PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

ESCUELA DE POSGRADO

DESARROLLO DE UN SISTEMA DE AUDITORÍA DE EQUIPOS DE SEGURIDAD DE REDES

Tesis para optar por el Grado de

MAGÍSTER EN INGENIERÍA DE LAS TELECOMUNICACIONES

Presentado por:

Jorge Luis Pomachagua Sotomayor

Asesor:

Mg. Ing. Agurto Hoyos, Oscar Pedro.

Lima, junio del 2020

Dedicatoria

A mi familia,

Por siempre creer en mí y apoyarme incondicionalmente.

Agradecimientos

A mi asesor de tesis, Mg. Ing. Oscar Agurto por su constante apoyo en el desarrollo de la presente tesis.

Al Dr. Carlos Silva, director de la Maestría de Ingeniería de las Telecomunicaciones, por su constante apoyo y guía a lo largo de toda la carrera.

RESUMEN

La presente tesis propone desarrollar un sistema auditor de información que brinde visibilidad a solicitud del usuario del estado actual de los equipos de seguridad. Esto abarca poder validar la configuración del directorio activo, así como sus equipos registrados, usuarios y/o grupos; de igual forma con el firewall de seguridad en el cual se hará una revisión de la configuración del equipo y de las políticas de seguridad habilitadas.

Mantener un adecuado control de las múltiples configuraciones que se realizan a diario sobres los equipos de seguridad puede llegar a ser una tarea muy complicada, teniendo en cuenta que muchas veces diferentes administradores son los que realizan cambios sobre las plataformas desde su activación inicial. Es por ello que cada cierto tiempo las empresas solicitan auditorías externas las cuales reportan el estado actual de la configuración de los equipos de seguridad y el nivel de cumplimiento de las políticas vigentes.

Con el avance de la tecnología se han automatizado muchas tareas y el uso de una computadora es imprescindible dentro de una empresa, ello conlleva a considerar obligatoriamente la seguridad aplicada a la información que viaja a través de las redes internas como factor clave. Hoy en día es común que constantemente surjan nuevas vulnerabilidades en los sistemas y/o equipos de red, por ello contar con una herramienta que ofrezca visibilidad de lo que realmente se encuentra configurado en los equipos de seguridad se vuelve una necesidad.

Esta tesis se centra en dar a conocer las posibles brechas de seguridad dentro de la infraestructura de red de una empresa, las cuales pueden generar un alto costo en caso de ser vulneradas por un atacante externo o interno. Ello resalta la importancia de un correcto planeamiento y control al momento de realizar configuraciones en los equipos de seguridad. Un ejemplo de brecha de seguridad en las diferentes empresas ocurre cuando un administrador configura una política de prueba brindando acceso al puerto TCP/80 y se olvida de eliminar dicha política, ello puede conllevar a que algún ataque de tipo Ransomware infecte una máquina y este a su vez se propague a toda la red interna, generando un bloqueo masivo y ocasionando un corte parcial o total de las operaciones.

El sistema auditor se conecta al directorio activo y al firewall, vía LDAP y API respectivamente, por medio de una sola interfaz de usuario y mediante diferentes consultas es capaz de extraer información relevante ("*actionable insights*"), la cual se utiliza para tomar acción rápida ante cualquier evento de seguridad.

ÍNDICE GENERAL

Índice de Figuras

Índice de Tablas

ACRÓNIMOS

AAA	American Accounting Association.
AD	Active Directory.
API	Application Programming Interface.
DDOS	Distributed Denial of Service.
DHCP	Protocolo de configuración dinámica de un host.
FRAMEWORK	Entorno de trabajo o marco de trabajo.
FTP	File Transfer Protocol
IETF	Internet Engineering Task Force
HTML	Lenguaje de programación utilizado para el desarrollo de páginas web.
ISO	Organización Internacional de Normalización.
LAN	Local Area Network.
LDAP	Lightweight Directory Access Protocol.
NAT	Network Address Translation.
OS	Operating System.
PHISHING	Abuso informático explotado mediante ingeniería social.
PSF	Python Software Foundation
RANSOMWARE	Programa que restringe el acceso a archivos del sistema operativo y a cambio de quitar la restricción pide un rescate monetario.
SAM	Security Account Manager
SPAM	Correo electrónico no solicitado.
SDK	Software Development Kit.
SID	Security Identifier
SPYWARE	Programa espía que recopila información de una PC.
TCP	Transmission Control Protocol.

UDP	User Datagram Protocol.
VPN	Virtual Private Network.
XML	Extensible Markup Language
WAN	Wide Area Network.

INTRODUCCIÓN

Actualmente las redes de comunicación en los diferentes tipos de organizaciones son implementadas con base en diferentes tecnologías. A través de dichas redes viaja uno de los activos más importantes de cualquier empresa: la información, la cual puede ser vulnerada por causas externas o internas; debido a ello, el establecimiento de lineamientos de seguridad acordes con el nivel de protección que se desee es fundamental para asegurar el funcionamiento óptimo de una red de datos y, por ende, las operaciones de la empresa.

Para asegurar un buen manejo de los datos se recomienda a las empresas realizar consultorías relacionadas a la seguridad de la información, así como auditorías que cubran tanto los sistemas como las redes que soportan el flujo de dichos datos. De la mano con las auditorías se debe elaborar y ejecutar todo un plan de sensibilización de los usuarios sobre las prácticas seguras al momento de utilizar sistemas y/o aplicaciones.

Cabe indicar que los objetivos principales de cualquier consultoría en seguridad de datos son la validación de los métodos adecuados de manejo de la información y el control y/o acceso a los sistemas mediante los cuales se pueda mantener la autenticidad, confidencialidad, disponibilidad e integridad de los datos críticos de una organización. [1]

Una vez realizada la consultoría en una organización, se entrega un reporte con las potenciales vulnerabilidades halladas en los sistemas y las recomendaciones según normas o estándares necesarias para poder reducir o anular las brechas de seguridad encontradas. Con dicha información se procede a elaborar un plan de acción para realizar los cambios necesarios en la infraestructura de redes. Cada empresa cuenta con diferentes necesidades en cuanto al grado de protección de la información, una vez definido ello y de la mano del reporte de consultoría se plantean políticas de seguridad.

En este contexto, la tesis propone como objetivo principal el diseño de un sistema de auditoría que se encargue de obtener los parámetros de configuración de los equipos de seguridad a solicitud del usuario e indicar si el estado actual de la infraestructura de red cumple con las normas y/o estándares definidos en las políticas de seguridad que hayan sido solicitados en una auditoría de seguridad informática previa.

En el capítulo 1 se presenta una explicación sobre la problemática de las auditorías de seguridad, los distintos tipos de amenazas vigentes, como también los diferentes tipos de seguridad que se puede aplicar en cualquier entorno de red, se presentan los equipos involucrados dentro de una auditoria de seguridad, además de los diferentes tipos de programación y técnicas de conexión disponibles en la actualidad para extraer información.

En el capítulo 2 se desarrolla el detalle de los tipos y fases de una auditoría de seguridad, así como los diferentes estándares internacionales relacionados.

En el capítulo 3 se realizará una propuesta de implementación del sistema auditor para equipos de seguridad, asimismo, se indicarán todas las herramientas y consideraciones necesarias para un correcto funcionamiento.

En el capítulo 4 se realizará una evaluación integral del sistema y se aplicará en diferentes ambientes de laboratorio y de producción. De igual manera se presentarán los reportes emitidos por el sistema y el análisis brindado.

En el capítulo 5 se plantean recomendaciones para la implementación del sistema ya descrito. Finalmente se presentan las conclusiones del proyecto de tesis considerando algunas mejoras a futuro.

CAPÍTULO 1: MARCO TEÓRICO

1.1 Objetivo

La presente tesis tiene como objetivo implementar un sistema que realice una auditoría de estándares de seguridad de manera automática en una organización que cuenta con diferentes plataformas informáticas. Se busca aplicar conocimientos de Seguridad de Redes generando un sistema evaluador. Para aplicar la auditoría mediante este sistema se requiere:

- Indicar el equipo de seguridad en el cual se realizará la auditoria.
- Validar los parámetros ingresados para realizar la auditoria.
- Realizar la conexión entre el sistema auditor y los diferentes equipos de seguridad.

En la práctica, todo sistema que maneje información de una organización debe de manejar estándares de seguridad.

1.2 Metodología

La metodología por seguir en la presente tesis se basa en el análisis del estado de configuración de los equipos de seguridad en una organización y su análisis según los lineamientos establecidos. Luego de ello se creará un sistema capaz de realizar validaciones de manera automática a solicitud del usuario. El sistema será capaz de realizar las siguientes acciones:

- Escaneo de máquinas registradas en el directorio activo.
- Escaneo de usuarios y sus respectivas configuraciones en el directorio activo.
- Escaneo de grupos de usuarios y sus respectivas configuraciones en el directorio activo.
- Escaneo de políticas de configuración base del directorio activo.
- Escaneo de políticas de seguridad en el firewall.
- Escaneo de configuración base en el firewall.
- Auditoria del directorio activo en base a los escaneos realizados y alineados a las mejores prácticas de Microsoft. [2]
- Auditoria del firewall en base a los escaneos realizados y alineados a las mejores prácticas de Palo Alto Networks. [3]

1.3 Descripción de la problemática

Las auditorías de seguridad informática, aplicadas a los diferentes tipos de organizaciones, han intentado mejorar las prácticas en cuanto al manejo de la información, integridad, privacidad y disponibilidad. [4]

La base fundamental de las auditorías son normas y/o estándares de seguridad establecidas por organizaciones internacionales encargadas de facilitar el intercambio seguro de información y promover el desarrollo de la estandarización de la información, una de las más aplicadas es la norma ISO[1].

A pesar de que una organización realice el proceso de auditoría de seguridad muchas veces el control y seguimiento de las actividades necesarias para mantener en el tiempo los niveles de seguridad requeridos, se vuelven tediosos con respecto a los sistemas de seguridad y redes.

[1] ISO: International Organization for Standardization

Por consiguiente, de manera manual se debe de revalidar si la configuración de los equipos de seguridad aún cumple con los estándares de seguridad establecidos en el "Plan General de Seguridad de la Información", dicho proceso se suele volver más complejo según el tamaño de la organización. Como se puede observar en la Figura 1, existe una tendencia a nivel mundial en cuanto a las certificaciones internacionales, para este caso puntual nos referimos a la ISO 27001, ello debido al gran interés, y a la vez preocupación, que existe en el ámbito de la seguridad de la información.

Figura 1 - Certificados ISO 27001 expedidos a nivel mundial
Fuente: Organización Internacional de Normalización (ISO)

1.4 Antecedentes

En la actualidad existen diferentes herramientas de software que son utilizadas para analizar la seguridad técnica de los sistemas informáticos.

La herramienta llamada ***CLARA*** es un software que ha sido diseñado para funcionar exclusivamente en sistemas operativos Microsoft Windows. El análisis del cumplimiento de normas está basado en las plantillas de seguridad de las Guías CCN-STIC 850A, 850B, 851, 851B, 870A, 870B, 899A y 899B aplicadas a España. [5]

Otra de las herramientas actuales es el sistema ***AD Audit Tools***, el cual permite a los administradores de Microsoft Active Directory (AD) estar al tanto de la información de acceso compartido de archivos de los usuarios del dominio, así como también, realizar un seguimiento de la actividad de cualquier usuario y ver la duración de inicio de sesión; todo lo anterior mencionado se encuentra relacionado solo al Directorio Activo. [6]

Una de las herramientas que ha ido creciendo en cuando a compatibilidad de equipos de terceros es la solución de ***Manage Engine***, esta herramienta es capaz de integrarse con el

directorio activo y con firewalls mediante API y LDAP. El servicio que se brinda requiere de una suscripción anual por equipo de seguridad y se maneja mediante consolas separadas. [9]

Existen algunas empresas que manejan sistemas propios de auditoría, por ejemplo, ***Ralco Networks***, la cual ofrece a sus clientes el servicio de análisis y auditoría de redes LAN/WAN. Cabe indicar que se realiza la revisión de la infraestructura lógica y física, posibles problemas, rendimiento y utilización de la red. Dicha auditoría se basa en buenas prácticas que la empresa ha recolectado en el tiempo. [7]

Finalmente, el ente encargado de brindar las normas y/o estándares, la Organización Internacional de Normalización (ISO), también ofrece una herramienta llamada ***ISO Tools*** la cual identifica las vulnerabilidades y amenazas de los procesos y activos de una organización mediante una matriz de riesgo. Asimismo, permite gestionar de forma ágil todos los controles necesarios, los cuales fueron identificados previamente y posterior a ello aplicados a los documentos sensibles de toda empresa. [8]

Podemos evidenciar que existen sistemas que realizan la validación de una parte de la auditoría la cual apunta a los documentos sensibles y al correcto control de éstos. En otros casos se realiza una auditoría parcial sobre los equipos de redes. La única solución que se asemeja a los objetivos de la presente tesis es ***Manage Engine***, sin embargo, esta solución cuenta con un licenciamiento por equipo y con una consola de administración por tipo de solución. Un crecimiento en la red corporativa implicaría aumentar los costos asociados a esta herramienta.

Tabla 1 - Comparativo entre soluciones actuales de auditoria
Fuente: Elaboración propia

	AUDITORIA		COSTOS		CONEXION VIA LDAP Y API		CANTIDAD DE EQUIPOS		OTROS	
	Directorio Activo	Firewall	Directorio Activo	Firewall	Directorio Activo	Firewall	Directorio Activo	Firewall	VERSION GRATUITA	NUMERO DE USUARIOS
CLARA	SI	X	X	X	SI	X	ILIMITADO	X	SI	ILIMITADO
AD AUDIT TOOLS	SI	X	$ 1776	X	SI	X	30	X	SI (30 días)	ILIMITADO
ISO TOOLS	X	X	X	X	X	X	1	X	NO	ILIMITADO
MANAGE ENGINE	SI	SI	$ 595	$ 595	SI	SI	1	1	SI (30 días)	2 USUARIOS
SOFTWARE DE AUDITORIA	SI	SI	X	X	SI	SI	ILIMITADO	ILIMITADO	SI	ILIMITADO

1.5 Seguridad Informática

Es la protección de los sistemas informáticos contra el robo o daño del hardware, software o datos electrónicos, así como de la interrupción o mala dirección de los servicios que prestan. Debido a lo antes mencionado existen una serie de protocolos, métodos, reglas, dispositivos y

herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información y/o infraestructura de una organización.

1.5.1 Seguridad Activa y Pasiva

La seguridad activa son todas las medidas que se utilizan diariamente para prevenir cualquier tipo de ataque en un sistema. En caso de detectar alguna amenaza se debe de generar los mecanismos adecuados para evitar el problema. [18]

Algunas consideraciones dentro de una organización son:

- Tener un antivirus actualizado.
- Realizar copias de seguridad.
- Emplear contraseñas seguras.

Por otro lado, la seguridad pasiva comprende todo el conjunto de medidas utilizadas para que una vez que se produzca el ataque o el fallo de seguridad de nuestro sistema se pueda minimizar al máximo los daños causados por el usuario, un accidente o un malware residente en los sistemas. [18]

Algunas prácticas por considerar son:

- Aislar la máquina de la red hasta que se esclarezca la causa raíz del problema.
- Usar hardware adecuado contra accidentes.
- Escanear el sistema completamente.

1.5.2 Seguridad Física y Lógica

La seguridad física se utiliza para proteger un sistema informático mediante procedimientos de control y barreras físicas. Tener controlado el ambiente y acceso físico permite disminuir siniestros y tener los medios para luchar contra accidentes. [18]

Las principales amenazas que se prevén son:

- Desastres naturales, incendios accidentales y cualquier variación producida por las condiciones ambientales.
- Amenazas ocasionadas por el hombre como robos o sabotajes.

La seguridad lógica se encarga de asegurar la parte software de un sistema informático, mediante la aplicación de barreras y procedimientos que protejan el acceso a los datos y a la información contenida en él. [18]

La seguridad lógica trata de conseguir los siguientes objetivos:

- Restringir el acceso a los sistemas informáticos y archivos autorizados, ya sea dentro del sistema informático, como desde fuera, es decir, desde una VPN (Virtual Private Network).
- Asegurar que se estén utilizando los datos, archivos y programas siguiendo los procedimientos correctos.
- Verificar que se mantenga la integridad de la información a través del canal de comunicación entre un emisor y receptor.
- Disponer de pasos alternativos de emergencia para la transmisión de información.

1.5.3 Tipos de amenaza

a) Enmascaramiento

El ataque de enmascaramiento tiene lugar cuando un equipo pretende ser un equipo diferente. Un ataque de enmascaramiento es uno de los tipos de ataques más activos.

b) Modificación de mensajes

Significa que alguna parte de un mensaje se modifica o que el mensaje se retrasa o se reordena para producir un efecto no autorizado. Por ejemplo, un mensaje que significa "Permitir que Jorge lea el archivo confidencial Y" se modifica como "Permitir que Alex lea el archivo confidencial Y".

c) Repudio

Este ataque es realizado por el remitente o el receptor. Por ejemplo, el cliente le pide a su banco "transferir una cantidad a alguien" y luego el remitente (cliente) niega haber realizado dicha solicitud.

d) Repetir

Implica la captura pasiva de un mensaje y su posterior transmisión para producir un efecto autorizado.

e) **Denegación de Servicio**

Previene el uso normal de las instalaciones de comunicación. Este ataque puede tener un objetivo específico. Por ejemplo, una entidad puede suprimir todos los mensajes dirigidos a un destino en particular. Otra forma de denegación de servicio es la interrupción de una red completa al desactivar la red o sobrecargarla con mensajes para degradar el rendimiento.

1.6 Equipos involucrados en las auditorías

1.6.1 Firewall

Los firewalls se utilizan para proteger las redes domésticas y corporativas. Un cortafuegos (firewall) es un dispositivo que realiza un filtrado de paquetes de datos a partir de unas reglas definidas por el administrador de la red, teniendo en cuenta las direcciones IP fuente o destino. [7]

Los firewalls de última generación contienen módulos API[2] embebidos los cuales permiten obtener información del equipo de manera segura mediante comandos predefinidos y dicha información es entregada en formato XML.

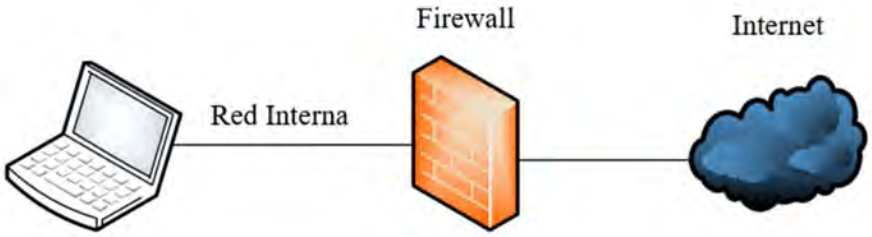


Figura 2 - Esquema de trabajo de un firewall
Fuente: Elaboración propia

Existen varios tipos de técnicas de firewall que evitarán que la información potencialmente dañina se transmita:

a) **Filtrado de paquetes:** analiza los paquetes entrantes/salientes de la red y los acepta o rechaza según las reglas configuradas por los administradores de dicho equipo. El filtrado de paquetes es transparente para los usuarios.

[2] application programming interface

b) **Puerta de enlace a aplicaciones:** aplica mecanismos de seguridad a aplicaciones específicas, tales como ftp y telnet. Esta configuración es muy efectiva, pero puede mermar el rendimiento del equipo.

c) **Puerta de enlace de nivel de circuito:** aplica mecanismos de seguridad cuando una conexión TCP o UDP se establece. Una vez que se ha realizado la conexión, los paquetes pueden fluir entre los hosts sin necesidad de comprobaciones adicionales.

d) **Servidor proxy:** intercepta todos los mensajes que entran y salen de la red. El servidor proxy oculta las verdaderas direcciones de red y solo muestra la IP configurada en la regla NAT.

1.6.2 Directorio Activo (AD)

El servicio de directorio activo es una base de datos distribuida que permite almacenar información relativa a los recursos de una red con el fin de facilitar su localización y administración. Dicho sistema se compone del propio servicio de directorio junto con un servicio secundario que permite el acceso a la base de datos y admite las convenciones de denominación X.500.

Los servicios de directorio también ofrecen la ventaja de suponer un único punto de entrada para los usuarios a la red de toda la empresa. Los usuarios pueden buscar y usar recursos en la red sin conocer el nombre o la ubicación exactos del recurso. Igualmente, puede administrar toda la red con una vista lógica y unificada de la organización de la red y de sus recursos [10].

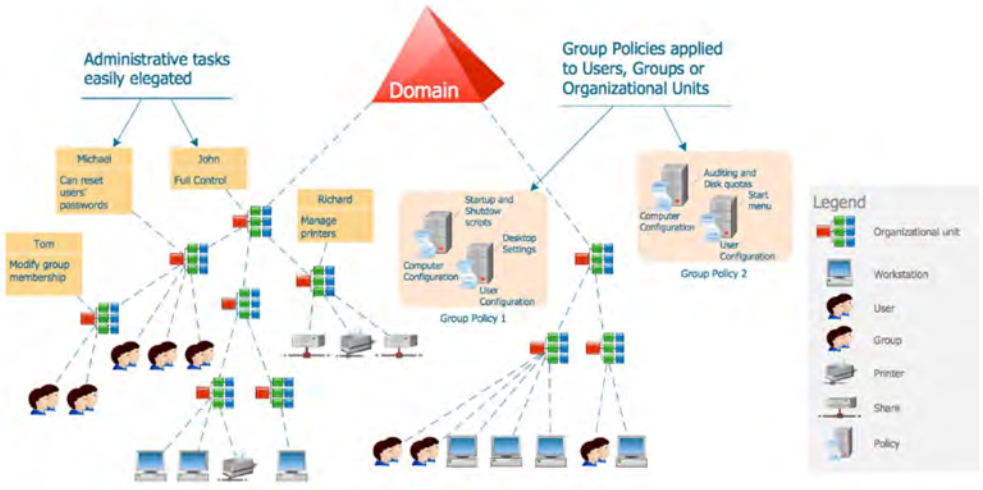


Figura 3 – Esquema de Trabajo del Directorio Activo
Fuente: Concept Draw [14]

La configuración de cada usuario se encuentra almacenada en el atributo *userAccountControl* el cual nos permitirá obtener toda la información relacionada a los usuarios y/o máquinas.

Tabla 2 - Valores de los parámetros del userAccountControl
Fuente: Active Directory Administration Cookbook (2019) [18]

Name	Value	Value	Value	Description
SCRIPT	1	2^0	0x00000001	A log-on script is executed.
ACCOUNTDISABLE	2	2^1	0x00000002	The account is disabled.
HOMEDIR_REQUIRED	8	2^3	0x00000008	A home folder is required.
LOCKOUT	16	2^4	0x00000010	
PASSWD_NOTREQD	32	2^5	0x00000020	A password is not required.
PASSWD_CANT_CHANGE	64	2^6	0x00000040	The user cannot change the password.
ENCRYPTED_TEXT_PWD_ALLOWED	128	2^7	0x00000080	Store password using reversible encryption.
TEMP_DUPLICATE_ACCOUNT	256	2^8	0x00000100	This is an account for users whose primary account is in another domain.
NORMAL_ACCOUNT	512	2^9	0x00000200	This is a normal, enabled user account.
INTERDOMAIN_TRUST_ACCOUNT	2048	2^{11}	0x00000800	This is a permit to trust an account for a system domain that trusts other domains.
WORKSTATION_TRUST_ACCOUNT	4096	2^{12}	0x00001000	This is a normal computer account.
SERVER_TRUST_ACCOUNT	8192	2^{13}	0x00002000	This is a computer account for a domain controller.
DONT_EXPIRE_PASSWORD	65536	2^{16}	0x00010000	The password will not expire.
MNS_LOGON_ACCOUNT	131072	2^{17}	0x00020000	This is the **Majority Node Set (MNS)** logon account, used for clustering.
SMARTCARD_REQUIRED	262144	2^{18}	0x00040000	The user is forced to use a smartcard.

Name	Value	Value	Value	Description
TRUSTED_FOR_DELEGATION	524288	2^{19}	0x00080000	The service account is trusted for Kerberos delegation.
NOT_DELEGATED	1048576	2^{20}	0x00100000	The user will not be delegated to a service even if the service account is set as trusted for Kerberos delegation.
USES_DES_KEY_ONLY	2097152	2^{21}	0x00200000	The user uses only **Data Encryption Standard (DES)** encryption.
DONT_REQ_PREAUTH	4194304	2^{22}	0x00400000	The user does not require Kerberos pre-authentication for log-on.
PASSWORD_EXPIRED	8388608	2^{23}	0x00800000	The user's password has expired.
TRUSTED_TO_AUTH_FOR_DELEGATION	16777216	2^{24}	0x01000000	The account is enabled for delegation.
PARTIAL_SECRETS_ACCOUNT	67108864	2^{26}	0x04000000	The account is a **Read-only Domain Controller (RODC)**.

1.6.3 Routers

Un router o enrutador es un dispositivo físico o virtual que transmite información entre dos o más redes, este equipo analiza la dirección IP destino de un paquete de datos determinado, calcula la mejor manera de que llegue a ese destino y luego lo reenvía a donde corresponde.

Los routers tradicionales son dispositivos informáticos independientes compuestos por software propietario cargado en un hardware dedicado. Un enrutador virtual es una instancia de software que realiza las mismas funciones que un enrutador físico, mientras se ejecuta en un equipo de caja blanca.

1.7 Lenguajes de programación

1.7.1 Python

Python es un lenguaje de programación orientado a objetos interpretado que permite a los programadores usar diferentes estilos de programación para crear programas simples o complejos. Algunos de los sistemas y aplicaciones populares que han empleado Python durante el desarrollo incluyen Google Search, YouTube, BitTorrent, Google App Engine, Eve Online, Maya e iRobot.

Cabe mencionar que hay dos atributos que hacen que el tiempo de desarrollo en Python sea más rápido que en otros lenguajes de programación:

1. Python excluye la necesidad de compilar código antes de ejecutar un programa ya que la compilación se realiza en segundo plano. Debido a que Python es un lenguaje de programación de alto nivel, abstrae muchos detalles sofisticados del código de programación.

2. El código de Python tiende a ser más corto que en otros lenguajes de programación. Aunque Python ofrece tiempos de desarrollo rápidos, se retrasa ligeramente en términos de tiempo de ejecución.

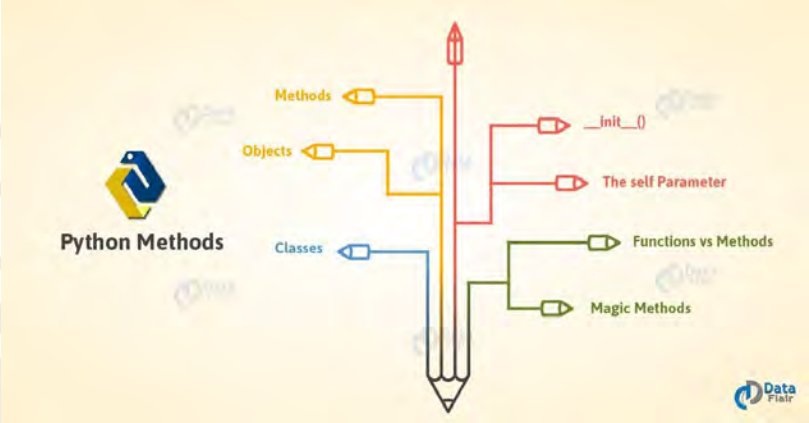


Figura 4 - Método de trabajo utilizando Python
Fuente: Data-Flair [20]

1.7.2 Java

Java es un lenguaje de programación que produce software para múltiples plataformas y que nació en 1975. Cuando un programador escribe una aplicación Java, el código compilado (conocido como bytecode) se ejecuta en la mayoría de los sistemas operativos (SO), incluidos Windows, Linux y Mac OS. Java deriva gran parte de su sintaxis de los lenguajes de programación C y C++.

El desarrollo del programa Java requiere un kit de desarrollo de software Java (SDK) que generalmente incluye un compilador, un intérprete, un generador de documentación y otras herramientas utilizadas para producir una aplicación completa.

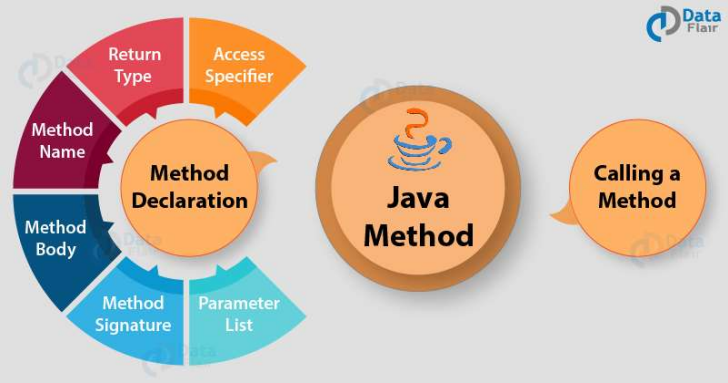


Figura 5 - Lenguaje de programación Java, basado en métodos
Fuente: Data-Flair [20]

1.7.3 Visual Basic. NET

Visual Basic .NET (VB.NET) es una versión de Visual Basic de Microsoft que fue diseñada, como parte del grupo de productos .NET de la compañía, para facilitar el desarrollo de aplicaciones de servicios web. Según Microsoft, VB .NET fue rediseñado, en lugar de lanzarse como VB 6.0 con características adicionales, para facilitar la realización de cambios fundamentales en el lenguaje. VB.NET es la primera versión de programación completamente orientada a objetos (OOP) de Visual Basic y, como tal, admite conceptos de OOP como abstracción, herencia, polimorfismo y agregación.

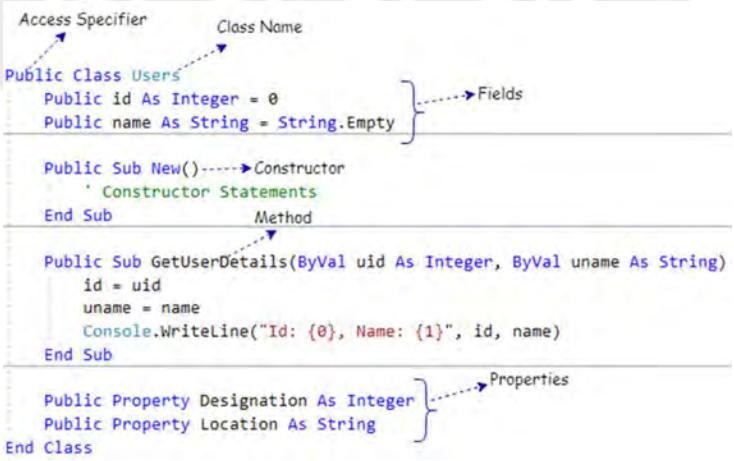


Figura 6 - Lenguaje Visual Basic, basado en clases
Fuente: Tutlane Services [15]

1.8 Técnicas de conexión

Existen diferentes tipos de conexión para poder obtener información relevante de los equipos de seguridad, se debe de tener en cuenta que algunas proporcionan mayor seguridad en la conexión que otras.

1.8.1 TELNET

De acuerdo con la Internet Engineering Task Force (IETF) la finalidad principal de este protocolo es proporcionar una instalación de comunicaciones orientada a bytes de ocho bits bastante general, bidireccional. Su objetivo principal es permitir un método estándar de interfaz de dispositivos terminales y procesos orientados a terminales entre sí. [13]

Cabe mencionar que este protocolo utiliza el puerto TCP/23, una de las principales desventajas de este protocolo es él envió del usuario y la clave, el cual se trasmite en texto plano, es decir, no es encriptada. Ello podría generar una brecha de seguridad abierta ante cualquier atacante.

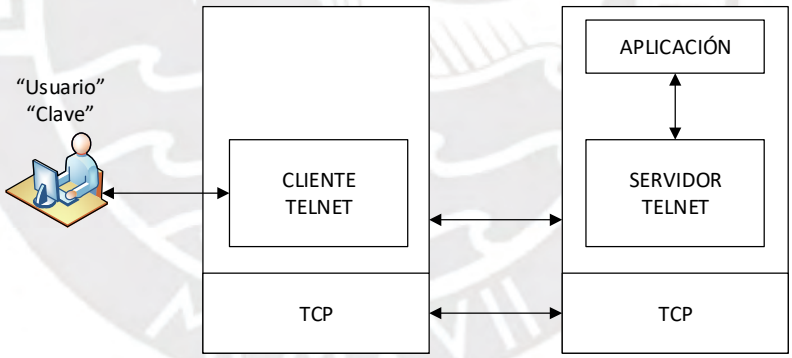


Figura 7 - Esquema de conexión para el protocolo Telnet
Fuente: Elaboración propia

1.8.2 Secure Socket Shell (SSH)

SSH es un protocolo de red que trabaja bajo el mismo esquema que el protocolo telnet, sin embargo, cabe indicar que este protocolo brinda una forma segura de conexión. Mediante el puerto TCP/22 este protocolo basa su modelo en pares de claves públicas para poder autenticar el cliente y el servidor entre sí. Toda comunicación requiere un

par de claves públicas para autenticar la máquina remota en la máquina local y un segundo par de claves públicas para autenticar la máquina local en la máquina remota.

1.8.3 Application Programming Interface (API)

API es un conjunto de definiciones y herramientas para crear aplicaciones de software. Las APIs se utilizan al programar componentes de la interfaz gráfica de usuario (GUI). La principal ventaja de las APIs es la simplificación al momento de interactuar con un sistema, ya que permite realizar acciones de manera sencilla mediante comando predefinidos. Existen 4 tipos de APIs:

- **APIs abiertas:** se encuentran disponibles de manera pública y no hay restricciones para acceder a ellas.
- **APIs de socios:** requieren derechos o licencias específicos para acceder a ellas.
- **APIs internas:** destinadas para su uso dentro de una empresa, sea puede usar este tipo de APIs en diferentes equipos internos para poder mejorar los servicios.
- **APIs compuestas:** combinan diferentes datos y APIs de servicio. El objetivo principal de este tipo de API es acelerar el proceso de ejecución y mejorar el rendimiento de las interfaces web.

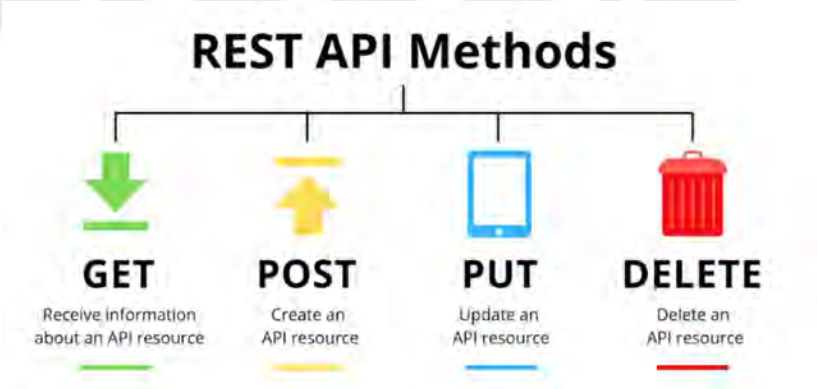


Figura 8 - Métodos de conexión vía API
Fuente: Arcadier [21]

1.8.4 Lightweight Directory Access Protocol (LDAP)

LDAP es un protocolo que permite obtener datos sobre organizaciones, individuos y otros recursos, como archivos y dispositivos en una red, ya sea en Internet o en una intranet corporativa. LDAP se usa en Active Directory de Microsoft, pero también se puede usar en otras herramientas como Open LDAP, Red Hat Directory Servers, etc. Cabe indicar que con LDAP también se puede autenticar, vincular sesiones, eliminar entradas, buscar y comparar entradas usando diferentes comandos, modificar entradas existentes, extender entradas, abandonar solicitudes y/o desvincular operaciones.

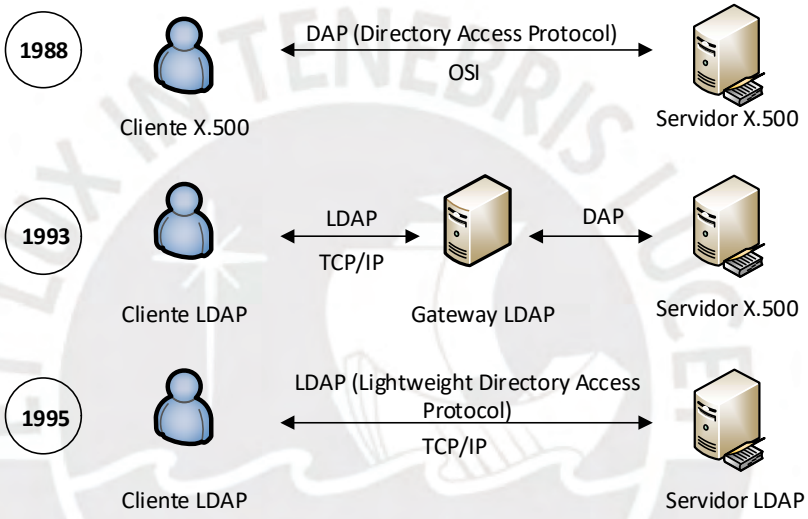


Figura 9 - Evolución del protocolo LDAP
Fuente: Elaboración propia

CAPÍTULO 2: AUDITORIA DE LA SEGURIDAD

2.1 Auditoría

En la actualidad las organizaciones a nivel mundial respaldan sus negocios en sistemas informáticos que manejan información sensible de las empresas, así como la información necesaria para asegurar las operaciones diarias. Con la finalidad de gestionar dicha información de manera correcta se crearon 3 pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad. Es por ello, que cada empresa implementa dentro de su red interna diferentes equipos de seguridad los cuales restringen el acceso a los datos y solo permite su visibilidad al personal autorizado.

Con la finalidad de asegurar que los equipos de seguridad y las configuraciones realizadas sobre los mismos vayan acorde con las normas y/o procedimientos establecidos por la empresa es que se requiere realizar procedimientos de auditoría.

La *American Accounting Association* (AAA) define el concepto de auditoría como "un proceso sistemático de obtención y evaluación objetiva de evidencia con respecto a afirmaciones sobre acciones y eventos económicos para determinar el grado de correspondencia entre esas afirmaciones y criterios establecidos y comunicar los resultados a los usuarios interesados". [11]

2.2 Tipos de Auditoria

Las auditorías se clasifican de dos formas, auditoría externa y auditoría interna.

2.2.1 Auditoría Externa

La auditoría externa es un examen realizado por un personal independiente, el cual se encuentra en facultad de mediante diferentes tipos de técnicas, métodos y/o herramientas realizar el proceso de auditoría. Este tipo de auditoría está destinado comúnmente a dar como resultado una certificación luego de finalizado el proceso y subsanadas las posibles observaciones del informe final.

2.2.2 Auditoría Interna

La auditoría interna se refiere al área ubicada dentro de una empresa que monitorea la eficacia de sus procesos y controles. La función de auditoría interna es necesaria en organizaciones con altos niveles de complejidad de procesos, donde es más fácil que se generen brechas de seguridad y violaciones de control. El personal de auditoría interna es responsable de lo siguiente:

- ✓ Detección de fraude
- ✓ Evaluaciones de control interno
- ✓ Cumplimiento legal y regulatorio
- ✓ Evaluaciones de procesos
- ✓ Evaluaciones de riesgo

2.3 Fases de una auditoría

Cada servicio de auditoría consta de las siguientes fases:

2.3.1 Definir el alcance de la auditoría

La primera fase es definir el alcance de la auditoría, para ello se deben listar todos los activos de la empresa. Los activos hacen referencia a los equipos informáticos y/o datos confidenciales del cliente. Una vez que se tenga completa la lista de activos de la empresa, se debe delimitar el alcance de la auditoría, para ello se definirá que activos se auditarán y cuáles no. No es recomendable tratar de auditar todos los activos en un solo proyecto.

2.3.2 Definir las amenazas

Una vez completado el listado de activos se debe de enumerar las posibles amenazas a las que pueden verse afectados, las cuales pueden variar desde contraseñas deficientes de los empleados hasta ataques DDoS e incluso daños causados por un desastre natural. Se debe considerar cualquier amenaza potencial, siempre que la amenaza pueda costar al negocio la reducción parcial o total de sus actividades.

Algunas de las principales amenazas a considerar son las siguientes:

- **Trabajadores negligentes:** dentro de una empresa se debe de considerar: ¿qué tan bien capacitados están los trabajadores para notar actividades sospechosas (spam, phishing, etc.) y seguir los protocolos de seguridad establecidos por su área de seguridad informática? ¿Los trabajadores utilizan las mismas claves de sus cuentas personales en sistemas corporativos?
- **Ataques de phishing:** los atacantes están recurriendo cada vez más a estafas de phishing para obtener acceso a información confidencial. Según el reporte anual "State of the Phish" elaborado por la empresa Proofpoint se ha detectado que el robo de credenciales se incrementó en más del 70% desde el 2017 para este tipo de ataques (2019). En la *Figura 9* se puede observar la información que brindo la población de estudio sobre el impacto ocurrido luego de haber sido víctima de phishing. [12]

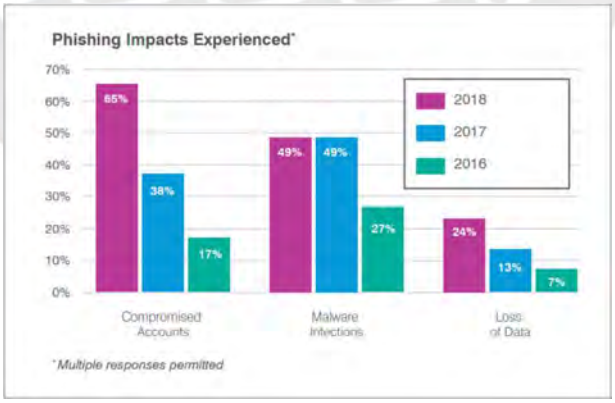


Figura 10 – Porcentaje anual de impacto experimentado al ser víctima de phishing
Fuente: https://www.wombatsecurity.com/state-of-the-phish [12]

- **Contraseñas deficientes:** las contraseñas débiles o robadas son el método # 1 utilizado por los perpetradores.

- **Atacantes internos:** es importante tener en cuenta que es posible que exista alguien dentro de la empresa, o que un tercero que tenga acceso a datos de la compañía, que robe o use indebidamente información confidencial.
- **Ataques DDoS:** un ataque de denegación de servicio distribuido (DDoS) es lo que sucede cuando varias máquinas inundan un sistema objetivo (por lo general un servidor web) y lo sobrecargan, lo que lo vuelve inútil.
- **BYOD (Traiga su propio dispositivo):** cuando una empresa permite que los usuarios trabajen con sus propios dispositivos se debe de tener en cuenta que la superficie de ataque para los perpetradores es más grande y débil.
- **Malware:** representa varias amenazas diferentes, como gusanos, troyanos, spyware e incluye una amenaza que ha incrementado su popularidad en los últimos años: ransomware.
- **Desastres naturales:** aunque es poco probable, las consecuencias pueden ser muy costosas.

2.3.3 Evaluar el rendimiento la seguridad actual

Con la lista de amenazas lista, se debe evaluar al interno la capacidad de reacción ante los eventos listados. Cabe mencionar que se evaluará el rendimiento actual de las estructuras de seguridad y de los procedimientos internos. Para esta fase la intervención de una auditoría externa proporciona un valor adicional, ya que garantiza que la evaluación pueda ser completamente objetiva y que no se vean afectados los resultados de la auditoría.

2.3.4 Priorización (puntuación de riesgos)

Se debe de tomar la lista de amenazas y evaluar el daño potencial de la ocurrencia de alguna amenaza versus las posibilidades de que realmente pueda ocurrir (asignando una puntuación de riesgo a cada una). Por ejemplo, un desastre natural puede destruir una empresa (puntaje de riesgo alto), pero si los activos existen en un lugar que nunca se ha visto afectado por una catástrofe natural, el puntaje de riesgo debe reducirse.

2.3.5 Formular soluciones de seguridad

El paso final de la auditoría de seguridad es escribir una lista correspondiente de mejoras de seguridad o mejores prácticas para eliminar las amenazas.

Algunas soluciones de seguridad comunes son:

- **Concienciación sobre la educación de los empleados:** los trabajadores son el eslabón más débil en la seguridad de la información, por tal motivo se debe capacitar a los nuevos empleados y actualizar constantemente la información relacionada a las políticas y procedimientos de seguridad para los trabajadores ya existentes, todo ello con el fin de crear conciencia sobre las mejores prácticas de seguridad.
- **Protección del correo electrónico:** los filtros de spam ayudan, sin embargo, crear un identificador sobre los correos electrónicos y que se puedan clasificar como "internos" o "externos" es muy valioso para que el usuario pueda estar alerta ante correos externos.
- **Seguridad de contraseñas y gestión de acceso:** las contraseñas son complicadas porque deben ser complejas y exclusivas para cada cuenta. Es por ello, que los trabajadores tienden a reutilizar las claves y almacenarlas en documentos o blocks de notas sin protección. Se recomienda invertir en un administrador de contraseñas, ello permite habilitar el intercambio seguro de contraseñas. Cabe recordar que la autenticación de dos factores es una capa adicional de seguridad muy útil para confirmar la identidad del personal encargado.
- **Monitoreo de red:** los atacantes externos a menudo intentan obtener acceso a la red de una empresa. Es por ello, que un software de monitoreo de red puede ayudar en la alerta sobre cualquier actividad inusual, tales como intentos de acceso desconocidos. Algunos sistemas ofrecen protección las 24 horas del día, los 7 días de la semana y utilizan inteligencia artificial para correlacionar eventos y ayudar a identificar los delitos cibernéticos antes de que ocurran.
- **Copia de seguridad:** es altamente recomendado que cada empresa realice una copia de seguridad de sus datos de manera constante y a su vez se asegure de que los datos se ubiquen un lugar seguros y separados en caso de un ataque de malware o un ataque físico a sus servidores principales. La identificación de la criticidad y ubicación de los datos es fundamental como parte de este proceso.
- **Actualizaciones de software:** mantener todos los equipos de la red con el último software estable es mandatorio para asegurar los puntos de acceso. Se recomienda obtener sistemas que gestionen la actualización constante de los diferentes sistemas de la red.

2.4 Estándares Internacionales

Existen varias entidades internacionales relacionadas a sistemas de información tales como ISO, ISACA, CISA, CISM, etc., las cuales brindan conceptos generales sobre como preservar la confidencialidad, integridad, disponibilidad de la información entre otras.

Los sistemas de la información son un conjunto de componentes interrelacionados que reúnen, procesan, almacenan y distribuyen datos e información y proporcionan un mecanismo de retroalimentación con el fin de cumplir un objetivo. [22]

Otro término relacionado con la seguridad de la información son los mismos activos de la información, los cuales son bienes o servicios los cuales procesan o almacenan información.

El activo de información también se puede definir como algo a lo que una organización directamente le asigna un valor y, por lo tanto, la organización debe proteger. [22]

A todos los activos de la información identificados en una organización se les asigna un valor según su criticidad dentro de la operación del negocio y con ello se puede elaborar un plan de acción a ejecutar.

2.4.1 ISO 27001

La ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos de la información, así como de los sistemas que la procesan. [23]

Según lo indicado en el punto anterior, justamente eso es lo que busca este sistema de auditoria, brindar visibilidad al usuario sobre si la configuración de los equipos de seguridad cumple o no con los criterios que aseguren que el tratamiento de la información se dará de manera segura.

Figura 11 - Estructura de la ISO 27001
Fuente: ADVISERA [24]

2.4.2 ISO 27037

La norma ISO 27037 se encuentra orientada al procedimiento de la actuación pericial en el escenario de la recogida, identificación y secuestro de la evidencia digital y no entra en la fase de Análisis de la evidencia. [25]

Cabe indicar que la norma mencionada comprende la auditoria de los equipos que se encuentran por detrás de los equipos que analizaremos (firewalls y directorio activo) como se puede observar en la *figura 12* el procedimiento es focalizado hacia eventos determinados una vez ocurridos. El análisis antes mencionado no se encuentra dentro del alcance de la presente tesis.

Figura 12 - Etapas del procedimiento de actuación ISO/IEC 27037
Fuente: Peritoit [25]

2.4.3 ISO 27042

La norma ISO 27042 proporciona orientación sobre el análisis e interpretación de la evidencia digital de una manera que aborda los problemas de continuidad, validez, reproducibilidad y repetibilidad. [26]

Si bien la intención del software realizado en la presente tesis es la de recopilar información de los equipos de seguridad y realizar un análisis posterior, no se genera

una evidencia digital, solo se emiten reportes en base a las buenas prácticas de configuración de los equipos de seguridad.

Finalmente, cabe mencionar, que tanto la norma ISO 27037 como la norma ISO 2742 forman parte de la preservación de evidencia digital, lo cual no se encuentra presente dentro del alcance de la presente tesis.

Figura 13 - Relación entre ISO 27037 e ISO 27042
Fuente: ISO [26]

CAPÍTULO 3: PLANTEAMIENTO DE PROPUESTA DE SOLUCIÓN

3.1 Problemática

Las empresas continuamente intentan reducir las brechas de seguridad y concientizar a sus empleados sobre los posibles riesgos que existen cuando se utilizan los diferentes sistemas corporativos. A medida que las empresas se expanden es necesario generar un área dedicada a la seguridad de la información, en muchos casos estas áreas buscan alinear sus procedimientos a las normas y estándares mencionados en el capítulo 2.

Para obtener una certificación internacional se debe de pasar por una auditoría interna, la cual es realizada por personal externo y que representa al ente internacional correspondiente. Luego de realizar la revisión de los procesos y validar el estado actual de los diferentes sistemas de seguridad, se procede a emitir un informe con las recomendaciones respectivas para subsanar cualquier brecha de seguridad o procedimiento deficiente.

Luego de realizada la auditoría las empresas por lo general obtienen sistemas que gestionan sus documentos internos (almacenamiento, gestión de cambios, etc.). Sin embargo, la

problemática surge con respecto a los sistemas de seguridad ya que al ser equipos en los cuales se realizan cambios constantemente no es sencillo gestionar los mismos, en virtud de ello, se requiere de un sistema que realice una auditoría interna a solicitud del usuario para que en cualquier momento pueda contar con un reporte actual de los sistemas.

3.2 Arquitectura Propuesta

Los activos considerados dentro de la presente tesis son los siguientes:

- Firewall Internos y/o Externos.
- Sistema de Directorio Activo.

Este proyecto de tesis consiste en desarrollar un sistema auditor de información el cual se encargará de realizar consultas al directorio activo mediante LDAP (Lightweight Directory Access Protocol) y a los firewalls mediante API (Application Programming Interface) con la finalidad de obtener los parámetros configurados en los equipos y con ello poder brindar una fotografía al momento de dichos equipos.

Como se puede observar en la *figura 14* el sistema auditor se encontrará en una de las zonas por detrás del firewall interno. Luego de configurar las reglas de acceso necesarias que permitan la comunicación mediante LDAP y API hacia los equipos antes mencionados, el sistema ya podrá funcionar correctamente. El análisis realizado por el recolector de información permitirá salvaguardar la red de servidores de posibles configuraciones erróneas dentro de los equipos de seguridad.

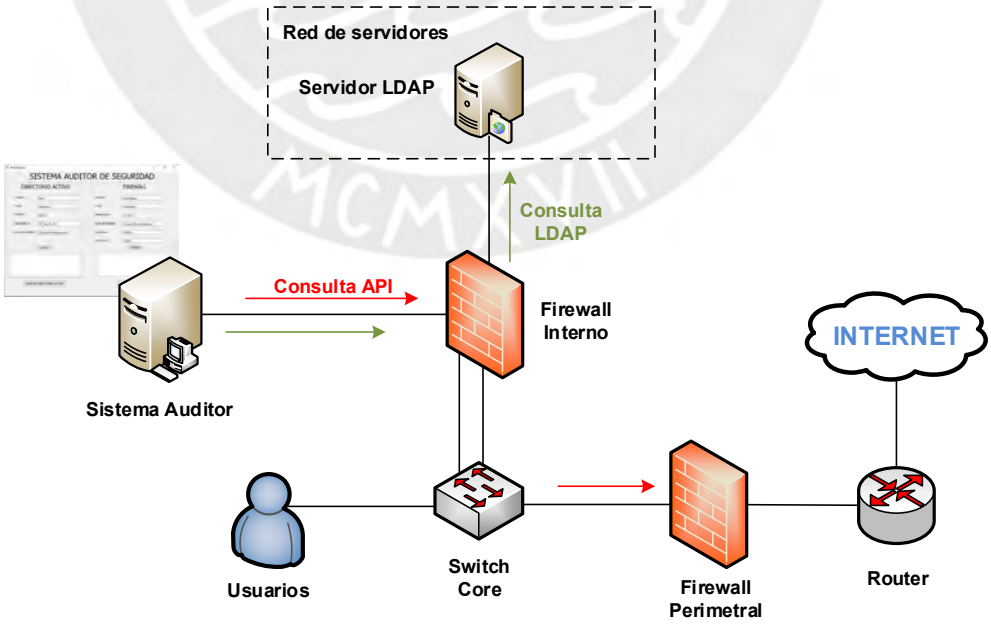


Figura 14 - Arquitectura de solución propuesta
Fuente: Elaboración propia

3.3 Herramientas y métodos

En este apartado se describirá el detalle de las herramientas, procedimientos y métodos que se utilizarán para esta tesis. En la tabla 3, se puede observar el detalle de lo indicado, así como el resultado esperado.

Tabla 3 - Resultados esperados y herramientas a utilizarse
Fuente: Elaboración propia

Resultados Esperados	Herramientas por utilizar
Realizar la conexión hacia el Directorio Activo (AD) mediante LDAP y obtener los siguientes parámetros: • Tiempo de inactividad de los usuarios • Fecha de último cambio de clave. • Fecha de último acceso de los usuarios. • Nombre, apellidos, fecha de caducidad, opción de cambio de clave de los usuarios. • Tiempo máximo de duración de la clave en el directorio activo. • Longitud mínima de la clave de los usuarios. • Listado de grupo de usuarios. • Cuentas de usuarios deshabilitadas. • Tiempo de cambio de clave de los usuarios.	• Lenguaje de programación Python. • Software Anaconda. • Pyqt designer • Google Chrome
Realizar la conexión hacia el firewall interno y/o perimetral mediante API y obtener los siguientes parámetros: • Nombre del equipo, dirección IP, fecha, hora, versión de sistema operativo actual, modelo, tiempo de encendido, número de serie, dirección MAC[3], versión de global protect, versión de filtro URL, versión de antivirus, versión de	• Lenguaje de programación Python. • Software Anaconda. • Google Chrome • Microsoft Excel • Pyqt designer

[3] Identificador de 48 bits asignado de forma única a un dispositivo de red

Resultados Esperados	Herramientas por utilizar
aplicaciones, versión de Wildfire, configuración DNS y NTP. • Archivo de configuración del equipo en formato XML. • Las políticas de seguridad configuradas en el equipo.	

3.4 Alcance, Limitaciones y Riesgos

3.4.1 Alcance

El proyecto de tesis se encargará de obtener toda la información en texto plano tanto del firewall como del Directorio Activo y plasmar dicha información en sus respectivas tablas, para luego realizar un análisis y posteriormente emitir un reporte de cumplimiento basado en la información obtenida.

Las validaciones por realizar serán las siguientes:

Directorio Activo

- Tiempo de inactividad del usuario dentro del dominio analizado.
- Fecha del último cambio de clave.
- Los usuarios deberán de contar con todos los parámetros correctamente configurados (nombre, apellidos, correo electrónico, fecha de caducidad, etc.) y la opción de cambio de clave.
- Tiempo máximo de cambio de clave en el servidor.
- Longitud mínima para establecer la clave de los usuarios.
- Las cuentas deshabilitadas y los grupos configurados.
- Tiempo de cambio de clave.

Firewall

- Políticas de seguridad en las cuales los puertos inseguros se encuentran habilitados.
- Existencia de políticas de seguridad configuradas con acceso *any* (origen/destino/zona/puertos/aplicación).

- Existencia de perfil de seguridad asociada a todas las políticas de seguridad.
- Existencia de políticas de seguridad sin reenvió de logs activo.
- Configuración de permisos para las interfaces de administración y de servicio.

3.4.2 Limitaciones

Las limitaciones en el desarrollo del proyecto de tesis son las siguientes:

- Se depende de las políticas de seguridad en el firewall interno para poder realizar la conexión mediante LDAP y API a los diferentes equipos involucrados en la red interna a la cual se aplicarán las pruebas.
- Se considerarán dos (2) tipos de categorías generales para las políticas de seguridad, políticas internas y externas.
- El tiempo de ejecución del código python puede variar según las características del hardware de la computadora en la que se ejecuta el sistema. Asimismo, el tiempo puede variar en base a la cantidad de políticas de seguridad que tenga configurado cada sistema.
- El sistema no propone una versión mejorada de las políticas de seguridad o de las configuraciones halladas, solo las puntúa en un porcentaje de acuerdo con su cumplimiento.
- Se requiere de un usuario administrador en ambas plataformas para poder realizar las consultas extendidas vía LDAP y las consultas vía API.

3.4.3 Riesgos

En la *tabla 4* se consideran los riesgos identificados, así como su impacto y control de mitigación.

Tabla 4 - Riesgos, impacto y control de mitigación
Fuente: Elaboración propia

Riesgo	Impacto en el proyecto	Control de mitigación
Pérdida del código desarrollado en Python	Se perderá el trabajo desarrollado	- El código se encuentra almacenado en una cuenta corporativa de OneDrive.
Indisponibilidad del asesor	No se podrá validar la información obtenida del sistema con el asesor	- Realizar reuniones virtuales mediante Zoom. - Mantener comunicación constante mediante el correo PUCP.
Obtener tiempos altos al momento de ejecutar el código	Podría afectar el desarrollo del sistema	- Configurar tiempo máximo de respuesta. - Permitir al sistema que extraiga la información a solicitud del usuario. - Realizar la programación mediante funciones independientes y no todo en un solo código.

3.5 Requerimientos del sistema

En la *tabla 5* se indican los requerimientos con los cuales debe de cumplir el sistema de auditoria.

Tabla 5 - Requerimientos funcionales para el directorio activo
Fuente: Elaboración propia

Referencia	Requerimiento funcional para el directorio activo
R 1.1	El sistema mostrará todos los usuarios del dominio solicitado con sus respectivas configuraciones (tiempo de inactividad, fecha de último cambio de clave, cuentas deshabilitadas, grupos configurados)

R 1.2	El sistema mostrará la configuración del servidor de dominio (tiempo máximo de cambio de clave, longitud mínima de las claves)
Referencia	**Requerimiento funcional para el directorio activo**
R 1.3	El sistema mostrará las características básicas de los equipos (nombre, IP, sistema operativo).
R 1.4	El sistema mostrará la información completa de los usuarios (nombre, apellidos, grupos asignados, fecha de creación, fecha de modificación, ultimo inicio de sesión, etiquetas de configuración y descripción).
R 1.5	El sistema será implementado en Python utilizando el framework Anaconda.
R 1.6	La interfaz gráfica del sistema se realizara mediante el programa pyqt designer.
R 1.7	El sistema emitirá un reporte basado en la información obtenida y en las buenas prácticas de configuración recomendadas por Microsoft.

Tabla 6 - Requerimientos funcionales para el Firewall
Fuente: Elaboración propia

Referencia	**Requerimiento funcional para el firewall**
R 2.1	El sistema mostrará todas las reglas de seguridad configuradas en el equipo.
R 2.2	El sistema mostrará el nombre del equipo, dirección IP, fecha, hora, versión de sistema operativo actual, modelo, tiempo de encendido, número de serie, dirección MAC, versión de global protect, versión de filtro URL, versión de antivirus, versión de aplicaciones, versión de Wildfire, configuración DNS y NTP.
R 2.3	El sistema mostrará todos los perfiles de seguridad asociados a las políticas de seguridad
R 2.4	El sistema mostrará la configuración de las interfaces de administración y de servicio
R 2.5	El sistema alertara sobre las políticas configuradas con acceso *any* ya sea origen/destino/zona/puertos/aplicación.
R 2.7	El sistema será implementado en Python utilizando el framework Anaconda.
R 2.8	La interfaz gráfica del sistema se realizara mediante el programa pyqt designer.
R 2.9	El sistema emitirá un reporte basado en la información obtenida y en las buenas prácticas de configuración recomendadas por Palo Alto Networks.

3.6 Interfaz gráfica del sistema

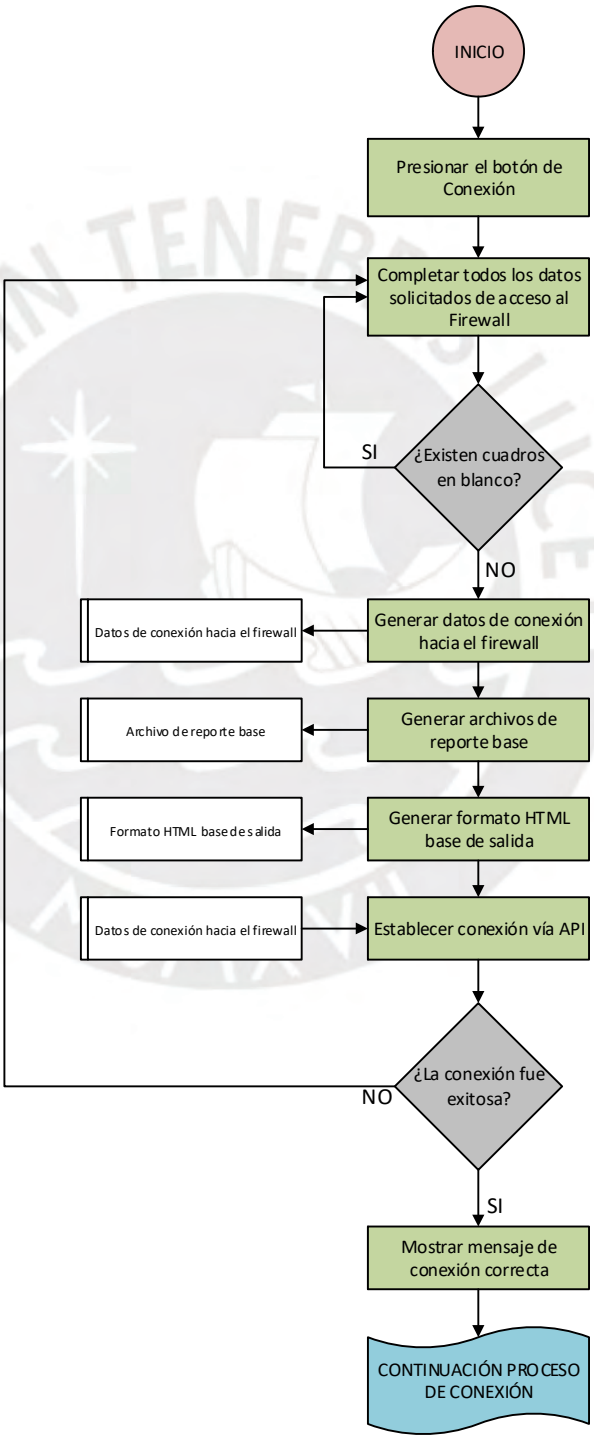
Para la presente tesis se elaboró una interfaz gráfica que cuenta solo con una ventana de navegación la cual se puede observar en la *figura 15* y que fue elaborada utilizando el programa PyQt designer. El sistema se divide en 2 auditorías diferentes, una aplicada al sistema de directorio activo y otra aplicada al equipo firewall.

Figura 15 - Interfaz gráfica del sistema auditor
Fuente: Elaboración propia

3.7 Flujo de procesos - Firewall

3.7.1 Proceso de conexión hacia Firewall

En la *figura 16* se presenta el proceso de conexión el cual se encuentra relacionado directamente con el sub-proceso de búsqueda de información indicado en la *figura 17*.



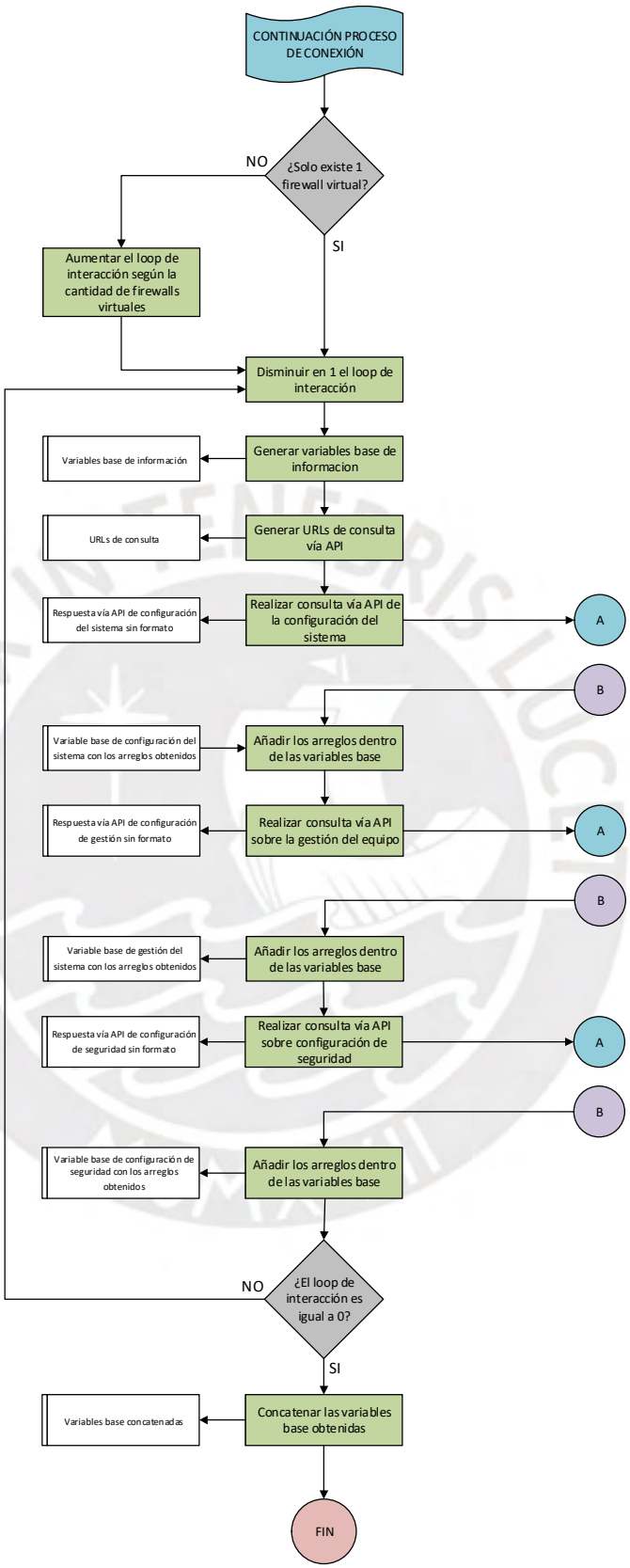


Figura 16 – Proceso de conexión hacia el firewall
Fuente: Elaboración propia

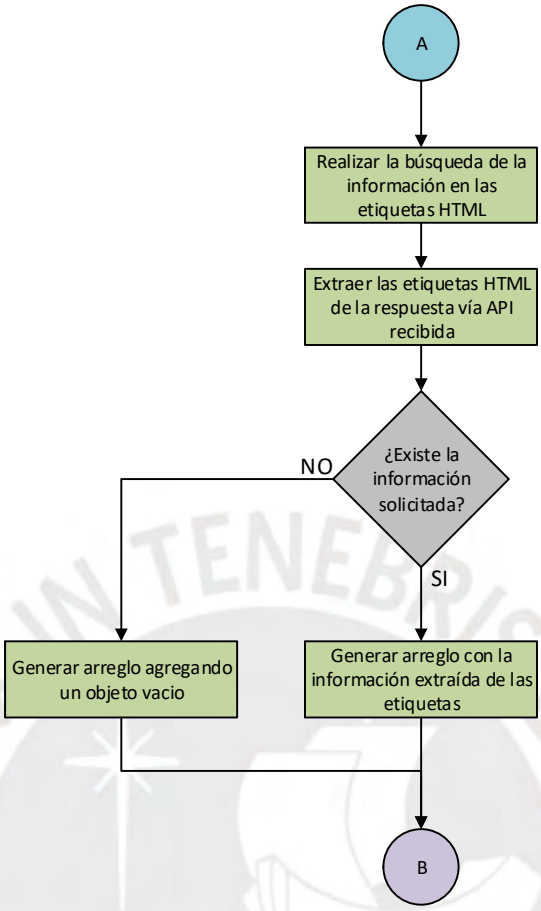
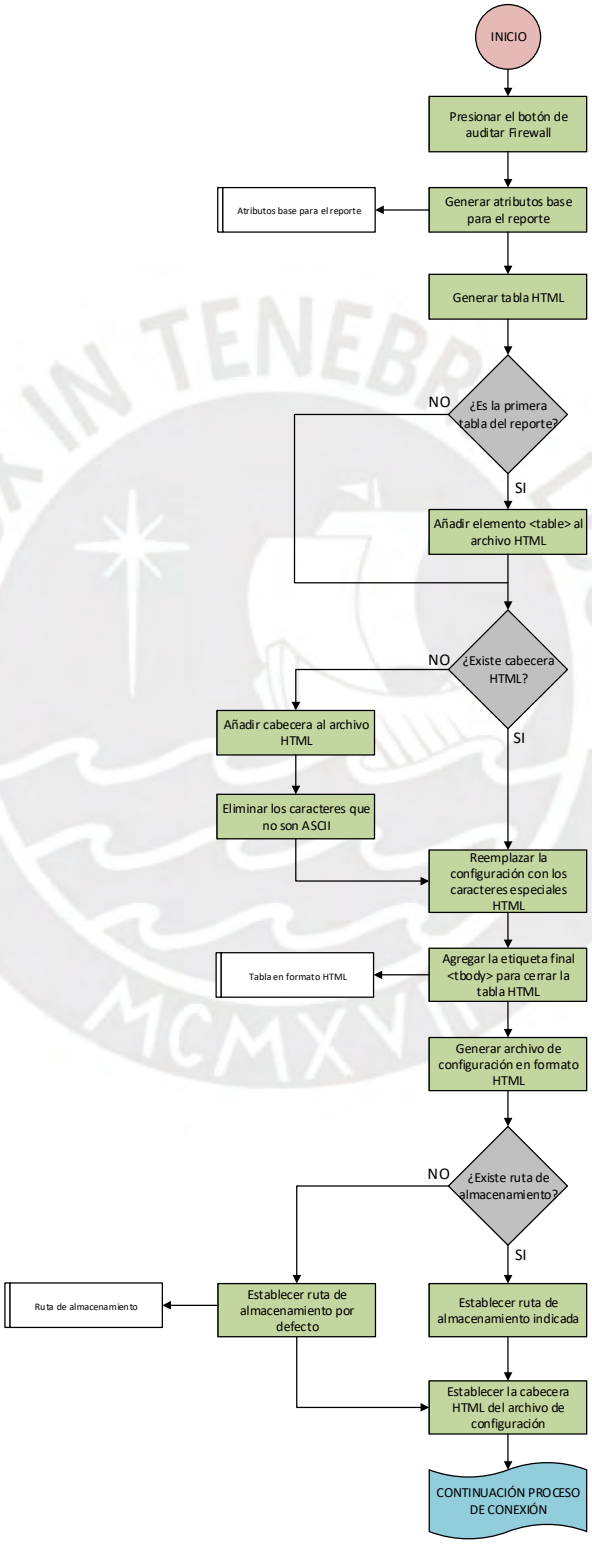


Figura 17 - Proceso de búsqueda de información en el firewall
Fuente: Elaboración propia

3.7.2 Proceso de auditoría sobre el firewall

En la *figura 18* se presenta el proceso de auditoría el cual se encuentra relacionado directamente con el sub-proceso de construcción HTML indicado en la *figura 19*.



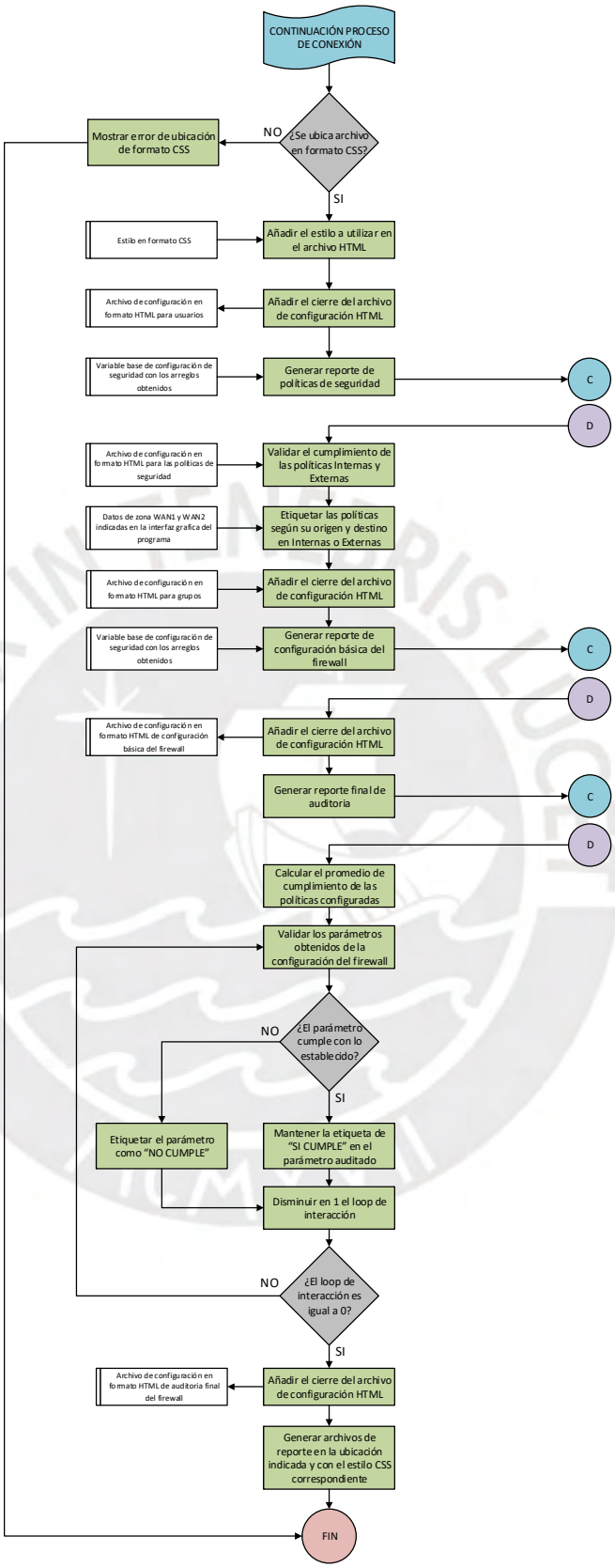


Figura 18 - Proceso de auditoría sobre el firewall
Fuente: Elaboración propia

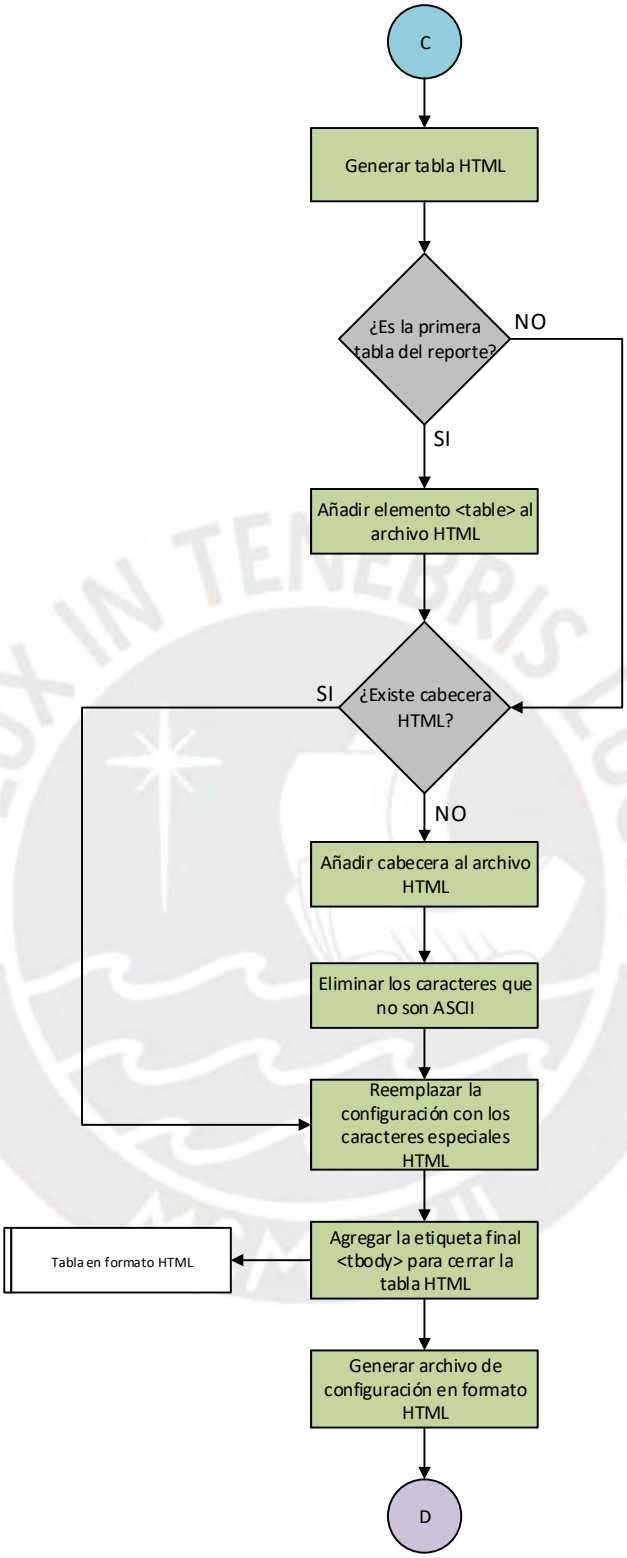
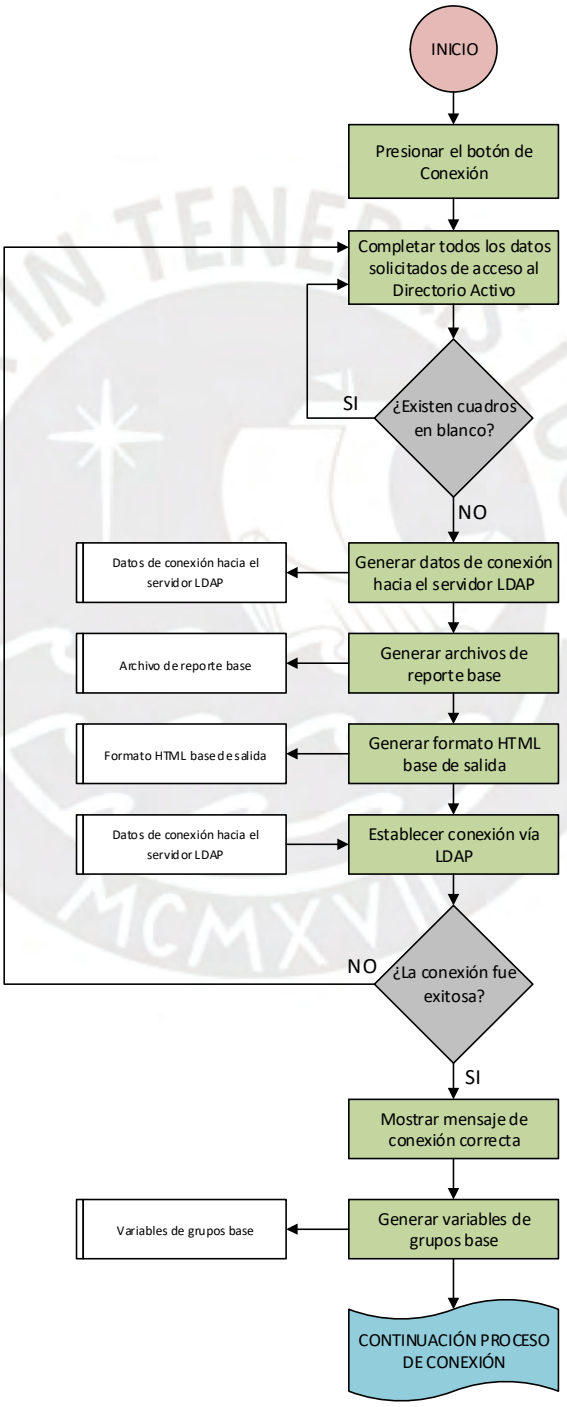


Figura 19 - Proceso de construcción HTML para el reporte del firewall
Fuente: Elaboración propia

3.8 Flujo de procesos – Directorio Activo

3.8.1 Proceso de conexión hacia Directorio Activo

En la *figura 20* se presenta el proceso de conexión el cual se encuentra relacionado directamente con el sub-proceso de consulta LDAP indicado en la *figura 21*.



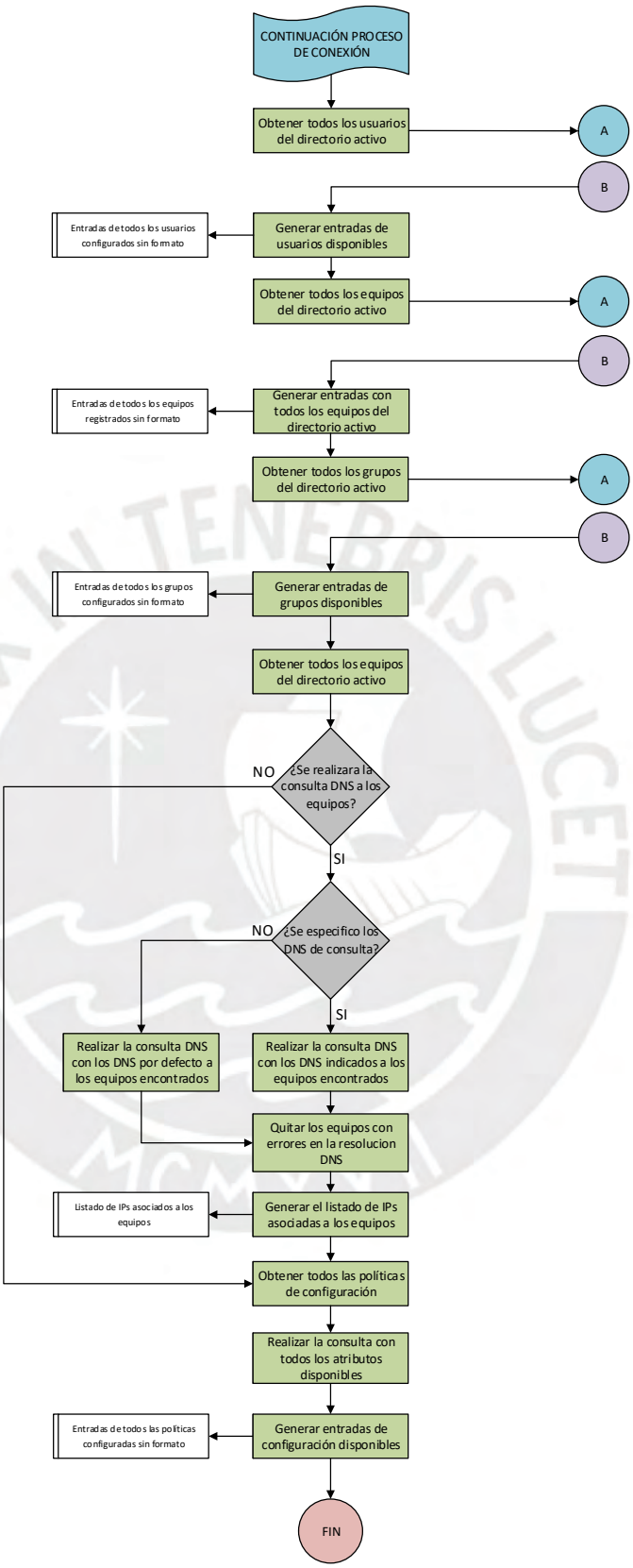


Figura 20 - Proceso de conexión hacia el directorio activo
Fuente: Elaboración propia

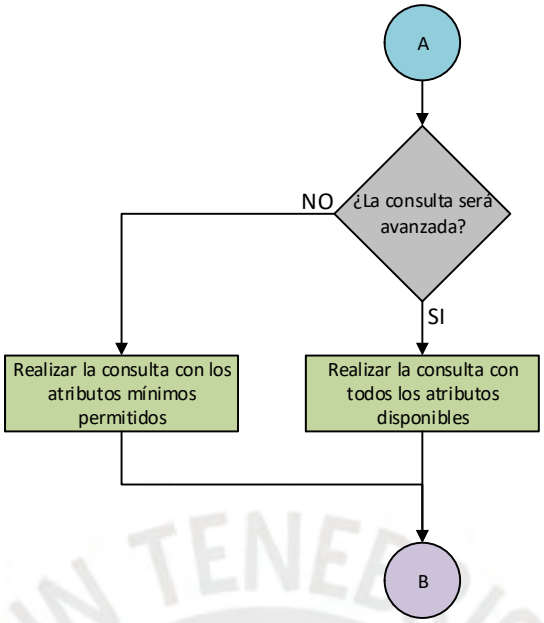
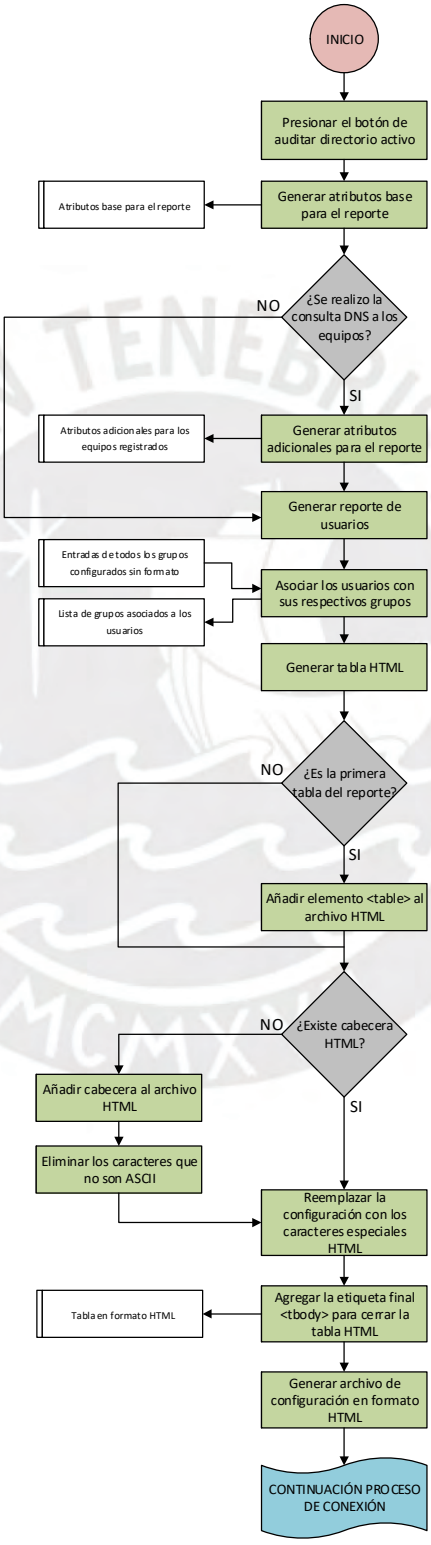


Figura 21 - Proceso de consulta LDAP hacia el directorio activo
Fuente: Elaboración propia

3.8.2 Proceso de auditoría sobre el directorio activo

En la *figura 22* se presenta el proceso de auditoría el cual se encuentra relacionado directamente con el sub-proceso de construcción HTML indicado en la *figura 23*.



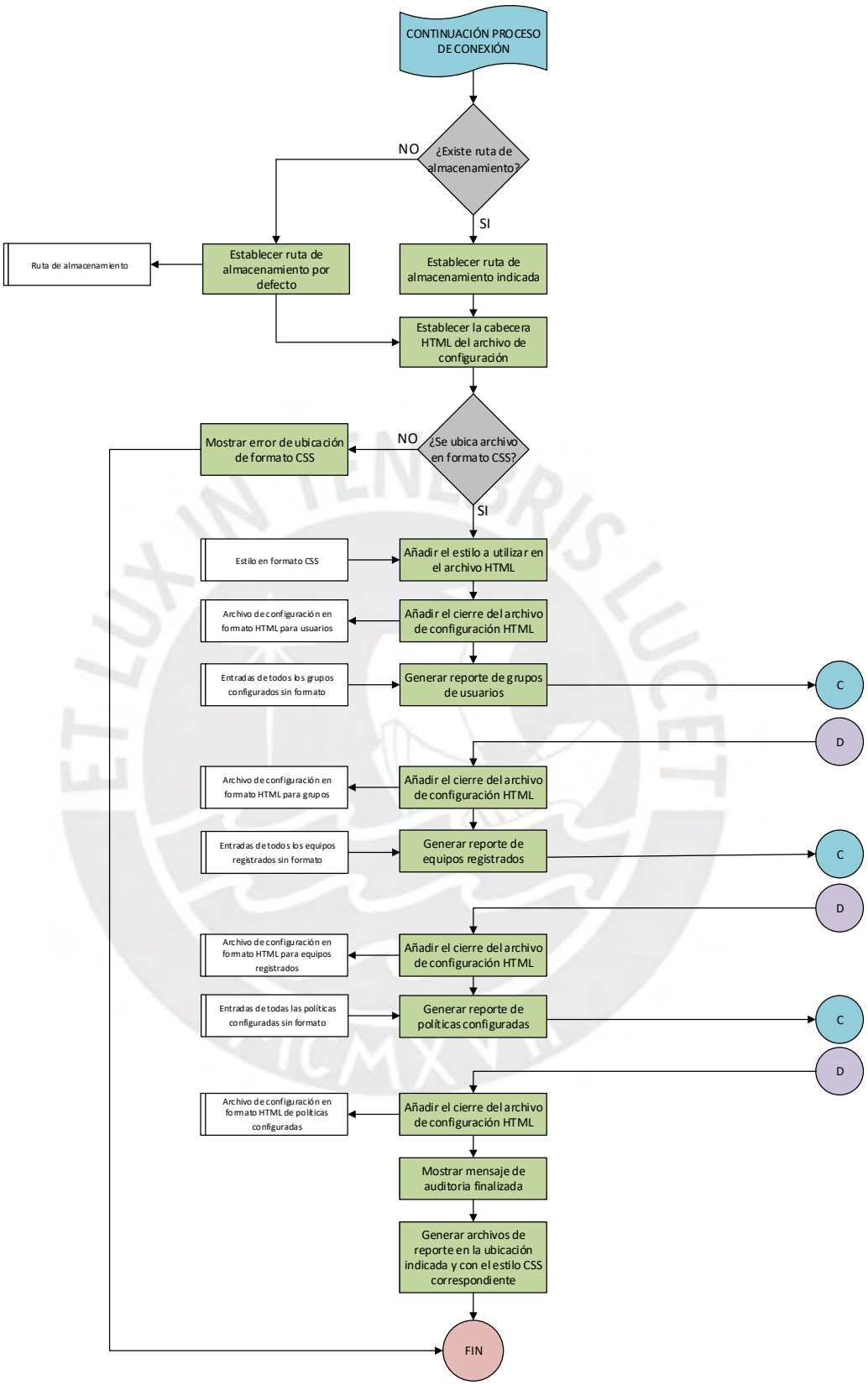


Figura 22 - Proceso de auditoría sobre el directorio activo
Fuente: Elaboración propia

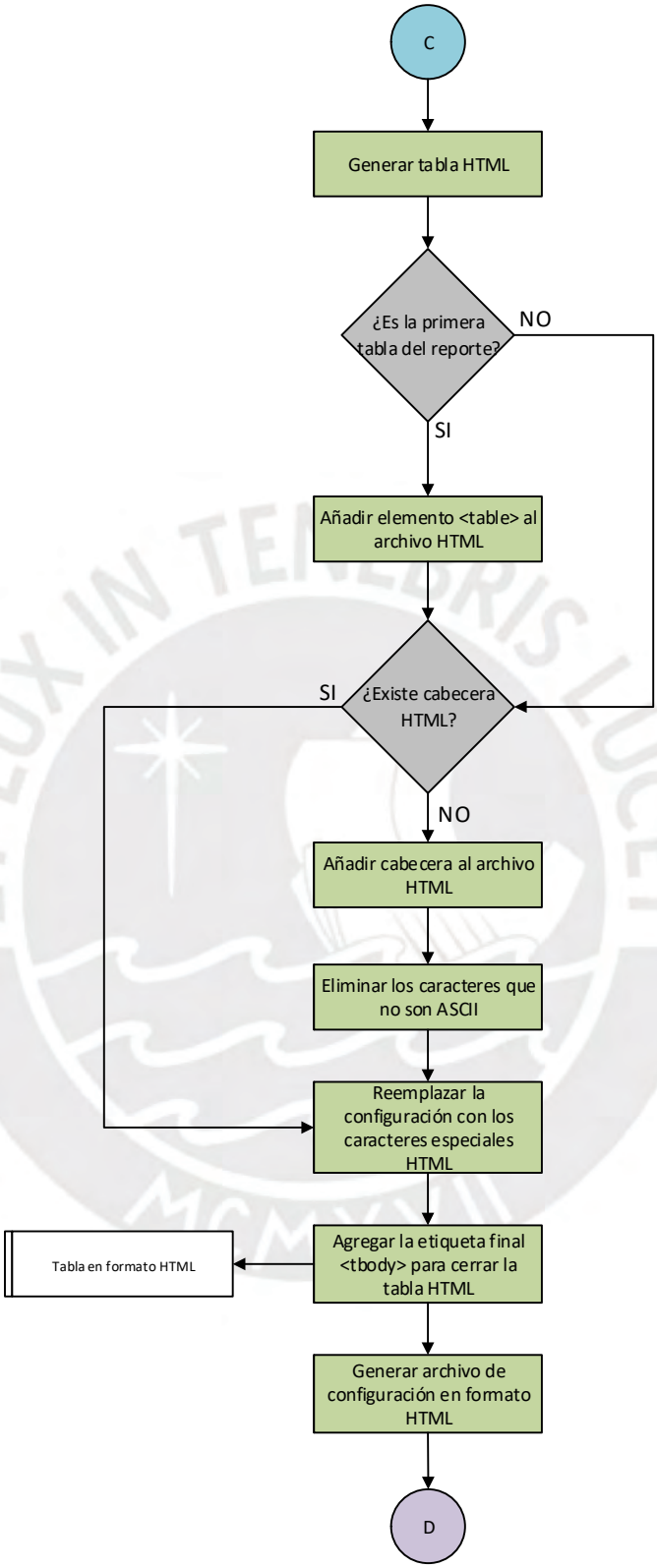


Figura 23 - Proceso de construcción HTML para el reporte del directorio activo
Fuente: Elaboración propia

CAPÍTULO 4: EVALUACIÓN DEL SISTEMA DE AUDITORÍA

4.1 Objetivos

En este capítulo se realizarán las pruebas correspondientes con el sistema desarrollado en un entorno de laboratorio, ello con la finalidad de demostrar el funcionamiento de todas las opciones desarrolladas.

4.2 Requisitos de las pruebas

Las siguientes pruebas fueron realizadas utilizando los siguientes sistemas en un entorno de laboratorio:

- Un (1) Firewall Palo Alto Virtual VM-200.
- Un (1) Servidor Virtual de Directorio Activo (Windows Server 2012).
- Una (1) máquina con Windows 10 Home.
- Un (1) usuario administrador de solo lectura del directorio activo.
- Un (1) usuario administrador de solo lectura del firewall.

4.3 Métricas Directorio Activo

Luego de recopilar la información del directorio activo se procederá a evaluar los puntos clave según las mejores prácticas y recomendaciones de Microsoft.

4.3.1 Configuración del equipo

Con respecto a la configuración general del equipo se han asignado los siguientes puntajes indicados en la *tabla 7*.

Tabla 7 - Métricas consideradas en la configuración general del directorio activo
Fuente: Elaboración propia

	0%	100%
Tiempo de bloqueo	Mayor a 30 minutos	Menor o igual a 30 minutos
Duración de bloqueo	Mayor a 30 minutos	Menor o igual a 30 minutos
Umbral de bloqueo	Mayor a 3 intentos	Menor o igual a 3 intentos
Tiempo maximo de vigencia de la clave	Mayor a 45 dias	Menor o igual a 45 dias
Tiempo minimo de vigencia de la clave	Mayor a 30 dias	Menor o igual a 30 dias
Longitud minima de la clave	Menor a 8 caracteres	Mayor a igual a 8 caracteres
Cuota de cuenta de maquinas	Mayor a 2 maquinas	Menor o igual a 2 maquinas
Cuentas no deshabilitadas	Todas las cuentas se encuentran deshabilitadas	Todas las cuentas se encuentran habilitadas
Cuentas sin clave de duración ilimitada	Todas las cuentas cuentan con duracion de clave ilimitada	Todas las cuentas cuentan con duracion de clave definidas

4.4 Métricas Firewall

Luego de recopilar la información del firewall se procederá a evaluar los puntos clave según las mejores prácticas del fabricante.

4.4.1 Configuración del equipo

Con respecto a la configuración general del equipo se han asignado los siguientes puntajes indicados en la *tabla 8*.

Tabla 8 - Métricas consideradas en la configuración general del firewall
Fuente: Elaboración propia

	0%	50%	100%
Nombre del equipo	No contiene nombre	X	Contiene nombre
Interfaz de Administración dedicada	No cuenta con IP de gestion fuera de banda	X	Interfaz de gestion fuera de banda configurada
Fecha	Fecha desactualizada	X	Fecha actual configurada
Versión de sistema operativo	El equipo cuenta con una version menor a la 8.1.13	X	El equipo cuenta con la version 8.1.13
Versión Global Protect	El global protect cuenta con una version menor a la 5.0.9	X	El global protect equipo cuenta con la version 5.0.9
Servidores DNS (Domain Name System)	No cuenta con servidores DNS configurados	Cuenta con 1 servidor DNS configurado	Cuenta con 2 servidores DNS configurados
Servidores NTP (Network Time Protocol)	No cuenta con servidores NTP configurados	Cuenta con 1 servidor NTP configurado	Cuenta con 2 servidores NTP configurados

4.4.2 Configuración de políticas de seguridad

Con respecto a las políticas de seguridad del equipo se han asignado los siguientes puntajes tanto para las políticas Internas como para las políticas Externas tal y como se indica en la *tabla 9* y *tabla 10*:

Tabla 9 - Métricas para políticas Internas
Fuente: Elaboración propia

	Zona Origen	IP Origen	Zona Destino	IP Destino	Usuario	Applicacion	Servicio	Logs	Perfil de Seguridad	Total
Porcentaje de Cumplimiento	10%	10%	10%	10%	5%	15%	15%	10%	15%	100%

Tabla 10 - Métricas para políticas Externas
Fuente: Elaboración propia

	Zona Origen	IP Origen	Zona Destino	IP Destino	Usuario	Applicacion	Servicio	Logs	Perfil de Seguridad	Total
Porcentaje de Cumplimiento	5%	10%	5%	10%	0%	20%	20%	10%	20%	100%

4.5 Módulo de Inicio

El primer paso para utilizar el sistema es inicializarlo, para realizar ello se debe de acceder mediante una consola python ejecutando el siguiente comando:

- *python Sistema_Auditor.py*

Luego de ejecutar dicho comando, se abrirá en una ventana emergente la consola de administración, la cual ya se mostró en la *figura 15*.

4.6 Auditoria de Directorio Activo

Para realizar la auditoria del directorio activo se debe de completar toda la información solicitada en los recuadros indicados en la *Figura 24*.

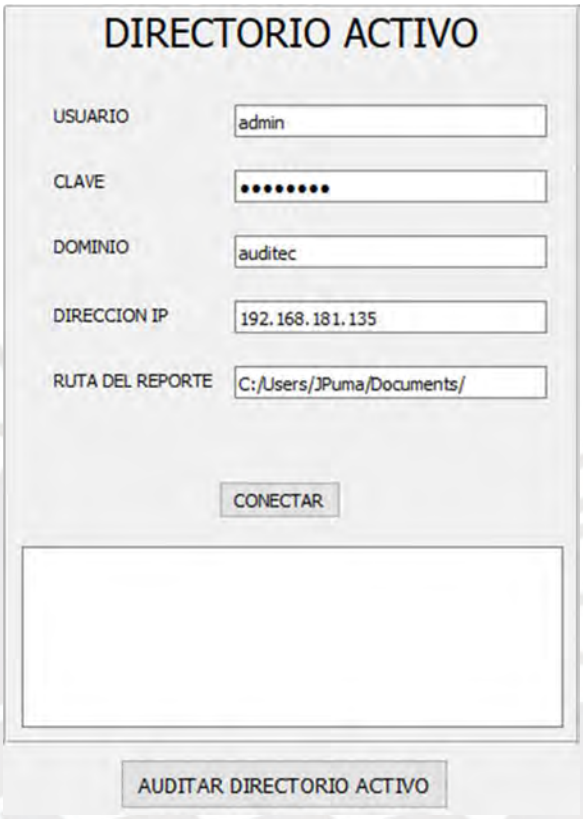


Figura 24 - Auditoria de directorio activo
Fuente: Elaboración propia

Una vez ingresados los datos solicitados se debe dar clic en el botón “Conectar”, en caso de que la conexión LDAP sea válida el recuadro en blanco mostrara un mensaje indicado que la conexión fue correcta. Finalmente, luego de establecer la conexión con el directorio activo se debe de dar clic en el botón “Auditar Directorio Activo” y con ello se exportarán los reportes en formato HTML a la ruta previamente indicada como se puede observar en la *Figura 24*.

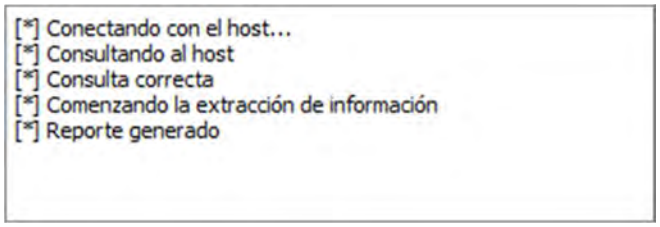


Figura 25 - Mensajes de conexión hacia el directorio activo
Fuente: Elaboración propia

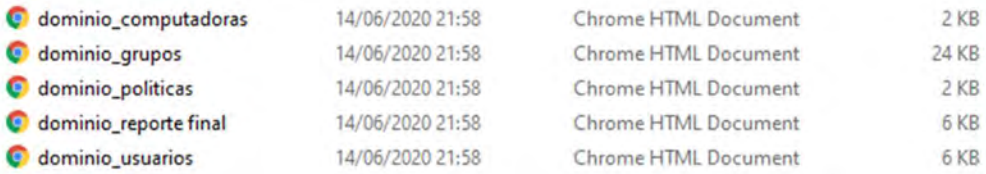


Figura 26 – Reportes generados mediante el sistema auditor para el directorio activo
Fuente: Elaboración propia

4.7 Reportes generados para el Directorio Activo

4.7.1 Reporte de Usuarios

Como se puede observar en la *figura 27* el sistema nos brinda los siguientes datos:

- Nombre común del usuario (CN)
- Nombre del usuario
- SAM[4]
- Grupos en los cuales el usuario es miembro
- Fecha de creación del usuario
- Fecha de último cambio en la configuración del usuario
- Ultimo inicio de sesión del usuario
- Etiquetas correspondientes a cada usuario según su configuración
- Fecha de último cambio de clave del usuario
- Identificador de seguridad (SID)
- Descripción del usuario

[4] Security Account Manager

Usuarios de dominio

CN	Nombre	Nombre SAM	Miembro de los grupos	Creado en	Cambiado en	Ultimo inicio de sesión	Etiqueta	Ultimo cambio de clave	Identificador de seguridad(SID)	Descripción
Teresa Reyes	Teresa Reyes	treyes		06/26/20 02:32:47	06/26/20 02:32:47	01/01/01 00:00:00	Cuenta deshabilitada, Cuenta Normal	06/26/20 02:32:47	1142	
Claudia Huapaya	Claudia Huapaya	chuapaya	Navegacion_NIVEL2, Navegacion_NIVEL1	06/26/20 02:32:30	06/26/20 02:53:34	01/01/01 00:00:00	Cuenta Normal, La clave no expira	06/26/20 02:32:30	1141	Supervisora
Angel Chuchon	Angel Chuchon	achuchon	Navegacion_NIVEL2	06/26/20 02:32:02	06/26/20 02:53:16	01/01/01 00:00:00	Cuenta Normal, La clave no expira	06/26/20 02:32:02	1140	Ingeniero de Sistemas
Guillermo Castanon	Guillermo Castanon	gcastanon		06/26/20 02:31:37	06/26/20 02:53:49	01/01/01 00:00:00	Cuenta Normal, La clave no expira	06/26/20 02:31:37	1139	Ingeniero TI
Victor Tirado	Victor Tirado	vtirado	Navegacion_NIVEL3	06/26/20 02:31:20	06/26/20 02:31:20	01/01/01 00:00:00	Cuenta Normal	01/01/01 00:00:00	1138	
Renzo Crispin	Renzo Crispin	rcrispin		06/26/20 02:31:05	06/26/20 02:31:05	01/01/01 00:00:00	Cuenta Normal	01/01/01 00:00:00	1137	
Victor Guerrero	Victor Guerrero	vguerrero	Navegacion_NIVEL3	06/26/20 02:30:21	06/26/20 02:30:21	01/01/01 00:00:00	Cuenta Normal	01/01/01 00:00:00	1136	
Antony Beltran	Antony Beltran	abeltran		06/26/20 02:30:09	06/26/20 02:53:26	01/01/01 00:00:00	Cuenta Normal	01/01/01 00:00:00	1135	Tecnico en fibra
Axel Roman	Axel Roman	aroman	Navegacion_NIVEL2	06/26/20 02:29:45	06/26/20 02:29:46	01/01/01 00:00:00	Cuenta deshabilitada, Cuenta Normal	06/26/20 02:29:45	1134	
Francisco Alvarez	Francisco Alvarez	falvarez	Navegacion_NIVEL3, Navegacion_NIVEL2	06/26/20 02:29:25	06/26/20 02:53:42	01/01/01 00:00:00	Cuenta Normal	01/01/01 00:00:00	1133	Gerente general
Pedro Telles	Pedro Telles	ptelles	Navegacion_NIVEL2	06/26/20 02:29:04	06/26/20 02:29:04	01/01/01 00:00:00	Cuenta Normal	01/01/01 00:00:00	1132	
Paul Tello	Paul Tello	ptello		06/26/20 02:28:35	06/26/20 02:28:35	01/01/01 00:00:00	Cuenta Normal	01/01/01 00:00:00	1131	
Joel Diaz	Joel Diaz	jdiaz	Navegacion_NIVEL2, Navegacion_NIVEL1	06/26/20 02:28:05	06/26/20 02:54:23	01/01/01 00:00:00	Cuenta Normal	01/01/01 00:00:00	1130	Seguridad
Isabel Flores	Isabel Flores	iflores		06/26/20 02:27:46	06/26/20 03:00:17	01/01/01 00:00:00	Cuenta deshabilitada, Cuenta Normal	01/01/01 00:00:00	1129	Gerenta de Logistica
Alex Mendez	Alex Mendez	amendez		06/26/20 02:27:32	06/26/20 03:00:24	01/01/01 00:00:00	Cuenta deshabilitada, Cuenta Normal	01/01/01 00:00:00	1128	Supervisor
Julio Suarez	Julio Suarez	jsuarez	Navegacion_NIVEL3	06/26/20 02:27:15	06/26/20 02:54:34	01/01/01 00:00:00	Cuenta Normal	01/01/01 00:00:00	1127	Administrador de Finanzas

Figura 27 - Reporte de usuarios del directorio activo
Fuente: Elaboración propia

Asimismo, el reporte también nos muestra los grupos creados en el directorio activo:

Grupos de dominio

CN	Nombre SAM	Miembro de los grupos	Descripción	Creado en	Cambiado en	Identificador de seguridad(SID)
Navegacion_NIVEL3	Navegacion_NIVEL3	falvarez,jsuarez,rmendoza,vguerrero,vtirado		06/26/20 02:34:48	06/26/20 02:35:37	1145
Navegacion_NIVEL2	Navegacion_NIVEL2	achuchon,aromsan,chuapaya,falvarez,jdiaz,ptelles		06/26/20 02:33:52	06/26/20 02:56:29	1144
Navegacion_NIVEL1	Navegacion_NIVEL1	chuapaya,jdiaz,jpomachagua,rmendoza		06/26/20 02:33:12	06/26/20 02:55:59	1143
Administradores de DHCP	Administradores de DHCP	mpomachagua	Miembros que tienen acceso administrativo al servicio DHCP	09/22/19 22:09:41	06/26/20 02:21:22	1125
Usuarios de DHCP	Usuarios de DHCP		Miembros que tienen acceso de solo vista al servicio DHCP	09/22/19 22:09:41	09/22/19 22:09:41	1124
Acceso_VIP	Acceso_VIP		Grupo de Prueba para Sistema Auditor	09/21/19 22:17:12	06/26/20 02:41:18	1123
WseManagedGroups	WseManagedGroups		Grupos administrados por Windows Server Essentials	08/12/19 03:36:56	08/12/19 03:36:56	1116
WseInvisibleToDashboard	WseInvisibleToDashboard		Usuarios del dominio ocultos del panel de Windows Server Essentials.	08/12/19 03:36:56	09/22/19 21:38:59	1115
WseRemoteAccessUsers	WseRemoteAccessUsers		Usuarios con permisos para usar VPN para conectarse a la red del servidor remotamente.	08/12/19 03:36:55	08/12/19 03:36:56	1114
WseAlertAdministrators	WseAlertAdministrators		Usuarios con permisos para ver alertas en la red.	08/12/19 03:36:55	09/22/19 22:04:10	1113
WseAllowHomePageLinks	WseAllowHomePageLinks		Usuarios con permisos para acceder al gadget de vínculos en Acceso Web remoto.	08/12/19 03:36:55	08/12/19 03:36:56	1112
WseAllowDashboardAccess	WseAllowDashboardAccess		Usuarios con permisos para acceder al panel remotamente en Acceso Web remoto.	08/12/19 03:36:55	08/12/19 03:36:56	1111
WseAllowAddInAccess	WseAllowAddInAccess		Usuarios con permisos para obtener acceso a complementos de Windows Server Essentials.	08/12/19 03:36:55	08/12/19 03:36:56	1110
WseAllowMediaAccess	WseAllowMediaAccess		Usuarios con permisos para acceder a la biblioteca multimedia en Acceso web remoto	08/12/19 03:36:55	08/12/19 03:36:56	1109
WseAllowComputerAccess	WseAllowComputerAccess		Usuarios con permisos para acceder a un equipo remotamente en Acceso Web remoto.	08/12/19 03:36:55	08/12/19 03:36:56	1108
WseAllowShareAccess	WseAllowShareAccess		Usuarios con permisos para obtener acceso a carpetas compartidas en Acceso Web remoto.	08/12/19 03:36:54	08/12/19 03:36:56	1107
WseRemoteWebAccessUsers	WseRemoteWebAccessUsers		Usuarios con permisos para usar Acceso Web remoto.	08/12/19 03:36:54	08/12/19 03:36:56	1106
DnsUpdateProxy	DnsUpdateProxy		Clientes DNS que tienen permiso para efectuar actualizaciones dinámicas en nombre de otros clientes (tales como servidores DHCP).	08/12/19 03:35:25	08/12/19 03:35:25	1105
DnsAdmins	DnsAdmins		Grupo de administradores de DNS	08/12/19 03:35:25	08/12/19 03:35:25	1104
Protected Users	Protected Users		Los miembros de este grupo tienen protecciones adicionales frente a las amenazas contra la seguridad de autenticación. Consulte http://go.microsoft.com/fwlink/?LinkId=298939 para obtener más información.	08/12/19 03:34:45	08/12/19 03:34:45	525
Controladores de dominio clonables	Controladores de dominio clonables		Se pueden clonar los miembros del grupo que sean controladores de dominio.	08/12/19 03:34:45	08/12/19 03:34:45	522
Enterprise Domain Controllers de sólo lectura	Enterprise Domain Controllers de sólo lectura		Los miembros de este grupo son controladores de dominio de solo lectura en la empresa.	08/12/19 03:34:45	08/12/19 03:34:45	498

Figura 28 - Reporte de grupos del directorio activo
Fuente: Elaboración propia

4.7.2 Reporte del servidor

El sistema brinda información sobre la configuración actual del servidor que funciona como directorio activo:

- Nombre de dominio
- Tiempo de bloqueo de los usuarios

- Duración de bloqueo de los usuarios
- Tiempo máximo de duración de la clave
- Tiempo mínimo de duración de la clave
- Longitud máxima de la clave del usuario

Politica de dominio

nombre de dominio	Tiempo de bloqueo	Duracion de bloqueo	Tiempo maximo de la clave	Tiempo minimo de la clave	Longitud minima de la clave
DC=AUDITEC,DC=local	30.0 minutos	30.0 minutos	42.00 dias	30.00 dias	0

Figura 29 - Reporte de configuración del directorio activo
Fuente: Elaboración propia

4.7.3 Reporte de máquinas

El sistema brinda información sobre las máquinas que se encuentran conectadas al directorio activo y nos brinda la siguiente información:

- Nombre común del host (CN)
- SAM
- Nombre de host incluyendo dominio
- Sistema Operativo de la máquina
- Paquete de Servicio
- Versión de Sistema Operativo
- Último inicio de sesión
- Etiquetas
- Fecha de creación
- Identificador de seguridad (SID)
- Descripción del host

Cuentas de computadoras de dominio

CN	Nombre SAM	Nombre de Host	Sistema Operativo	Paquete de servicio	Version de Sistema Operativo	Ultimo inicio de sesión	Etiqueta	Creado en	Identificador de seguridad(SID)	Descripción
WIN-2ITSN27A9NS	WIN-2ITSN27A9NS$	WIN-2ITSN27A9NS.AUDITEC.local	Windows 7 Ultimate	Service Pack 1	6.1 (7601)	09/22/19 22:42:51	Cuenta de estacion de Trabajo	08/12/19 05:40:04	1119	
MediaAdmin	MediaAdmin$					01/13/20 04:03:08	Cuenta de estacion de Trabajo	08/12/19 03:37:13	1117	
AUDITECSERVER	AUDITECSERVER$	AUDITECServer.AUDITEC.local	Windows Server 2012 R2 Essentials		6.3 (9600)	01/20/20 07:56:29	Servidor de cuenta de confianza, Estacion de confianza	08/12/19 03:34:45	1003	

Figura 30 - Reporte de máquinas del directorio activo
Fuente: Elaboración propia

4.7.4 Reporte final de auditoría Directorio Activo (AD)

El sistema indicara en el reporte final si alguno de los siguientes puntos cumple o no con los parámetros recomendados a nivel de configuración indicados en la *tabla 7*.

Reporte Final de Auditoria del Directorio Activo

N°	Parametro	Porcentaje obtenido	Porcentaje recomendado	Resultado
1	Tiempo de bloqueo	100%	100%	SI CUMPLE
2	Duración del bloqueo	100%	100%	SI CUMPLE
3	Umbral de bloqueo	0%	100%	NO CUMPLE
4	Tiempo maximo de la clave	100%	100%	SI CUMPLE
5	Tiempo mínimo de la clave	100%	100%	SI CUMPLE
6	Longitud minima de la clave	0%	100%	NO CUMPLE
7	Cuota de cuenta de maquinas	0%	100%	NO CUMPLE
8	Cuentas no deshabilitadas	67%	90%	NO CUMPLE
9	Cuentas sin clave de duración ilimitada	70%	95%	NO CUMPLE

Figura 31 - Reporte final de auditoria del directorio activo
Fuente: Elaboración propia

4.8 Auditoria de Firewall

Para realizar la auditoria de los equipos Firewall se debe de seleccionar el botón del lado derecho con el nombre Firewall y se deben de completar toda la información solicitada en los recuadros indicados en la *figura 32*.

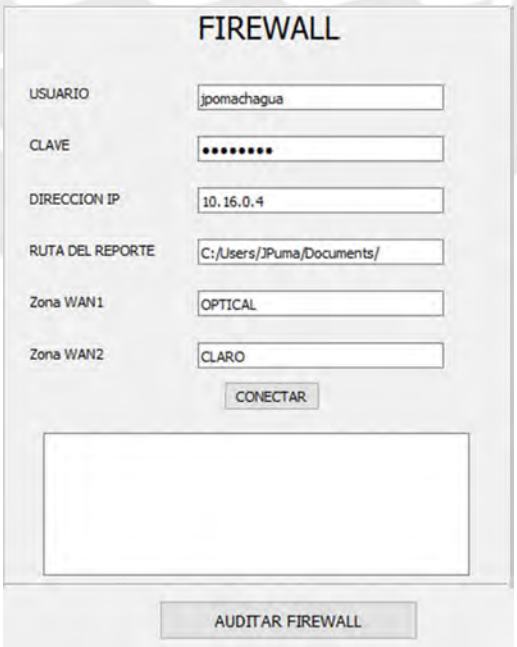


Figura 32 - Auditoria de firewall
Fuente: Elaboración propia

Una vez ingresados los datos solicitados se debe dar clic en el botón “Conectar”, en caso de que la conexión vía API sea válida el recuadro en blanco mostrara un mensaje indicado que la conexión fue correcta. Finalmente, luego de establecer la conexión con el firewall correspondiente se debe de dar clic en el botón “Auditar Firewall” y con ello se exportarán los reportes en formato HTML a la ruta previamente indicada como se puede observar en la *figura 34*.

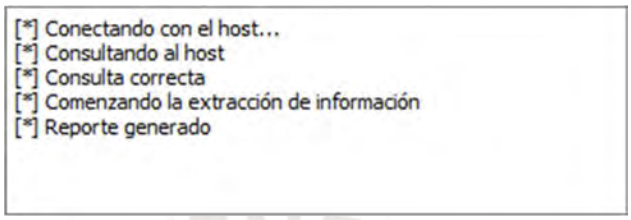


Figura 33 - Mensajes de conexión hacia el firewall
Fuente: Elaboración propia

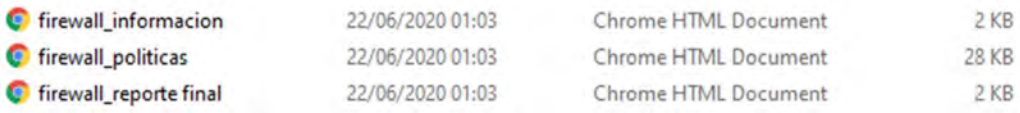


Figura 34 - Reportes generados mediante el sistema auditor para el firewall
Fuente: Elaboración propia

4.9 Reporte generado para el Firewall

4.9.1 Reporte del equipo

El sistema nos permite conocer algunos datos importantes del equipo al cual se audita, tales como:

- Nombre del equipo
- IP y máscara del sistema
- Fecha y hora del equipo
- Versión de sistema operativo
- Modelo del equipo
- Tiempo de encendido
- Número serial
- Dirección MAC
- Versión de global protect
- Versión de filtro URL

- Versión de aplicaciones
- Versión de wildfire
- Configuración DNS
- Configuración NTP

Informacion General del Firewall

Hostname	IP de gestión	Fecha y hora del equipo	Versión de SO	Modelo	Tiempo de encendido	Serial	Mac Address	Versión de Global Protect	Versión Filtro URL	Versión Antivirus	Versión Aplicaciones	Versión Wildfire	DNS	NTP
NEO-FW-PAN-PERU01	10.16.0.4/255.255.255.0	Fri Jun 26 01:36:52 2020	8.1.6	PA-3020	194 días, 10:16:54	001801030308	58:49:3b:f4:38:bc	5.0.8	20200602.20136	3366-3877	8286-6150	459181-462115	10.16.0.60, 8.8.8.8	10.16.0.60

Figura 35 – Información básica del firewall
Fuente: Elaboración propia

4.9.2 Reporte de políticas de seguridad

El sistema nos envía un reporte indicando todas las políticas configuradas en el equipo, asimismo, nos podrá brindar los siguientes detalles:

- Nombre de las políticas
- Zona de origen
- IP origen
- Zona destino
- IP destino
- Usuario
- Aplicaciones utilizadas
- Servicios utilizados
- Acción tomada por la política
- Perfil de reenvió de logs
- Porcentaje de cumplimiento
- Tipo de política (Interna/Externa)

Reporte de Políticas de Seguridad

Nombre	Zona Origen	IP Origen	Zona Destino	IP Destino	Usuario	Applicacion	Servicio	Accion	Logs	Perfil de Seguridad	Cumplimiento	Tipo de Política
APP Block	any	any	CLARO, OPTICAL	any	any	bittorrent	application-default	deny	Log_Forw_QRadar	NEO-SPG	65	Externa
Joel Calegua	LAN	10.16.0.19	LABORATORIO	10.16.1.42_32	any	any	any	allow	Log_Forw_QRadar	NEO-SPG	65	Interna
Bloqueo OUT	any	any	CLARO, OPTICAL	Objetos Maliciosos	any	any	any	deny	Log_Forw_QRadar	NEO-SPG	45	Externa
Bloqueo OUT AD	LAN	10.16.0.60	CLARO, OPTICAL	any	any	any	tcp-53, udp-53	deny	Log_Forw_QRadar	NEO-SPG	75	Interna
SEG - WCry Block Inbound	CLARO, OPTICAL	any	DMZ, LABORATORIO, LAN	any	any	any	SAMBA, SMB	deny	Log_Forw_QRadar	NEO-SPG	65	Interna
SEG - WCry Block Outbound	any	any	CLARO, OPTICAL	any	any	any	SAMBA, SMB, NBDS, NBNAME	deny	Log_Forw_QRadar	NEO-SPG	55	Externa
VPN PRISMA NEO Servicio 8444	VPN_PRISMA_NEO	any	LABORATORIO	10.16.1.79	any	any	TCP_8444	allow	Log_Forw_QRadar	NEO-SPG	75	Interna
VPN PRISMA NEO	VPN_PRISMA_NEO	any	LABORATORIO, LAN, SERVICIOS	net-lab-pe, net-lan-pe, net-terceros-pe	any	active-directory-base, dns, kerberos, ldap, ms-ds-smb-base, ms-ds-smbv3, ms-local-security-management, ms-netlogon, ms-rdp, msrpc-base, netbios-ns, netbios-ss, ntp, ping, snmp-base, ssh, ssl, web-browsing	application-default	allow	Log_Forw_QRadar	NEO-SPG	85	Interna
CI-VPN PRISMA NEO	VPN_PRISMA_NEO	any	LABORATORIO, LAN, SERVICIOS	net-lab-pe, net-lan-pe, net-terceros-pe	any	any	application-default	allow	Log_Forw_QRadar	NEO-SPG	75	Interna
VPN PRISMA NEO-VPNCHILE	VPN_PRISMA_NEO	any	VPNCHILE	checkscore.neosecure.cl, ironmail-tic, mpn.neosecure.cl, neo-pvt-win-tmx01.neosecure.cl, otrs.neosecure.cl	any	netbios-ns, ssl, web-browsing	application-default	allow	Log_Forw_QRadar	NEO-SPG	85	Interna
CI-VPN PRISMA NEO-VPNCHILE	VPN_PRISMA_NEO	any	VPNCHILE	checkscore.neosecure.cl, ironmail-tic, mpn.neosecure.cl, neo-pvt-win-tmx01.neosecure.cl, otrs.neosecure.cl	any	any	application-default	allow	Log_Forw_QRadar	NEO-SPG	75	Interna
VPN NEO-FOH-ping	SERVICIOS	10.20.0.80, PVT-Servicios	VPN_FOH	FOH_PA_01, FOH_PA_02	any	ping	application-default	allow	Log_Forw_QRadar	NEO-SPG	95	Interna
VPN NEO-FOH	SERVICIOS	10.20.0.80, PVT-Servicios	VPN_FOH	FOH_PA_01, FOH_PA_02	any	ssh, ssl	VPN_SERVICIOS	allow	Log_Forw_QRadar	NEO-SPG	95	Interna
CI-VPN NEO-FOH	SERVICIOS	10.20.0.80, PVT-Servicios	VPN_FOH	FOH_PA_01, FOH_PA_02	any	any	VPN_SERVICIOS	allow	Log_Forw_QRadar	NEO-SPG	85	Interna
VPN - OUT RIMAC-NEO	LAN, SERVICIOS	10.20.0.80, PVT-Servicios, 10.16.0.173, 10.16.0.204, ccantillo-pc, kdurand-nb	VPN_RIMAC_ARAM	172.24.0.0_13	any	snmp-base, snmpv2, ssh, ssl, web-browsing	VPN_SERVICIOS	allow	Log_Forw_QRadar	NEO-SPG	95	Interna
CI-VPN - OUT RIMAC-NEO	LAN, SERVICIOS	10.20.0.80, PVT-Servicios, 10.16.0.173, 10.16.0.204, ccantillo-pc, kdurand-nb	VPN_RIMAC_ARAM	172.24.0.0_13	any	any	VPN_SERVICIOS	allow	Log_Forw_QRadar	NEO-SPG	85	Interna
VPN - OUT RIMAC-NEO-ping	SERVICIOS	10.20.0.80, PVT-Servicios	VPN_RIMAC_ARAM	172.24.0.0_13	any	ping	application-default	allow	Log_Forw_QRadar	NEO-SPG	95	Interna
CRC - VPNSSL BCP	LAN	net-lan-pe	CLARO, OPTICAL	216.244.162.247/27	any	any	any	allow	Log_Forw_QRadar	NEO-SPG	65	Interna
NEO - APP Amazon	LAN	10.16.0.107, 10.16.0.124	CLARO, OPTICAL	any	any	amazon-workspace, pcoip	application-default	allow	Log_Forw_QRadar	NEO-SPG	85	Interna

Figura 36 - Políticas de seguridad del firewall
Fuente: Elaboración propia

4.9.3 Reporte final de auditoría firewall

El sistema indicara en el reporte final si alguno de los siguientes puntos cumple o no con los parámetros recomendados a nivel de configuración indicadas en la *tabla 8, tabla 9* y *tabla 10*.

Reporte Final de Auditoria del Firewall

N°	Parametro	Porcentaje obtenido	Porcentaje recomendado	Resultado
1	Nombre del equipo	100%	100%	SI CUMPLE
2	Interfaz de Administración dedicada	100%	100%	SI CUMPLE
3	Fecha	100%	100%	SI CUMPLE
4	Versión de sistema operativo	100%	100%	SI CUMPLE
5	Versión Global Protect	0%	100%	NO CUMPLE
6	Servidores DNS (Domain Name System)	100%	100%	SI CUMPLE
7	Servidores NTP (Network Time Protocol)	50%	100%	NO CUMPLE
8	Reglas para el filtrado de ataques externos	90%	90%	SI CUMPLE
9	Reglas para el filtrado de ataques internos	74%	95%	NO CUMPLE

Figura 37 - Reporte final de auditoria del firewall
Fuente: Elaboración propia

4.10 Casos de uso

El sistema auditor ha sido configurado para ser utilizados en ambientes que con las siguientes características:

- Firewall palo alto funcionando de manera interno o perimetral.
- Servidor de directorio activo que cuente con Windows Server 2012 o 2016.
- El firewall debe de trabajar en modo Standalone[5].
- El firewall debe de contar con licencias activas correspondientes a perfiles de seguridad (antivirus, spyware, wildfire y filtro URL).
- El equipo debe de contar con la configuración de global protect[6] activa.
- Para la conexión hacia el firewall y el directorio activo se requiere de un usuario administrador.

4.11 Ambiente de pruebas firewall

El sistema auditor se aplicó en cinco (5) ambientes diferentes (1 ambiente de prueba y 4 de producción) y se obtuvieron los siguientes resultados:

Tabla 11 - Análisis realizado a los directorio activo de prueba
Fuente: Elaboración propia

	Equipo 1	Equipo 2	Equipo 3	Equipo 4	Equipo 5
Tiempo de bloqueo	100%	0%	0%	100%	100%
Duración de bloqueo	100%	100%	100%	100%	0%
Umbral de bloqueo	0%	100%	100%	100%	100%
Tiempo maximo de vigencia de la clave	100%	100%	100%	0%	0%
Tiempo minimo de vigencia de la clave	100%	100%	100%	0%	0%
Longitud minima de la clave	100%	100%	100%	100%	100%
Cuota de cuenta de maquinas	0%	0%	100%	100%	100%
Cuentas no deshabilitadas	67%	50%	95%	90%	70%
Cuentas sin clave de duración ilimitada	70%	65%	80%	55%	75%

[5] Modo de trabajo en el cual no se considera un equipo de contingencia
[6] Servicio de VPN site to site de Palo Alto

4.12 Ambiente de pruebas Directorio Activo (AD)

El sistema auditor se aplicó en cinco (5) ambientes diferentes (1 ambiente de prueba y 4 de producción) y se obtuvieron los siguientes resultados:

Tabla 12 - Análisis realizado a los firewalls de prueba
Fuente: Elaboración propia

	Equipo 1	Equipo 2	Equipo 3	Equipo 4	Equipo 5
Nombre del equipo	100%	0%	100%	100%	100%
Interfaz de Administración dedicada	100%	100%	100%	100%	100%
Fecha	100%	100%	100%	100%	0%
Versión de sistema operativo	100%	0%	0%	100%	100%
Versión Global Protect	0%	0%	100%	0%	0%
Servidores DNS (Domain Name System)	100%	50%	100%	100%	50%
Servidores NTP (Network Time Protocol)	100%	50%	50%	50%	100%
Reglas para el filtrado de ataques externos	65%	70%	55%	90%	80%
Reglas para el filtrado de ataques internos	51%	80%	78%	74%	45%

CAPÍTULO 5: CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- El sistema de auditoría desarrollado contribuye en mejorar el análisis de nivel de cumplimento de las políticas de seguridad, y ayudar en la toma de decisiones a las áreas encargadas de la seguridad informática de las empresas. Con el sistema se puede lograr obtener visibilidad del panorama actual de configuración de los equipos, los cuales cambian de manera continua, y evaluar los riesgos de seguridad.

- Luego de realizar el análisis de los datos obtenidos se observó que a medida que cambian las versiones de los sistemas operativos el formato XML recibido por los firewalls cambia en algunos puntos. Es por ello que se tuvo que agregar validaciones adicionales para mantener la fiabilidad del reporte en todo momento.

- Las respuestas a las consultas vía LDAP realizadas al Directorio Activo muestran información codificada para los usuarios, grupo y maquinas por lo que es necesario contar con la tabla de parámetros predefinidos de Microsoft. La decodificación de los parámetros se encuentra insertada dentro del código de programación, así como en la bibliografía de la presente tesis.

- Las respuestas a las consultas vía API realizadas al firewall se obtienen en formato XML el cual se recibe con etiquetas de apertura y de cierre, es por ello que se debe de realizar el filtrado correspondiente para obtener la información requerida. El punto clave de este formato es que se puede agrupar información de manera rápida según sus etiquetas por lo que el sistema no requerirá de múltiples búsquedas sobre la configuración actual.

- Las métricas asociadas a los equipos de seguridad fueron definidas de acuerdo a la información brindada en los manuales de buenas prácticas de cada fabricante, tanto en el Directorio Activo (Microsoft) como en el Firewall (Palo Alto Networks). Para el Directorio Activo se consideraron los parámetros asociados al servicio de directorio activo y para el caso del Firewall se consideraron los parámetros asociados a políticas de seguridad, perfiles de seguridad y configuración base.

- En un inicio se consideró extraer la información de los Firewalls mediante una conexión SSH, sin embargo, la información obtenido se recibía en texto plano y sin ningún parámetro de relación entre objetos. Debido a ello se optó por cambiar el método de conexión hacia API, el cual permitió utilizar las librerías de comandos predefinidos, así como la facilidad de obtener la información en formato XML con etiquetas de agrupación de objetos lo cual redujo la complejidad del presente trabajo.

- Una vez establecidos los métodos de conexión hacia los equipos involucrados se procedió a elaborar la arquitectura correspondiente. Las pruebas se han realizado en directorios activos que cuentan con más de 400 usuarios y en firewalls con más de 1500 políticas de seguridad. El sistema auditor realiza consultas especificas hacia los equipos de seguridad, es por ello que el servidor en el cual se ejecute no requiere de grandes capacidades de procesamiento. Los reportes se generan de manera individual para cada equipo por lo que el sistema se puede ejecutar sobre múltiples equipos de seguridad con los requisitos indicados previamente.

- Se eligió la programación en Python por su facilidad para poder trabajar con sus diferentes librerías, adicional a ello es unos de los lenguajes más utilizados en programación web y aplicaciones empresariales. De igual manera, se eligió el programa PyQt Designer para la creación de la interfaz gráfica del sistema auditor por su fácil integración con el código Python elaborado.

- Se aplicaron los siguientes conocimientos adquiridos al desempeñarme en la rama de Seguridad Informática:

    - Evaluación, implementación y soporte post-implementación de proyectos de seguridad de TI en diversas empresas gubernamentales y privadas.
    - Adopción de medidas preventivas y/o correctivas a través del monitoreo permanente de equipos de seguridad.
    - Elaboración y actualización de políticas, normas y procedimientos relacionados a la seguridad informática.

- Se aplicó el conocimiento adquirido en los siguientes cursos de la Maestría de Ingeniera de las Telecomunicaciones:

    - Criptografía y Hacking Ético.
    - Seguridad en Negocios y Comercio Electrónico.
    - Minería Web.

5.2 Recomendaciones y Trabajos Futuros

- El sistema se puede utilizar en cualquier empresa que cuente con los equipos de seguridad y que cumpla con los requisitos previamente mencionados.

- Es posible incrementar el análisis de sistema de auditoria actual incluyendo un análisis de la conexión de los equipos que se conectan mediante VPN a la red corporativa siempre que estas sean recibidas por el Firewall Palo Alto. Este análisis permitirá tener visibilidad de los equipos conectados de manera interna como de manera externa.

- A futuro, planeo implementar reportes que se apliquen en conjunto con inteligencia artificial. Para conseguir ello se requeriría que el sistema se encuentre operando en la red interna de la empresa y recopilando información por un tiempo determinado. La información recopilada se almacenaría en una base de datos y con dichos datos se podrían analizar, correlacionar y proporcionar lineamientos de seguridad que se ajusten a la red monitoreada.

- Adicionalmente, planteo agregar a los reportes de auditoria las configuraciones adicionales realizadas en los firewalls y directorio activo, las cuales no son usadas en las soluciones comunes de seguridad.

- Actualmente el sistema se ejecuta mediante un programa en Python y se visualiza en un programa elaborado en PyQt designer, se recomienda migrar el programa a un entorno web ya que sería mucho más amigable la interacción entre el usuario y el sistema de auditoria, asimismo, permitiría un despliegue más rápido en un ambiente de producción.

- La herramienta cuenta con un grado de confiabilidad de 100% de acuerdo con los requisitos pre-establecidos y las funcionalidades acotadas. Como se indica en el documento el sistema ha sido ejecutado sobre cuatro (4) clientes distintos que se encuentran en producción, sin presentar afectación del servicio.

- Finalmente, se propone extender la solución a otras marcas de Firewall, tales como Checkpoint, Cisco FirePower, Fortinet, etc. Ello debido a que no todas las empresas cuentan con firewalls Palo Alto. Cabe indicar que se deben de analizar los manuales de buenas prácticas de cada uno de los equipos lo cual puede tomar entre uno (1) a dos (2) meses por equipo.

BIBLIOGRAFÍA

[1] CNSS, "National on the use of the Advanced Encryption Standard (AES) to Protect Security Systems and National Information CNSS Policy No. 15 Fact Sheet No. 1", 2003. [Online]. Disponible: https://www.hsdl.org/?view&did=453540. [Revisado: 14-Abr-2020]

[2] Microsoft, "Procedimientos recomendados para proteger Active Directory", 2017. [Online]. Disponible: https://docs.microsoft.com/es-es/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory. [Revisado: 15-Abr-2020]

[3] Palo Alto Networks, "Best Practice Assessment for NGFW and Panorama", 2020. [Online]. Disponible: https://www.paloaltonetworks.com/services/bpa. [Revisado: 15-Abr-2020]

[4] Came R, Christian & Duque P, Diego. *"Tesis: Auditoria de Seguridad Informática ISO 27001 para la empresa de alimentos "Italimentos CIA. LTDA."* Universidad Politécnica Salesiana, Cuenca, Ecuador, 2012.

[5] KPMG, "KPMG Clara", 2017 [Online]. Disponible: https://assets.kpmg/content/dam/kpmg/es/pdf/2017/12/kpmg-clara.pdf. [Revisado: 10-Jul-2019]

[6] Manage Engine, "Windows Server Auditing Tool", 2019. [Online]. Disponible: https://www.manageengine.com/products/active-directory-audit/windows-server-auditing.html. [Revisado: 10-Jul-2019]

[7] Ralco Networks, "Auditoria y Gestión de Redes", 2019. [Online]. Disponible: http://www.ralco-networks.com/servicios/auditoria-y-gestion-de-redes/. [Revisado: 10-Jul-2019]

[8] ISO Tools, "Software ISO 27001", 2019. [Online]. Disponible: https://www.isotools.org/software/riesgos-y-seguridad/iso-27001. [Revisado: 10-Jul-2019]

[9] Manage Engine, 2020 [Online]. Disponible: https://www.manageengine.com/. [Revisado: 25-Abr-2020]

[10] Microsoft, "Introducción a Active Directory", 2000. [Online]. Disponible: https://support.microsoft.com/es-pe/help/196464. [Revisado: 10-Jul-2019]

[11] Comité de Conceptos de Auditoría, Asociación Estadounidense de Contabilidad, "Informe del Comité de Conceptos Básicos de Auditoría", The Accounting Review, 1971.

[12] Proofpoint (2019). State of the pish annual report. Disponible: https://www.wombatsecurity.com/state-of-the-phish [Revisado: 08-Dic-2019]

[13] Internet Engineering Task Force (1983). Telnet Protocol Specifications. Disponible: https://tools.ietf.org/html/rfc854. [Revisado: 10-Ene-2020]

[14] Concept Draw, Odessa. Active Directory Diagram. Disponible: https://www.conceptdraw.com/examples/active-directory-structure. [Revisado: 10-Ene-2020]

[15] Tutlane. Visual Basic Classes and Objects. Disponible: https://www.tutlane.com/tutorial/visual-basic/vb-classes-and-objects. [Revisado: 10-Jun-2020]

[16] Buildmedia. Python-ldap Documentation. Disponible: https://buildmedia.readthedocs.org/media/pdf/python-ldap/python-ldap-3.0.0/python-ldap.pdf. [Revisado: 3-Nov-2019]

[17] Techdocs, Palo Alto Networks. Explore the API. Disponible: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-panorama-api/get-started-with-the-pan-os-xml-api/explore-the-api.html. [Revisado: 3-Nov-2019]

[18] Pavan, Ramchandani., Deepika, Naik (2019). *Active Directory Administration Cookbook.* (1ra ed). Reino Unido: Birmingham.

[19] Vietes G, Álvaro (2014). *Auditoria de Seguridad Informática.* (1ra ed). España: Madrid.

[20] Data-flair. Java Method – Declaring and Calling Method with Example. Disponible: https://data-flair.training/blogs/java-method/. [Revisado: 2-Jun-2020]

[21] Arcadier. Introduction to Arcadier´s APIs. Disponible: https://api.arcadier.com/introduction-to-arcadier-api. [Revisado: 3-Jun-2020]

[22] Stair, Ralph M., Reynolds, George (2010). *Principios de sistemas de la información*. (9na ed). México: Cengage.

[23] ISO Tools, "Software ISO Riesgos y Seguridad", 2019. [Online]. Disponible: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/. [Revisado: 13-Jun-2020]

[24] Advisera, "¿Qué es norma ISO 27001?", 2019. [Online]. Disponible: https://advisera.com/27001academy/es/que-es-iso-27001/. [Revisado: 15-Jun-2020]

[25] Peritoit, "ISO/IEC 27037:2012 Nueva norma para la recopilación de Evidencias" 2012. [Online]. Disponible: https://peritoit.com/2012/10/23/isoiec-270372012-nueva-norma-para-la-recopilacion-de-evidencias/. [Revisado: 15-Jun-2020]

[26] ISO, "Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence" 2015. [Online]. Disponible: https://www.iso.org/standard/44406.html. [Revisado: 18-Jun-2020]