscan –move=/home/marcelo/.clamav/virus \ -r /Descargas
```

Mientras que para eliminar los archivos es necesario digitar lo siguiente:

```
clamscan –remove=yes \ -r /Descargas
```

Por otro lado, si se desea que clamscan haga la revisión de un directorio, pero sólo se muestre la información de los archivos infectados hay que colocar el siguiente coman do:

```
clamscan --infected \ -r /Descargas
```

Finalmente, para que clamscan guarde la información de su actividad se escribe este comando:

```
clamscan --log=/home/usuario/clamscan.log \ --infecteted \ --remove=yes \ -r /Descargas
```

5.3.5. VPNs en las conexiones remotas.

Con la implementación del sistema Pfsense en la red de la UTN, se realizó pruebas de seguridad para las conexiones remotas, dentro de este sistema se obtuvo conexiones seguras por medio de VPNs. El criterio para que se considere una seguridad como óptima

es que se maneje la confidencialidad en la manipulación de este sistema, ya que se maneja un archivo encriptado descargado desde Pfsense para su posterior conexión remota.

En la Figura 70 se indica el primer paso para el proceso de configuración VPN en PfSense.

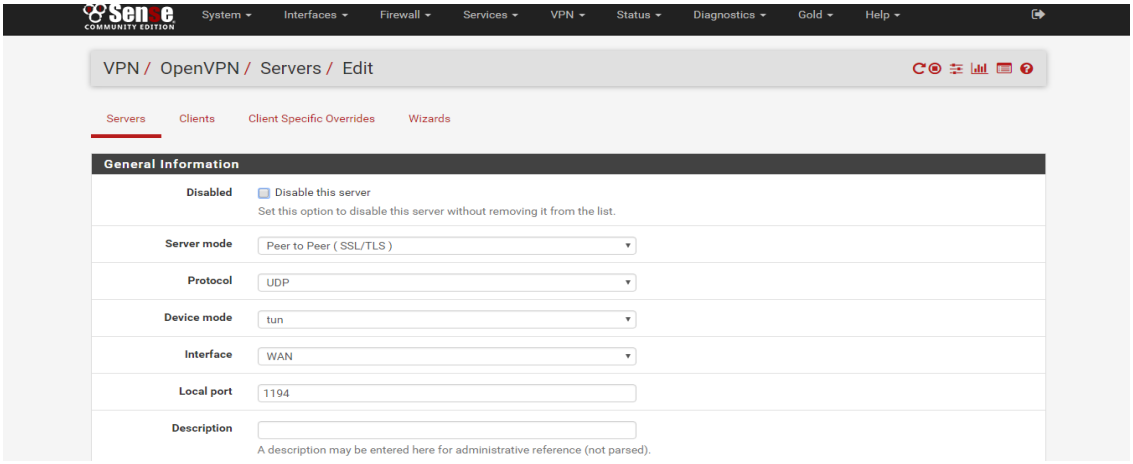


Figura 70. Habilitación de puerto 1194.
Fuente: Captura del sistema operativo PfSense

La Figura 71 muestra la habilitación de la autenticación TLS, para tener mejor seguridad en las conexiones por OpenVPN.

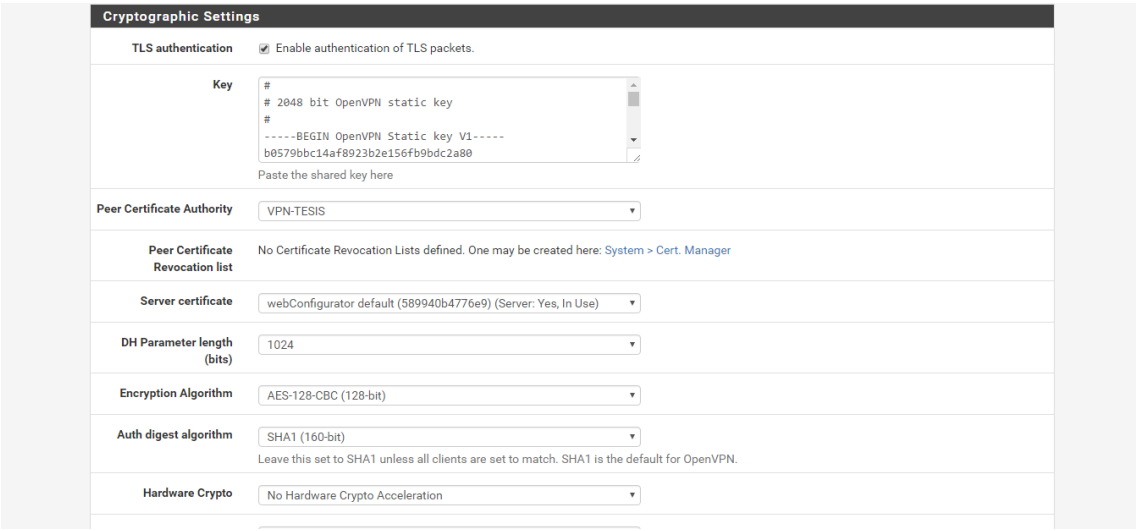


Figura 71. Autenticación TLS.
Fuente: Captura del sistema operativo Pfsense

Se ingresa la dirección de red a Tunnel en Ipv4 para realizar la conexión OpenVPN como se puede observar en la Figura 72.

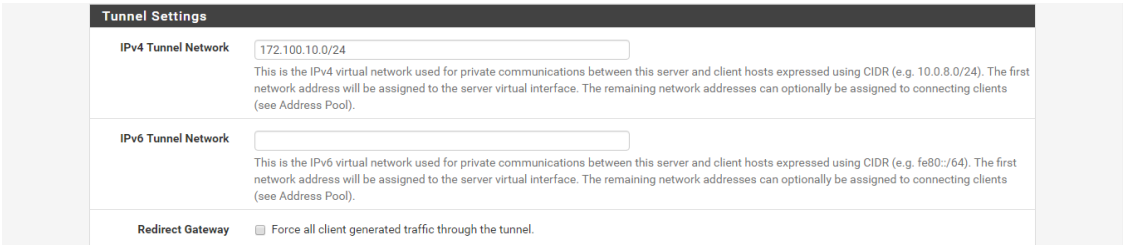


Figura 72. Tunnel Ipv4.
Fuente: Captura del sistema operativo PfSense.

Se habilita el adaptado virtual para que el cliente pueda ver la red Tunnel como se muestra en la Figura 73.

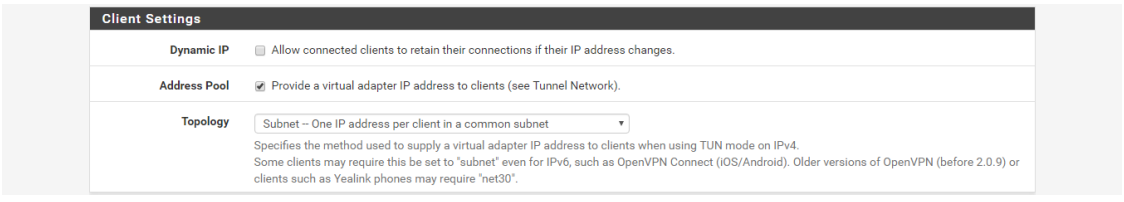


Figura 73. Ip Address Cliente.
Fuente: Captura del sistema operativo PfSense

En la Figura 74 se culmina con la configuración del servidor VPN y después se verifica que este corra sin ninguna falla.

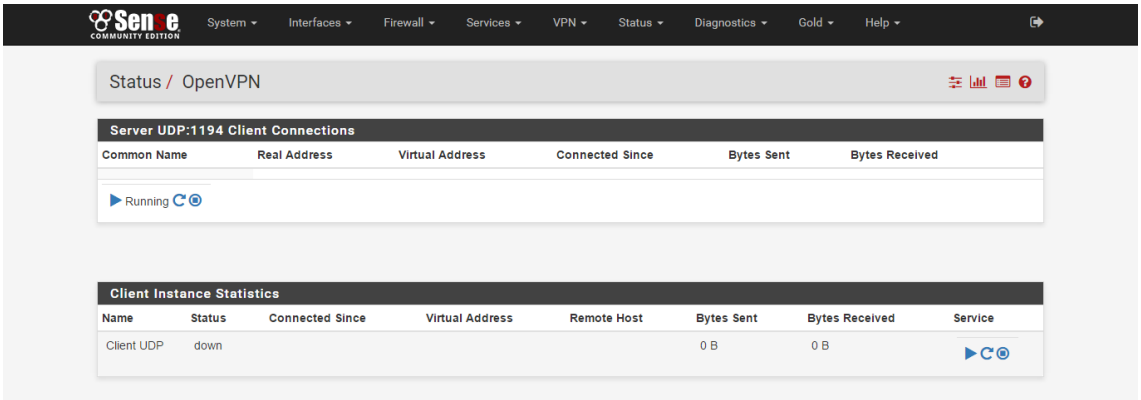


Figura 74. Status OpenVPN.
Fuente: Captura del sistema operativo PfSense.

Luego, en la Figura 75, se muestra cómo se debe aumentar las reglas en el Firewall para que acepte al cliente.

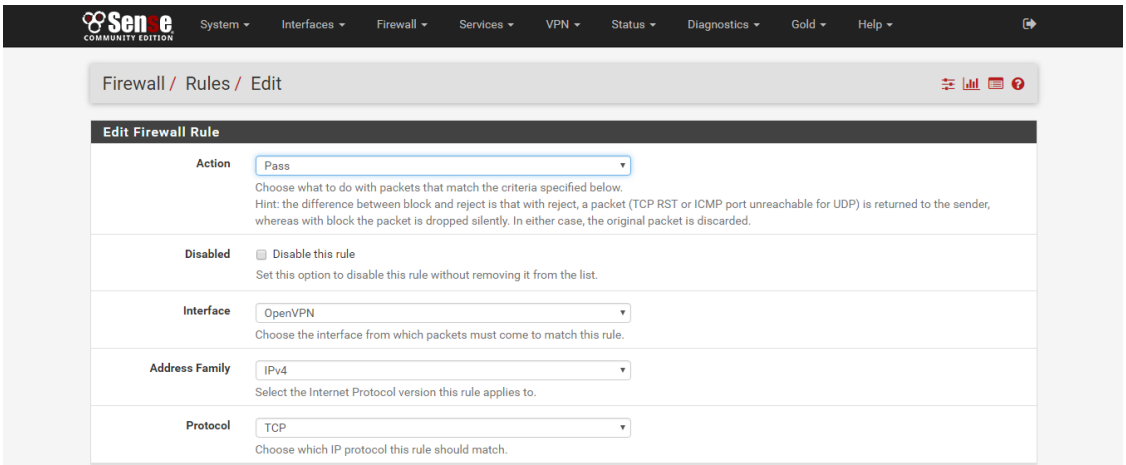


Figura 75. Firewall Open VPN.
Fuente: Captura del sistema operativo PfSense.

Posteriormente, se verifica que la regla en el Firewall esté correctamente creada para seguir con el proceso de realizar la Open VPN como se presenta en la Figura 76.

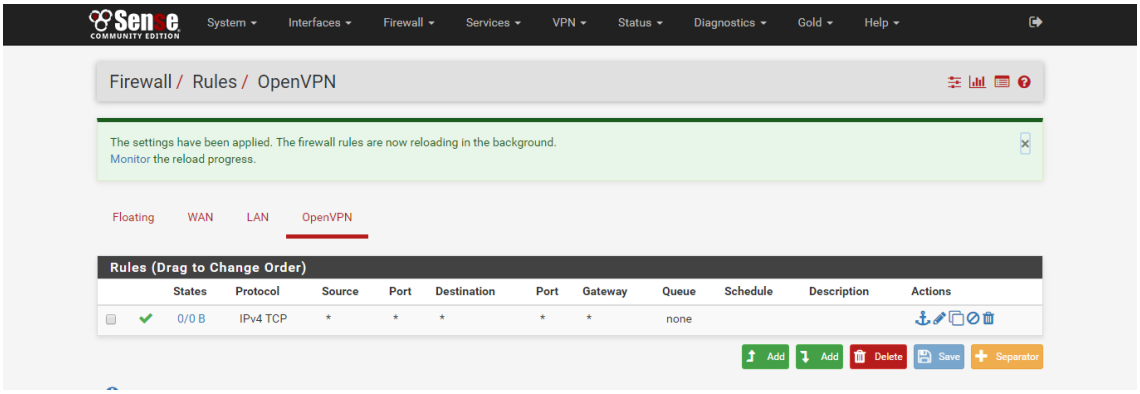


Figura 76. Creación Firewall OpenVPN.
Fuente: Captura del sistema operativo PfSense.

La Figura 77 indica el siguiente paso que es la configuración de los clientes y la creación de sus certificados.

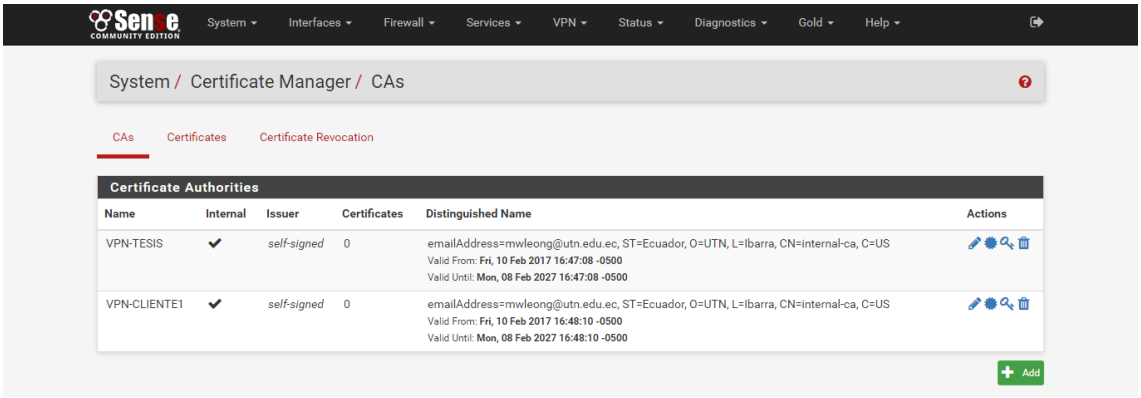


Figura 77. Certificados OpenVPN.
Fuente: Captura del sistema operativo PfSense.

Una vez hecho todo lo anterior, se debe crear un grupo para los usuarios que se van a conectar por medio de la VPN, esto se muestra en la Figura 78.

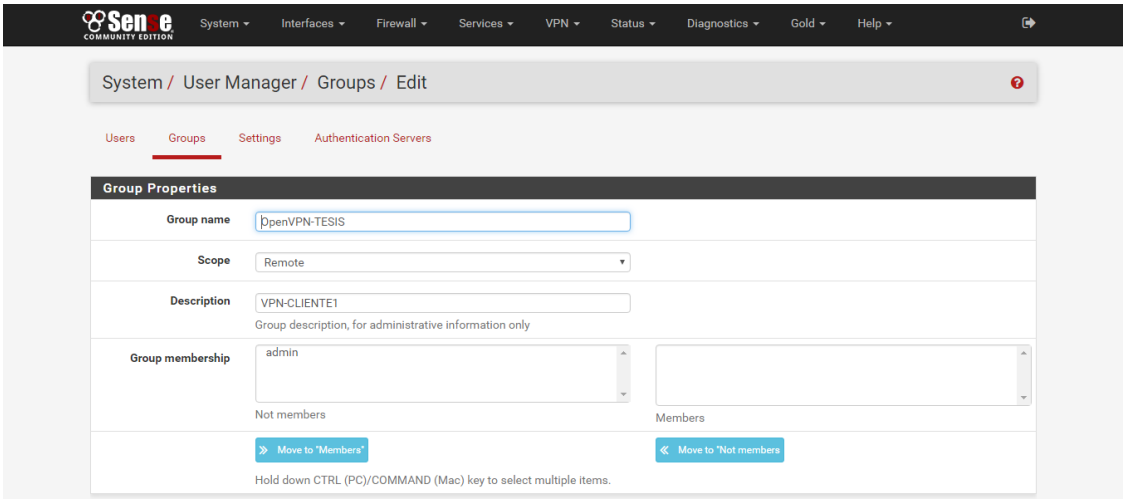


Figura 78. Grupo VPN.
Fuente: Captura del sistema operativo PfSense.

Para ello primero se agrega al usuario al grupo VPN como se puede observar en la Figura 79.

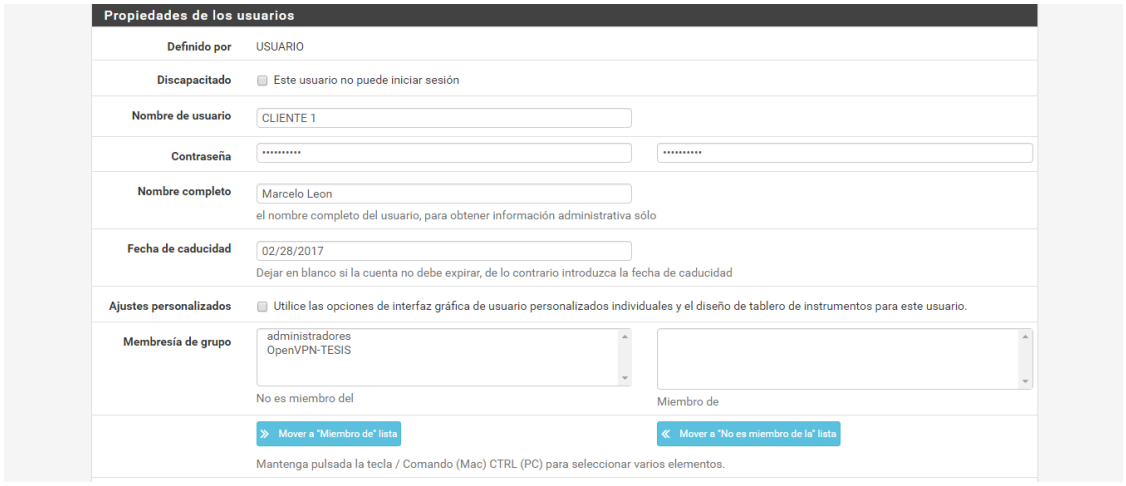


Figura 79. Usuario VPN.
Fuente: Captura del sistema operativo PfSense.

Contraseña: *******

Pasado esto, al momento de crear un usuario para el grupo VPN, se tiene que crear el Certificado del usuario, como se puede identificar en la Figura 80.

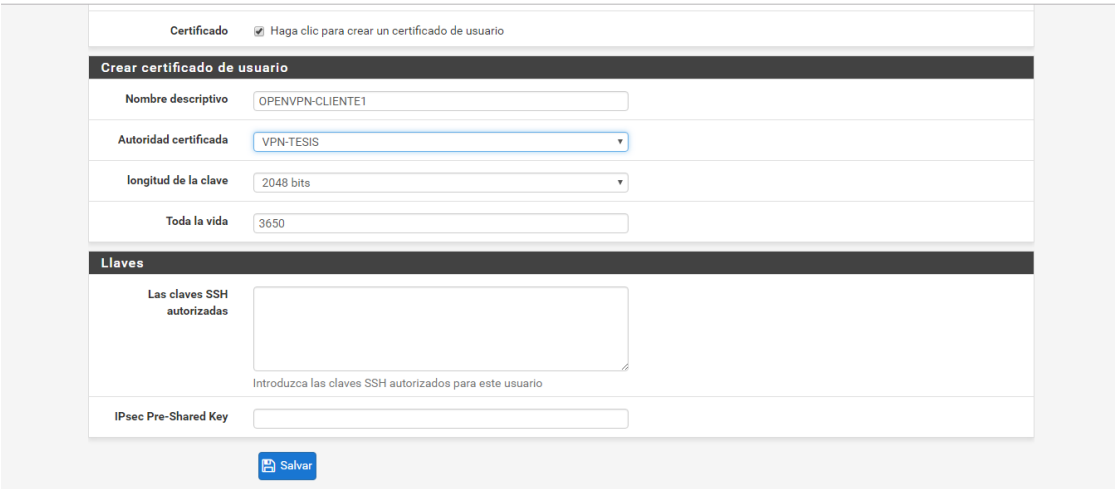


Figura 80. Certificado de usuario.
Fuente: Captura del sistema operativo PfSense.

Luego, una vez más, hay que dirigirse al apartado de certificados para verificar que el certificado del usuario esté correctamente creado como se ve en la Figura 81.

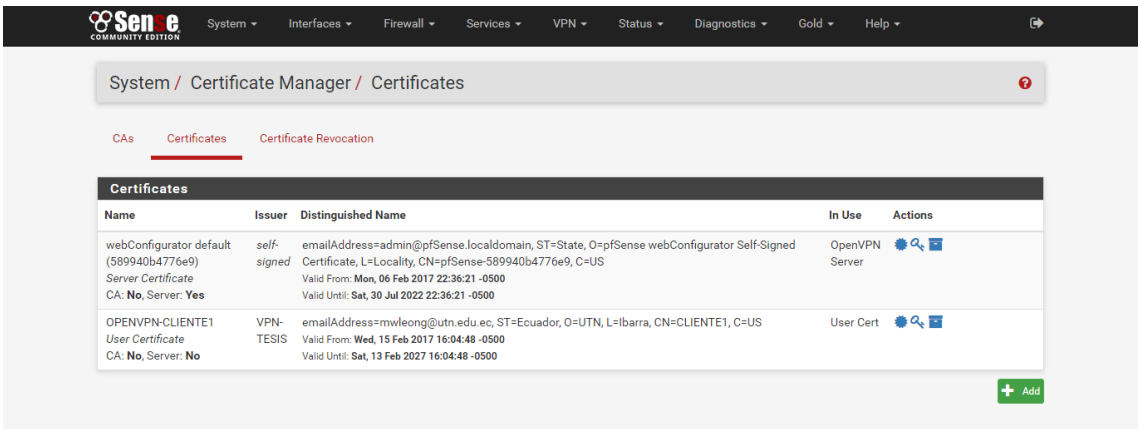


Figura 81. Verificación Certificado Cliente.
Fuente: Captura del sistema operativo PfSense.

Después es necesario instalar Open VPN con la finalidad de extraer los certificados para la conexión VPN, esto se puede ver en la Figura 82.

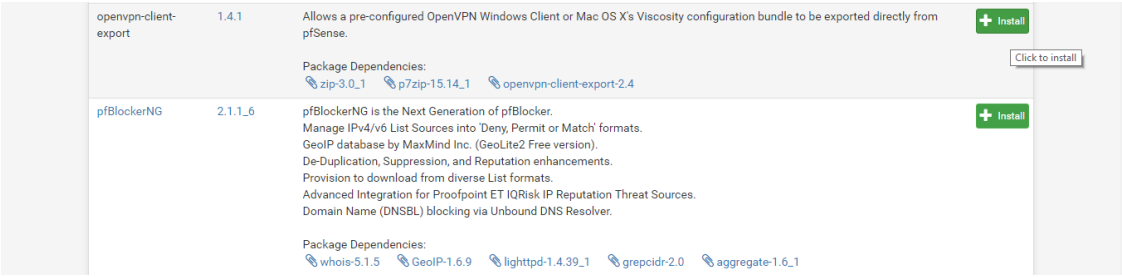


Figura 82. Instalación Open VPN-Client.
Fuente: Captura del sistema operativo PfSense.

Hecho esto hay que volver al servidor para realizar el último paso que es el acceso al servidor para la conexión remota como se ve en la Figura 83.

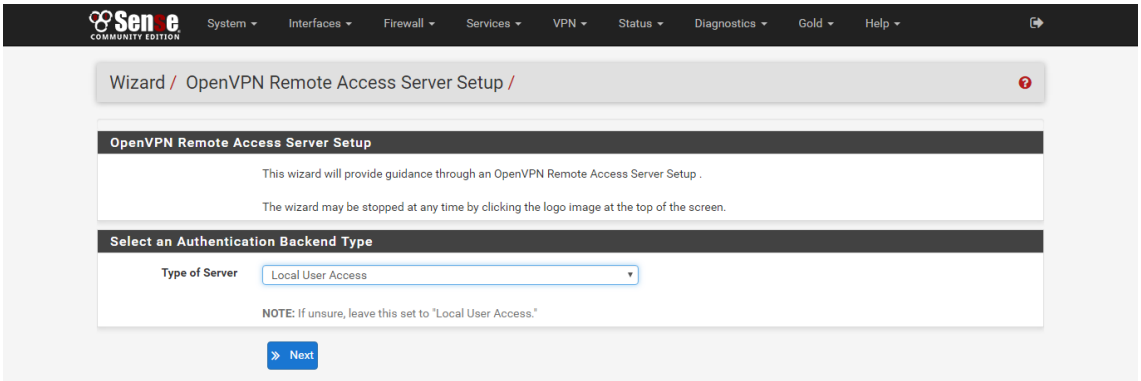


Figura 83. Creación Conexión Remota.
Fuente: Captura del sistema operativo PfSense.

La Figura 84 permite observar el siguiente paso que es la creación de la autoridad certificadora, la cual permite la seguridad en las conexiones VPN.

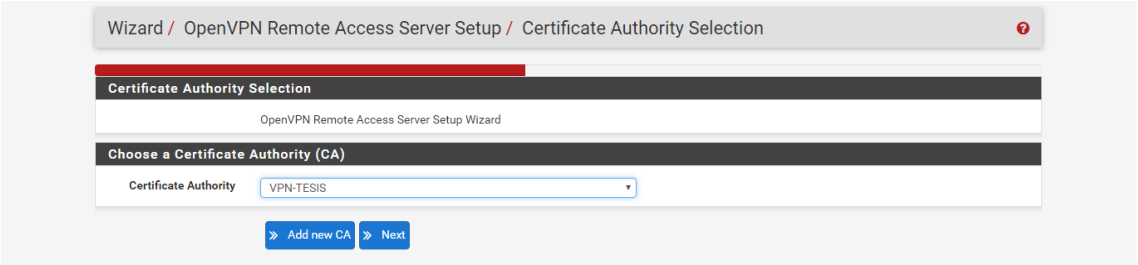


Figura 84. Certificate Auhority (CA).
Fuente: Captura del sistema operativo Pf Sense.

Luego, se llena los datos necesarios para generar el certificado CA del cliente para que pueda posteriormente conectarse a la VPN, esto se puede ver en la Figura 85.

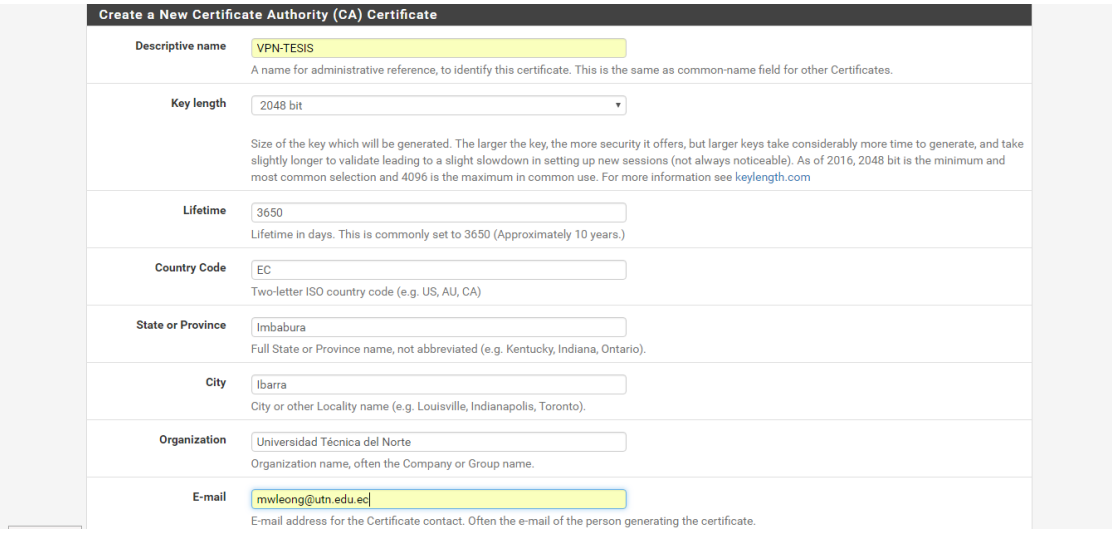


Figura 85. Datos para la CA.
Fuente: Captura del sistema operativo PfSense.

En este paso se tiene la opción de agregar la regla para el cliente en el Firewall (Figura 86), se habilita y automáticamente se crea la regla, esto se puede verificar en Firewall Open VPN.

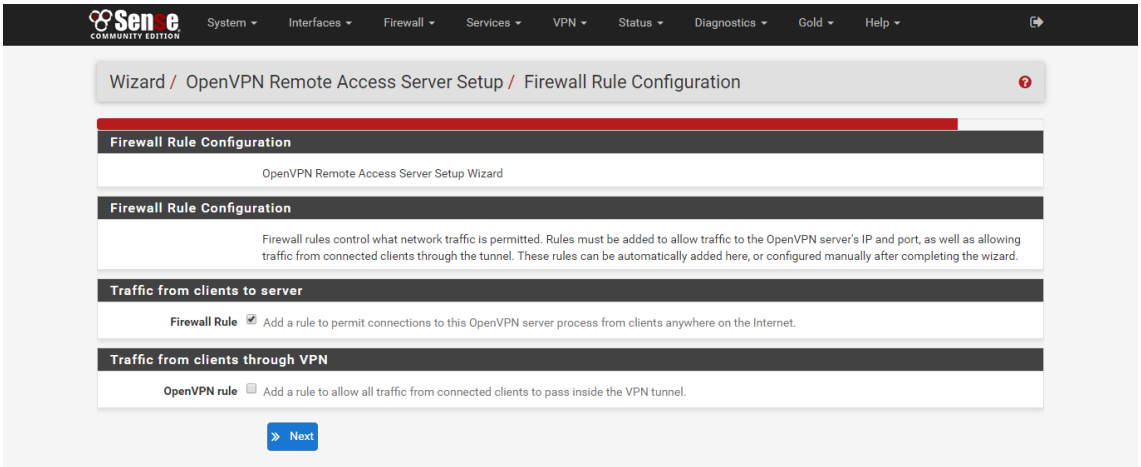


Figura 86. Firewall Rule.
Fuente: Captura del sistema operativo PfSense.

Se sigue al siguiente y penúltimo paso, donde se habilita el Servidor Remoto por el puerto establecido para este tipo de conexiones, y la interfaz por donde se va a conectar los clientes, para luego cómo último paso extraer el certificado, para que se conecte el cliente remotamente, esto se muestra en la Figura 87.

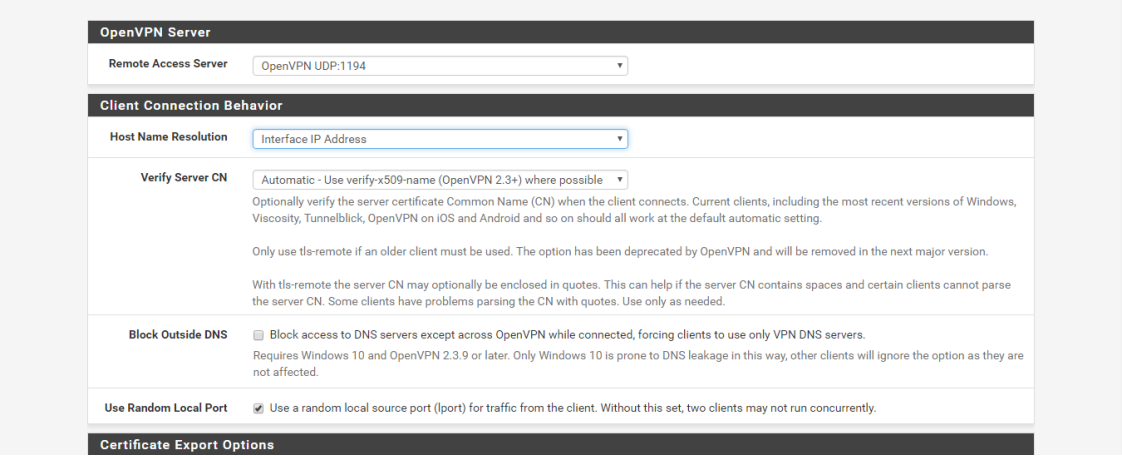


Figura 87. OpenVpnServer-Descarga del Certificado.
Fuente: Captura del sistema operativo PfSense.

5.3.6. Iptables en el Servidor WEB.

Una posible solución al ataque de fuerza bruta, es restringir el número de conexiones paralelas a un servidor por dirección Ip del cliente. Se puede usar connlimit para crear algunas restricciones, para permitir 3 conecciones ssh por cliente se coloca la siguiente regla:

```
iptables –A INPUT –p tcp –-syn –dport 22 –m connlimit –connlimit-above 3 –j REJECT
```

Por otro lado, para bloquear y prevenir ataques DDoS se emplea la siguiente regla:

```
iptables –A INPUT –p tcp –dport 80 –m limit –limit 25/minute –limit-burst 100 –j ACCEPT
```

Para prevenir un ataque DDoS se puede aplicar una regla en el Firewall que permita limitar el número de peticiones en el puerto 80 que pertenece al servidor Web.


```
iptables –A INPUT –p tcp –dport 80 –m limit –limit 25/minute –limit-burst 100 –j ACCEPT
```


5.3.7. Cambio de puerto SSH.

El cambio de puerto SSH incrementa la seguridad en este tipo de conexiones ya que el puerto por defecto es el 22. Por lo tanto, es conveniente cambiar este puerto por uno superior a 1024 que complique a un atacante la conexión por esta vía.

Para realizar este cambio se ingresa al servidor, para luego entrar al fichero /etc/ssh/sshd_config, una vez aquí se cambia el puerto y se elimina el símbolo # para que se complete el cambio de puerto (Figura 88).

```
# This sshd was compiled with PATH=/usr/local/bin:/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options change a
# default value.

Port 3525
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

# Disable legacy (protocol version 1) support in the server for new
# installations. In future the default will change to require explicit
# activation of protocol 1
Protocol 2

# HostKey for protocol version 1
#HostKey /etc/ssh/ssh_host_key
# HostKeys for protocol version 2
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key

# Lifetime and size of ephemeral version 1 server key
#KeyRegenerationInterval 1h
#ServerKeyBits 1024

"/etc/ssh/sshd config" 139L, 3898C written
```

Figura 88. Cambio de Puerto SSL.
Fuente: Captura del servidor web de la UTN.

Como siguiente paso, se debe reiniciar el servicio de SSH con el comando service sshd restart (Figura 89), para que todos los cambios de la configuración del fichero sean implentados.

```
[root@dns ~]# service sshd restart
Stopping sshd:                                             [  OK  ]
Starting sshd:                                             [  OK  ]
[root@dns ~]#
```

Figura 89. Resetear el Servicio de SSH.
Fuente: Captura del servidor web de la UTN.

Realizado esto, se tiene agregar o modificar la regla que habilita el puerto 22; aceptar las peticiones por el puerto que se modificó en el fichero del servicio de SSH, y por último resetear el servicio de iptables para que se implemente la nueva regla y empezar con la funcionalidad del nuevo puerto.

Solución para el ataque de Fuerza Bruta a SSH.

El ataque de Fuerza Bruta a SSH trata de crear un diccionario e intentar ingresar por este medio al servidor utilizando supuestas claves para el usuario root, para ello existe una solución muy sencilla pero eficiente que es restringir conexiones para que solo el administrado pueda ingresar, de igual manera restringir los intentos de autenticación; con esto se disminuye la probabilidad de ataques al servidor por este medio. La configuración se muestra en la Figura 90.

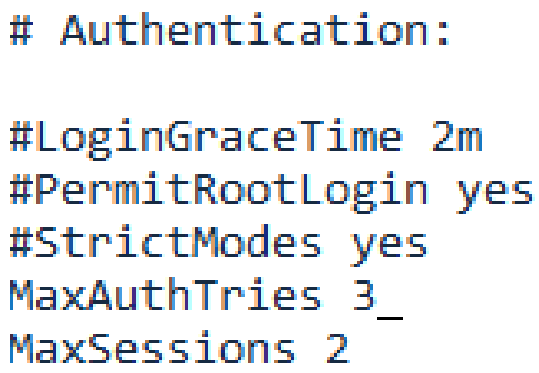


Figura 90. Autenticación SSH.
Fuente: Captura del servidor web de la UTN.

En la Figura 91 se muestra la verificación de que, al tercer intento fallido de conexión, envía una alerta y ya no permite el intento de nuevas conexiones, es decir, cuando se realice un ataque como el que se hizo en el proceso del pen testing, solo se ingresarán las dos primeras contraseñas almacenas en el diccionario y se cancelará la conexión.

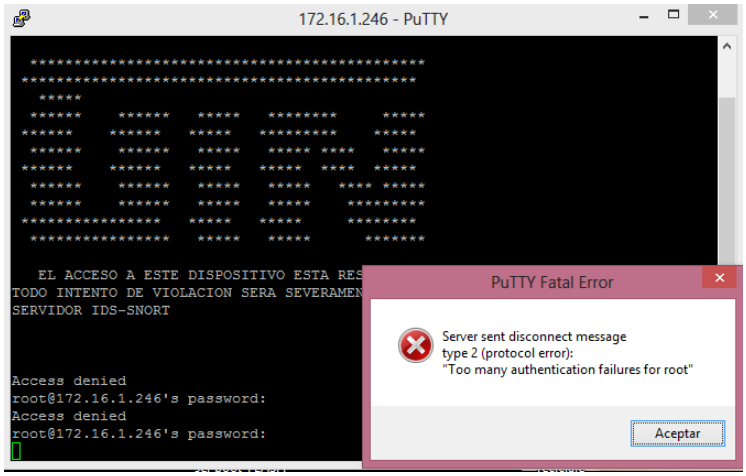


Figura 91. Verificación de la Autenticación SSH.
Fuente: Captura del servidor web de la UTN.

5.3.8. Web Aplication Firewall (WAF).

Es un firewall de aplicación web, se encarga de filtrar, supervisar y bloquear el tráfico HTTP hacia y desde una aplicación web. WAF se diferencia de un firewall regular porque es capaz de filtrar el contenido de aplicaciones web específicas, mientras que el firewall regular sirve como puerta de seguridad entre los servidores. El objetivo de WAF es evitar ataques como Cross Site Scripting (XSS), SQL Injection (SQLi), Remote File Inclusion (RFI), Local File Inclusion (LFI), envenenamientos, manipulación de cabeceras, entre otros. Tratando de proteger lo que los IDS/IPS no lo hacen.

5.3.8.1. Tipos de modelos de seguridad WAF.

Seguridad Positiva. - Se encarga de denegar todas las transacciones, acepta las que cree que son seguras. Esto mediante reglas predefinidas previamente o cargadas de algún script, o auto-aprendidas. Tiene como ventaja la protección ante ataques desconocidos al no coincidir con las reglas predefinidas.

Seguridad Negativa. - Acepta todas las peticiones, únicamente deniega las que son posibles amenazas o ataques reales. Depende de firmas y actualizaciones, por lo que no le hace tan preciso.

5.3.8.2. Aqtronix.

Es un tipo de WAF de código abierto que se presta a la implementación en entornos de IIS y otros servidores web y se publica bajo la General Public License (GNU). Es un filtro ISAPI que protege su servidor web al bloquear ciertas solicitudes y activar alertas, WebKnight se hará cargo de la protección del servidor.

5.3.8.3. ModSecurity.

ModSecurity es un tipo de WAF de código abierto para entornos apache. Se recomienda usar Apache 2.2.x. o superior pasa su servidor web.

Para mejorar la seguridad del Portal Web de la UTN se recomienda la implementación de ModSecurity, ya que con este se evita ataques como Cross Site Scripting (XSS), SQL Injection (SQLi), Remote File Inclusion (RFI), Local File Inclusion (LFI), envenenamientos, manipulación de cabeceras. A continuación, se tiene la instalación:

Instalación de ModSecurity

```
Yum install httpd

Yum install httpd-devel
```

Ahora la instalación de ModSecurity mediante:

```
Yum install mod_security
```

También se requiere alguna compilación de mod_proxy:

```
Wget http://www.manticmoo.com/articles/jeff7programming/proxy/mod_proxy_html.c

Yum install libxm12-devel yum install gcc apxs -c -I /usr/include/libxm12/ -i mod_proxy_html.c
```

Los extras no son necesarios, así que se procede a desinstalar:

```
Yum erase kernel-headers yum erase cpp yum erase libgomp
```

ModSecurity require el modulo libxml, asi que dd las siguientes lineas a httpd.conf

```
LoadFIle /usr/lib/libxm12.so LoadModule proxy_html_module modules/mod_proxy_html.so
```

Sobre la linea:

```
LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
```

Ahora el proxy sera activado con estos parámetros en httpd.conf

```
Order deny, allow
```

```
Allow from all

</proxy>

SSLProxyEngine On ProxyPass / http://X.X.X.X:8080/ ProxyPassReverse / http://website.domain.com/

<Location>

ProxyHTMLExtended On </Location>
```

El parámetro ProxyPass y ProxyPass reverse definiens a dónde enviar el tráfico real. Normalmente, este será el nombre del dominio complete de la direccion de carga de servidores web equilibrada.

5.4. Análisis de Riesgos Final.

Una vez que se han solucionado los problemas críticos de la red mediante la implementación de políticas y manuales de procedimientos de seguridad basados en la norma ISO 27001, se tiene una notoria mejoría en cuanto a la seguridad de la red.

Cabe recalcar que el enfoque del proyecto de titulación era brindar seguridad en las aplicaciones, específicamente en el servidor WEB y DNS; no obstante, también se produjeron mejorías en la seguridad de la infraestructura gracias a las soluciones planteadas. En el caso de la seguridad de las áreas de Operaciones y Personal, indirectamente también se logró mejoras mediante la socialización de las políticas y los procedimientos de seguridad a los empleados de la DDTI.

De acuerdo a las respuestas acerca de la evaluación de riesgos que se realizó posterior a la implementación de políticas y manuales de procedimientos de seguridad a cargo del personal de la DDTI, se tiene las siguientes medidas de defensa que se han calificado de la siguiente forma.

- Cumple las mejores prácticas recomendadas.
- Necesita mejorar.
- Carencias severas.

En la Tabla 23 se muestra la notable mejoría en cuanto a la seguridad de la red de la Universidad Técnica del Norte, pero se recomienda siempre estar a la vanguardia en el estudio de la seguridad, ya que, así como se va mejorando la seguridad, los delincuentes informáticos buscan nuevas formas de vulnerar la red de su objetivo.

Tabla 23. Comparación de los Análisis de Riesgos.

ÁREAS EVALUADAS	ANÁLISIS INICIAL	ANÁLISIS FINAL
Infraestructura		
Aplicaciones		
Operaciones		
Personal		

Fuente: Captura del software Microsoft Security Assessment Tool.

La tabla muestra de manera clara como mejoró notablemente la infraestructura, de un estado que necesita mejorar a uno que cumple con las mejores prácticas recomendadas.

En cuanto a las aplicaciones y las operaciones que tenían carencias críticas, pasaron a un estado que necesitan mejorar y finalmente en el área del personal no se pudo observar mayores mejoras.

Infraestructura

En las áreas que se evaluó previamente en Infraestructura se hará una comparación entre cómo estaba la red interna universitaria y cómo esta después de tomar las medidas correspondientes.

En Defensa del Perímetro se tomó en cuenta para la mejora del sistema a la parte crítica, como es el caso de antivirus en los servidores. Este punto no queda implementado ya que los antivirus afectan al rendimiento de los servicios, pero se deja como sugerencia su instalación.

El acceso remoto se evaluó y se determinó la mejor solución en la actualidad que es el uso de Vpns como medida de seguridad para las conexiones remotas, como también la instalación de un sistema de detección de intrusiones (IDS), para esto se sugiere el sistema operativo PfSense.

Tabla 24. Comparación Defensa del perímetro.

ÁREAS EVALUADAS	ANÁLISIS INICIAL	ANÁLISIS FINAL
Defensa del perímetro		
Reglas y filtros de cortafuegos		
Antivirus		

Antivirus – Equipos de escritorio		
Antivirus – Servidores		
Acceso remoto		
Segmentación		
Sistema de detección de intrusiones (IDS)		
Inalámbrico		

Fuente: Captura del software Microsoft Security Assessment Tool.

En el área de autenticación para los usuarios administrativos se implementó políticas de seguridad cómo medida de seguridad, de la misma manera se determinó directivas de contraseñas para las cuentas de acceso remoto.

Tabla 25. Comparación Autenticación.

ÁREAS EVALUADAS	ANÁLISIS INICIAL	ANÁLISIS FINAL
Autenticación		
Usuarios administrativos		
Usuarios internos		
Usuarios de acceso remoto		
Directivas de contraseñas		
Directivas de contraseñas – Cuenta administrador		
Directivas de contraseñas – Cuenta de usuario		

Directivas de contraseñas – Cuenta de acceso remoto		
Cuentas inactivas		

Fuente: Captura del software Microsoft Security Assessment Tool.

Para el caso del área de gestión y control de seguridad, se llevó a cabo procedimientos para la DDTI, y la propuesta del IDS que mejorará el control y emitirá informes de intrusiones.

Tabla 26. Comparación Gestión y Control.

ÁREAS EVALUADAS	ANÁLISIS INICIAL	ANÁLISIS FINAL
Gestión y control		
Informes sobre incidentes y respuesta		
Creación Segura		
Seguridad Física		

Fuente: Captura del software Microsoft Security Assessment Tool.

Aplicaciones

Para el área de implementación y uso se tiene políticas y procedimientos a seguir permitiendo un mejor control en cuanto a la implementación de nuevos sistemas dentro de la red universitaria.

Tabla 27. Comparación Implementación y uso.

ÁREAS EVALUADAS	ANÁLISIS INICIAL	ANÁLISIS FINAL
Implementación y uso		
Equilibrio de carga		

Clústeres	🔴	🔴
Aplicación y recuperación de datos	🔴	🔴
Fabricante de software independiente (ISV)	🔴	🟢
Desarrollo internamente	🔴	🟢
Vulnerabilidades	🔴	🟢

Fuente: Captura del software Microsoft Security Assessment Tool.

En cuanto al área de diseño de aplicaciones, se manejará políticas de seguridad para la autorización y control de acceso tanto para empleados y personas ajenas de la empresa, también se deja cómo procedimiento la metodología de desarrollo de seguridad de software.

Tabla 28. Comparación de Diseño de aplicaciones.

ÁREAS EVALUADAS	ANÁLISIS INICIAL	ANÁLISIS FINAL
Diseño de aplicaciones	🔴	🟡
Autenticación	🟢	🟢
Directivas de contraseñas	🟢	🟢
Autorización y control de acceso	🔴	🟢
Registro	🟡	🟡
Validación de datos de entrada	🟡	🟡
Metodologías de desarrollo de seguridad de software	🔴	🟢

Fuente: Captura del software Microsoft Security Assessment Tool.

En esta área de Almacenamiento y comunicaciones de datos, se propone como política de seguridad la implementación de certificados digitales SSL/TLS para las aplicaciones web de la institución.

Tabla 29. Comparación Almacenamieto y comunicaciones de datos.

ÁREAS EVALUADAS	ANÁLISIS INICIAL	ANÁLISIS FINAL
Almacenamiento y comunicaciones de datos		
Cifrado		
Cifrado – Algoritmo		

Fuente: Captura del software Microsoft Security Assessment Tool.

Operaciones

Para el área de Entorno en operaciones, se tiene la implementación del servidor PfSense que permite el monitoreo y gestión de servidores y dispositivos de red en cuanto a seguridad.

Tabla 30. Comparación Entorno.

ÁREAS EVALUADAS	ANÁLISIS INICIAL	ANÁLISIS FINAL
Entorno		
Host de gestión		
Host de gestión – Servidores		
Host de gestión – Dispositivos de red		

Fuente: Captura del software Microsoft Security Assessment Tool.

La directiva de seguridad se mejoró mediante procesos para la clasificación y eliminación de datos, gestión para las cuentas de usuarios, la regulación y la dirección de seguridad.

Tabla 31. Comparación directiva de seguridad.

ÁREAS EVALUADAS	ANÁLISIS INICIAL	ANÁLISIS FINAL
Directiva de seguridad		
Clasificación de datos		
Eliminación de datos		
Protocolos y servicios		
Uso aceptable		
Gestión de cuentas de usuarios		
Regulación		
Directiva de seguridad		

Fuente: Captura del software Microsoft Security Assessment Tool.

La gestión de actualizaciones y revisiones cuenta con procesos para la documentación de la red y gestión de las actualizaciones, para ello las medidas correspondientes por parte de los administradores de la red.

Tabla 32. Comparación de actualizaciones y revisiones.

ÁREAS EVALUADAS	ANÁLISIS INICIAL	ANÁLISIS FINAL
Gestión de actualizaciones y revisiones		
Documentación de la red		
Flujo de datos de la aplicación		
Gestión de actualizaciones		
Gestión de cambios y configuración		

Fuente: Captura del software Microsoft Security Assessment Tool.

Para el caso de copias de seguridad y recuperación se realizó manuales de procedimientos para los archivos de registro y la planificación de recuperación ante desastres y reanudación de negocio.

Tabla 33. Comparación copias de seguridad y recuperación.

ÁREAS EVALUADAS	ANÁLISIS INICIAL	ANÁLISIS FINAL
Copias de seguridad y recuperación		
Archivos de registro		
Planificación de recuperación ante desastres y reanudación de negocio		

Copias de seguridad		
Dispositivos de copia de seguridad		
Copias de seguridad y restauración		

Fuente: Captura del software Microsoft Security Assessment Tool.

5.5. Análisis de Costo.

El análisis de costo corresponde a todo lo que se utilizó para la implementación de las políticas de seguridad y la evaluación previa para llegar a obtener la información necesaria para ser implementadas, incluyendo el uso de los equipos que se encuentran en la red universitaria.

Se realizó configuraciones en los equipos de pruebas que se encuentran en la red universitaria, para posteriormente ser revisadas y aprobadas por parte de la DDTI para que sean implementadas en el ambiente de producción. Los servidores que se manipuló usan software libre y privado, dónde se analiza el costo de las licencias de ser el caso, en mencionado análisis de costo se toma en cuenta el software y hardware necesario para la elaboración del proyecto.

5.5.1. Presupuesto.

La auditoría de seguridad informática se realizó en los servidores WEB y DNS que se encuentran en la red universitaria en el equipo Blade Hp Proliant BL460c y que está conectado al Switch The Core Catalys, a continuación, se muestra en la Tabla 34, el detalle y el valor de los equipos:

Tabla 34. Presupuesto del Hardware de la UTN.

Hardware	Cantidad	Precio U.	Valor (USD)
Blade Hp Proliant BL460c G8	1	$ 5601.00	$ 5601.00
Blade Hp Proliant BL460c G1	1	$ 1128.00	$ 1128.00
Switch The Core Catalys	1	$ 4493.00	$ 4493.00
Total			$11222.00

Fuente: Anexo 6 – Cotización de servicios y equipos.

Adicional a lo anterior se necesitó un ordenador para la realización del pen testing y se dejó la propuesta de la adquisición de un servidor para la instalación de un IDS/IPS. Dicho servicio para que funcione adecuadamente necesita de un mínimo de 500mhz (CPU), 256mb (ram), 1gb de almacenamiento y dos tarjetas de red. A continuación, se nuestra en la Tabla 35, el detalle y el valor de los equipos:

Tabla 35. Presupuesto del Hardware Adicional.

Hardware	Cantidad	Precio U.	Valor (USD)
Laptop Dell i7	1	$ 1099.00	$ 1099.00
Servidor IDS/IPS	1	$ 5298.00	$ 5298.00
Total			$ 6397.00

Fuente: Anexo 6 – Cotización de servicios y equipos.

En cuanto al software se tuvo la posibilidad de utilizar, software comercial y Open Source (software libre) para los servicios, esto se detalla en la Tabla 36.

Tabla 36. Presupuesto del Software de la UTN.

Software	Cantidad	Precio U.	Valor (USD)
Linux Centos 6.7	1	$ 0.00	$ 0.00
Microsoft Windows Server 2012 R2 Essentials	1	$ 501.00	$ 501.00
Total			$ 501.00

Fuente: Anexo 6 – Cotización de servicios y equipos.

Para el pen testing e implementación de soluciones, todas las herramientas utilizadas corresponden a Open Source a excepción del Certificado Digital que tiene un valor considerable, pero con la finalidad de mejorar la seguridad en el Portal Web de la UTN se recomienda su adquisición, el detalle económico se detalla en la Tabla 37.

Tabla 37. Presupuesto Software Adicional.

Software	Cantidad	Precio U.	Valor (USD)
Certificado Digital	1	$ 119.00	$ 119.00
MSAT 3.0	1	$ 0.00	$ 0.00
Kali Linux	1	$ 0.00	$ 0.00
FOCA	1	$ 0.00	$ 0.00
WinSCP	1	$ 0.00	$ 0.00
PUTTY	1	$ 0.00	$ 0.00
ZOC7	1	$ 0.00	$ 0.00
Linset	1	$ 0.00	$ 0.00
Wireshark	1	$ 0.00	$ 0.00
Pfsense	1	$ 0.00	$ 0.00
Total			$ 119.00

Fuente: Anexo 6 – Cotización de servicios y equipos.

Por último, se realizó gastos varios en adquisiciones adicionales que indirectamente aportaron al desarrollo de la investigación, los costos se muestran en la Tabla 38.

Tabla 38. Otros Gastos.

Otros Gastos	**Cantidad**	**Precio U.**	**Valor (USD)**
Norma Iso 27001	1	$ 18.46	$ 18.46
Resma de papel bon	5	$ 4.90	$ 24.50
Impresiones	1000	$ 0.10	$ 100.00
Anillados	5	$ 2.00	$ 10.00
Copias	200	$ 0.016	$ 3.20
CDs	5	$ 0.50	$ 2.50
Internet (mensuales)	6	$ 28.97	$ 173.82
Movilización (mensuales)	6	$ 20	$ 120
Total			$ 432.48

Fuente: Papelería Alpha y Omega.

En el desarrollo del proyecto se necesitó hardware y software adicional, como por ejemplo, el ordenador para el pen testing y los programas para la elaboración de la auditoría de seguridad informática, cabe mencionar que se utilizó herramientas Open Source para disminuir costos, puesto que este es un proyecto con fines educativos.

5.5.2. Costo Beneficio.

El presente proyecto de titulación se realizó con fines educativos, orientado a la mejora en la seguridad de los servidores Web y DNS que se encuentran en producción, tuvo la finalidad de optimizar recursos existentes en la red universitaria y la intención de

proponer una mejora en el equipamiento e implementación de medidas preventivas y correctivas, para que de esta manera la Universidad siempre esté a la vanguardia en cuando seguridad informática.

Tabla 39. Análisis de Costo.

Descripción	**Costo Implementación Valor (USD)**	**Costos Reales Valor (USD)**
Hardware UTN	$ 11222.00	$ 0.00
Hardware Adicional	$ 6397.00	$ 0.00
Software UTN	$ 501.00	$ 0.00
Software Adicional	$ 119.00	$ 119.00
Otros Gastos	$ 432.48	$ 432.48
Asesoramiento de la auditoría de seguridad	$ 10000.00	$ 0.00
Instalación IDS-IPS	$ 2000.00	$ 0.00
Total	$ 30671.48	$ 551.48

Fuente: Anexo 6 – Cotización de servicios y equipos.

El costo de implementación se refiere a todo el hardware, software y gastos varios que se necesita para la implementación de un sistema seguro en la red interna de la Universidad Técnica del Norte y la mejora del servicio Web y Dns de la institución en cuánto a rendimiento y seguridad. El costo real se refiere a todos los valores que se gastó, por el motivo de que la Universidad no consta con el equipamiento necesario.

Beneficio.

La Universidad Técnica del Norte se benefició con una mejora en cuanto a la seguridad informática de la red interna, sobre todo en lo que respecta a los servicios del Portal Web y Dns. Mediante la implementación de políticas, procedimientos y sistemas de seguridad se mejoró las áreas tecnológicas de infraestructura, aplicaciones, operaciones y personal.

El presente proyecto implícitamente tiene beneficio económico, ya que la finalidad de la auditoría informática es solucionar problemas en cuanto a seguridad de red, y así brindar un mejor servicio para la comunidad universitaria.

Beneficios administradores.

- Capacidad de respuesta ante incidentes informáticos.
- Recuperación de datos.
- Control de contraseñas.
- Capacidad de identificar intrusiones.

Beneficios para los usuarios.

- Disponibilidad del Portal Web.
- Integridad del Portal Web.
- Confidencialidad de la información de los usuarios.

CONCLUSIONES

Al terminar el presente proyecto se obtiene las siguientes conclusiones:

Se realizó una auditoria informática utilizando la metodología Offensive Security con la finalidad de buscar falencias en la red interna de la Universidad y la aplicación de la norma ISO 27001 para dar soluciones específicas a los problemas encontrados de la red, mejorando la seguridad de la red mediante políticas y procedimientos de seguridad, que abarca soluciones de hardware y software reduciendo problemas de seguridad.

Se escogió la metodología Offensive Security debido a que, a diferencia de otras metodologías esta realiza una retroalimentación para verificar las soluciones planteadas, la norma ISO/IEC 27001 es la guía para la realización de manuales y políticas de seguridad, trabajando conjuntamente con la legislación nacional e internacional de delitos informáticos, obteniendo información necesaria para el desarrollo del proyecto y para la socialización del mismo, y así dar a conocer la necesidad de mejorar los sistemas de seguridad.

Se realizó un levantamiento de información de la situación actual de la infraestructura tecnológica de la institución. A simple vista se encontró ciertas falencias como: equipos obsoletos, accesos no seguros, problemas de traducción de dominios internos, colapso del portal web debido a la gran cantidad de peticiones.

El análisis de riesgos se realizó con la herramienta MSAT la misma que abarcó todas las áreas de seguridad de la información, a pesar de que el proyecto se delimitó en los servicios DNS y WEB; se identificó que las áreas de infraestructura y operaciones

tienen problemas leves en cuanto a seguridad y en las áreas de aplicaciones y personal estos son críticos, mismos que se solucionaron mediante políticas y procedimientos de seguridad.

Se utilizó Kali Linux como la principal herramienta de auditoria informática, debido a que es Open Source y es un potente sistema operativo que permite detectar vulnerabilidades mediante métodos de escaneos de redes y software para la explotación de las falencias de la red; adicionalmente se utilizó aplicaciones para explotar otras áreas como es el caso de FOCA que puede ser instalado bajo cualquier sistema operativo; sistemas y aplicaciones que normalmente usan los ciberdelincuentes, permitiendo dar soluciones mediante políticas y procedimientos para mejorar la seguridad. Todo esto para convertir a la seguridad en un ciclo constante de mejoramiento.

Se presentaron políticas y manuales de procedimientos basados en la norma ISO 27001 al personal de la Dirección de Desarrollo Tecnológico e Informático de la Universidad Técnica del Norte, las mismas que fueron revisadas para su posterior aprobación e implementación, y que sirven como directrices para que los empleados mejoren su desempeño laboral con respecto a la seguridad de la información y poder minimizar las vulnerabilidades que existen en la red institucional.

La seguridad de la información es un tema en el Ecuador que se ha dejado en segundo plano en las instituciones públicas y privadas, sumado a esto, no existen suficientes profesionales en este campo debido a la falta de apoyo financiero, esto ha provocado que las instituciones se vean afectadas en la seguridad de sus servicios en los últimos tiempos y existan cuantiosas pérdidas.

RECOMENDACIONES

Al terminar el presente proyecto se tiene las siguientes recomendaciones:

Se recomienda que las aplicaciones que manejan un gran número de peticiones como es el caso del portal web, aplicaciones de monitoreo, entre otras; manejen equipos robustos, o se independice el servicio en un equipo de ser necesario, para que los usuarios tengan servicios de calidad.

En el data center los servicios de internet no manejan el mismo sistema operativo, se recomienda realizar pruebas correspondientes antes de ser implementadas, ya que cada sistema operativo maneja sistemas de protección diferentes y para brindar soluciones de seguridad se debe tomar en cuenta tanto hardware y software.

Se recomienda que las políticas y procesos de seguridad sean aplicadas y revisadas periódicamente, para poder mejorarlas y actualizarlas cada cierto tiempo. De este punto se debe encargar el personal de la DDTI, así como también, de las capacitaciones de nuevas herramientas, para mejorar la potencialidad de los administradores.

El proyecto no debe quedar en propuesta, la institución debe tomar las medidas respectivas para completar el trabajo realizado y así la universidad sea certificada por un ente internacional como la ISO, y a su vez mejorar el servicio ante la comunidad universitaria y ser reconocida por los entes regulatorios nacionales.

El personal de la DDTI debe estar en constante capacitación en cuanto a seguridad de redes y aplicaciones, ya que lo que ahora se mejoró en un tiempo no será suficiente;

esto se debe a la constancia de los atacantes informáticos al encontrar vulnerabilidades en los sistemas.

Es importante contar con todas las herramientas, equipos, software y más aun de personal adecuado para realizar el proceso de auditorías informáticas, con la finalidad de mantener la costumbre de revisar las vulnerabilidades y prevenir ataques informáticos.

Para los procesos de implementación de seguridad se debe tener la autorización y apoyo por parte de la dirección de la DDTI, para que todo lo que se proponga en beneficio de la organización se cumpla a cabalidad una vez que sea aprobado y socializado.

Es recomendable que la DDTI complete este proyecto en las áreas que no fueron explotadas completamente, esto es para el caso de las Operaciones y Personal, ya que para mejorar el sistema de seguridad a cabalidad es necesario tomar en cuenta todas las áreas, para ello se debe realizar una capacitación a todos los que conforman la Universidad Técnica del Norte.

Se recomienda a la DDTI crear un área dedicada a la seguridad de redes, con la finalidad de tener personal que se encargue de proteger la red institucional ante ataques cibernéticos y así mantenerla segura.

GLOSARIO DE TÉRMINOS

DDTI. - Es la Dirección de Desarrollo Tecnológico e Informático de la Universidad Técnica del Norte.

SSL. - Significa "Secure Sockets Layer" es un protocolo para transmitir información de manera segura y cifrada.

WEB. – Se refiere a red, este vocablo se utiliza para mencionar un sitio que se encuentra en la Internet, en este caso hace referencia a la página web.

DNS. – (Domain Name System) sirve para interpretar y reconocer la dirección IP del servidor donde está alojado el dominio al que queremos acceder.

FTP .- "File Transfer Protocol" es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP.

TCP. - "Transmission Control Protocol" es un protocolo de control de transmisión, fundamental en Internet.

Active Directory. – Servicio de directorio en una red distribuida de computadores, se puede decir que es un servicio donde se crean objetos tales como usuarios, equipos o grupos.

Antivirus. – Programa que detecta la presencia de un virus en dispositivos de almacenamiento y los elimina.

VPN. – Es una red privada virtual, permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como internet.

LAN. – Es una red que conecta ordenadores en un área relativamente pequeña.

BIBLIOGRAFÍA

Fiscalía General del Estado. (2015). *Los delitos informáticos van desde el fraude hasta el espionaje*.

Aguilera, P. (2010). *Seguridad Informática.* EDITEX.

Allen Harper, J. N. (2015). *GRAY HAT HACKING.*

Asamblea Nacional del Ecuador. (2008). Código Orgánico Integral Penal.

Asamblea Nacional del Ecuador. (2008). Constitución de la República del Ecuador.

Asamblea Nacional del Ecuador. (2008). Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

Asamblea Nacional del Ecuador. (2008). Ley de Propiedad Intelectual.

Asamblea Nacional del Ecuador. (2008). Ley Especial de Telecomunicaciones.

Asamblea Nacional del Ecuador. (2008). Ley Orgánica de Comunicación.

Asamblea Nacional del Ecuador. (2008). Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional.

Asamblea Nacional del Ecuador. (2008). Ley Orgánica de Transparencia y Acceso a la Información Pública.

Baudes, G. (2002). *Auditoría Informática.*

Carlos Andrés Gil, J. M. (2008).

Collazos Balaguer, M. (2013). Obtenido de file:///C:/Users/Home%20Pc/Downloads/PRESENTACION_MANUEL_COLLAZOS_-_1.pdf

INAI, I. N. (2014). *Metodología de Análisis de Riesgo BAA.*

ISACA, J. Á. (2010). *Metodologías y Normas para el Análisis de riesgo.*

Isaza, M. A. (2013). *Metodologías Ethical Hacking.*

ISO. (2013). *Tecnologías de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos.*

Malkin, G. (1993). *RFC 1392.*

Malkin, G. R. (1993). *1392, RFC.*

Ministerio de Obras Públicas. (2012). *Metodología de Análisis y Gestión de Riesgos.*

Organización de Cooperación y Desarrollo Económico. (1992). Organización de Cooperación y Desarrollo Económico.

Organización de las Naciones Unidas. (2017). Organización de las Naciones Unidas.

Organización Mundial de Comercio. (2013). Organización Mundial de Comercio.

Organización Mundial de la Propiedad Intelectual. (2016). Organización Mundial de la Propiedad Intelectual.

Ortiz Beltrán, B. F. (2015). *Hacking Ético* .

Ramirez, A. O. (2013). *Gestión de Riesgos Tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios.*

Ramos, J. L. (2008). Pruebas de Penetración.

Rojas, D. (2014). *Hackeo Ético en el Ecuador.*

Tools sf, I. (2015). *ISO Tools Excellence*. Obtenido de https://www.isotools.org/2015/02/12/iso-27001-pasos-implantacion-politica-seguridad-procedimientos/

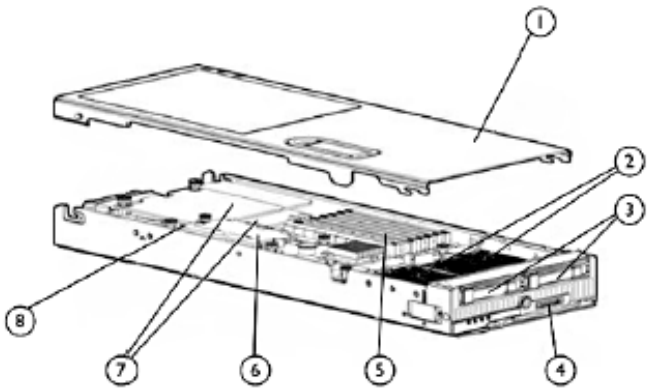
ANEXOS

Anexo 1 – Datasheet HP ProLiant BL460c Server Blade.

QuickSpecs

HP ProLiant BL460c Server Blade

Overview



HP ProLiant BL460c Server Blade

1. Access Panel
2. Up to two Quad-Core or Dual-Core Intel® Xeon® 5000 Sequence processors
3. Small form factor (SFF) hot-plug drive bays (standard BTO models)
4. Local I/O connector
5. Eight (8) PC2-5300, Fully Buffered DIMMs (DDR2-667) Memory Slots
6. HP Smart Array E200i Controller with optional battery-backed write cache (standard BTO models)
7. Two Mezzanine slots
8. Internal USB Connector (standard BTO models)

What's New

- Support for Intel® Xeon® Quad-Core X5470 Processors
- Support for HP Hot Plug SATA 5.4K SFF ETY HDD
- Support for HP NC382m Dual Port 1GbE Multifunction BL-c Adapter
- Support for up to 64 GB of Memory with 16 GB REG PC2-5300 2x8 GB Dual Rank memory option kit
- Support for QLogic QMH4062 1GbE iSCSI Adapter for HP BladeSystem c-Class

At A Glance

This document covers the HP ProLiant BL460c server blade only. For more information on HP BladeSystems c-Class Infrastructure and HP BladeSystem c-Class Interconnect Components, please see the following QuickSpecs:

HP BladeSystem c-Class Enclosures QuickSpecs:
HP BladeSystem c3000 Enclosure QuickSpecs:
http://h18000.www1.hp.com/products/quickspecs/12790_na/12790_na.html

QuickSpecs

HP ProLiant BL460c Server Blade

Overview

HP BladeSystem c7000 Enclosure QuickSpecs:
http://h18000.www1.hp.com/products/quickspecs/12810_na/12810_na.html

HP BladeSystem c-Class Interconnect Components QuickSpecs:
http://h18000.www1.hp.com/products/quickspecs/12524_na/12524_na.html

The HP ProLiant BL460c provides greater 2P x86 server blade density without compromise and maximum power-efficiency with flexibility and choice.

HP ProLiant BL460c server blade includes:

- **Processor:**
  - Up to two Quad-Core Intel® Xeon® 5400 Series processors
  - Up to two Quad-Core Intel® Xeon® 5300 Series processors
  - Up to two Dual-Core Intel® Xeon® 5200 Series processors
  - Supports up to 2 Dual-Core 3.33GHz, 1333 MHz FSB-1X6 MB Level 2 cache memory, and up to 2 Quad-3.33 GHz 1333MHz-2x6 MB Level 2 cache memory
  - Intel 5000P chipset supporting up to a 1333 MHz Front Side Bus
- **Memory:**
  - Up to 64 GB of memory, supported by (8) slots of PC2-5300 Fully Buffered DIMMs at 667 MHz
    - **NOTE:** 64 GB of memory is supported with 80W processors and below. Not supported with 120W processors.
  - Supporting low-power memory
  - Advanced ECC memory support
  - Supporting memory interleaving (2x1); memory mirroring and online spare capacity.
- **Storage Controller:**
  - Integrated HP Smart Array E200i RAID controller with 64 MB cache (with optional battery-backed write-cache with an upgrade to 128 MB cache in standard BTO models. Supports RAID 0,1 in standard BTO models
    - **NOTE:** Drive-less model available through CTO for customers not utilizing internal disk drives and attaching directly to SAN. Please note that this model does not replace any prior model offerings. The feature listed above is not included in the standard Drive-less configure to order model. However, all configure to order models offer optional support for small form factor (SFF) hot-plug drive bays, HP Smart Array E200i Controller (with optional battery-backed write cache), and Internal USB Connector. See Factory Integrated Model section for more information.
- **Internal Drive Support:**
  - Up to 2 small form factor (SFF) SAS or SATA hot plug hard disk drives in standard BTO models
    - **NOTE:** Drive-less model now available through CTO for customers not utilizing internal disk drives and attaching directly to SAN. Please note that this model does not replace any prior model offerings. **The feature listed above is not included in the standard Drive-less configure to order model.** However, all configure to order models offer optional support for small form factor (SFF) hot-plug drive bays, HP Smart Array E200i Controller (with optional battery-backed write cache), and Internal USB Connector. See Factory Integrated Model section for more information.
- **Network Controller:**
  - Two (2) embedded NC373i Multifunction Gigabit Server Adapters with iSCSI boot, TCP/IP offload engine, and optional accelerated iSCSI
  - One (1) additional embedded 10/100 network adapter dedicated to iLO 2 management

  NOTE: The Gigabit Ethernet adapters transmit from the server at 2000 Mbps only, full duplex per port. For more information, see the "Network Controller" item in Standards Features section.
- **Mezzanine Support:**
  - Two (2) additional I/O expansion slots via mezzanine card.
  - Supports up to two (2) mezzanine cards
    - Dual-Port Fibre Channel Mezzanine (4-Gb) options for SAN connectivity (Choice of Emulex or QLogic).
    - Wide variety of 10GbE and 1GbE network adapter options for additional network ports

Overview

- QLogic QMH4062 Gigabit Ethernet iSCSI initiator
- 4X DDR InfiniBand (IB) Mezzanine (20 Gb/s) options for low latency server interconnectivity (based on Mellanox technology

- **Internal USB Support:**
  - One (1) internal USB 2.0 connector for security key devices and USB drive keys in standard BTO models
    - **NOTE:** Drive-less model now available through CTO for customers not utilizing internal disk drives and attaching directly to SAN. Please note that this model does not replace any prior model offerings. **The feature listed above is not included in the standard Drive-less configure to order model.** However, all configure to order models offer optional support for small form factor (SFF) hot-plug drive bays, HP Smart Array E200i Controller (with optional battery-backed write cache), and Internal USB Connector. See Factory Integrated Model section for more information.
- **VMware ESX Server 3i and Citrix XenServer virtualization technology:**
  - Integrated Hypervisors: (Optional)
    - VMware ESX Server 3i virtualization technology
    - Citrix XenServer virtualization technology
- **Form Factor:**
  - HP ProLiant BL460c server blade plugs vertically into the BladeSystem c3000 and c7000 enclosures
- **Management:**
  - HP Integrated Lights-Out 2 (iLO 2) Standard Blade Edition with virtual KVM graphical remote console, with the option to upgrade to the iLO Select Pack. iLO Select Pack is a no installation upgrade offering automatic video footage of the events leading up to the server event (like bluescreens), automatic video footage of the server blade's last boot sequence, on-demand video record and playback for training videos, team collaboration features for up to four users on a single iLO session, and much more. Learn more at: www.hp.com/go/iLO.
- **Operating Systems:**
  - Supports Windows, Linux, Netware, and Solaris Operating Systems
- **Enclosures:**
  - HP offers three different c-Class server blade enclosures to meet your individual needs:
    - The HP BladeSystem c7000 rack enclosure is 10U high and holds up to 16 ProLiant BL460c servers plugged vertically.
    - The HP BladeSystem c3000 rack enclosure is 6U high and holds up to 8 HP ProLiant BL460c servers plugged horizontally.
    - The HP BladeSystem c3000 tower enclosure is designed with casters for sites without racks and holds up to 8 HP ProLiant BL460c servers plugged vertically.
  - Server blades, storage blades, interconnect modules, power supplies, fans, and redundant Onboard Administrator modules are all designed to fit into the c3000 and c7000 enclosures.
- For additional enclosure information, please see: http://h18004.www1.hp.com/products/blades/components/enclosures/c-class/index.html.
- **Warranty:**
  - This product is covered by a global limited warranty and supported by HP Services and a worldwide network of HP Authorized Channel Partners. Hardware diagnostic support and repair is available for three years from date of purchase. Support for software and initial setup is available for 90 days from date of purchase.. Enhancements to warranty services are available through HP Care Pack services or customized service agreements. Certain restrictions and exclusions apply. SATA hard drives have a one year warranty. SAS drives have a 3 year warranty.
  - **NOTE:** Server warranty includes 3 year Parts, 3 year Labor, 3-year on-site support. Warranty repairs may be accomplished through the use of Customer Self Repair (CSR) parts. These parts fall into two categories: 1) Mandatory CSR parts are designed for easy replacement. A travel and labor charge will result when customers decline to replace a Mandatory CSR part; 2) Optional CSR parts are also designed for easy replacement but may involve added complexity. Customers may choose to have HP replace Optional CSR parts at no charge. Additional information regarding worldwide limited warranty and technical support is available at: http://h18004.www1.hp.com/products/servers/platforms/warranty/index.html

QuickSpecs

Standard Features

NOTE: For a brief, printer friendly data sheet that describes this product and informs you of the essential capabilities and specifications, please visit: http://h71028.www7.hp.com/erc/downloads/4AA0-6087enw.pdf.

Processor	**Quad-Core Processor Option Kits**
	Quad-Core Intel® Xeon® Processor X5460 (3.160 GHz, 1333 FSB, 120W)*
	Quad-Core Intel® Xeon® Processor X5450 (3.00 GHz, 1333 FSB, 120W)*
	Quad-Core Intel® Xeon® Processor E5450 (3.0 GHz, 1333 FSB, 80W)
	Quad-Core Intel® Xeon® Processor E5440 (2.83 GHz, 1333 FSB, 80W)
	Quad-Core Intel® Xeon® Processor E5430 (2.66 GHz, 1333 FSB, 80W)
	Quad-Core Intel® Xeon® Processor E5420 (2.50 GHz, 1333 FSB, 80W)
	Quad-Core Intel® Xeon® Processor L5420 (2.50 GHz, 1333 FSB, 50W, LV)
	Quad-Core Intel® Xeon® Processor E5410 (2.33 GHz, 1333 FSB, 80W)*
	Quad-Core Intel® Xeon® Processor L5410 (2.33GHz, 1333FSB, 50W, LV)*
	Quad-Core Intel® Xeon® Processor E5405 (2.0 GHz, 1333 FSB, 80W)
	Quad-Core Intel® Xeon® Processor X5365 (3.00 GHz, 1333 FSB, 120W)
	Quad-Core Intel® Xeon® Processor X5355 (2.66 GHz, 1333 FSB, 120W)
	Quad-Core Intel® Xeon® Processor E5345 (2.33 GHz, 1333 FSB, 80W)
	Quad-Core Intel® Xeon® Processor E5335 (2.00 GHz, 1333 FSB, 80W)*
	Quad-Core Intel® Xeon® Processor L5335 (2.00 GHz, 1333 FSB, 50W)
	Quad-Core Intel® Xeon® Processor E5320 (1.86 GHz, 1066 FSB, 80W)
	Quad-Core Intel® Xeon® Processor L5320 (1.86 GHz, 1066 FSB, 50W)
	Quad-Core Intel® Xeon® Processor E5310 (1.60 GHz, 1066 FSB, 80W)
	Dual-Core Processor Option Kits
	Dual-Core Intel® Xeon® processor X5260 (3.33 GHz, 1333 FSB, 80W)
	Dual-Core Intel® Xeon® processor L5240 (3.00 GHz, 1333 FSB, 40 W, LV)
	Dual-Core Intel® Xeon® processor E5205 (1.86GHz, 1333 FSB, 65W)
	*Offered through Configure-To-Order only. See Factory Integrated Models section for more details. **NOTE:** Intel 5400, 5300, and 5200 Series processors are 64-bit and support Intel VT. Intel. 5200 Series processors are dual-core; Intel 5400 and 5300 Series processors are quad-core. **NOTE:** For the Intel 5200, 5300 and 5400 Series, the letter preceding the model number indicates the performance/wattage of the processor. "X" denotes High Performance/Wattage; "E" denotes Enterprise Performance/Wattage (Mainstream); and "L" denotes Lower Wattage.
Upgradeability	Upgradeable to 2 processors
Cache Memory	2 x 6 MB shared L2 cache (5400 Series) 1 x 6 MB L2 cache (5200 Series) 2 x 4 MB Level 2 cache memory (5300 Series)
Chipset	Intel® 5000P Chipset

QuickSpecs

Standard Features

Memory	Type	PC2-5300 Fully Buffered DIMMs at 667 MHz
	Standard	1 GB (2 x 512 MB) 2 GB (2 x 1 GB)
	Maximum	64 GB (8 x 8 GB) **NOTE:** Memory must be installed in pairs. **NOTE:** 64GB of memory is supported with 80W processors and below. Not supported with 120W processors.
Network Controller	Two (2) embedded NC373i Multifunction Gigabit Server Adapters with iSCSI boot, TCP/IP offload engine, and optional accelerated iSCSI One (1) additional 10/100 NIC dedicated to iLO 2 Management **NOTE:** The Gigabit Ethernet adapters transmit from the server at 2000 Mbps, full duplex per port only. However, within a Linux environment, the speed can be reduced or "throttled" using a feature available within the Linux operating system; see the white paper at: http://h71028.www7.hp.com/ERC/downloads/4AA1-5513ENW.pdf for more information. Once the adapter signal reaches the interconnect within the blade enclosure and communicates outside the blade enclosure to the LAN, the blade interconnect uplink types and settings determine the cable media, speed, duplex mode, and auto negotiation mode. Interconnects are available with Ethernet uplinks supporting 10/100/1000T, 10/100/1000 SFP, 1000 SX fiber, and 10Gb KX-4.	
Multifunction Networking	The embedded multifunction NC373i adapters combine standard Gigabit Ethernet networking, TCP/IP offload engine (TOE), iSCSI boot and optional accelerated iSCSI into a single adapter. • TOE moves the processing of data in the TCP protocol stack from the server CPU to the network card, freeing CPU cycles for other activities. With TOE, network communications are improved, and server efficiency is increased. The NC373i offers TOE for Microsoft® Windows 2000 and 2003 environments. • The iSCSI network boot (iSCSI boot) allows the BL460c to boot from a remote operating system (OS) image located on a storage area network (SAN). The BL460c uses an iSCSI firmware image (iSCSI boot option ROM) making the remote disk drive appear as a local, bootable C: drive. The BL460c is configured to connect to and boot from the iSCSI target disk on the network and download the OS image from the iSCSI target disk. The iSCSI boot option ROM is supplied by HP at no cost. The additional cost and mezzanine slot usage of an add-in iSCSI HBA card is not required. Additionally, the HP iSCSI boot solution includes scripts to significantly simplify the installation process.	
I/O Expansion Slots	Two I/O expansion mezzanine slots (one x8 and one x4)	
Integrated Manageability	Integrated Lights-Out 2 (iLO 2) Standard Blade Edition (integrated on motherboard)	

QuickSpecs

Standard Features

Storage Controller	HP Smart Array E200i Controller	64 MB memory module supports RAID 0,1 Available upgrades: 128 MB with Battery-backed write cache	
	NOTE: For customers who choose to configure a driveless model via CTO, a storage controller is not required. See Factory Integrated Models section for more information.		
Maximum Internal Storage	Hot Plug Serial Attach SCSI (SAS)	292GB SAS	2 x 146GB Serial SCSI
	Hot Plug Serial ATA (SATA)	500GB SATA	2 x 250GB Serial ATA
	NOTE: For customers who choose to configure a driveless model via CTO, internal storage is not required. See Factory Integrated Models section for more information.		
Graphics	Integrated ATI RN-50 1600x1280x64K 16M color (32 MB DDR1 memory)		
Graphics Resolution Supported	Resolution Color Depths	1600 x 1280, 64K, 256, 16 1280 x 1024, 16.7M, 64k, 256, 16 1024 x 768, 16.7M, 64k, 256,16 800 x 600, 16,7M, 64k, 256, 16 640 x 480, 16,7M, 64k, 256, 16	

Fibre Channel Support

Two optional Fibre Channel HBAs are supported by the HP ProLiant BL460c. Both mezzanine circuit boards connect directly to the server blade system board. These Fibre Channel HBAs are available via option kits and must be ordered separately.

Two option kits

Emulex LPe1105-HP 4Gb FC HBA for HP c-Class BladeSystem (403621-B21)

- Based on the same field-proven ASIC, firmware, and driver technology as Emulex's renowned LPe1150 HBA, the Emulex LPe1105-HP is fully driver compatible with all Emulex HBAs

QLogic QMH2462 4Gb FC HBA for HP c-Class BladeSystem (403619-B21)

- Uses common drivers which means that customers can standardize on one QLogic driver whether they are using the QMH2462 or other 4Gb and 2Gb HBAs powered by QLogic

Emulex and QLogic Fibre Channel HBAs feature:

- Optimal performance utilizing PCI Express
- 4/2/1Gb/s auto negotiating speeds
- Dual-ports for redundant path connections
- Up to two FC HBAs per server blade providing redundant FC HBA support
- Optimized for HP StorageWorks and supported by third party SAN vendors
- Support for Microsoft® Windows® and Linux operating systems environments

Standard Features

Compatible SAN	HP ProLiant BL460c server blades are optimized for HP StorageWorks MSA, EVA and XP HP ProLiant 460c server blades are compatible with select 3rd party SANs (please see blade storage page for more details: http://h18000.www1.hp.com/products/servers/proliant-bl/c-class/storage.html

Anexo 2 – Plan de Pruebas.

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

Autor: Marcelo León	
Revisado y Aprobado por: Ing. Vinicio Guerra, Administrador de la red DDTI.	
Revisado y Aprobado por: Ing. Alex Guevara, Gestión WEB DDTI.	

1. **TEMA:** PLAN DE PRUEBAS PARA LA AUDITORÍA DEL SERVIDOR WEB Y DNS DE LA UNIVERSIDAD TÉCNICA DEL NORTE.

2. **OBJETIVOS:**

Objetivo General:

Realizar un plan de pruebas para la auditoría informática en el servidor WEB y DNS de la Universidad Técnica del Norte.

Objetivos Específicos:

Identificar los errores de configuración de los servidores que se encuentran en producción.

Realizar buenas prácticas de configuración con su debida documentación.

3. PROPÓSITO:

El propósito del plan de pruebas es proveer la información necesaria para planear y controlar los esfuerzos de pruebas del proyecto. Describe el enfoque para probar la seguridad que tienen los servidores en cuanto a su configuración.

Este plan de pruebas soporta los siguientes objetivos:

- Identificar los ítems a probar.
- Identifica los recursos requeridos y un estimado de sus esfuerzos.
- Determina los tipos de pruebas a utilizar en la ejecución del plan de pruebas.
- Solucionar errores de configuración de los servidores.

4. ALCANCE

Definir las pruebas de configuración de los servidores, para detectar vulnerabilidades en el sistema con la respectiva comprobación mediante ataques informáticos para dar una solución a los errores en la seguridad; mediante la utilización de la metodología OFFENSIVE SECURITY.

5. ESTRATEGIA DE PRUEBAS

La estrategia de pruebas tiene como base un modelo de ejecución, técnicas, herramientas, criterios de aceptación que se utilizarán en la realización de las pruebas y ejecución de las mismas.

6. PROCEDIMIENTOS Y REQUERIMIENTOS PARA LAS PRUEBAS:

FASE	OBJETIVO	ESTRATEGIA	HERRAMIENTAS	OBSERVACIONES
1	Recolectar información acerca de la página WEB. Pruebas a ciegas Pruebas con información.	Utilizar buscadores como google para obtener información acerca del objetivo. Entrevista al personal de informática con preguntas claves de seguridad (análisis de riesgos).	Internet, MSAT 4.0	Esto se debe realizar conjuntamente con la autorización de la DDTI.
2	Análisis de Vulnerabilidades (Escaneo de Puertos y Enumeración).	Entrevista al personal de informática con preguntas claves de seguridad. Utilizar comandos propios de la herramienta Kali Linux para obtener información acerca de los dominios, puertos abiertos, etc.	NMAP, Símbolo del Sistema y Kali Linux	Es un proceso que no modifica ni altera a los servicios que se encuentran en producción.
3	Determinar los objetivos que van a ser atacados.	Analizar la información de los datos obtenidos en las fases anteriores.	Internet.	
4	Atacar a la red interna y servidores.	Utilizar herramientas de auditoría informática, para explotar las vulnerabilidades encontradas.	FOCA, WinSCP, PUTTY, Símbolo del sistema, Hydra, Crunch, Beef.	Los servicios pueden alterarse durante el ataque, una vez terminado el ataque los servicios vuelven a funcionar correctamente.

5	Verificación de la información recolectada en las anteriores fases. Lo positivo que se encontró en el sistema. Aspectos en los que se puede mejorar el sistema.	Analizar la información de los datos obtenidos en las fases anteriores y dar soluciones mediante la revisión de la configuración de los servidores.	Servidor WEB y Servidor DNS.	Se necesita claves de acceso a los servidores.

Ataques informáticos.

ATAQUE	OBJETIVO	HERRAMIENTA
Escaneo de Puertos	Servidor WEB	NMAP
Escaneo de Puertos	Servidor DNS	NMAP
Phishing	Servidor WEB y DNS	Beef y Kali Linux
Extraer Metadata	Servidor WEB	FOCA
Snooping	Servidor DNS	FOCA
Ataque de Autenticación	Servicio SSH	Winscp.
Ataque a la red Inalálmbrica	AP Inalámbrico	Linset.
Ataque a la red Cableada	Puntos de Red	Ingeniería Social.
Ataque de Fuerza Bruta	Servicio SSH	Hydra y Crunch.
Ataque DoS	Servidor WEB	Kali Linux

Anexo 3 – Análisis de Riesgos MSAT.

Microsoft Security Assessment Tool
Universidad Técnica del Norte
Completado 15-dic-16 15:26

Informe completo

Este informe consta de las siguientes secciones:

Un socio de Microsoft puede revisar este informe con usted y ayudarle a elaborar un plan de acción detallado para poner en práctica las recomendaciones. Si aún no mantiene ninguna relación comercial con un socio de Microsoft, puede consultar una lista de socios de Microsoft para las soluciones de seguridad en https://solutionfinder.microsoft.com.

La herramienta Microsoft Security Assessment Tool se ha diseñado para ayudarle a determinar los riesgos a los que se enfrenta su infraestructura informática y las medidas que ha adoptado para combatirlos, además de sugerir medidas adicionales para contribuir aún más a la reducción del nivel de riesgos. No debe en ningún caso reemplazar a cualquier otra auditoría llevada a cabo por profesionales.

El uso de Microsoft Security Assessment Tool se rige por las condiciones del contrato de licencia que acompaña al software, y este informe está sujeto a las exclusiones, renuncias y limitaciones de responsabilidad que se incluyen en el contrato de licencia.

El propósito de este informe es meramente informativo. Ni Microsoft Corporation, ni sus proveedores o socios realizan o expresan implícitamente, ninguna declaración formal ni garantía alguna acerca de la herramienta Microsoft Security Assessment Tool, así como tampoco del uso, la precisión o la fiabilidad de los resultados de la evaluación e información que se incluye en este informe.

Resumen ejecutivo

Introducción

La herramienta Microsoft Security Assessment Tool se ha diseñado para ayudarle a identificar y abordar riesgos de seguridad en su entorno informático. Desde un enfoque holístico, se analiza la estrategia de seguridad al tratar distintos temas como el personal, los procesos y la tecnología. Los resultados se asocian con las soluciones recomendadas, incluyendo enlaces a más información de orientación adicional, en caso necesario. Estos recursos podrían ayudarle a asimilar más conceptos sobre las herramientas y los métodos específicos que puedan aumentar la seguridad de su entorno.

Esta sección de resumen pretende ofrecer a los responsables de TI y encargados senior una visión de los niveles de seguridad globales de

la empresa. Puede consultar los resultados y las recomendaciones de forma detallada en el informe que le mostramos a continuación.

Historial del personal: Proceso y ámbito de autoevaluación

La evaluación se ha diseñado para identificar el riesgo comercial de su empresa y las medidas de seguridad utilizadas para mitigar dicho riesgo. A partir de los problemas más comunes del sector, se han desarrollado preguntas con las que es posible realizar una evaluación de alto nivel de las tecnologías, los procesos y el personal de la empresa.

La herramienta comienza con una serie de preguntas sobre el modelo de su empresa, para ir construyendo un perfil de riesgo para la empresa (BRP) mediante la valoración del riesgo al que su empresa está expuesta conforme al modelo y sector empresarial seleccionados. Se plantea una segunda serie de preguntas para compilar las medidas de seguridad que su empresa ha ido implantado a lo largo del tiempo. Todas juntas, esas medidas de seguridad forman capas de defensa, lo que proporciona una mayor protección frente a los riesgos de seguridad y las vulnerabilidades específicas. Cada capa contribuye a una estrategia combinada de defensa en profundidad. Esta suma se denomina Índice de defensa en profundidad (DiDI). A continuación, se comparan el BRP y el DiDI para medir la distribución de riesgos a lo largo de las áreas de análisis (AoAs): infraestructura, aplicaciones, operaciones y personal.

Además de centrarse en la correspondencia entre los riesgos de seguridad y las defensas, esta herramienta también valora la madurez de la seguridad en su empresa. La madurez de la seguridad hace referencia a la evolución hacia una mayor seguridad y prácticas sostenibles. En la escala inferior, se emplean pocas defensas de seguridad y las acciones son reactivas. En el lado opuesto, los procesos establecidos y probados permiten a la empresa ser más proactiva, además de responder de forma más eficaz y sistemática cuando es necesario.

En este contexto, a partir de las tecnologías, los aspectos de seguridad y las estrategias de defensa en profundidad existentes, se ofrecen sugerencias sobre la gestión de riesgos para los entornos específicos. Estas sugerencias tienen como fin conducirle a buen ritmo hacia la consecución de las mejores prácticas para su caso particular.

La presente evaluación, incluidas las preguntas, medidas y recomendaciones, está diseñada para empresas medianas que tengan entre 50 y 500 equipos de escritorio. Su objetivo es estudiar de forma general las áreas de riesgos potenciales, en lugar de proporcionar un análisis en profundidad de una tecnología o un proceso concretos. Como resultado, la herramienta no puede medir la eficacia de las medidas de seguridad utilizadas. Con este fin, la información que recibe debe servirle de guía preliminar para centrarse en las áreas específicas que exigen una atención más rigurosa y no debe en ningún caso reemplazar a cualquier otra evaluación específica realizada por equipos de evaluación independientes cualificados.

Análisis de la situación

Este gráfico de la sección representa los conceptos de su empresa descritos anteriormente y se basa en las respuestas que proporcionó. Recuerde:

- BRP es una medición del riesgo relacionado al modelo empresarial y al sector de la empresa
- DiDI es una medición de las defensas de seguridad utilizadas en el personal, los procesos y la tecnología para ayudar a reducir los riesgos identificados en una empresa.
- La madurez de la seguridad es una medición de la capacidad de la empresa para utilizar de forma eficaz las herramientas disponibles de forma que se cree un nivel de seguridad sostenible a lo largo de diversas disciplinas.

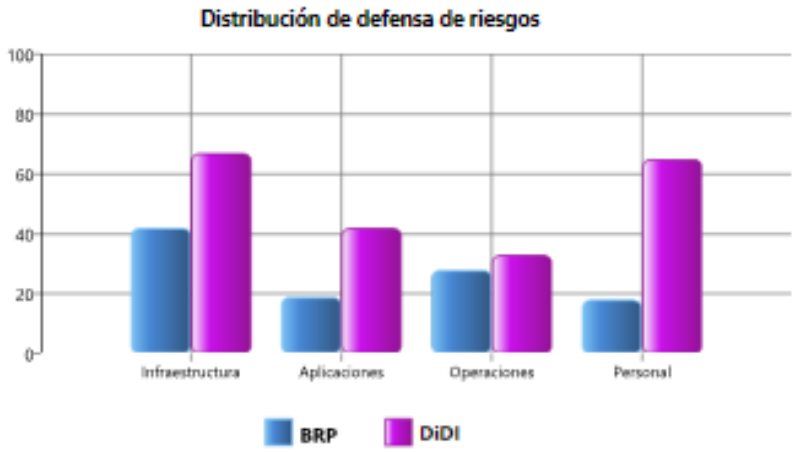
[Consulte los apéndices para obtener información adicional acerca de estos términos y cómo interpretar los gráficos.]

Resultados:

Áreas de análisis	Distribución de defensa de riesgos	Madurez de la seguridad
Personal	🔴	🟢
Operaciones	🟢	🟡
Aplicaciones	🔴	🟢
Infraestructura	🔴	🟢

Distribución de defensa de riesgos

Este gráfico, dividido en áreas de análisis, muestra las diferencias en el resultado de la defensa en profundidad.



Por lo general, es mejor contar con una calificación de DiDI del mismo nivel que otra de BRP para la misma categoría. Un desequilibrio, ya sea dentro de una categoría o entre categorías, en cualquier dirección, puede indicar la necesidad de volver a alinear sus inversiones de TI.

Madurez de la seguridad

La madurez de la seguridad incluye los controles (tanto físicos como técnicos), la competencia técnica de los recursos informáticos, las directivas, los procesos y las prácticas sostenibles. La madurez de la seguridad se puede medir únicamente a través de la capacidad de la empresa para utilizar de forma eficaz las herramientas disponibles de forma que se cree un nivel de seguridad sostenible a lo largo de muchas disciplinas. Debe establecerse una línea de partida de la madurez de la seguridad y usarse para definir las áreas en las que centrar los programas de seguridad de la empresa. No todas las empresas deben esforzarse por alcanzar el nivel óptimo, pero todas deben evaluar en qué punto se encuentran y determinar el lugar que deberían ocupar en vista de los riesgos comerciales a los que se enfrentan. Por ejemplo, puede que una empresa con un entorno de bajo riesgo no necesite nunca subir encima del límite superior del nivel básico o el límite inferior del nivel estándar. Las empresas con un entorno de alto riesgo probablemente entren de lleno en el nivel optimizado. Los resultados del perfil de riesgos para la empresa le permiten hacer un balance de los riesgos.

Madurez de la seguridad	Una medida de las prácticas de una empresa con respecto a las mejores prácticas de la industria para la seguridad sostenible. Todas las empresas deben esforzarse en alinear su nivel de madurez y estrategia de seguridad asociada, en relación a los riesgos que conlleva su actividad comercial.
Básica	Algunas medidas eficaces de seguridad utilizadas como primer escudo protector; respuesta de operaciones e incidentes aún muy reactiva
Estándar	Capas múltiples de defensa utilizadas para respaldar una estrategia definida
Optimizada	Protección efectiva de los asuntos de forma correcta y garantía de la utilización del mantenimiento de las mejores prácticas recomendadas

Tarjeta de puntuación

De acuerdo con sus respuestas acerca de la evaluación de riesgos, sus medidas de defensa se han calificado de la siguiente forma. Las secciones Detalles de la evaluación y Lista de acciones recomendadas de este informe incluyen más detalles, como resultados, mejores prácticas y recomendaciones.

Leyenda: ● Cumple las mejores prácticas recomendadas ● Necesita mejorar ● Carencias severas

Infraestructura	●
Defensa del perímetro	●
Reglas y filtros de cortafuegos	●
Antivirus	●
Antivirus - Equipos de escritorio	●
Antivirus - Servidores	●
Acceso remoto	●
Segmentación	●
Sistema de detección de intrusiones (IDS)	●
Inalámbrico	●
Autenticación	●
Usuarios administrativos	●
Usuarios internos	●
Usuarios de acceso remoto	●
Directivas de contraseñas	●
Directivas de contraseñas-Cuenta de administrador	●
Directivas de contraseñas-Cuenta de usuario	●
Directivas de contraseñas-Cuenta de acceso remoto	●
Cuentas inactivas	●
Gestión y control	●
Informes sobre incidentes y respuesta	●
Creación segura	●
Seguridad física	●

Aplicaciones	●
Implementación y uso	●
Equilibrio de carga	●
Clústeres	●
Aplicación y recuperación de datos	●
Fabricante de software independiente (ISV)	●
Desarrollado internamente	●
Vulnerabilidades	●

Operaciones	●
Entorno	●
Host de gestión	●
Host de gestión-Servidores	●
Host de gestión - Dispositivos de red	●
Directiva de seguridad	●
Clasificación de datos	●
Eliminación de datos	●
Protocolos y servicios	●
Uso aceptable	●
Gestión de cuentas de usuarios	●
Regulación	●
Directiva de seguridad	●
Gestión de actualizaciones y revisiones	●
Documentación de la red	●
Flujo de datos de la aplicación	●
Gestión de actualizaciones	●
Gestión de cambios y configuración	●
Copias de seguridad y recuperación	●
Archivos de registro	●
Planificación de recuperación ante desastres y reanudación de negocio	●
Copias de seguridad	●
Dispositivos de copia de seguridad	●
Copias de seguridad y restauración	●

Personal	●
Requisitos y evaluaciones	●
Requisitos de seguridad	●
Evaluaciones de seguridad	●
Directiva y procedimientos	●
Comprobaciones del historial personal	●

Diseño de aplicaciones	🔴
Autenticación	🟢
Directivas de contraseñas	🟢
Autorización y control de acceso	🔴
Registro	🟡
Validación de datos de entrada	🟡
Metodologías de desarrollo de seguridad de software	🔴
Almacenamiento y comunicaciones de datos	🔴
Cifrado	🟡
Cifrado - Algoritmo	🔴

Directiva de recursos humanos	🟢
Relaciones con terceros	🟡
Formación y conocimiento	🟡
Conocimiento de seguridad	🟡
Formación sobre seguridad	🟢

Iniciativas de seguridad

Las siguientes áreas no cumplen las mejores prácticas recomendadas y deben dirigirse a aumentar la seguridad de su entorno. Las secciones Detalles de la evaluación y Lista de acciones recomendadas de este informe incluyen más detalles, como resultados, mejores prácticas y recomendaciones.

Prioridad alta	Prioridad intermedia	Prioridad baja
• Acceso remoto • Desarrollado internamente • Usuarios administrativos • Vulnerabilidades • Cifrado - Algoritmo	• Creación segura • Seguridad física • Relaciones con terceros • Requisitos de seguridad • Cifrado	• Protocolos y servicios • Copias de seguridad • Antivirus - Equipos de escritorio • Directivas de contraseñas-Cuenta de administrador • Directivas de contraseñas-Cuenta de usuario

Evaluación detallada

Esta sección del informe ofrece los resultados detallados para cada categoría, así como las mejores prácticas, recomendaciones y referencias de información adicional. Las recomendaciones son prioritarias en la siguiente sección.

Áreas de análisis

La siguiente tabla enumera las áreas incluidas para el análisis de alto nivel de esta evaluación de riesgos para la seguridad y explica la relación entre cada área y la seguridad. La sección "Detalles de la evaluación" describe los niveles de seguridad de su empresa (según las respuestas aportadas en la evaluación) con respecto a cada una de estas áreas. Asimismo, indica las prácticas más reconocidas del sector, además de ofrecerle recomendaciones para implantar tales prácticas.

Categoría	Importancia para la seguridad
Perfil de riesgos para la empresa (BRP)	
Perfil de riesgos para la empresa (BRP)	Comprender como la propia naturaleza de la empresa afecta a los riesgos es importante a la hora de decidir dónde aplicar los recursos que ayuden a paliar tales riesgos. El reconocimiento de las áreas le

	permitirá optimizar la asignación del presupuesto de seguridad.
Infraestructura	
Defensa del perímetro	La defensa del perímetro trata la seguridad del perímetro de la red, donde su red interna conecta con el exterior. Este es su primer escudo protector contra los intrusos.
Autenticación	Los procedimientos estrictos de autenticación de usuarios, administradores y usuarios remotos ayudan a asegurar que los intrusos no accedan sin autorización a la red mediante ataques locales o remotos.
Gestión y control	La gestión, supervisión y el registro adecuados son elementos vitales para mantener y analizar los entornos informáticos. Estas herramientas son aún más importantes después de un ataque, cuando se necesita un análisis del incidente.
Aplicaciones	
Implantación y utilización	Cuando se implantan aplicaciones críticas para la empresa, hay que asegurar la seguridad y la disponibilidad de esas aplicaciones y de los servidores. El mantenimiento continuo es imprescindible para ayudarle a asegurarse de que los errores de seguridad se corrigen y que no se introducen nuevas vulnerabilidades en el entorno.
Diseño de aplicaciones	Un diseño que no aborda adecuadamente los mecanismos de seguridad como la autenticación, la autorización, y la validación de datos podría permitir que los atacantes aprovechen las vulnerabilidades de seguridad para acceder a información confidencial.
Almacenamiento y comunicaciones de datos	La integridad y confidencialidad de los datos son dos de las prioridades que debe garantizar cualquier empresa. La pérdida o el robo de datos puede afectar negativamente tanto a los ingresos de una entidad como a su reputación. Es importante comprender como las aplicaciones controlan y protegen los datos críticos.
Operaciones	
Entorno	La seguridad de una empresa depende de los procedimientos operativos, los procesos y las pautas que se aplican en el entorno. Pueden aumentar la seguridad incluyendo más que meras defensas tecnológicas. La capacidad del equipo de operaciones para mantener la seguridad del entorno depende de forma crucial de la documentación exacta del entorno y de las pautas.
Directiva de seguridad	La política de seguridad corporativa hace referencia a las directivas y a pautas individuales para regular el uso adecuado y seguro de las tecnologías y los procesos de la empresa. Esta área incluye las directivas para todos los aspectos de la seguridad, como los usuarios, los sistemas y los datos.
Gestión de actualizaciones y revisiones	La gestión adecuada de actualizaciones y revisiones es un factor importante para la seguridad del entorno informático de las empresas. La aplicación oportuna de actualizaciones y revisiones es necesaria para contribuir a la protección del entorno contra las vulnerabilidades conocidas y aquellas que podrían ser un frente de ataque.
Copias de seguridad y recuperación	Las copias de seguridad y la recuperación de datos son imprescindibles para el mantenimiento de la continuidad de los servicios comerciales en caso de un accidente o fallo de hardware o de software. La falta de procedimientos adecuados para realizar copias de seguridad y recuperación podría producir una pérdida significativa de datos y de productividad.

Personal	
Requisitos y evaluaciones	Todos los encargados de la toma de decisiones deben comprender los requisitos de seguridad para que las decisiones comerciales y técnicas adoptadas aumenten la seguridad, en lugar de contradecirse entre sí. Las evaluaciones periódicas realizados por terceros independientes pueden ayudar a la empresa a revisar, evaluar e identificar las posibles mejoras.
Directivas y procedimientos	Los procedimientos claros y prácticos en la gestión de las relaciones con los fabricantes y socios pueden ayudarle a minimizar el nivel de riesgos al que se expone la empresa. Los procedimientos para contratar aspirantes y finalizar sus contratos pueden proteger a la empresa contra empleados sin escrúpulos o descontentos.
Formación y conocimiento	Los empleados deben recibir formación para que sean conscientes de cómo las medidas de seguridad afectan a sus actividades diarias, para que no expongan a la empresa a mayores riegos de forma inadvertida.

Análisis de la evaluación

Esta sección está dividida en las cuatro principales áreas de análisis: infraestructura, aplicaciones, operaciones y personal.

Infraestructura

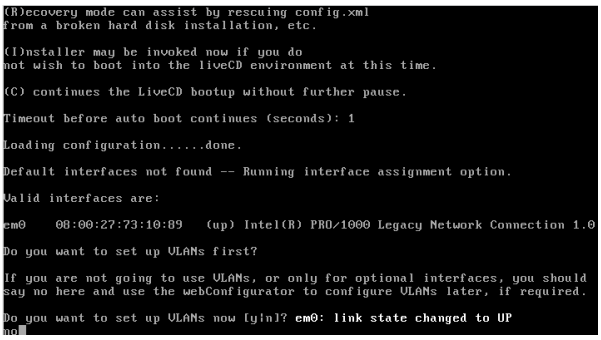
La seguridad de las infraestructuras se centra en cómo debe funcionar la red, los procesos comerciales (internos o externos) que se deben implantar, cómo se crean y utilizan los hosts y la gestión y el mantenimiento de la red. La seguridad de la infraestructura efectiva puede ayudarle a mejorar significativamente la defensa de la red, las reacciones a incidentes, la disponibilidad de la red y el análisis de fallos. Al establecer un diseño de la infraestructura que todos puedan comprender y seguir, podrá identificar las áreas de riesgo y desarrollar métodos para reducir las amenazas. La evaluación revisa los procedimientos de alto nivel que una empresa puede seguir para ayudarle a mitigar el riesgo para la infraestructura enfocándose en las áreas de seguridad de infraestructura que siguen:

- Defensa del perímetro—cortafuegos, antivirus, acceso remoto, segmentación
- Autentificación—directivas de contraseñas
- Gestión y control—hosts de gestión, archivos de registro
- Estación de trabajo—configuración de creación

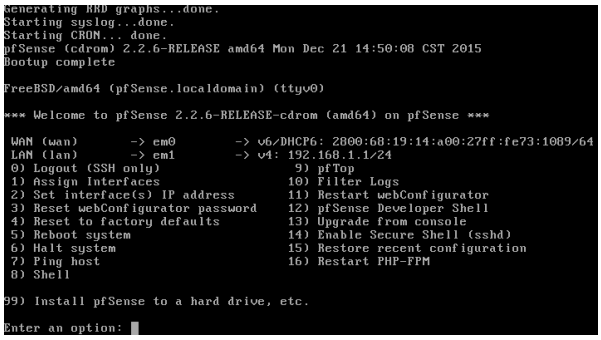
Defensa del perímetro	
Subcategoría	**Mejores prácticas recomendadas**
Reglas y filtros de cortafuegos	Los firewalls son un mecanismo de primera línea de defensa y se deben colocar en todas las ubicaciones de borde de red. Las reglas implementadas en los firewalls deben ser muy restrictivas y establecerse host a host y servicio a servicio. Al crear reglas de firewall y listas de control de acceso (ACL) de enrutador, céntrese primero en la protección de los dispositivos de control y de la red frente a ataques. El firewall debe estar establecido con una posición de denegación predeterminada, permitiendo únicamente el tráfico necesario. * Aplique el flujo de datos utilizando las ACL de red y las reglas de firewall. * Pruebe las reglas de firewall y ACL de enrutador para determinar si las reglas existentes contribuyen a ataques de denegación de servicio (DoS). * Implemente una o más DMZ como parte de una implementación de firewall sistemática y formal.

Anexo 4 – Instalación de Pfsense.

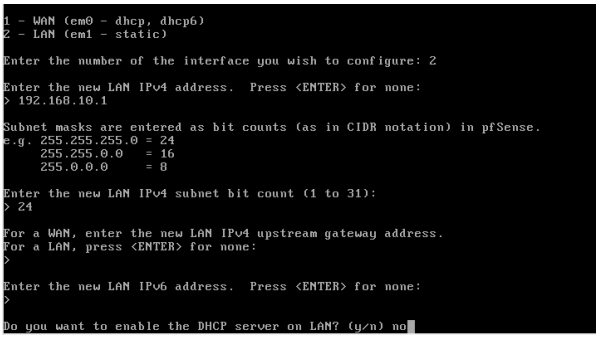
Paso 1.- Configurar al equipo de tal manera que arranque desde el dispositivo que contiene el sistema operativo Pfsense.



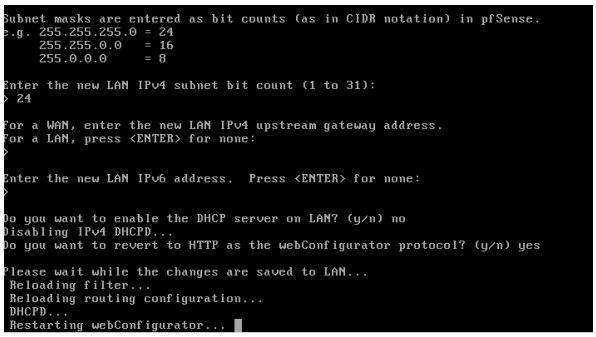
Paso 2.- Asignar las interfaces em0 para la WAN y la em1 para la LAN.



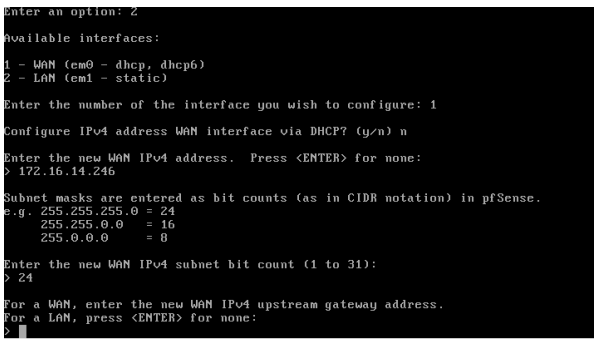
Paso 3.- Asignar direcciones IP a la interfaz creada como em1 que corresponde a la LAN.



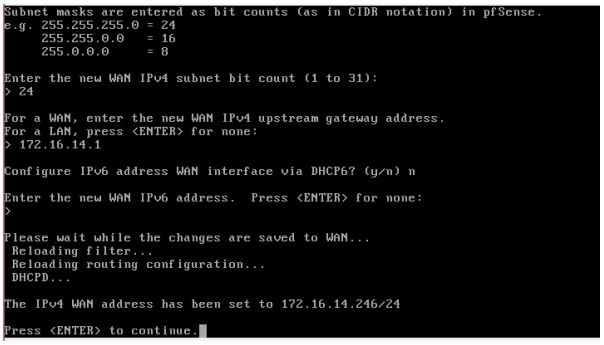
Paso 4.- Se activa el Configurador Web en la LAN para poder acceder al entorno gráfico del servidor Pfsense.



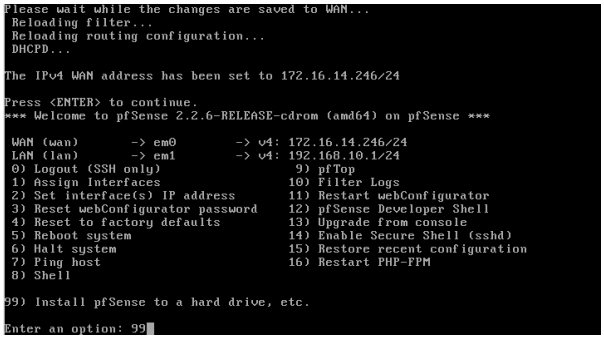
Paso 5.- Asignar direcciones IP a la interfaz creada como em0 que corresponde a la WAN.



Paso 6.- Desactivar DHCP ya que en este caso se utiliza sólo direcciones estáticas.

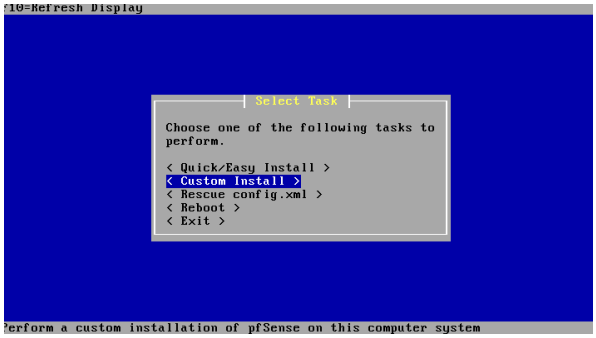


Paso 7.- Se ingresa a la opción 99 para proceder a la instalación.

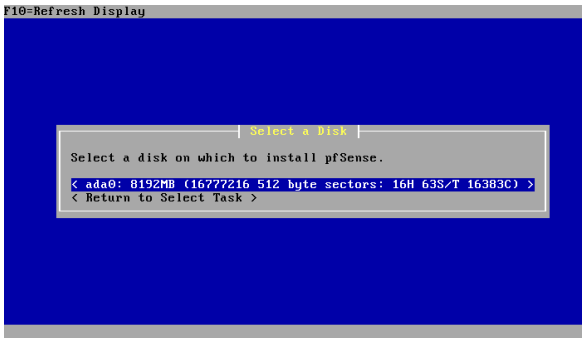


Paso 8.- Se acepta los ajustes para continuar con la instalación.

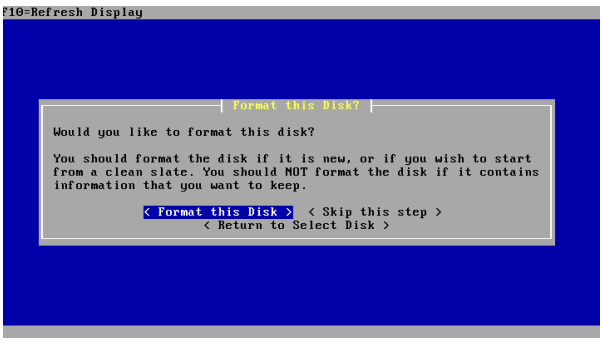
Paso 9.- Se inicia la instalación en Custom Install.



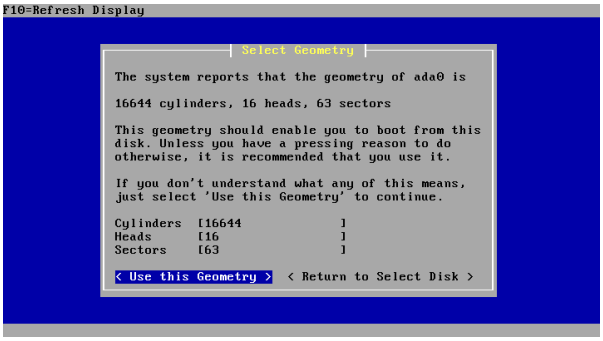
Paso 10.- Se escoge el disco duro donde se va montar el servidor.



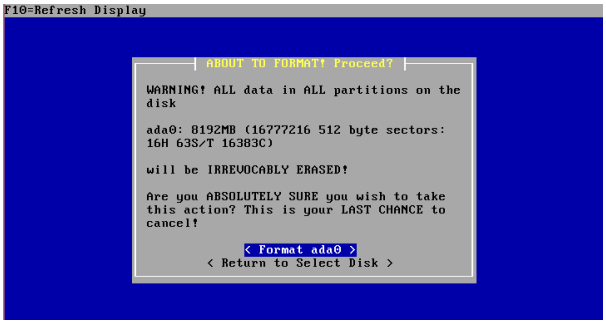
Paso 11.- Se formatea el disco para luego sea instalado el nuevo sistema operativo.



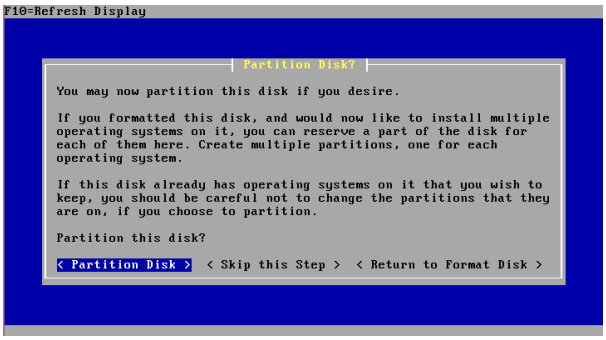
Paso 12.- En este caso se usa el disco completo.



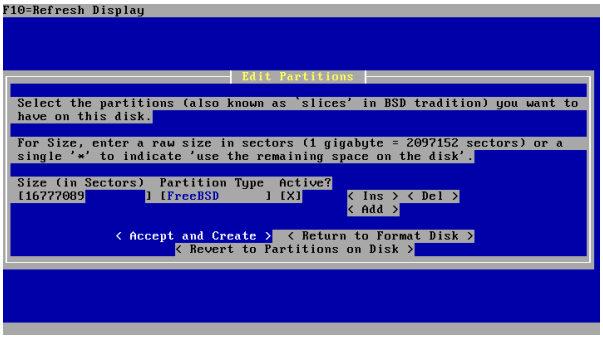
Paso 13.- Se formatea la partición, que en este caso sería un solo disco primario.



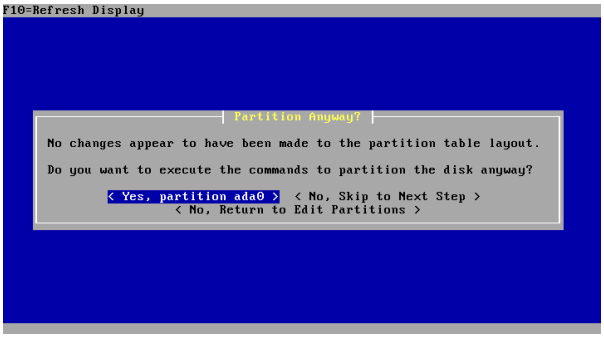
Paso 14.- Se realiza una partición primaria en el disco.



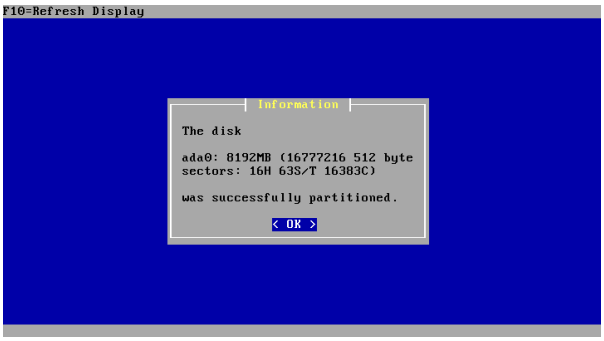
Paso 15.- Se acepta y se crea la partición primaria.



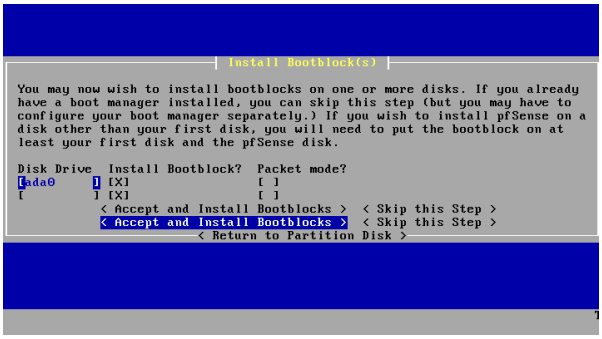
Paso 16.- Enter en Yes en la partición de ada0.



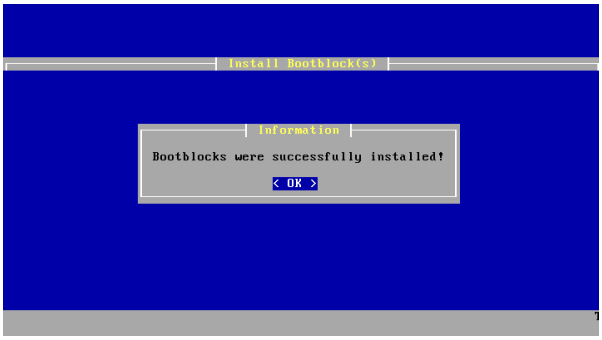
Paso 17.- La partición ha sido exitosa, por lo tanto enter en OK.



Paso 18.- Se acepta y se instala el Bootblocks.

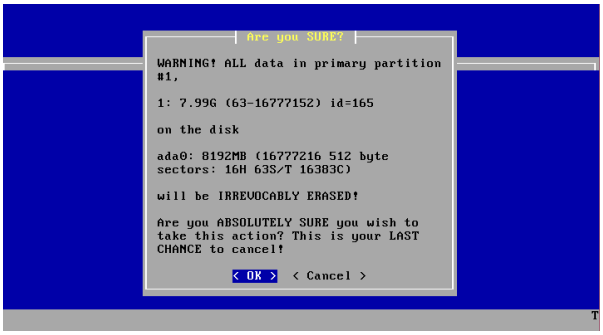


Paso 19.- Ok ya que se instaló correctamente.

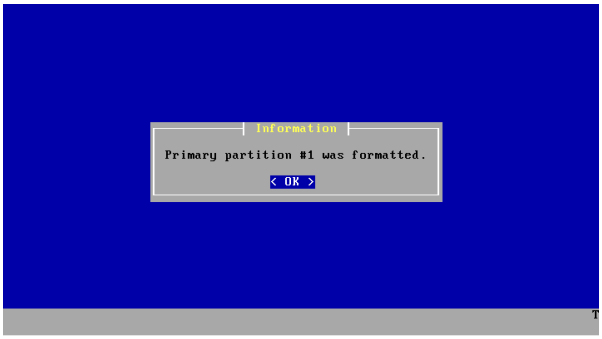


Paso 20.- Se selecciona el disco primario.

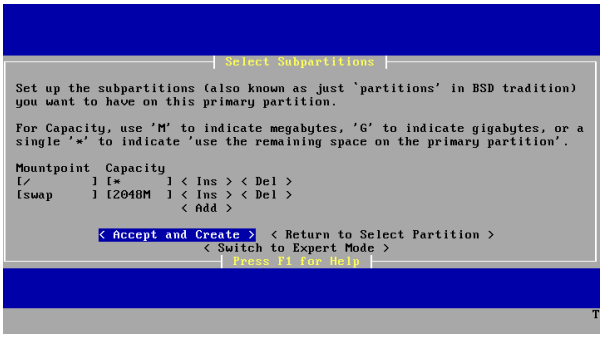
Paso 21.- Ok en la pregunta de que si está seguro en instalar en el disco primario.



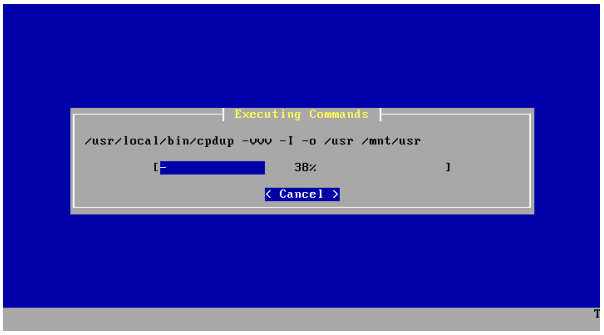
Paso 22.- Ha sido instalado correctamente, asi que se le da OK.



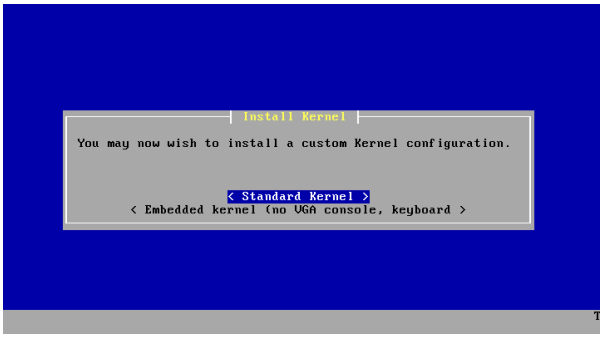
Paso 23.- Se crea una partición SWAP.



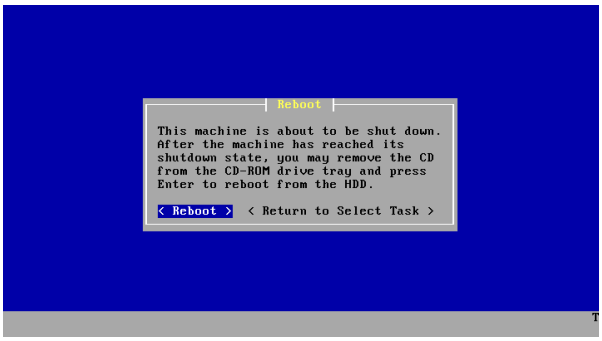
Paso 24.- Se espera hasta que termine de crear la partición SWAP.



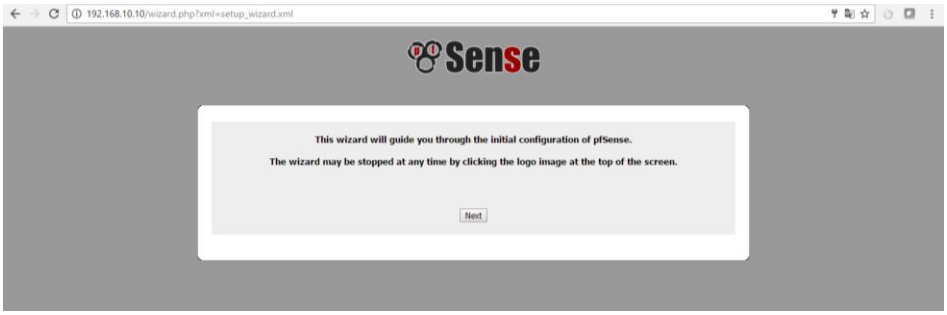
Paso 25.- Se instala el Kernel.



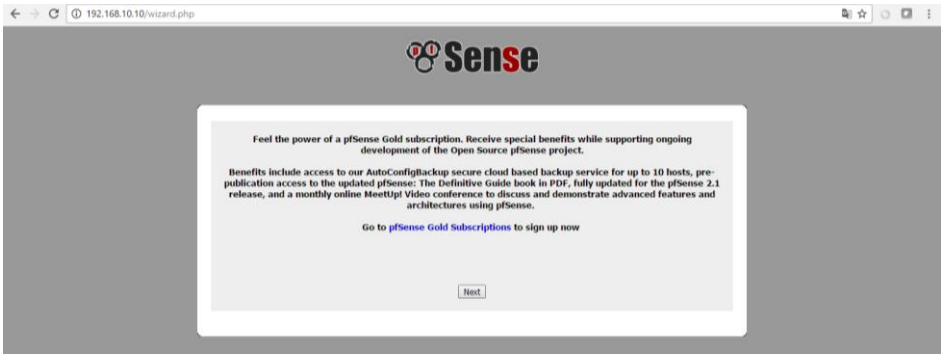
Paso 26.- Se reinicia el servidor y se saca el disco de instalación.



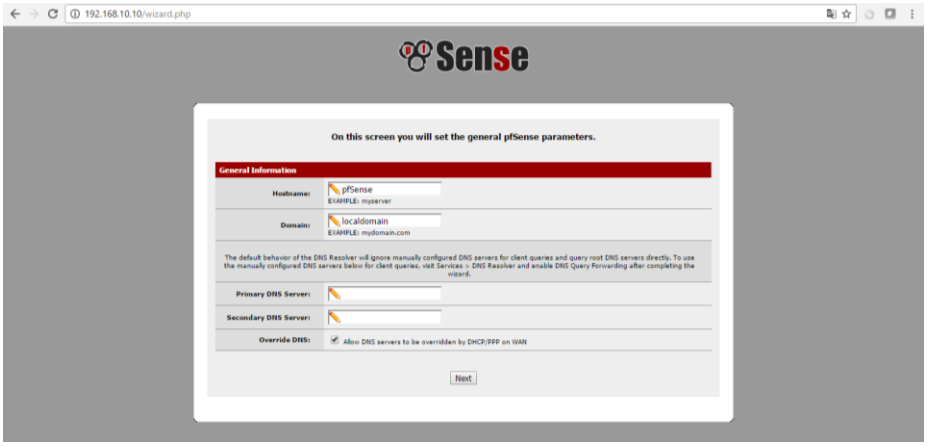
Paso 27.- Configuración e Instalación del entorno gráfico de Pfsense.



Paso 28.- Se acepta todos los requerimientos para instalar el entorno gráfico.

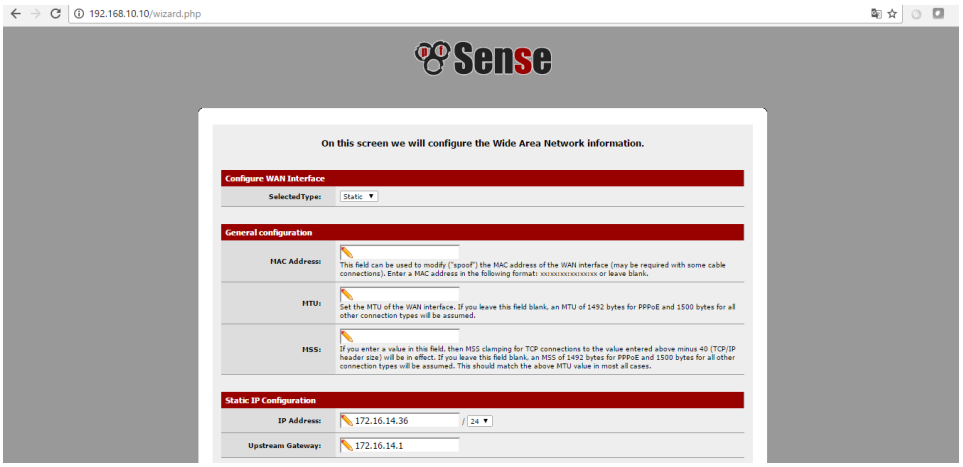


Paso 29.- Determinar el nombre del servidor y el dominio.

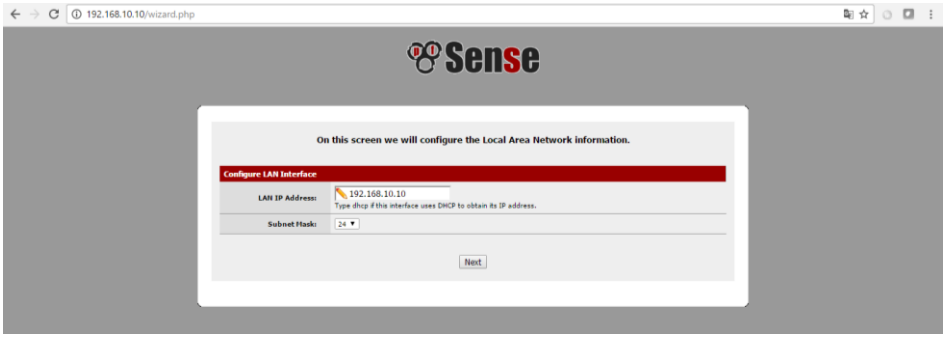


Paso 30.- Se ingresa la zona horaria de acuerdo a la ubicación física del servidor.

Paso 31.- Se tiene el direccionamiento de la interfaz WAN que previamente se asignó, se continúa con la instalación.



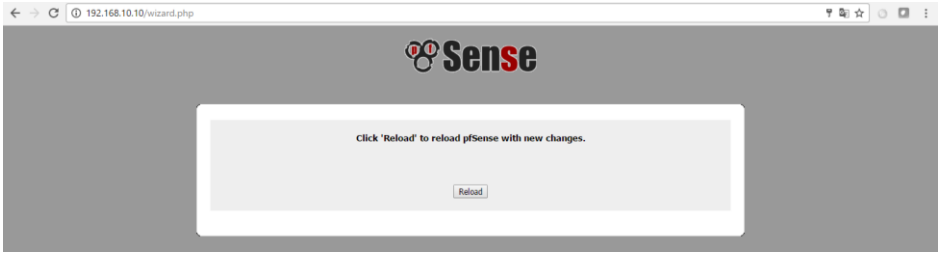
Paso 32.- De igual manera se continúa sin problema ya que previamente se configuró la interfaz LAN.



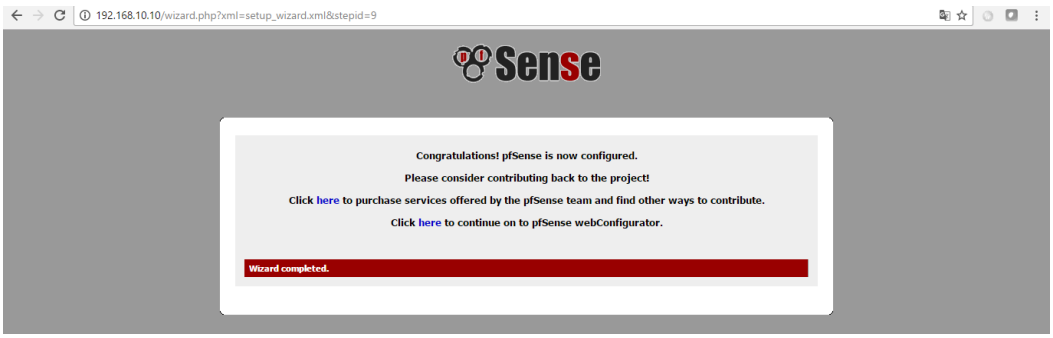
Paso 33.- Por seguridad se cambia la clave que está por defecto en el servidor.

Contraseña: Marcelo01#

Paso 34.- Se graban los cambios.



Paso 35.- Se accede otra vez al servidor con la ip asignada, se ingresa con la contraseña que se asignó.



Anexo 5 – Oficios de autorización y entrega de documentación.

Ibarra, 15 de febrero del 2017

Señor

Ing. Juan Carlos García

DIRECTOR DDTI

De mis consideraciones:

Yo, MARCELO WLADIMIR LEÓN GUDIÑO estudiante de 10mo Semestre de la Carrera de Ingeniería en Electrónica y Redes de Comunicación, en calidad de autor del proyecto de grado "AUDITORÍA DE SEGURIDAD INFORMÁTICA EN LA RED INTERNA DE LA UNIVERIDAD TÉCNICA DEL NORTE SEGÚN LA METODOLOGÍA OFFENSIVE SECURITY PROFESSIONAL TRAINING AND TOOLS FOR SECURITY SPECIALISTS Y PLANTEAMIENTO DE POLÍTICAS DE SEGURIDAD BASADO EN LA NORMA ISO/IEC 27001", actualmente tesista de la Dirección de Desarrollo Tecnológico e Informático cordialmente solicito, me permita hacer la entrega del Informe Técnico de Análisis de Riesgos realizado en la red Universitaria, con la finalidad de que esta información sea divulgada hacia los encargados en las áreas de infraestructura de red y aplicaciones, para su conocimiento del estado de la red con respecto a seguridad informática.

Atentamente,

Marcelo Wladimir León Gudiño

C.I: 1003636717

RECIBIDO 15 FEB 2017

Ibarra, 15 de febrero del 2017

Señor

Ing. Juan Carlos García

DIRECTOR DDTI

De mis consideraciones:

Yo, MARCELO WLADIMIR LEÓN GUDIÑO estudiante de 10mo Semestre de la Carrera de Ingeniería en Electrónica y Redes de Comunicación, en calidad de autor del proyecto de grado "AUDITORÍA DE SEGURIDAD INFORMÁTICA EN LA RED INTERNA DE LA UNIVERIDAD TÉCNICA DEL NORTE SEGÚN LA METODOLOGÍA OFFENSIVE SECURITY PROFESSIONAL TRAINING AND TOOLS FOR SECURITY SPECIALISTS Y PLANTEAMIENTO DE POLÍTICAS DE SEGURIDAD BASADO EN LA NORMA ISO/IEC 27001", actualmente tesista en la Dirección de Desarrollo Tecnológico e Informático cordialmente solicito, me permita hacer la entrega de las Políticas y Manuales de Procedimientos de Seguridad Informática realizado en beneficio de la red Universitaria, con la finalidad de que esta información sea divulgada hacia los encargados de las áreas de infraestructura de red y aplicaciones, para su conocimiento sea revisado y aplicado.

Atentamente,

Marcelo Wladimir León Gudiño

C.I: 1003636717

RECIBIDO 15 FEB 2017
10:25

Ibarra, 15 de febrero del 2017

Señor

Ing. Juan Carlos García

DIRECTOR DDTI

De mis consideraciones:

Yo, MARCELO WLADIMIR LEÓN GUDIÑO estudiante de 10mo Semestre de la Carrera de Ingeniería en Electrónica y Redes de Comunicación, en calidad de autor del proyecto de grado "AUDITORÍA DE SEGURIDAD INFORMÁTICA EN LA RED INTERNA DE LA UNIVERIDAD TÉCNICA DEL NORTE SEGÚN LA METODOLOGÍA OFFENSIVE SECURITY PROFESSIONAL TRAINING AND TOOLS FOR SECURITY SPECIALISTS Y PLANTEAMIENTO DE POLÍTICAS DE SEGURIDAD BASADO EN LA NORMA ISO/IEC 27001", actualmente tesista en la Dirección de Desarrollo Tecnológico e Informático cordialmente solicito, me permita realizar pruebas de funcionamiento de las soluciones para las vulnerabilidades encontradas en el transcurso del proyecto de tesis, esto en beneficio de la red Universitaria, y tiene como finalidad mejorar la Seguridad Informática, para su conocimiento sea revisado y aplicado en la red de producción.

Atentamente,

Marcelo Wladimir León Gudiño

C.I: 1003636717

RECIBIDO 15 FEB 2017
10H25

Anexo 6 – Cotización de servicios y equipos.

Licencia para el servidor DNS.

Información general de precios y licencias

Con el fin de brindarle una experiencia más uniforme con las licencias en entornos de varias nubes, estamos haciendo la transición desde las licencias basadas en procesador a las licencias basadas en núcleo con las ediciones Datacenter y Standard de Windows Server 2016. Para conocer los precios exactos, póngase en contacto con el distribuidor de Microsoft.

Edición de Windows Server 2016	Ideal para	Modelo de licencias	Requisitos de CAL*	Precios de Open NL ERP (USD)
Datacenter**	Entornos de centros de datos definidos por software y altamente virtualizados	Basado en núcleo	CAL de Windows Server	$6,155
Standard**	Entornos de baja densidad o no virtualizados	Basado en núcleo	CAL de Windows Server	$882
Essentials	Pequeñas empresas con hasta 25 usuarios y 50 dispositivos	Basado en procesador	No se requiere CAL	$501

* Se requiere una CAL para cada usuario o dispositivo que acceda a un servidor. Consultar detalles en los derechos de uso de los productos.

** El precio de las ediciones Datacenter y Standard es para licencias de 16 núcleos.

Fuente: Recuperado de https://www.microsoft.com/es-xl/cloud-platform/windows-server-pricing

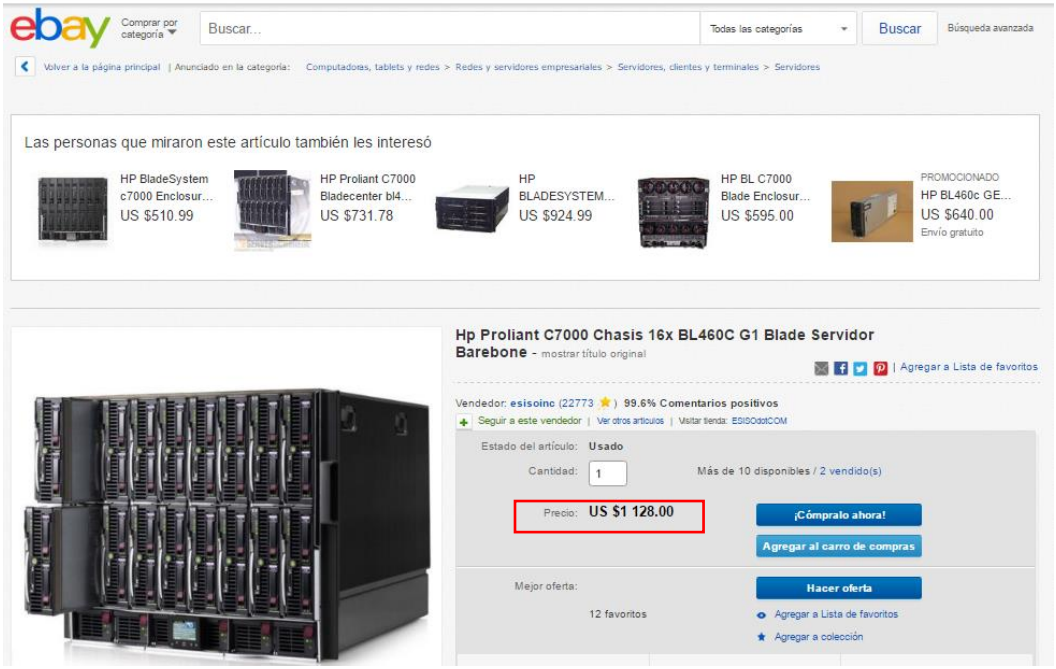
Certificado SSL.

Fuente: Recuperado de https://www.neothek.com/certificados-ssl/Ecuador/

Servidor WEB.

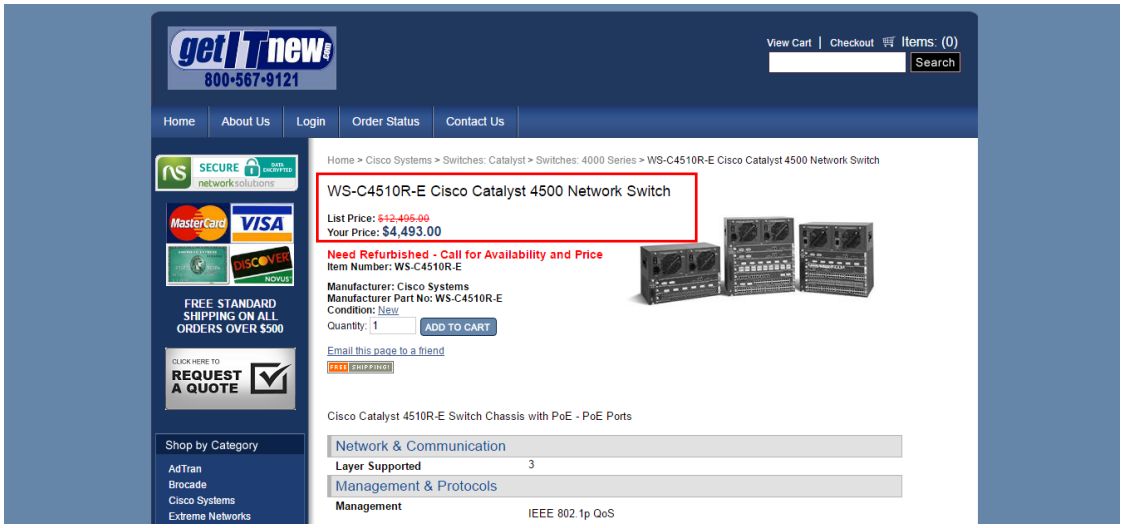
Fuente: Recuperado de http://www.ebay.com/itm/HP-Proliant-C7000-Chassis-8x-BL460C-G8-Blade-8-CORE-E5-2660-16GB-256GB-SSD-/131578140432?hash=item1ea2ab1710:g:5UQAAOSwzgRW11ru

Servidor DNS.



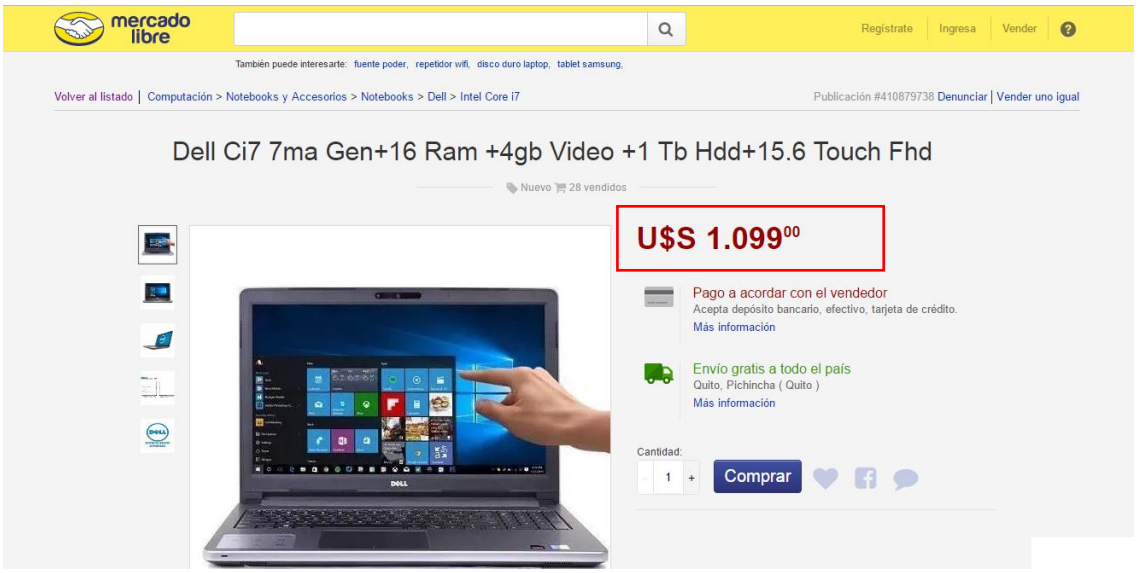
Fuente: Recuperado de http://www.ebay.com/itm/HP-Proliant-C7000-Chassis-16x-BL460C-G1-Blade-Server-Barebone-/350891719510?hash=item51b2c6bb56:g:gMEAAOSwB4NW0N~J

Switch The Core.



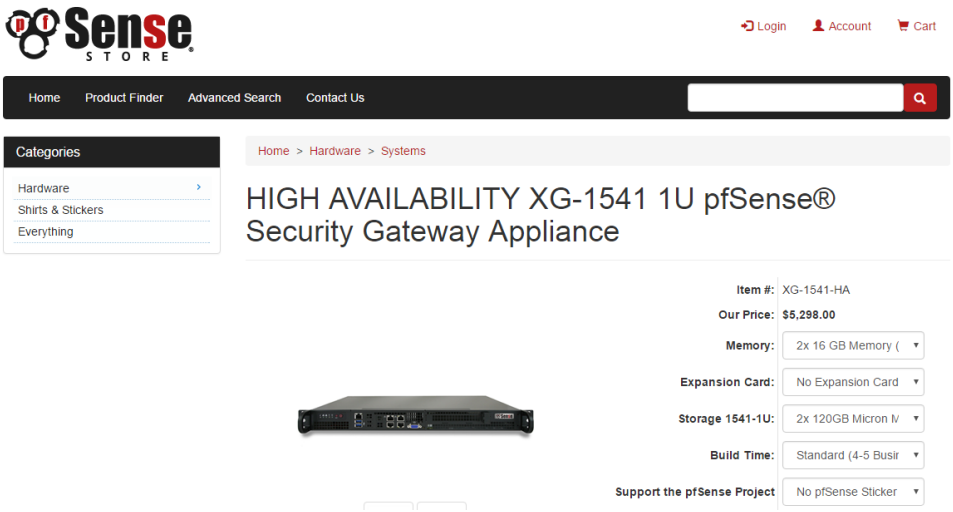
Fuente: Recuperado de http://getitnew.com/ws-c4510r-eciscocatalyst4510r-eswitchchassiswithpoe.aspx

Laptop del auditor informático.



Fuente: Recuperado de http://articulo.mercadolibre.com.ec/MEC-410879738-dell-ci7-7ma-gen16-ram-4gb-video-1-tb-hdd156-touch-fhd-_JM

Servidor IDS/IPS



Fuente: Recuperado de https://store.pfsense.org/HIGH-AVAILABILITY-XG-1541-1U-pfSense-Security-Gateway-Appliance-P111.aspx

Cotización Norma ISO 27001.

Servicio Ecuatoriano de Normalización

PROFORMA No. CI 026-2017

Cliente:	Marcelo Wladimir León Gudiño
Atención:	Marcelo Wladimir León Gudiño
Dirección:	Ibarra
CI/RUC:	1003636717
Teléfono:	991329677
Fecha:	lunes 20 de marzo de 2017

CANTIDAD	DESCRIPCIÓN	C.IMPRESO	C. DIGITAL	C. TOTAL
2	NTE INEN-ISO/IEC 27001:2017 (34 PÁGINAS)	$7,48	$7,48	$14,96
1	CD		$1,00	$1,00
1	ENVÍO FUERA DE LA CIUDAD	$2,50		$2,50
				$18,46
SON:	DIECIOCHO CON 46/100 USD			

NOTA: El pago se debe realizar mediante transferencia bancaria o depósito bancario, estamos exentos de retenciones.
BENEFICIARIO: SERVICIO ECUATORIANO DE NORMALIZACIÓN
RUC INEN: 1768046530001
BANCO PICHINCHA, Cta. Corriente, Nro. 3245330504, **código/sublínea** 140399
Email: centrodeinformacion@normalizacion.gob.ec
PROFORMA VÁLIDA POR 60 DÍAS

Gabriela Vallejo Giler
Centro de Manejo y Divulgación de la Información
SERVICIO ECUATORIANO DE NORMALIZACIÓN-INEN

Baquerizo Moreno E8-29 y Diego de Almagro
Telf.: +(593 2) 3825960 / 3825999 EXT.121 | Casilla: 17-01-3999
Facebook: /inen.ec | Twitter: @INEN_ec
www.normalizacion.gob.ec
Quito – Ecuador

Cotización servicios profesionales.

PLUS
SERVICIOS TECNOLÓGICOS

CLIENTE: Universidad Técnica del Norte

REFERENCIA: PROFORMA

INTRODUCCIÓN

De mi mayor consideración

De acuerdo a su requerimiento, envío la siguiente propuesta, donde se detalla la realización de una auditoría de seguridad informática y la instalación de un servidor IDS/IPS. Esto se encuentra sujeto a modificaciones solicitadas por el cliente.

ANTECEDENTES

La seguridad de la información es un bien critico en las organizaciones, por tal razón la necesidad de tomar medidas de seguridad en cuanto a la disponibilidad, confidencialidad e integridad de los datos.

CARACTERÍSTICAS

- Herramientas utilizadas por expertos en la materia de seguridad informática.
- Capacidad de resolver problemas críticos de seguridad.
- Optimización de recursos informáticos existentes.
- Amplio conocimiento de instalación y configuración de sistemas de seguridad informática.

BENEFICIOS

- Sistemas preventivos y correctivos para la seguridad de la información.
- Análisis de Riesgos de la red de datos.
- Planteamiento de soluciones a las vulnerabilidades encontradas.
- Instalación de un sistema de protección (IDS/IPS).

TARIFA

TIPO	MÁXIMO	PROMEDIO	MÍNIMO	PAGOS
Auditoría de seguridad informática.	10000	20000	30000	2
Instalación y configuración de un servidor IDS/IPS.	2000	2500	3000	2
TOTAL:	12000	22500	33000	2

Nota: Los valores de las tarifas incluyen IVA.

AIRMAX TELECOM
PLUS
SERVICIOS TECNOLÓGICOS
RUC: 1091732455001
Soluciones Tecnológicas SA

Sr. Alex Medina
Jefe Técnico