DESARROLLAR UN ANÁLISIS DE VULNERABILIDADES EN COOPERATIVA ALIANZA, PARA LA IDENTIFICACIÓN Y CORRECCIÓN DE LAS VULNERABILIDADES Y ACCESOS NO AUTORIZADOS A LOS DIFERENTES SISTEMAS DE INFORMACIÓN

MARIO ANDRÉS CERVANTES MORENO

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2018

DESARROLLAR UN ANÁLISIS DE VULNERABILIDADES EN COOPERATIVA ALIANZA, PARA LA IDENTIFICACIÓN Y CORRECCIÓN DE LAS VULNERABILIDADES Y ACCESOS NO AUTORIZADOS A LOS DIFERENTES SISTEMAS DE INFORMACIÓN.

MARIO ANDRÉS CERVANTES MORENO

Proyecto para optar por título de especialista en seguridad informática

Ing. Álvaro Escobar Escobar
Director Especialización en Seguridad Informática

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2018

Nota de Aceptación

_____

_____

_____

_____
Firma presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá D.C., enero de 2018

DEDICATORIA

A mi amada esposa Martha Elena Flórez Bahamón gracias por su apoyo incondicional, confianza, paciencia y consejos brindados a través de los cuales contribuyó a la realización de este trabajo.

A mis hijos Nicolás, Daniel Andrés y Ana María quienes, con su apoyo y amor incondicional, me han dado la inspiración y fuerza para mi continuo desarrollo personal y profesional.

A mi madre Amira Moreno Triviño por apoyo constante en todas las etapas de mi vida.

AGRADECIMIENTOS

A la Cooperativa Alianza, en cabeza de su gerente Juan Carlos Borda Fernández quien facilitó la infraestructura necesaria para realizar este análisis de vulnerabilidades.

Al Ing. Álvaro Escobar Escobar, Director de Tesis; por su ayuda, interés y colaboración para la realización de este trabajo.

CONTENIDO

LISTA DE FIGURAS

pág.

LISTA DE TABLAS

LISTA DE CUADROS

GLOSARIO[1]

ADWARE*:* Adware es un software, generalmente no deseado, que facilita el envío de contenido publicitario a un equipo[2].

AMENAZA: Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS)[3].

AMENAZAS POLIMORFAS: Las amenazas polimorfas son aquellas que tienen la capacidad de mutar y en las cuales cada instancia del malware es ligeramente diferente al anterior a este. Los cambios automatizados en el código realizados a cada instancia no alteran la funcionalidad del malware, sino que prácticamente inutilizan las tecnologías tradicionales de detección antivirus contra estos ataques[4].

ANTISPAM: Antispam es un producto, herramienta, servicio o mejor práctica que detiene el spam o correo no deseado antes de que se convierta en una molestia para los usuarios. El antispam debe ser parte de una estrategia de seguridad multinivel.[5]

ANTIVIRUS: Antivirus es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles[6].

APLICACIONES ENGAÑOSAS: Las aplicaciones engañosas son programas que intentan engañar a los usuarios informáticos para que emprendan nuevas acciones que normalmente están encaminadas a causar la descarga de malware adicional o para que los usuarios divulguen información personal confidencial. Un

---

[1] SYMANTEC. Glosario de Seguridad 101 [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad

[2] SPYWARE. ¿Qué es adware? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.segu-info.com.ar/malware/spyware.htm

[3] CYIDIGITAL. ¿Qué es amenaza? ? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.cyldigital.es/articulo/amenazas-en-internet

[4] ECURED. ¿Qué son amenazas polimorfas? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.ecured.cu/ Amenazas _polimorfas

[5] ABARTIATEAM. ¿Qué es antispam?. [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: www.abartiateam.com/antispam-antivirus

[6] DEFINICIONES ABC. ¿Qué significa antivirus?. ?. [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.definicionabc.com/tecnologia/antivirus.php

ejemplo es el software de seguridad fraudulento, que también se denomina scareware.[7]

ATAQUES MULTI-ETAPAS: Un ataque en múltiples etapas es una infección que normalmente implica un ataque inicial, seguido por la instalación de una parte adicional de códigos maliciosos. Un ejemplo es un troyano que descarga e instala adware[8].

ATAQUES WEB: Un ataque Web es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta[9].

BLACKLISTING O LISTA NEGRA: La lista negra es el proceso de identificación y bloqueo de programas, correos electrónicos, direcciones o dominios IP conocidos maliciosos o malévolos[10].

BOT: Un bot es una computadora individual infectada con malware, la cual forma parte de una red de bots (bot net)[11].

BOTNET: Conjunto de equipos bajo el control de un bot maestro, a través de un canal de mando y control. Estos equipos normalmente se distribuyen a través de Internet y se utilizan para actividades malintencionadas, como el envío de spam y ataques distribuidos de negación de servicio. Las botnet se crean al infectar las computadoras con malware, lo cual da al atacante acceso a las máquinas. Los propietarios de computadoras infectadas generalmente ignoran que su máquina

---

[7] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN. ¿Qué son Aplicaciones engañosas? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: www.mintic.gov.co/ portal/ 604/w3-article-18745.html.

[8] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN. **¿Qué son ataques multi-etapas?** [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: www.mintic.gov.co/portal/ 604/w3-article-18750.html

[9] REVISTA DE SEGURIDAD UNAM. ¿Qué son Ataques WEB? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://revista.seguridad.unam.mx/numero-05/ataques-web

[10] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN. ¿Qué es Blacklisting o lista negra? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: www.mintic.gov. co/portal/ 604/w3-article-18749.html.

[11] CNET. ¿Qué es un bot? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.cnet.com/es/como-se-hace/que-es-un-bot/

forma parte de una botnet, a menos que tengan software de seguridad que les informe acerca de la infección[12].

CABALLO DE TROYA: Son un tipo de código malicioso que parece ser algo que no es. Una distinción muy importante entre troyanos y virus reales es que los troyanos no infectan otros archivos y no se propagan automáticamente. Los caballos de troya tienen códigos maliciosos que cuando se activan causa pérdida, incluso robo de datos. Por lo general, también tienen un componente de puerta trasera, que le permite al atacante descargar amenazas adicionales en un equipo infectado. Normalmente se propagan a través de descargas inadvertidas, archivos adjuntos de correo electrónico o al descargar o ejecutar voluntariamente un archivo de Internet, de manera general después de que un atacante ha utilizado ingeniería social para convencer al usuario de que lo haga[13].

CANAL DE CONTROL Y COMANDO: Un canal de mando y control es el medio por el cual un atacante se comunica y controla los equipos infectados con malware, lo que conforma un botnet.

CARGA DESTRUCTIVA: Una carga destructiva es la actividad maliciosa que realiza el malware. Una carga destructiva es independiente de las acciones de instalación y propagación que realiza el malware[14].

CRIMEWARE: Software que realiza acciones ilegales no previstas por un usuario que ejecuta el software. Estas acciones buscan producir beneficios económicos al distribuidor del software[15].

CIBERDELITO: El ciberdelito es un delito que se comete usando una computadora, red o hardware. La computadora o dispositivo puede ser el agente, el facilitador o el objeto del delito. El delito puede ocurrir en la computadora o en otros lugares[16].

---

[12] SOFTDOIT. ¿Qué es Botnet? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.softwaredoit.es/definicion/definicion-botnet.html

[13] ECURED. ¿Qué es caballo de troya? Qué es Botnet? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://techlandia.com/definicion-del-virus-informatico-caballo-troya-sobre_54996/

[14] SEGURIDAD INFORMÁTICA. ¿Qué es Carga destructiva? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://seguinfo.wordpress.com/2009/04/06/ ¿carga destructiva?/

[15] ¿Qué es Crimeware? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://seguinfo.wordpress.com/2009/04/06/ ¿que-es-crimeware/

[16] SEO. ¿Qué es ciberdelitos? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: www.seo-posicionamientoweb.com/ciberdelitos-definicion-tipos-frecuentes

DEFINICIONES DE VIRUS: Una definición de virus es un archivo que proporciona información al software antivirus, para identificar los riesgos de seguridad. Los archivos de definición tienen protección contra todos los virus, gusanos, troyanos y otros riesgos de seguridad más recientes. Las definiciones de virus también se denominan firmas antivirus.[17]

DESCARGA INADVERTIDA: Una descarga inadvertida es una descarga de malware mediante el ataque a una vulnerabilidad de un navegador Web, equipo cliente de correo electrónico o plug-in de navegador sin intervención alguna del usuario. Las descargas inadvertidas pueden ocurrir al visitar un sitio Web, visualizar un mensaje de correo electrónico o pulsar clic en una ventana emergente engañosa[18].

ECONOMÍA CLANDESTINA: La economía clandestina en línea es el mercado digital donde se compran y se venden bienes y servicios obtenidos a través de la ciberdelincuencia, con el fin de cometer delitos informáticos. Dos de las plataformas más comunes a disposición de los participantes en la economía clandestina en línea son los canales en servidores IRC y foros Web. Los dos tienen grupos de discusión que utilizan participantes para comprar y vender bienes y servicios fraudulentos. Los artículos vendidos son datos de tarjetas de crédito, información de cuentas bancarias, cuentas de correo electrónico y toolkits de creación de malware. Los servicios incluyen cajeros que pueden transferir fondos de cuentas robadas en moneda real, phishing y hosting de páginas fraudulentas y anuncios de empleo para cargos como desarrolladores de fraude o socios de phishing.[19]

ENCRIPTACIÓN: La encriptación es un método de cifrado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña o clave pueden descifrar y utilizar los datos. A veces, el malware utiliza la encriptación para ocultarse del software de seguridad. Es decir, el malware cifrado revuelve el código del programa para que sea difícil detectarlo[20].

[17] INFOSPYWARE. ¿Qué son los virus informáticos? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.infospyware.com/articulos/ ¿que-son-los-virus-informaticos/

[18] WIKISEGURIDAD. ¡Qué es descarga inadvertida? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: wikiseguridad.org/descarga-inadvertida

[19] EL UNIVERSAL. ¡Qué es economía clandestina? [En línea], [consultado el 3 de septiembre de 2017]. en: interactivo.eluniversal.com.mx/online/PDF.../PDF-ECONOMÍA CLANDESTINA.pdf

[20] CULTURACIÓN. ¿Qué es encriptación? [En línea], [consultado el 3 de septiembre de 2017]. en: culturacion.com/que-es-encriptación-o-cifrado-de-archivos/

EXPLOITS O PROGRAMAS INTRUSOS: Los programas intrusos son técnicas que aprovechan las vulnerabilidades del software y que pueden utilizarse para evadir la seguridad o atacar un equipo en la red[21].

FILTRACIÓN DE DATOS: Una filtración de datos sucede cuando se compromete un sistema, exponiendo la información a un entorno no confiable. Las filtraciones de datos a menudo son el resultado de ataques maliciosos, que tratan de adquirir información confidencial que puede utilizarse con fines delictivos o con otros fines malintencionados[22]

FIREWALL: Un firewall es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles[23].

FIRMA ANTIVIRUS: Una firma antivirus es un archivo que proporciona información al software antivirus para encontrar y reparar los riesgos. Las firmas antivirus proporcionan protección contra todos los virus, gusanos, troyanos y otros riesgos de seguridad más recientes. Las firmas antivirus también se denominan definiciones de virus[24].

GREYLISTING O LISTA GRIS: La lista gris es un método de defensa para proteger a los usuarios de correo electrónico contra el spam. Los mensajes de correo electrónico son rechazados temporalmente de un remitente que no es reconocido por el agente de transferencia de correos. Si el correo es legítimo, el servidor de origen tratará de nuevo y se aceptará el correo electrónico. Si el correo es de un remitente de spam, probablemente no se reintentará su envío y, por lo tanto, no logrará pasar el agente de transferencia de correos[25].

---

[21]MINISTERIO DE LA TECNOLOGÍA DE LA INFORMACIÓN Y DE LAS COMUNICACIONES. ¿Qué son Exploits o Programas intrusos? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: www.mintic.gov.co/portal/604/w3-article-18797.html

[22] TIBCO SOFTWARE. **Filtrado de datos.** [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://docs.tibco.com/.../GUID-6CF74B7C-9425-4BDE-B8C4-F9F45B1F1710.html

[23] REVISTA UNAM. ¿Qué es Firewall? https://revista.seguridad.unam.mx/numero-18/firewall-de-bases-de-datos

[24] WELIVESECURITY. ¿Qué significa firma antivirus? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.welivesecurity.com/la-es/2014/.../cumplimos-10000-faq-firmas-antivirus/

[25] HOSTING MONTEVIDEO. Greylisting o lista gris. [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.hostingmontevideo.com/clientes/index. php?rp=/.../82/ Greylisting.html

GUSANOS: Los gusanos son programas maliciosos que se reproducen de un sistema a otro sin usar un archivo anfitrión, lo que contrasta con los virus, puesto que requieren la propagación de un archivo anfitrión infectado[26].

INGENIERÍA SOCIAL: Método utilizado por los atacantes para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas, como la descarga de malware o la divulgación de información personal. Los ataques de phishing con frecuencia aprovechan las tácticas de ingeniería social.[27]

LISTA BLANCA O WHITELISTING: La lista blanca es un método utilizado normalmente por programas de bloqueo de spam, que permite a los correos electrónicos de direcciones de correo electrónicos o nombres de dominio autorizados o conocidos pasar por el software de seguridad[28].

KEYSTROKE LOGGER O PROGRAMA DE CAPTURA DE TECLADO (Keylogger): Es un tipo de malware diseñado para capturar las pulsaciones, movimientos y clics del teclado y del ratón, generalmente de forma encubierta, para intentar robar información personal, como las cuentas y contraseñas de las tarjetas de crédito[29].

MALWARE: El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer fechorías[30].

---

[26] KAPERSKY. ¿Qué son gusanos cibernéticos? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.kaspersky.es/resource-center/threats/viruses-worms

[27] ENTER.CO. ¿Qué es ingeniería social? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/

[28] ONIUP.COM. ¿Qué es lista blanca o whitelisting?? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://oniup.com/que-es/white-list/

[29] MINISTERIO DE LA TECNOLOGÍA DE LA INFORMACIÓN Y DE LAS COMUNICACIONES. ¿Qué es Keystroke Logger o Programa de captura del teclado? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: www.mintic.gov.co/portal/604/w3-article-18802.html

[30] GENBETA.COM. ¿Qué significa Malware? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.genbeta.com/.../malwarebytes-quiere-reemplazar-tu-antivirus-de-siempre.

MECANISMO DE PROPAGACIÓN: Un mecanismo de propagación es el método que utiliza una amenaza para infectar un sistema[31].

NEGACIÓN DE SERVICIO (DoS): La negación de servicio es un ataque en el que el delincuente intenta deshabilitar los recursos de una computadora o lugar en una red para los usuarios. Un ataque distribuido de negación de servicio (DDoS) es aquel en que el atacante aprovecha una red de computadoras distribuidas, como por ejemplo una botnet, para perpetrar el ataque[32].

PHARMING: Método de ataque que tiene como objetivo redirigir el tráfico de un sitio Web a otro sitio falso, generalmente diseñado para imitar el sitio legítimo. El objetivo es que los usuarios permanezcan ignorantes del redireccionamiento e ingresen información personal, como la información bancaria en línea, en el sitio fraudulento. Se puede cometer pharming cambiando el archivo de los equipos anfitriones en la computadora de la víctima o atacando una vulnerabilidad en el software del servidor DNS[33].

PHISHING: A diferencia de la heurística o los exploradores de huella digital, el software de seguridad de bloqueo de comportamiento se integra al sistema operativo de un equipo anfitrión y supervisa el comportamiento de los programas en tiempo real en busca de acciones maliciosas. El software de bloqueo de comportamiento bloquea acciones potencialmente dañinas, antes de que tengan oportunidad de afectar el sistema. La protección contra el comportamiento peligroso debe ser parte de una estrategia de seguridad estándar de múltiples niveles[34].

PROTECCIÓN HEURÍSTICA (Heuristics-Based Protection): Forma de tecnología antivirus que detecta las infecciones mediante el escrutinio de la estructura general de un programa, las instrucciones de sus computadoras y otros datos contenidos en el archivo. Una exploración heurística hace una evaluación sobre la probabilidad de que el programa sea malicioso con base en la aparente intención de la lógica. Este plan puede detectar infecciones desconocidas, ya que busca lógica generalmente sospechosa, en lugar de huellas específicas de malware, tales como los métodos tradicionales de antivirus de firmas. La

---

[31] MINISTERIO DE LA TECNOLOGÍA DE LA INFORMACIÓN Y DE LAS COMUNICACIONES. ¿Qué es, mecanismo de propagación? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: www.mintic.gov.co/portal/604/w3-article-18804.html

[32] WEBSECURITY. ¿Qué es un ataque de negación de servicio? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: www.websecurity.es/que-es-un-ataque-denegaci-n-servicio

[33] SYMANTEC. ¿Qué es pharming? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en:www.symantec.com/region/mx/avcenter/cybercrime/pharming.html

[34] INFOSPYWARE. ¿Qué es el phishing? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.infospyware.com/articulos/que-es-el-phishing/

protección heurística debería hacer parte de una estrategia de seguridad estándar de múltiples niveles[35]

REDES PUNTO A PUNTO (P2P): Red virtual distribuida de participantes que hacen que una parte de sus recursos informáticos estén a disposición de otros participantes de la red, todo sin necesidad de servidores centralizados. Las redes puntos a punto son utilizadas para compartir música, películas, juegos y otros archivos. Sin embargo, también son un mecanismo muy común para la distribución de virus, bots, spyware, adware, troyanos, rootkits, gusanos y otro tipo de malware[36].

ROOTKITS: Componente de malware que utiliza la clandestinidad para mantener una presencia persistente e indetectable en un equipo. Las acciones realizadas por un rootkit, como la instalación y diversas formas de ejecución de códigos, se realizan sin el conocimiento o consentimiento del usuario final[37].

Los rootkits no infectan las máquinas por sí mismos como lo hacen los virus o gusanos, sino que tratan de proporcionar un entorno indetectable para ejecutar códigos maliciosos. Los atacantes normalmente aprovechan las vulnerabilidades en el equipo seleccionado o utilizan técnicas de ingeniería social para instalar manualmente los rootkits. O, en algunos casos, los rootkits pueden instalarse automáticamente al ejecutarse un virus o gusano o incluso simplemente al navegar en un sitio Web malicioso.

Una vez instalados, el atacante puede realizar prácticamente cualquier función en el sistema, incluyendo acceso remoto, intercepción de comunicaciones, así como procesos de ocultamiento, archivos, claves de registro y canales de comunicación.

SEGURIDAD BASADA EN LA REPUTACIÓN: La seguridad basada en la reputación es una estrategia de identificación de amenazas que clasifica las aplicaciones con base en ciertos criterios o atributos para determinar si son probablemente malignas o benignas. Estos atributos pueden incluir diversos aspectos como la edad de los archivos, la fuente de descarga de los archivos y la prevalencia de firmas y archivos digitales. Luego, se combinan los atributos para determinar la reputación de seguridad de un archivo. Las calificaciones de reputación son utilizadas después por los usuarios informáticos para determinar mejor lo que es seguro y permitirlo en sus sistemas. La seguridad basada en la

---

[35] PANDA SECURITY. ¿Qué es **PROTECCIÓN HEURÍSTICA?** [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.pandasecurity.com/enterprise/ downloads/ docs/product/...00.../582.htm

[36] ECURED. ¿Que son redes punto a punto? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.ecured.cu/Redes_punto_a_punto

[37] AVAST. ¿Qué son rootkit? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.avast.com/es-es/c-rootkit

reputación debe ser parte de una estrategia de seguridad estándar de múltiples niveles[38].

SISTEMA DE DETECCIÓN DE INTRUSOS: Un sistema de detección de intrusos es un servicio que monitorea y analiza los eventos del sistema para encontrar y proporcionar en tiempo real o casi real advertencias de intentos de acceso a los recursos del sistema de manera no autorizada. Es la detección de ataques o intentos de intrusión, que consiste en revisar registros u otra información disponible en la red. Un sistema de detección de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles.[39]

SISTEMA DE PREVENCIÓN DE INTRUSOS: Un sistema de prevención de intrusos es un dispositivo (hardware o software) que supervisa las actividades de la red o del sistema en busca de comportamiento no deseado o malicioso y puede reaccionar en tiempo real para bloquear o evitar esas actividades. Un sistema de prevención de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles[40].

SOFTWARE DE SEGURIDAD FRAUDULENTO (rogue): Un programa de software de seguridad rogue es un tipo de aplicación engañosa que finge ser software de seguridad legítimo, como un limpiador de registros o detector antivirus, aunque realmente proporciona al usuario poca o ninguna protección y, en algunos casos, puede de hecho facilitar la instalación de códigos maliciosos contra los que busca protegerse.[41]

SPAM: También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. Un sinónimo común de spam es correo electrónico comercial no solicitado (UCE). El malware se utiliza a menudo para propagar mensajes de spam al infectar un equipo, buscar direcciones de correo electrónico y luego utilizar esa máquina para enviar mensajes de spam. Los mensajes de spam generalmente se utilizan como un método de propagación de los ataques de phishing[42]

---

[38] REDES TELECOM. Seguridad basada en la reputación. [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: www.redestelecom.es › Noticias › Informática Profesional

[39] VELAVERDE, Mario. Sistema de detección de intrusos. [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: www.aslan.es/boletin/boletin41/ironport.shtml

[40] PANDA SECURITY. Sistema de prevención de intrusos. [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.pandasecurity.com/usa-es/support/ card?id= 31452

[41] INFOSPYWARE. ¿Qué es software de seguridad fraudulento? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.infospyware.com/articulos/rogue-software-fakeav/

[42] VALOR TOP. ¿Qué es Spam? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: www.valortop.com/blog/que-significa-spam

SPYWARE: Paquete de software que realiza un seguimiento y envía información de identificación personal o información confidencial a otras personas. La información de identificación personal es la información que puede atribuirse a una persona específica, como un nombre completo. La información confidencial incluye datos que la mayoría de las personas no estaría dispuesta a compartir con nadie e incluye datos bancarios, números de cuentas de tarjeta de crédito y contraseñas. Los receptores de esta información pueden ser sistemas o partes remotas con acceso local[43].

TOOLKIT: Paquete de software diseñado para ayudar a los hackers a crear y propagar códigos maliciosos. Los toolkits frecuentemente automatizan la creación y propagación de malware al punto que, incluso los principiante delincuentes cibernéticos son capaces de utilizar amenazas complejas. También pueden utilizarse toolkits para lanzar ataques web, enviar spam y crear sitios de phishing y mensajes de correo electrónico[44].

VARIANTES: Las variantes son nuevas cepas de malware que piden prestado código, en diversos grados, directamente a otros virus conocidos. Normalmente se identifican con una letra o letras, seguido del apellido del malware; por ejemplo, W32.Downadup. A, W32.Downadup. B y así sucesivamente[45].

VECTOR DE ATAQUE: Un vector de ataque es el método que utiliza una amenaza para atacar un sistema.[46]

VIRUS: Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario. Un virus debe cumplir con dos criterios:[47]

Debe ejecutarse por sí mismo: generalmente coloca su propio código en la ruta de ejecución de otro programa.

---

[43] DEFINICION. Spyware. [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://definicion.de/spyware/

[44] FACEBOOK. ¿Qué significa Toolkit? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.facebook.com/toolkitfotografia/

[45] MALWAREBYTES. ¿Que son variantes? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://es.malwarebytes.com/pdf/white-papers/es/DefeatingRansomware.pdf

[46] DHAVE SECURITY. ¿Qué es vector de ataque a WPA2? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.facebook.com/DhavidSegundo/photos/a.../1444726995576688/?type=3

[47] SMARTERWORKSPACES. ¿Qué es virus? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://smarterworkspaces.kyocera.es/blog/8-tipos-virus-informaticos-debes-conocer/

Debe reproducirse: por ejemplo, puede reemplazar otros archivos ejecutables con una copia del archivo infectado por un virus. Los virus pueden infectar computadores de escritorio y servidores de red.

Muchos de los virus actuales están programados para operar sigilosamente la computadora del usuario con el fin de robar información personal y utilizarla para cometer delitos. Otros menoscaban el equipo dañando los programas, eliminando archivos o volviendo a formatear el disco duro. Aún existen otros que no están diseñados para causar daño, aunque simplemente se reproducen y hacen manifiestan su presencia presentando mensajes de texto, video y audio, aunque este tipo de ataques de notoriedad no son tan comunes, puesto que los autores de virus y demás malware tiene como fin obtener ganancias ilegales.

VULNERABILIDAD: Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad (CIA) de los sistemas. Las vulnerabilidades pueden hacer lo siguiente[48]:

Permitir que un atacante ejecute comandos como otro usuario

Permitir a un atacante acceso a los datos, lo que se opone a las restricciones específicas de acceso a los datos

Permitir a un atacante hacerse pasar por otra entidad

Permitir a un atacante realizar una negación de servicio

[48] INFOSEGUR. ¿Qué es Vulnerabilidad? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://infosegur.wordpress.com/tag/vulnerabilidades/

INTRODUCCIÓN

Hablar de seguridad informática, implica entender que un sistema de información nunca podrá ser completamente seguro e inmune a ataques, no obstante, es importante reconocer que uno de los activos más importantes que tiene una organización es su información y por ende se debe dar un manejo apropiado a la misma, ya que esta es de vital importancia para las operaciones diarias y la adecuada continuidad de negocio.

Actualmente la información almacenada en las organizaciones está expuesta a múltiples amenazas, en un mundo donde la tecnología avanza aceleradamente, implicando esto un desarrollo en los sistemas de seguridad para disminuir el impacto y probabilidad de un ataque cibernético.

Por lo anterior, Cooperativa Alianza, consciente de los riesgos a los que está expuesta, decidió realizar un hacking ético, donde se identificarán las principales vulnerabilidades que tienen los sistemas de información, buscando obtener los planes de acción necesarios que conlleven a las remediaciones correspondientes, de esta manera minimizar los riesgos a un nivel aceptable, identificando las oportunidades de mejora y garantizando el cumplimiento de los pilares de Seguridad de la Información, Confidencialidad, Integridad y Disponibilidad.

1. TITULO DE TRABAJO

DESARROLLAR UN ANÁLISIS DE VULNERABILIDADES EN COOPERATIVA ALIANZA, PARA LA IDENTIFICACIÓN Y CORRECCIÓN DE LAS VULNERABILIDADES Y ACCESOS NO AUTORIZADOS A LOS DIFERENTES SISTEMAS DE INFORMACIÓN.

2. FORMULACIÓN

2.1 PLANTEAMIENTO DEL PROBLEMA

Una vulnerabilidad se puede definir como una debilidad que compromete la integridad, confidencialidad y disponibilidad del sistema informático, con la aplicación de un análisis de vulnerabilidades para Cooperativa Alianza, se obtendrá una relación de las debilidades encontradas, verificando si existe algún control que mitigue dicha vulnerabilidad que permitan la mitigación del impacto o la probabilidad manteniendo los niveles de exposición en rangos aceptables para la organización.

2.2 FORMULACIÓN

¿Cuáles son las debilidades en los diferentes accesos a los sistemas de información de Cooperativa Alianza?

2.3 OBJETIVOS

2.3.1 Objetivo general.

Desarrollar un análisis de vulnerabilidades en Cooperativa Alianza, que permitirá su identificación en cuanto a accesos no autorizados, definiendo los planes de acción necesarios para mitigar estas debilidades.

2.3.2 Objetivos específicos

- Realizar un análisis interno y externo que permita identificar las debilidades de seguridad existentes para Cooperativa Alianza.

- Proponer recomendaciones que permitan mitigar y/o eliminar las vulnerabilidades.

- Sensibilizar a los funcionarios y directivos de Cooperativa Alianza en las debilidades encontradas, para lograr una conciencia general en la importancia de la seguridad informática.

2.4 JUSTIFICACIÓN

Según una publicación de la revista welivesecurity.com[49], donde se destaca un incremento entre las empresas que afirmaron ser víctimas de algún ciber ataque, pasando de 75% en el año 2013 al 78% en el año 2015, La mayoría de estos son causados por la falta de conocimiento de sus vulnerabilidades y falta de conocimiento sobre cómo prevenir o defenderse ante dichos ataques.

No es nuevo que la tecnología avanza de una manera sumamente rápida, aunque este avance en campos científicos es muy bueno, también tiene sus desventajas, ya que por esta razón los atacantes se aprovechan de la nueva tecnología, los conocimientos y habilidades, realizando diferentes ataques para perjudicar una organización, teniendo consecuencias de alto impacto, tales como: mala reputación de la organización, pérdida de información, pérdida de clientes, pérdida de dinero entre otras.

En Cooperativa Alianza, la información de los asociados es su activo más importante, por lo cual debe garantizar todas las medidas de protección necesarias para prevenir el acceso no autorizado y generar confianza con los mismos.

Con el desarrollo de análisis de vulnerabilidades es posible realizar un escaneo general que permita determinar las debilidades en los siguientes aspectos:

- Configuraciones no adecuadas en los equipos de cómputo, switch, firewall, etc.

- Sistemas de información que poseen vulnerabilidades por la no actualización de los mismos.

- Falta de conciencia en el personal de la organización

Una vez logren identificar las diferentes debilidades, es necesario generar un plan de acción que permita la corrección de las vulnerabilidades detectadas, permitiendo que Cooperativa Alianza cumpla con la protección necesaria en la información de sus asociados.

Una vez concluido el análisis, Cooperativa Alianza tendrá un panorama más claro sobre las debilidades a las que estaba expuesta, así como el tratamiento respectivo para mitigar estas vulnerabilidades.

[49] WELIVESECURITY.COM. ¿Cómo gestionan la seguridad las empresas en Latinoamérica? [En línea], [consultado el 21 de abril de 2016]. Disponible en: http://www.welivesecurity.com/la-es/2016/04/21/como-gestionan-seguridad-empresas-de-latinoamerica/

2.5 TIPO DE INVESTIGACIÓN

El tipo de investigación que se usará en el desarrollo de este proyecto es: Investigación Descriptiva, porque a través de esta metodología se logra generar conocimiento a través de los datos recolectados con el análisis minucioso de la información recolectada.

2.6 HIPÓTESIS

HI: A partir de un análisis de vulnerabilidades, es posible determinar las vulnerabilidades a las que se encuentra expuesta Cooperativa Alianza, y así determinar los planes de mitigación necesarios.

HO: A partir de un análisis de vulnerabilidades, no es posible determinar las vulnerabilidades a las que se encuentra expuesta Cooperativa Alianza, y no se determinarán los planes de mitigación necesarios.

2.7 VARIABLES

2.7.1 Variables independientes

- Hacking ético

2.7.2 Variables dependientes

- Amenazas detectadas
- Planes de Acción
- Controles por implantar

3. MARCO REFERENCIAL

3.1 MARCO TEÓRICO

3.1.1. Metodologías de Análisis. Para realizar el análisis de vulnerabilidades en cooperativa alianza, es necesario contar con una metodología, en el mercado existen varias que han sido desarrolladas por organizaciones que reúnen diferentes expertos y formalizan una serie de pasos estructurados para realizar el análisis, para este proyecto se realizó el análisis a 3 metodologías:

Web Application test methodology OWASP

Penetration testing execution standard PTES

Open Source Security Testing Methodology Manual OSSTMM

A continuación, se relaciona una descripción de las tres metodologías para identificar cual es la más apropiada

3.1.1.1 OWASP *(Web application test methodology)*[50]. Es una metodología desarrollada por OWASP (*Open web application security Project*), la cual busca identificar vulnerabilidades en aplicaciones web, basada en el método de caja negra, donde no se tiene información de la plataforma a la que se realizará el análisis buscando obtener la mayor información del objetivo sin información previa., la prueba está dividida en 2 fases

Fase Pasiva: en esta fase se trata de comprender la lógica que tiene la aplicación, recopilando toda la información posible observando todas las solicitudes y respuestas http, para entender todos los puntos de acceso a la aplicación.

Fase Activa: en esta fase se desarrolla la metodología siguiendo estas categorías

[50]OWASP. Web Application Penetration Testing. [En línea], [consultado el 20 de agosto de 2017]. Disponible en: https://www.owasp.org/index.php/Web_Application_Penetration_Testing

Testing Information Gathering. Se trata de obtener la mayor cantidad de información disponible acerca del sitio, esta a su vez se divide en 10 categorías que permiten obtener información del sitio, como se puede observar en la Tabla 1.

Tabla 1. *OWASP Testing Information Gathering*

Testing Information Gathering
Conduct search engine discovery/reconnaissance for information leakage
Fingerprint Web Server
Review Webserver Metafiles for Information Leakage
Enumérate Applications on Webserver
Review webpage comments and metadata for information leakage
Identify application entry points
Map execution paths through application
Fingerprint Web Application Framework
Fingerprint Web Application
Map Application Architecture
Fuente: https://www.owasp.org/index.php/Testing_Information_Gathering

Testing for Configuration management. Entender cómo está la configuración del servidor es igual de importante a la prueba de la aplicación web, dado que algunos errores de configuración pueden comprometer la seguridad de la aplicación, por tal razón se incluyen las siguientes etapas como se puede observar en la tabla 2:

Tabla 2. *OWASP Testing for configuration management*

Testing for configuration management
Test Network/Infrastructure Configuration
Test Application Platform Configuration
Test File Extensions Handling for Sensitive Information
Review Old, Backup and Unreferenced Files for Sensitive Information
Enumerate Infrastructure and Application Admin Interfaces
Test HTTP Methods
Test HTTP Strict Transport Security
Test RIA cross domain policy
Fuente: https://www.owasp.org/index.php/Testing_Information_Gathering

Identity Management Testing. El manejo de identidades y accesos a la aplicación y la seguridad y complejidad de las contraseñas requeridas pueden ser una gran amenaza a la seguridad de todo el sistema, en la tabla 3 se puede observar las categorías en la cuales está dividida:

Tabla 3. *OWASP Identity Management Testing*

OWASP Identity Management Testing
Test Role Definitions
Test User Registration Process
Test Account Provisioning Process
Testing for Account Enumeration and Guessable User Account
Testing for Weak or unenforced username policy
Fuente: https://www.owasp.org/index.php/Testing_Information_Gathering

***Authentication Testing*.** Autenticar es poder determinar la identidad digital del remitente del mensaje, en esta categoría se debe probar los esquemas de autenticación del sitio y tratar de eludir los mecanismos definidos para ingresar al sistema sin el uso de credenciales autorizadas, en la tabla 4 se observa las etapas en las que se divide este punto:

Tabla 4. *OWASP Authentication Testing*

Authentication Testing
Testing for Credentials Transported over an Encrypted Channel
Testing for default credential
Testing for Weak lock out mechanism
Testing for bypassing
Test remember password functionality
Testing for Browser cache weakness
Testing for Weak password policy
Testing for Weak security question/answer
Testing for weak password change or reset functionalities
Testing for Weaker authentication in alternative channel
Fuente: https://www.owasp.org/index.php/Testing_Information_Gathering

Authorization Testing. La autorización es el proceso mediante el cuales se autoriza o no el acceso a los recursos, se ejecuta posterior a la validación de la identidad, en esta categoría se debe entender cómo funciona el proceso de autorización y eludir el mecanismo para tener acceso a los recursos sin el proceso de validación, en la tabla 5 de observa cómo se divide en las siguientes etapas:

Tabla 5*. OWASP Authorization Testing*

Authorization Testing
Testing Directory traversal/file include
Testing for bypassing authorization schema
Testing for Privilege Escalation
Testing for Insecure Direct Object References
Fuente: https://www.owasp.org/index.php/Testing_Information_Gathering

Session Management Testing. La gestión de sesiones es el procedimiento por el cual se controla y mantiene una conexión entre el usuario y la aplicación, desde su autenticación hasta el cierre de sesión, se divide en las siguientes etapas como se puede observar en la tabla 6:

Tabla 6. *OWASP Session Management Testing*

Session Management Testing
Testing for Bypassing Session Management Schema
Testing for Cookies attributes las cookies
Testing for Session Fixation
Testing for Exposed Session Variables
Testing for Cross Site Request Forgery (CSRF)
Testing for logout functionality
Test Session Timeout
Testing for Session puzzling
Fuente: https://www.owasp.org/index.php/Testing_Information_Gathering

Input Validation Testing. Validar los datos de entrada en una aplicación web es tal vez el desafío más importante, los datos externos no se pueden dar como

confiables porque pueden ser manipulados, en la tabla 7 se puede observar la división de estos ataques.

Tabla 7. *OWASP Input Validation Testing*

Validation Testing
Testing for Cross site scripting
Testing for Reflected Cross Site
Testing for Stored Cross Site
Testing for HTTP Verb Tampering and Parameter Pollution
Testing for HTTP Verb Tampering
Testing for HTTP Parameter pollution
SQL Injection
LDAP Injection
ORM Injection
XML Injection
SSI Injection
XPath Injection
IMAP/SMTP Injection
Code Injection
OS Commanding
Buffer overflow
Incubated vulnerability
Fuente: https://www.owasp.org/index.php/Testing_Information_Gathering

Error Handling. El correcto manejo de los mensajes de error garantiza que nos e va a dar más información sobre el funcionamiento interno de la aplicación. El propósito de revisar el código de manejo de errores es asegurar que la aplicación falla de forma segura en todas las posibles condiciones de error, esperadas e inesperadas. No se presenta ninguna información sensible al usuario cuando se produce un error.

Cryptography. La criptografía es uno de los temas más avanzados de la seguridad de la información, y cuya comprensión requiere la mayoría de la educación y la experiencia. Es difícil acertar porque hay muchos enfoques para el cifrado, cada uno con ventajas y desventajas que necesitan ser completamente comprendidos por los arquitectos y desarrolladores de soluciones web. Además, la investigación criptográfica grave se basa típicamente en matemáticas avanzadas y teoría de números, proporcionando una seria barrera de entrada.

La aplicación correcta y precisa de la criptografía es extremadamente crítica para su eficacia. Un pequeño error en la configuración o codificación se traducirá en la eliminación de un gran grado de la protección que ofrece y rending la implementación de cifrado inútil contra ataques graves.

Business Logic Testing. Este tipo de pruebas obliga a pensar en métodos no convencionales y se basa en las habilidades y creatividad del atacante. La clasificación de las fallas de la lógica comercial ha sido sub-estudiada; Aunque la explotación de los defectos empresariales ocurre con frecuencia en los sistemas del mundo real, y muchos investigadores aplicados a la vulnerabilidad los investigan. El mayor interés está en las aplicaciones web. Existe un debate dentro de la comunidad acerca de si estos problemas representan conceptos particularmente nuevos, o si son variaciones de principios bien conocidos.

Client Side Testing. Las pruebas del lado del cliente se refieren a la ejecución del código en el cliente, normalmente de forma nativa dentro de un navegador web o un complemento de navegador. La ejecución del código en el lado del cliente es distinta de la ejecución en el servidor y devolver el contenido posterior. En la tabla 8 se puede observar las diferentes pruebas que se pueden realizar

Tabla 8. *OWASP Client-Side Testing*

Client-Side Testing
Testing for DOM based Cross Site Scripting
Testing for JavaScript Execution *Testing for HTML Injection*
Testing for Client-Side URL Redirect
Testing for CSS Injection
Testing for Client-Side Resource Manipulation
Test Cross Origin Resource Sharing
Testing for Cross Site
Testing for Clickjacking
Testing WebSockets
Test Web Messaging
Test Local Storage
Fuente: https://www.owasp.org/index.php/Testing_Information_Gathering

3.1.1.2 PTES (*Penetration testing execution standard*)[51]. PTES es un estándar diseñado por un grupo de profesionales en la seguridad de la información de todas las áreas de la industria que comenzó a principios de 2009 tras una discusión que provocó entre algunos de los miembros fundadores sobre el valor (o la falta de) de las pruebas de penetración en la industria.

Esta guía se divide en 7 secciones, que cubren todos los aspectos relacionados con un pen testing, desde la comunicación y obtención de la información, hasta la presentación final de los informes. A la fecha de la revisión se encontraba vigente la versión 1.0 y en desarrollo la versión 2.0. las siete secciones son:

Pre-engagement Interactions. En esta sección se definen las herramientas necesarias para realizar un correcto pre-compromiso a cerca del pentesting, definiendo el alcance, los tiempos y metodologías que se van a utilizar, la superficie de ataque. La metodología sugiere seguir estos para tener una etapa de planificación bien estructurada, como se puede observar en el cuadro 1.

Cuadro 1 *PTES Pre-engagement Interactions*

Pre-engagement Interactions	
Overview	
Introduction to Scope	
Metrics for Time Estimation	
Scoping Meeting	
Additional Support Based on Hourly Rate	
Questionnaires	
General Questions	*Network Penetration Test*
	Web Application Penetration Test
	Wireless Network Penetration Test
	Physical Penetration Test
	Social Engineering
	Questions for Business Unit Managers
	Questions for Systems Administrators
Scope Creep	
Specify Start and End Dates	
Specify IP Ranges and Domains	*Validate Ranges*
	Cloud Services
	ISP

[51] PENTEST STANDARD.ORG. The Penetration Testing Execution Standard. [En línea], [consultado el 20 de agosto de 2017]. Disponible en: http://www.pentest-standard.org/ index. php/Main_Page

Pre-engagement Interactions	
Dealing with Third Parties	*MSSPs*
	Countries Where Servers are Hosted
Define Acceptable Social Engineering Pretexts	
DoS Testing	
Payment Terms	*Net 30*
	Half Upfront
	Recurring
Goals	*Primary*
	Secondary
	Business Analysis
Cuadro 1 (Continuación)	
Establish Lines of Communication	
Emergency Contact Information	*Incident Reporting Process*
	Incident Definition
	Status Report Frequency
	PGP and Other Alternatives
Rules of Engagement	*Timeline*
	Locations
	Evidence Handling
	Regular Status Meetings
	Time of the Day to Test
	Dealing with Shunning
	Permission to Test
	Legal Considerations
Capabilities and Technology in Place	
Fuente: http://www.pentest-standard.org/index.php/Main_Page	

Inteligencie Gathering. El objetivo de esta sección es brindar una seria de pasos para poder obtener la información necesaria para definir un plan de ataque altamente estratégico. Así mismo otro de los objetivos en esta etapa es recolectar la mayor cantidad de información que pueda ser utilizada en las fases de evaluación y explotación de la vulnerabilidad, tener la mayor cantidad de información disponible puede garantizar mayor cantidad de vectores de ataque. Los pasos sugeridos en esta etapa se observan en el cuadro 2:

Cuadro 2*. PTES Inteligencie Gathering*

Inteligencie Gathering	
General	*Background Concepts*

Inteligencie Gathering	
Intelligence Gathering	*What it is*
	Why do it
	What is it not
Target Selection	*Identification and Naming of Target*
	Consider any Rules of Engagement limitations
	Consider time length for test
	Consider end goal of the test
OSINT	*Corporate*
	Individual
	Employee
Cuadro 2. (Continuación)	
Covert Gathering	*Corporate*
	HUMINT
Footprinting	*External Footprinting*
	Internal Footprinting
Identify Protection Mechanisms	*Network Based Protections*
	Host Based Protections
	Application Level Protections
	Storage Protections
	User Protections
Fuente: http://www.pentest-standard.org/index.php/Main_Page	

Threat Modeling. En esta sección el estándar define un correcto enfoque para el modelado de las vulnerabilidades y/o amenazas, lo cual se utilizará posteriormente en el pen test. Esta sección se centra en dos elementos claves *assets ans attacker* (activos y atacante), desglosando cada uno de ellos en activos empresariales y procesos empresariales, así como en comunidades de amenazas y sus capacidades, como mínimo en esta etapa se deben definir estos cuatro elementos. La fase de modelado de amenazas de cualquier compromiso de pruebas de penetración es crítica tanto para los atacantes como para la organización. Proporciona claridad en cuanto al apetito de riesgo y priorización de la organización (¿cuáles son los activos más importantes que otros?, ¿qué amenazas son más relevantes que otras?). Además, permite al probador concentrarse en entregar un compromiso que emula de cerca las herramientas, técnicas, capacidades, accesibilidad y perfil general del atacante, teniendo en cuenta cuáles son los objetivos reales dentro de la organización de tal manera que los controles, procesos más relevantes, Y la infraestructura se ponen a prueba en lugar de una lista de inventario de elementos de TI. Los pasos sugeridos en esta etapa se observan en el cuadro 3.

Cuadro 3. *PTES Threat Modeling*

Threat Modeling	
General	*High level threat modeling process*
	Example
	High level modeling tools
Business Asset Analysis	*Organizational Data*
	Human Assets
Cuadro 3. (Continuación)	
Business Process Analysis	*Technical infrastructure supporting process*
	Information assets supporting process
	Human assets supporting process
	3rd party integration and/or usage of/by process
Threat Agents/Community Analysis	*Employees*
	Management (Executive, middle)
Threat Capability Analysis	*Analysis of tools in use*
	Availability to relevant exploits/payloads
	Communication mechanisms
	Accessibility
Motivation Modeling	
Finding relevant news of comparable Organizations being compromised	
Fuente: http://www.pentest-standard.org/index.php/Main_Page	

Vulnerability Analysis. Las pruebas de vulnerabilidad, es el proceso mediante el cual se descubren fallas en sistemas y aplicaciones que pueden ser aprovechadas por un atacante, estas vulnerabilidades se pueden generar por una incorrecta configuración de la aplicación, se un servicio, por configuraciones de fábrica de las aplicaciones, o por un diseño de aplicación inseguro. El definir el alcance del pen test, es necesario también definir y evaluar adecuadamente la profundidad en la evaluación de las vulnerabilidades. Los pasos sugeridos en esta etapa se observan en la tabla 9.

Tabla 9. PTES Vulnerability Analysis

Testing
Active
Passive
Validation
Research
Fuente: http://www.pentest-standard.org/index.php/Main_Page

Exploitation. Esta fase se centra únicamente en establecer un acceso a los sistemas o recursos eludiendo las restricciones de seguridad definidas por la organización, para que esta etapa se desarrolle satisfactoriamente, es necesario que la etapa de análisis de vulnerabilidades se haya realizado correctamente y se debe tener una lista de objetivos de alto valor. El vector de ataque debe tener en cuenta las probabilidades de éxito y el impacto que genera el mismo la organización. Los pasos sugeridos en esta etapa se describen en el cuadro 4:

Cuadro 4*. PTES Explotation*

Purpose	
Countermeasures	*Anti-Virus*
	Human
	Data Execution Prevention (DEP)
	Address Space Layout Randomization
	Web Application Firewall (WAF)
Evasion	
Precision Strike	
Customized Exploitation Avenue	
Tailored Exploits	*Exploit Customization*
Zero-Day Angle	*Fuzzing*
	Source Code Analysis
	Types of Exploits
	Traffic Analysis
	Physical Access
	Proximity Access (WiFi)
Example Avenues of Attack	
Overall Objective	

Fuente: http://www.pentest-standard.org/index.php/Main_Page

Post Exploitation. El propósito de esta etapa es luego de lograr el acceso en la etapa anterior poder mantener el control de la misma, identificar el valor para la organización. Los métodos descritos en esta fase están diseñados para ayudar al tester a identificar y documentar datos confidenciales, identificar configuraciones, canales de comunicación y relaciones con otros dispositivos de red que se pueden utilizar para obtener más acceso a la red y configurar uno o más métodos de acceso a la máquina en un momento posterior. En los casos en que estos métodos difieren de las reglas de compromiso acordadas, se deben seguir las

reglas de compromiso. Los pasos sugeridos en esta etapa se muestran en el cuadro 5.

Cuadro 5*. PTES Post Exploitation*

Post Exploitation	
Purpose	
Rules of Engagement	*Protect the Client*
	Protecting Yourself
Infrastructure Analysis	*Network Configuration*
	Network Services
Cuadro 5. (Continuación)	
Pillaging	*Installed Programs*
	Installed Services
	Sensitive Data
	User Information
	System Configuration
High Value/Profile Targets	
Data Exfiltration	*Mapping of all possible exfiltration paths*
	Testing exfiltration paths
	Measuring control strengths
Persistence	
Further Penetration Into Infrastructure	*From Compromised System*
	Thru Compromised System
Cleanup	
Fuente: http://www.pentest-standard.org/index.php/Main_Page	

Reporting. Esta sección tiene por objeto definir los criterios mínimos que debe contener un informe sobre el pen testing. Se define la estructura básica del informe para que genere valor al lector, la cual se puede observar en la tabla 10.

Tabla 10. *PTES Reporting*

Overview
Report Structure
The Executive Summary
Technical Report
Fuente: http://www.pentest-standard.org/index.php/Main_Page

3.1.1.3 OSSTMM (*Open Source Security Testing Methodology Manual*)[52]. OSSTMM es una metodología distribuida por Institute for Security and Open Methodologies (ISECOM), en donde las organizaciones y los pen testing pueden obtener el mayor beneficio en la revisión y supervisión de su seguridad informática, haciendo especial énfasis en los informes, incluyendo plantillas prediseñadas para la presentación de los mismos.

Actualmente se encuentra en desarrollo la versión 4 de esta metodología, la versión vigente es la 3.0 que contiene las siguientes etapas:

Sección A -Seguridad de la Información

Revisión de la Inteligencia Competitiva
Revisión de Privacidad
Recolección de Documentos

Sección B – Seguridad de los Procesos

Testeo de Solicitud
Testeo de Sugerencia Dirigida
Testeo de las Personas Confiables

Sección C – Seguridad en las tecnologías de Internet

Logística y Controles
Exploración de Red
Identificación de los Servicios del Sistema
Búsqueda de Información Competitiva
Revisión de Privacidad
Obtención de Documentos
Búsqueda y Verificación de Vulnerabilidades
Testeo de Aplicaciones de Internet
Enrutamiento
Testeo de Sistemas Confiados
Testeo de Control de Acceso
Testeo de Sistema de Detección de Intrusos
Testeo de Medidas de Contingencia
Descifrado de Contraseñas

[52] ISECOM.ORG. Open Source Security Testing Methodology Manual [En línea], [consultado el 20 de agosto de 2017]. Disponible en: http://www.isecom.org/research/

Testeo de Denegación de Servicios
Evaluación de Políticas de Seguridad

Sección D – Seguridad en las Comunicaciones

Testeo de PBX
Testeo del Correo de Voz
Revisión del FAX
Testeo del Modem

Sección E – Seguridad Inalámbrica

Verificación de Radiación Electromagnética (EMR)
Verificación de Redes Inalámbricas [802.11]
Verificación de Redes Bluetooth
Verificación de Dispositivos de Entrada Inalámbricos
Verificación de Dispositivos de Mano Inalámbricos
Verificación de Comunicaciones sin Cable
Verificación de Dispositivos de Vigilancia Inalámbricos
Verificación de Dispositivos de Transacción Inalámbricos
Verificación de RFID
Verificación de Sistemas Infrarrojos
Revisión de Privacidad

Sección F – Seguridad Física

Revisión de Perímetro
Revisión de monitoreo
Evaluación de Controles de Acceso
Revisión de Respuesta de Alarmas
Revisión de Ubicación
Revisión de Entorno

3.1.2 Análisis de vulnerabilidades.

Según la definición del libro Introducción a las técnicas de ataque e investigación forense, un enfoque pragmático53, el análisis de vulnerabilidades se entiende como las pruebas relacionadas con la identificación de puertos abiertos, servicios

[53] Ethical Hacking. SALLIS Ezequiel, CAACCIOLO Claudio, RODRIGUEZ Marcelo. Editorial Alfaomega, Argentina 2010.

disponibles y vulnerabilidades conocidas en los sistemas de información objetivo, incluyendo la verificación y validación de falsos positivos.

En el Libro Introducción a la seguridad informática54, define:

Amenaza: Se entiende por amenaza, una condición del entorno de los sistemas, áreas o dispositivos que contienen información importante (persona, equipo, suceso o idea) que ante determinada circunstancia podría dar lugar a que se produjese una violación de seguridad.

De acuerdo con la recomendación UIT-T X 800, una amenaza de seguridad constituye una violación potencial de la seguridad. Es potencial porque existe la posibilidad que se genere un cambio intencional, pero no autorizado. Aunque también se considera una amenaza a la seguridad cuando es posible que haya una fuga de información, por supuesto no autorizada, pero no se modifica el estado del sistema, y simplemente se extraen datos importantes, como contraseñas con el fin de realizar movimientos bancarios, como transferencias electrónicas de dinero.

Vulnerabilidad: Constituye un hecho o una actividad que permite concretar una amenaza. Se es vulnerable en la medida en que no hay suficiente protección como para evitar que llegue a suceder una amenaza. En la actualidad se contempla que hay ataques intencionados y no intencionados, mismos a los que la empresa siempre es vulnerable, en mayor o menor medida. Cuando existe una vulnerabilidad en la seguridad informática, en general esta se considera como un defecto de diseño, en la implementación del sistema o en su funcionamiento.

Con base en estas definiciones se puede definir que este tipo de análisis busca identificar e informar fallas en los dispositivos y en los procesos tecnológicos, sugiriendo los planes de acción que permitan la remediación inmediata de la vulnerabilidad.

Este tipo de análisis no incluye la explotación de la vulnerabilidad encontrada, únicamente trabaja en la correcta identificación de la vulnerabilidad utilizando herramientas tecnológicas y también la visión analítica de quien está realizando el análisis descartando los falsos positivos identificados.

Este tipo de análisis es el más conveniente a utilizar en el desarrollo del presente trabajo e investigación, teniendo en cuenta que Cooperativa Alianza está

[54] Introducción a la seguridad informática, BACA URBINA Gabriel. Grupo Editorial Patria, México 2016.

interesada en contar con un diagnóstico inicial sobre sus vulnerabilidades expuestas, realizando los planes de acción necesarios para mitigar la vulnerabilidad descubierta.

Se desarrollará las siguientes etapas en el análisis de vulnerabilidades:

Reconocimiento Pasivo. Etapa también conocida como Information Gathering, es la etapa en la que, sin realizar un ataque o escaneo contra el objetivo, se recopila la mayor cantidad de información disponible que permitirá elaborar un mapa estratégico para desarrollar el análisis posterior.

Durante esta etapa vamos a obtener información relacionada con los dominios y subdominios de la compañía, los sistemas web expuestos online, datos de contacto, así como cuentas de correo electrónico corporativos, documentos públicos y metadatos de estos.

Para obtener información acerca de los dominios se utilizar el protocolo *WHOIS,* mediante el cual se obtiene información de quien realizo el registro de dominio, correo electrónico, ips asociadas a este dominio.

Se implementará una máquina que tendrá como sistema operativo LINUX versión KALI, en la cual encontraremos las herramientas necesarias para realizar el análisis.

Para la obtención de información sobre los subdominios y errores de configuración en los subregistros dns, se utilizará el servicio nslookup del sistema operativo KALI, así como la herramienta MALTEGO CE[55], desde donde se obtendrá información vital para diseñar la hoja de ruta del análisis posterior. Para finalizar esta etapa de reconocimiento, se utilizará la función GOOGLE HACKING[56], utilizando las bondades del buscador Google con sus opciones de búsqueda avanzadas, donde se puede encontrar información como mensajes de error de las aplicaciones obteniendo información del sistema operativo y web servers, archivos clasificados que se han publicado, archivos logs entre otra información, la cual será de mayor utilidad en las etapas posteriores del análisis.

Una vez descubiertos archivos de configuración o confidenciales, también es importante obtener la información de sus metadatos, para se utilizará la

[55] PATERVA.COM. ¿Qué es Maltego?, [En línea], [consultado el 20 de agosto de 2017]. Disponible en: https://www.paterva.com/web7/buy/maltego-clients/maltego-ce.php

[56] WIKIPEDIA. Google Hacking, [En línea], [consultado el 20 de agosto de 2017]. Disponible en: https://es.wikipedia.org/wiki/Google_Hacking

herramienta FOCA[57], en la cual se obtendrá los metadatos de los archivos encontrados.

Reconocimiento Activo. En la etapa de reconocimiento pasivo, se obtuvo información acerca de los rangos de ips que se encuentran asociadas a la Cooperativa Alianza, y a través de la herramienta NMAP incluida dentro del sistema operativo KALI para obtener una relación de los sistemas activos en los objetivos, los puertos abiertos en las ips objetivos, identificando los posibles servicios que están vinculados a estos puertos. Esta herramienta también realiza una comparación contra su base de conocimiento, para determinar a través de características especiales de cada sistema operativo (valor de TTL) puede inferir el sistema que tiene cada servicio o puerto encontrado, así como el servicio vinculado a cada puerto descubierto.

Análisis de Vulnerabilidades. En esta etapa se utilizará la herramienta OPENVAS[58], herramienta que realiza un escaneo identificando vulnerabilidades relacionadas con actualizaciones de sistemas operativos, malware y ataques, verificación de configuraciones por default.

Se correrá esta herramienta en dos entornos, las IPS públicas entregadas por la Cooperativa, y un análisis del pool de direcciones internas de la red en Cooperativa Alianza, esto para posicionarse en el análisis desde las dos perspectivas importantes para la organización.

Una vez obtenida la información, se hace necesario clasificarla según la importancia del activo informático comprometido en la vulnerabilidad, esto para poder realizar un informe más detallado y mitigando los falsos positivos que puedan encontrarse.

Para la validación de las vulnerabilidades, se utilizará la base de conocimiento CVE (*Common Vulnerabilities and Exposures*)

Reporte. El objetivo de realizar el análisis de vulnerabilidades es que la gerencia pueda tener un panorama más claro de los riesgos a los que está expuesta la organización, definiendo igualmente los planes de acción para mitigar los mismos.

[57] FOCA, Informática 64. [En línea], [consultado el 20 de agosto de 2017]. Disponible en: http://www.informatica64.com/

[58] OPENVAS, Open Vulnerability Assessment System. [En línea], [consultado el 20 de agosto de 2017]. Disponible en: http://www.openvas.org/

Por esta razón este informe de resultados, se clasificarán los niveles de seguridad en:

- Alto
- Medio – Alto
- Medio
- Medio – Bajo
- Bajo

Cada vulnerabilidad se clasificará en según las siguientes categorías:

- Criticidad
- Impacto
- Esfuerzo

Al final se obtendrá un mapa de calor en donde se definan los niveles de seguridad y la clasificación de cada vulnerabilidad, así como la recomendación que permita mitigar la vulnerabilidad encontrada.

3.1.3 Resultados esperados.

Con la realización de un análisis de vulnerabilidades para Cooperativa Alianza, se pueden identificar las amenazas y vulnerabilidades más significativas a las que está expuesta la organización, convirtiéndose en un factor de riesgo sobre la información sensible.

El objetivo final sobre el desarrollo del análisis es el determinar las acciones correctivas sobre las amenazas y/o debilidades encontradas, generando esto una disminución sobre los riesgos asociados a posibles ataques informáticos, adicionalmente se debe generar una sensibilización a los funcionarios de Cooperativa Alianza en la Importancia de la seguridad de la información y la importancia de darle el manejo adecuado a la misma.

3.2 MARCO INSTITUCIONAL

Cooperativa Alianza, es una entidad especializada en ahorro y crédito. Constituida el 14 de mayo de 1962 por 81 empleados de la embajada de los Estados Unidos, el Servicio de la Información de los Estados Unidos USIS y la Agencia

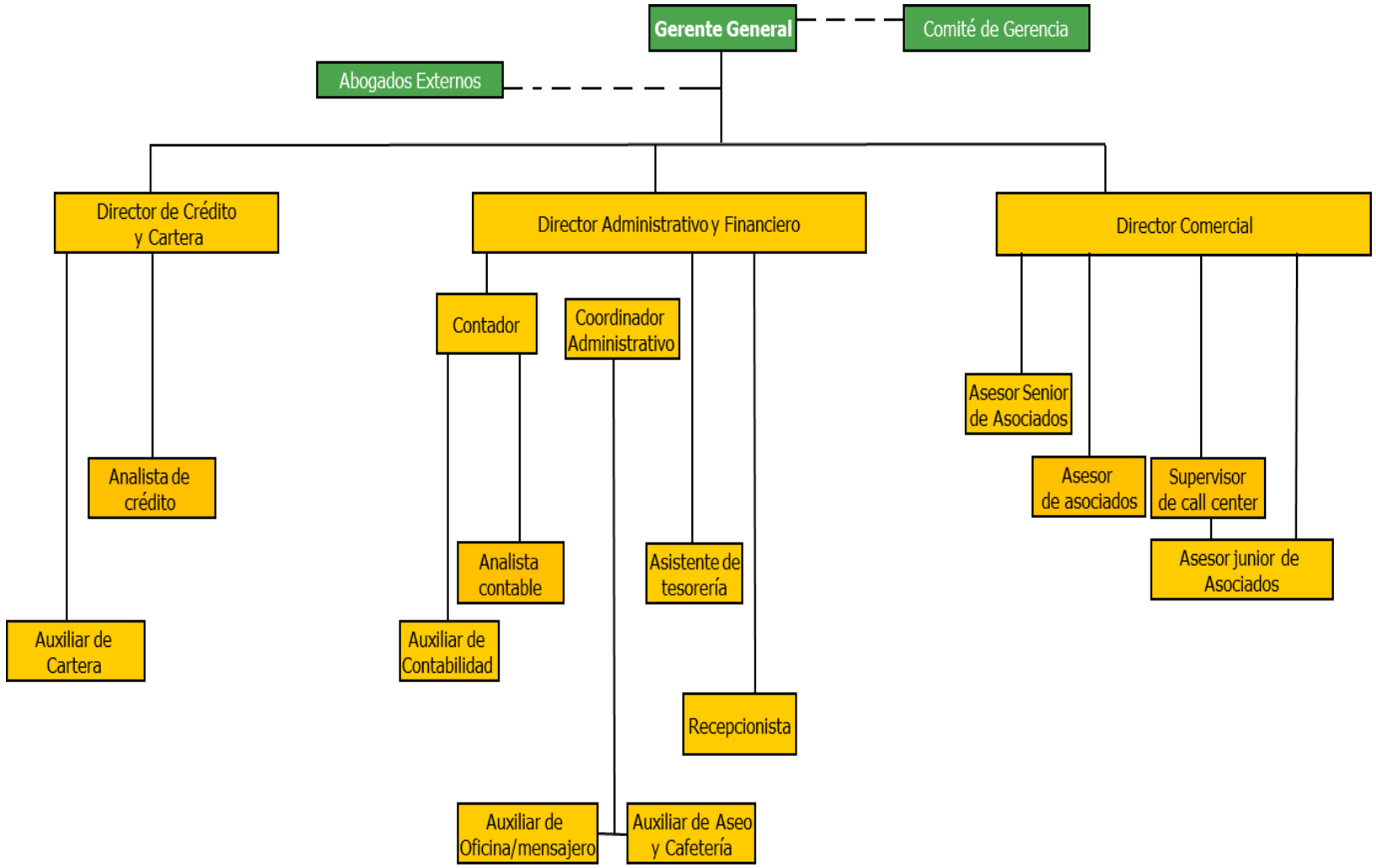
Internacional para el Desarrollo AID. Actualmente, asocia empleados de misiones diplomáticas, agencias de Naciones Unidas, organizaciones internacionales, entidades afines, empresas privadas y personas referidas de nuestros asociados.

Actualmente cuenta con 6760 asociados, principalmente en la ciudad de Bogotá, los cuales son atendidos en su única sede ubicada en la carrera 12 No. 89-28 piso 6 barrio Chico.

Cuenta actualmente con 130 convenios con empresas privadas y organizaciones diplomáticas, convirtiendo la cooperativa en el proveedor financiero de sus empleados, dando facilidad en créditos y ahorros.

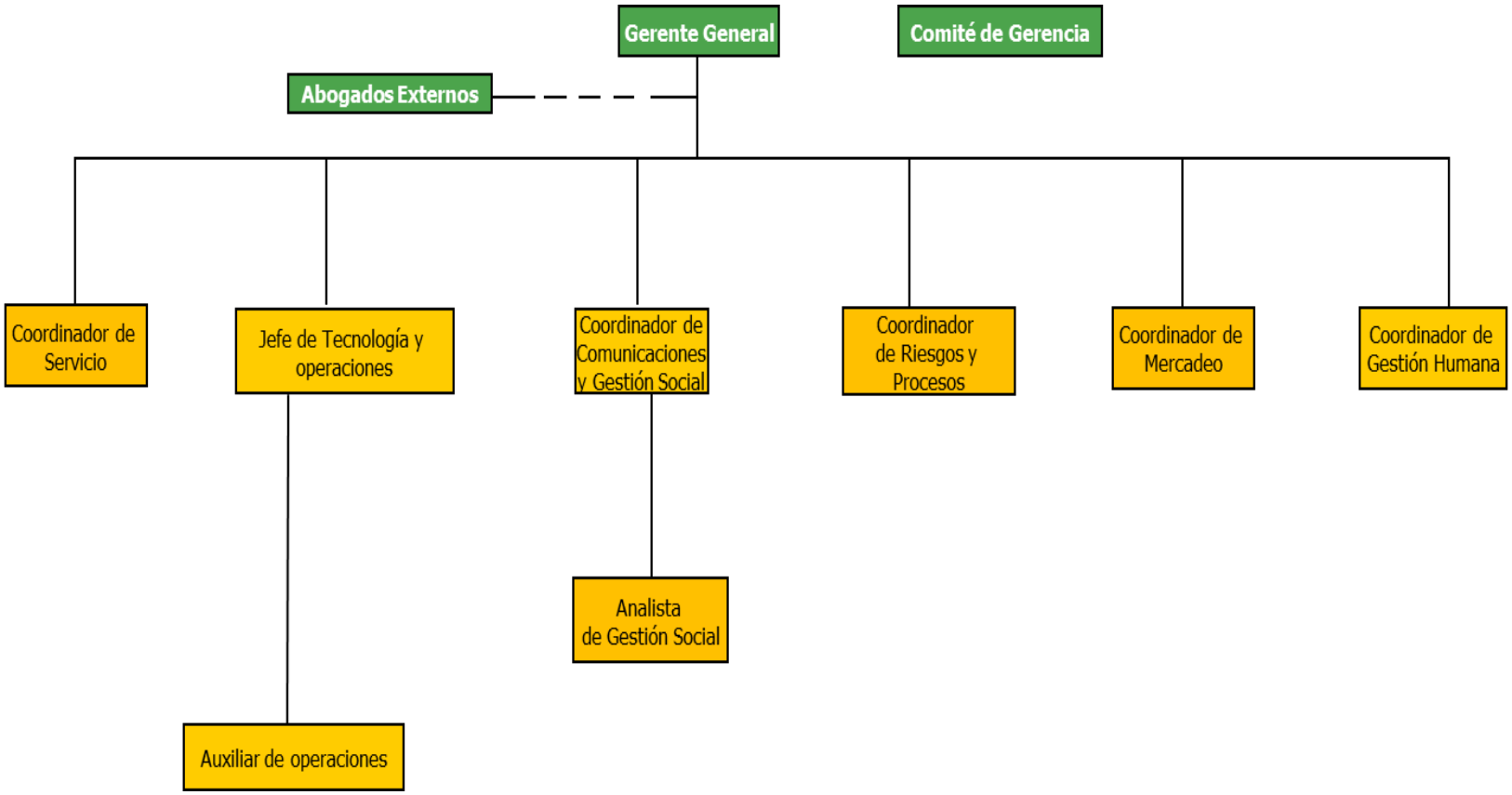
La planta de personal está distribuida como se puede observar en las Figura 1 y 2.

Figura 1. Organigrama



Fuente: Cooperativa Alianza

Figura 2. Organigrama

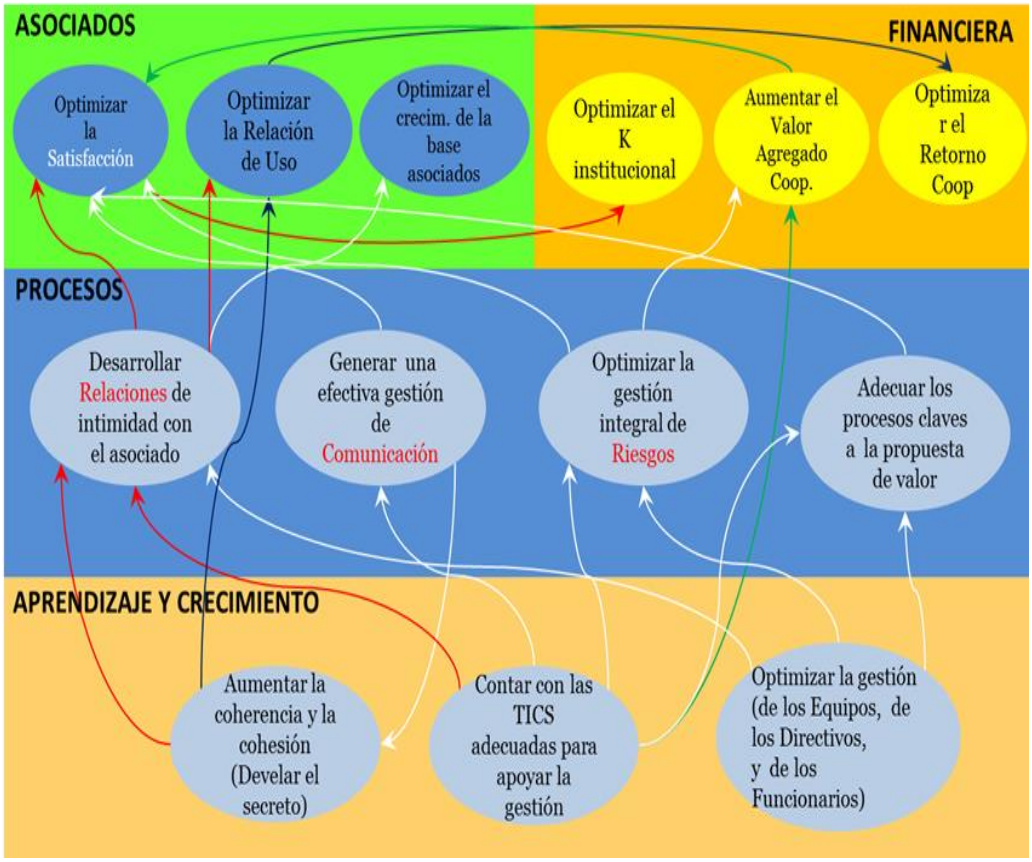


Fuente: Cooperativa Alianza

El objeto social de la cooperativa es la prestación de servicios de ahorro y crédito, en la actualidad posee unos activos por valor de $67.276 millones, de los cuales $56.057 están representados en cartera de crédito a los asociados. $51.179 millones de pesos en pasivos de los cuales $48.635 corresponden a ahorros de los asociados

La promesa de valor de la Cooperativa definida en su plan estratégico 2014-2018 es intimidad con el asociado la mejor solución total, para el desarrollo de esta estrategia se han diseñado los objetivos estratégicos que se observan en la figura 3.

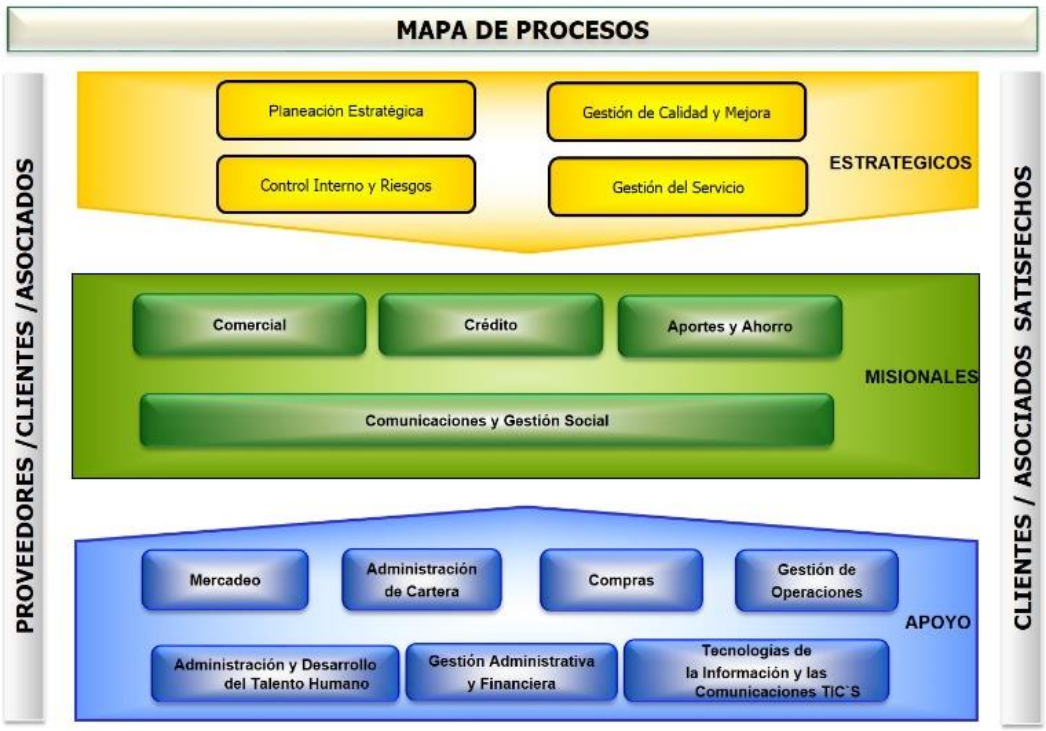
Figura 3. Mapa Estratégico



Fuente: Cooperativa Alianza

Para el cumplimiento de la estrategia, Cooperativa Alianza diseño los procesos que se observan en la figura 4.

Figura 4. Mapa de Procesos



Fuente: Cooperativa Alianza

Definiendo la siguiente filosofía[59] organizacional

En la Cooperativa Alianza, la Intimidad con el Asociado es el principio rector de todo nuestro accionar: creemos que en las relaciones estrechas y permanentes con nuestros asociados está la clave para personalizar integralmente nuestros servicios y ofrecer la mejor solución a cada asociado, en cada momento de su vida.

Creemos que el espíritu cooperativo y solidario está presente en el doble papel de nuestro asociado como socio y como beneficiario. Por eso nos caracteriza una

[59] COOPERATIVA ALIANZA. Planeación Estratégica 2014 – 2018. [En línea], [consultado el 20 de agosto de 2017]. Disponible en: https://www.aciamericas.coop/IMG/pdf/plan_estrategico_2017_2020 _v4.pdf

actitud asesora para ayudar a identificar sus cambiantes y personales necesidades, en todos los campos: financiero, laboral, educativo, familiar, médico, social y recreacional.

La calidad y la innovación son las características de nuestro servicio: debemos satisfacer a nuestros asociados y usuarios con las mejores soluciones, producto de la flexibilidad y la novedad en la prestación de nuestros servicios; así aseguramos su fidelidad y, en reciprocidad, debemos esperar e impulsar su participación por ser ellos los propietarios de la Cooperativa.

Se cree que la fortaleza en el servicio no está en lo que se tiene sino en lo que se sabe y sabe hacer: por eso nos preocupamos por constituir redes de proveedores financieros y de servicios complementarios que nos permitan entregar soluciones variadas, flexibles y a la medida.

Creemos que el éxito de nuestra Organización depende del desempeño calificado y responsable de nuestros Directivos y Colaboradores. Nuestros funcionarios deben ser personas experimentadas, talentosas, innovadoras, con iniciativa y con capacidad de riesgo y, en consecuencia, nuestra Entidad deberá apoyar su desarrollo y promoción con aprendizajes y programas internos y externos de formación.

La gestión, en todos sus niveles deberá estar orientada al logro de resultados porque entendemos que la productividad, la rentabilidad y la contribución al mejoramiento de la calidad de vida de los asociados, son una justa aspiración. En consecuencia, todos los directivos buscarán, en su diaria actuación, fortalecer una cultura organizacional basada en el compromiso, el respeto, la integridad y la cooperación, fuentes de enriquecimiento económico y social.

Nuestros colaboradores deberán sentir que sus líderes los aprecian, estimulan y apoyan en el logro de sus compromisos y le brindan los recursos físicos y tecnológicos indispensables a su labor, dentro de condiciones de comodidad, orden, aseo y actualidad, compatibles con su dignidad de seres humanos que logran resultados. Tendremos remuneraciones competitivas con incentivos para quienes se destaquen y deseen hacer de la Cooperativa su segunda familia.

Creemos que nuestros proveedores son esenciales para el éxito de nuestra labor cooperativa y, en consecuencia, estableceremos con ellos alianzas estables y mutuamente ventajosas.

Reconocemos nuestras obligaciones tributarias para con el Estado y creemos que es nuestro deber cumplirlas oportunamente y con ajuste cabal a lo estipulado en la Ley. Igualmente, creemos en la responsabilidad social empresarial y en que nada nos exime de proteger el medio ambiente, ampliar nuestros cometidos benéficos sociales, garantizar la seguridad en el empleo y apoyar la creación de nuevas

empresas porque nuestra misión cooperativa nos exige contribuir a un desarrollo equitativo económico y social.

3.2.1 Misión.[60]

Nuestro propósito es mejorar la calidad de vida de los asociados y sus familias, a través de la prestación de servicios oportunos de ahorro, crédito y complementarios a costo razonable y competitivo, brindando confianza y respaldo, alcanzando altos niveles de satisfacción, optimizando los recursos y la participación de cada uno de los asociados tanto en lo económico y social.

3.2.2 Visión.

Ser la mejor solución total para los asociados y acompañarlos a lo largo de su ciclo de vida.

3.2.3 Valores Corporativos

- Compromiso
- Respeto
- Integridad
- Cooperación

3.2.4 Política de Calidad.

En Cooperativa Alianza Ltda., ofrecemos servicios de ahorro, crédito, complementarios (sociales, culturales, recreativos y de previsión, entre otros) y todos aquellos que contribuyan al mejoramiento de la calidad de vida de nuestros asociados y su grupo familiar. Brindamos soluciones integrales y competitivas frente al mercado, con un equipo humano competente, comprometido y motivado, apoyado en procesos eficaces que garantizan el mejoramiento continuo del Sistema de Gestión de Calidad y la satisfacción del asociado.

[60] ALIANZA COOPERATIVA. Misión y Visión. [En línea], [consultado el 20 de agosto de 2017]. Disponible en: www.alianza.coop

3.2.5 Objetivos de calidad

- Alcanzar un nivel máximo del 80% en la satisfacción de los asociados a través del incremento del valor agregado transferido, mediante la oferta de productos y servicios que cumplan con sus expectativas y requerimiento.

- Capacitar y motivar continuamente el equipo humano con miras a lograr la calidad del desempeño y de los servicios ofrecidos a nuestros asociados, manteniendo un nivel del 60% de las competencias requeridas.

- Ofrecer servicios financieros flexibles, competitivos y personalizados que contribuyan al desarrollo integral de los asociados y su grupo familiar y a su interés social, aumentando la profundización de productos hasta un 60%.[61]

La administración actual de la cooperativa ha creído siempre en la tecnología como un factor importante para impulsar los planes y proyectos futuros de la Cooperativa, es por esta razón que está comprometido con la ejecución del Hacking Ético, esto para poder identificar y tomar las medidas necesarias en pro de minimizar las amenazas actuales.

3.2.6 Arquitectura Tecnológica.

ALIANZA cuenta actualmente con un sistema transaccional denominado LINIX sobre el cual se encuentra una aplicación denominada LINEG, adicionalmente cuenta con una herramienta E-BUSINESS llamada SINERGY, y cuenta actualmente con 31 puestos de trabajo en una red local.

Actualmente también se cuenta con 6 servidores así:

SERVIDOR HYPERV SERVER: es el servidor físico donde se virtualizaron los servidores de dominio y aplicaciones.

SERVIDOR DE DOMINIO: servidor bajo el sistema operativo Windows Small Server 2011 Standard, el cual funciona como servidor de dominio, servidor Exchange, Servidor de Archivos, Servidor de Impresión.

SERVIDOR DE APLICACIONES: servidor bajo el sistema operativo Windows 2003 Server, el cual funciona como servidor de aplicaciones y donde se encuentran alojadas las formas del aplicativo LINIX.

[61] COOPERATIVA ALIANZA. Misión, Visión y valores corporativos. [En línea], [consultado el 21 de abril de 2016]. Disponible en: www.alianza.coop

SERVIDOR DE BASES DE DATOS: servidor bajo el sistema operativo Linux Enterprise server, en el cual se encuentra instalado el motor de bases de datos Oracle 11g.

SERVIDOR DE BASE DE DATOS DE PRUEBA: servidor bajo el sistema operativo Linux en el cual se tiene un ambiente de pruebas del sistema Linix.

Se puede observar el performance de cada servidor en el cuadro 6.

Cuadro 6. Performance Servidores

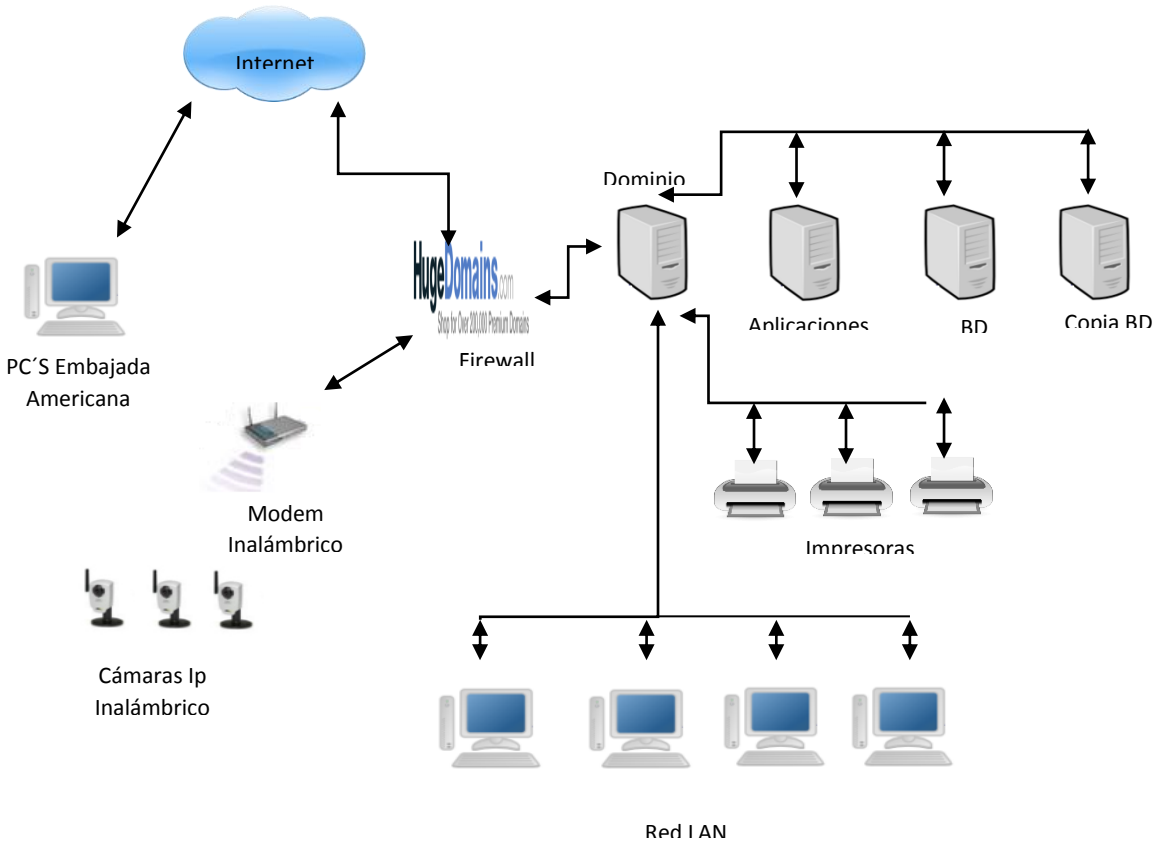
Servidor	Nombre	Modelo	Ip	S.O.	Servicios
HP	Hyper-v	Prolan ml1360	192.168.1.4	Hyper V Server 2012	Virtualizacion
Virtual	Dominio	Virtualizado	192.168.1.5	Windows Small Bussines 2011	Servidor de Dominio, Exchange, Archivos, Impresión
Virtual	Aplicaciones	Virtualizado	192.168.1.6	Windows Server 2003	Servidor de Aplicaciones, Antivirus
DELL	Base de Datos	Power Edge 2900	192.168.1.90	Windows Server 2003	Servidor de Base de Datos
DELL	Base de Datos	Power Edge 2600	192.168.1.92	Linux	Servidor de Base de Datos de prueba
IBM	Respaldo	x Series 236		Hyper V Server 2012	Servidor de Respaldo del Servidor de virtualizacion

Fuente: autor

Cuenta con un firewall Sophos como protección de entrada y salida hacia internet en la Figura 5 se puede observar el diagrama de conexión.

Figura 5. Mapa Tecnológico

.



Fuente: Cooperativa Alianza

La red LAN de ALIANZA está diseñada en estrella, y todos los equipos clientes están interconectados con un servidor central quien es el encargado del manejo del dominio ALIANZA LOCAL y sobre el cual se hacen las políticas de seguridad internas.

La red esta cableada en categoría 5, se cuenta actualmente con 1 switch de 48 posiciones, sobre los cuales está estructurada la red LAN, así como cableado estructurado para los puntos de voz y energía eléctrica.

Adicionalmente se cuenta con un servicio WIFI, proporcionado por dos acces point Sophos Ap55, gestionados desde la controla central.

4. DESARROLLO

4.1 DISEÑO

El análisis de vulnerabilidades se llevará a cabo en las instalaciones de Cooperativa alianza, en la ciudad de Bogotá, a través de herramientas como WHOIS de Kali, se puede obtener información acerca del dominio[62]

Según información suministrada por la cooperativa, el direccionamiento ip externo es 190.85.45.155 /248

El direccionamiento interno es

192.168.1.0/32, el análisis de vulnerabilidades se enfocará sobre los equipos de la red 192.168.1.5, 192.168.1.90, 192.168.1.7 servidores que soportan los sistemas de información core del negocio, 192.168.1.3 el cual es la dirección ip del firewall de la entidad.

El análisis de vulnerabilidades que se realizará sobre las ips externas, así como un mapeo de los equipos clientes de la red informados anteriormente, para verificar si se encuentran al día en los parches liberados por sus fabricantes, si existe algún equipo con infección de virus o troyanos, puertos abiertos en cada equipo de cómputo.

Se realizará remotamente a través de un equipo con sistema operativo KALI, en horas de la noche para no afectar la operación normal de la cooperativa.

El objetivo de realizar este análisis, como está planteado dentro de los objetivos del presente trabajo de grado, es desarrollar un análisis de vulnerabilidades en Cooperativa Alianza, que permitirá detectar las vulnerabilidades más significativas, definiendo los planes de acción necesarios para mitigar estas debilidades.

Se obtendrá una matriz donde se relacionan las vulnerabilidades encontradas, y los planes de acción para mitigar y/o controlarlas.

[62] COOPERATIVA ALIANZA. Quienes somos. [En línea], [consultado el 21 de abril de 2016]. Disponible en: www.alianza.coop

4.2 SENSIBILIZACIÓN A LOS FUNCIONARIOS

Durante el 2017 se desarrollaron dos jornadas de capacitación a los funcionarios, donde se dio una charla sobre los riesgos informáticos, desarrolladas en las instalaciones de la cooperativa los días 17 de mayo de 2017 y el 19 de octubre de 2017 con el siguiente temario:

“Buena tarde, el objetivo de la charla es la sensibilización a los funcionarios acerca de los siguientes temas

Que es un virus

Tipos de virus

Medidas de contención

Privacidad de la información

Espero contar con su activa participación”

Este es el resumen de asistencia y convocatoria de las capacitaciones se observa en la el cuadro 7.

Cuadro 7. *Capacitaciones Cooperativa Alianza*

Fecha	Titulo Capacitación	Funcionarios Convocados	Funcionarios Asistentes
15/05/2017	Charla Seguridad Informática	48	44
19/10/2017	Seguridad Informática	45	43
Fuente: autor			

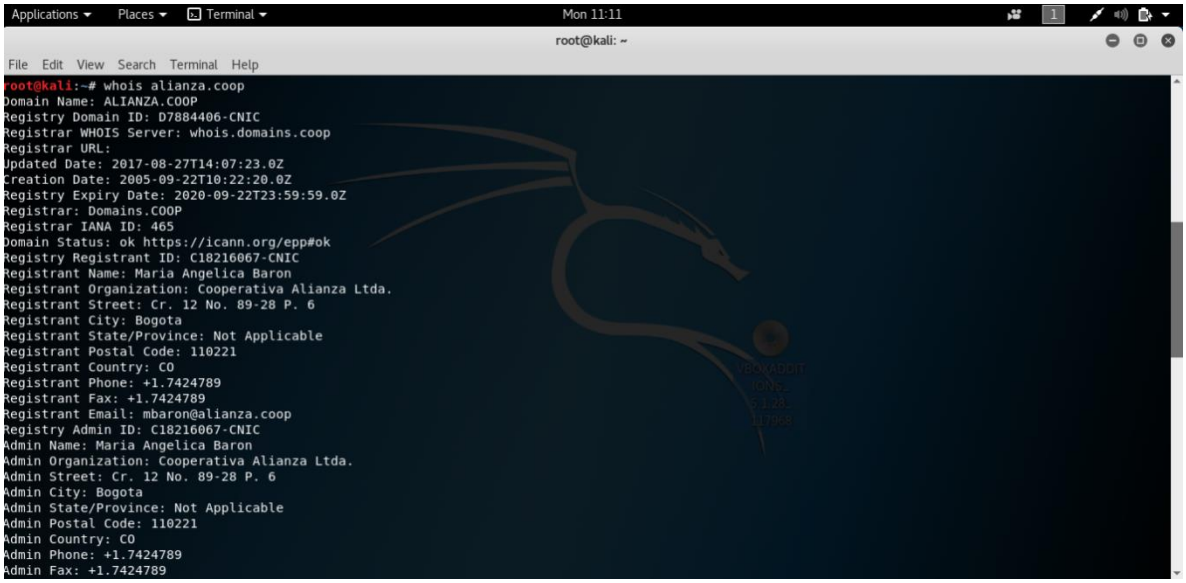
Estas charlas están enfocadas en lograr que los funcionarios de la cooperativa tengan presente en su vida cotidiana laboral y personal los riesgos a los que se encuentran expuestos y las posibles consecuencias que se tienen cuando se explotan estas vulnerabilidades.

4.3 EJECUCIÓN

Las herramientas de software que se utilizaran para el análisis, se determinó la utilización por el conocimiento que tiene el autor sobre las mismas, disminuyendo la curva de aprendizaje necesaria al utilizar otro programa.

A través de la herramienta whois del sistema operativo Kali, se puede observar en la Figura 6, donde se evidencia el propietario del dominio, la dirección registrada para el dominio, teléfonos y direcciones de contacto de los propietarios.

Figura 6. WHOIS alianza.coop



Fuente: Cooperativa Alianza

Esta información se utiliza para validar la propiedad del dominio. En la tabla 11 se observan los resultados obtenidos a través de la herramienta

Tabla 11. *Resultados WHOIS*

Resultados WHOIS
Domain Name: ALIANZA.COOP *Registry Domain ID: D7884406-CNIC* *Registrar WHOIS Server: whois.domains.coop* *Registrar URL:* *Updated Date: 2017-08-27T14:07:23.0Z* *Creation Date: 2005-09-22T10:22:20.0Z* *Registry Expiry Date: 2020-09-22T23:59:59.0Z* *Registrar: Domains.COOP* *Registrar IANA ID: 465*

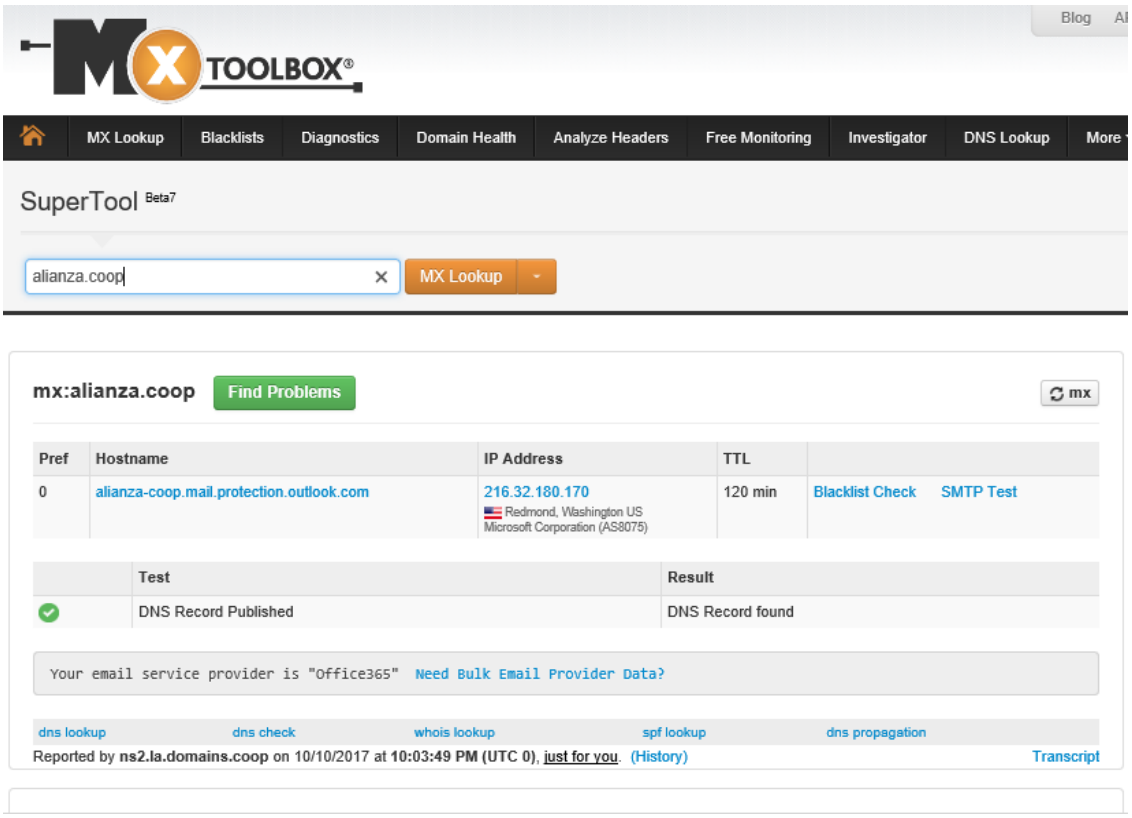
Resultados WHOIS
Tabla 11. (Continuación)
Domain Status: ok https://icann.org/epp#ok *Registry Registrant ID: C18216067-CNIC* *Registrant Name: Maria Angelica Baron* *Registrant Organization: Cooperativa Alianza Ltda.* *Registrant Street: Cr. 12 No. 89-28 P. 6* *Registrant City: Bogota* *Registrant State/Province: Not Applicable* *Registrant Postal Code: 110221* *Registrant Country: CO* *Registrant Phone: +1.7424789* *Registrant Fax: +1.7424789* *Registrant Email: mbaron@alianza.coop* *Registry Admin ID: C18216067-CNIC* *Admin Name: Maria Angelica Baron* *Admin Organization: Cooperativa Alianza Ltda.* *Admin Street: Cr. 12 No. 89-28 P. 6* *Admin City: Bogota* *Admin State/Province: Not Applicable* *Admin Postal Code: 110221* *Admin Country: CO* *Admin Phone: +1.7424789* *Admin Fax: +1.7424789* *Admin Email: mbaron@alianza.coop* *Registry Tech ID: C18216067-CNIC* *Tech Name: Maria Angelica Baron* *Tech Organization: Cooperativa Alianza Ltda.* *Tech Street: Cr. 12 No. 89-28 P. 6* *Tech City: Bogota* *Tech State/Province: Not Applicable* *Tech Postal Code: 110221* *Tech Country: CO* *Tech Phone: +1.7424789* *Tech Fax: +1.7424789* *Tech Email: mbaron@alianza.coop* *Name Server: NS1.LA.DOMAINS.COOP* *Name Server: NS2.LA.DOMAINS.COOP* *Name Server: NS3.LA.DOMAINS.COOP* *Name Server: NS4.LA.DOMAINS.COOP* *DNSSEC: unsigned* *Registry Billing ID: C18216067-CNIC* *Billing Name: Maria Angelica Baron* *Billing Organization: Cooperativa Alianza Ltda.* *Billing Street: Cr. 12 No. 89-28 P. 6* *Billing City: Bogota* *Billing State/Province: Not Applicable* *Billing Postal Code: 110221* *Billing Country: CO*

Resultados WHOIS
Tabla 11. (Continuación)
Billing Phone: +1.7424789 *Billing Fax: +1.7424789* *Billing Email: mbaron@alianza.coop*
Fuente: Cooperativa Alianza Ltda.

Se puede observar que el dominio tiene una vigencia hasta el 22 de septiembre de 2020, el propietario es Cooperativa alianza, ubicada en la carrera 12 No. 89-28 piso 6.

A través de la página mxtoolbox, se hace un rastreo para identificar los servicios registrados de correo electrónico como se puede observar en la Figura 7, donde se observa que la cooperativa cuenta con el servicio de correo electrónico a través de la plataforma office 365.

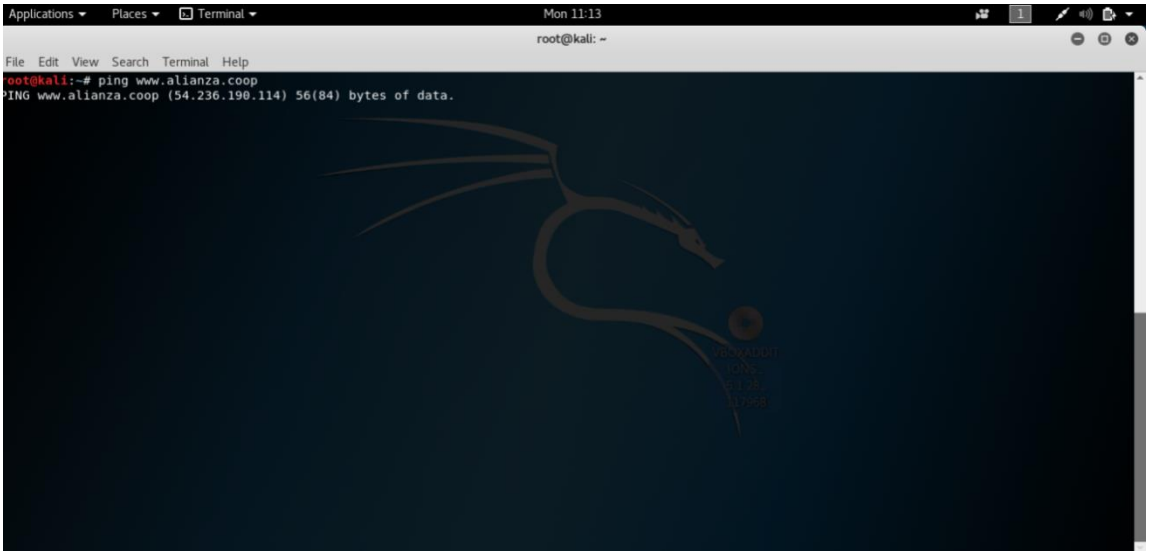
Figura 7. MX toolbox correo electrónico



Fuente: Cooperativa Alianza Ltda.

Se realiza un ping al dominio alianza.coop, como se observa en la Figura 8 la ip en la que se encuentra alojada la páginawww.alianza.coop es la 54.236.189.64, la cual no tiene habilitado el servicio ping y no se obtiene una respuesta favorable, siendo esto una medida de protección para minimizar el área expuesta a un atacante.

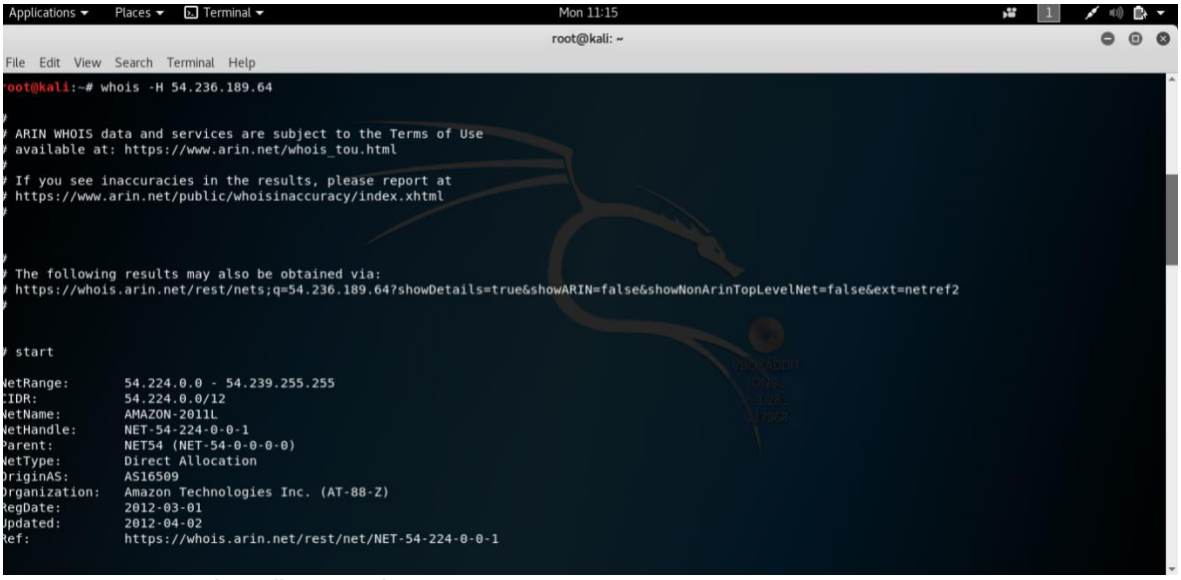
Figura 8. Ping alianza.coop



Fuente: Cooperativa Alianza Ltda.

A través de la herramienta WHOIS, se pudo identificar como se observa en la Figura 9, que el propietario de esta IP es AMAZON, por lo cual el hosting donde está alojada la página web de la entidad está contratado con esta plataforma. Dentro del alcance del presente trabajo de grado no está el análisis de vulnerabilidades sobre la página web de la entidad, se deja como recomendación realizar un análisis para verificar cuales son los riesgos a los que está expuesto a través de este servicio.

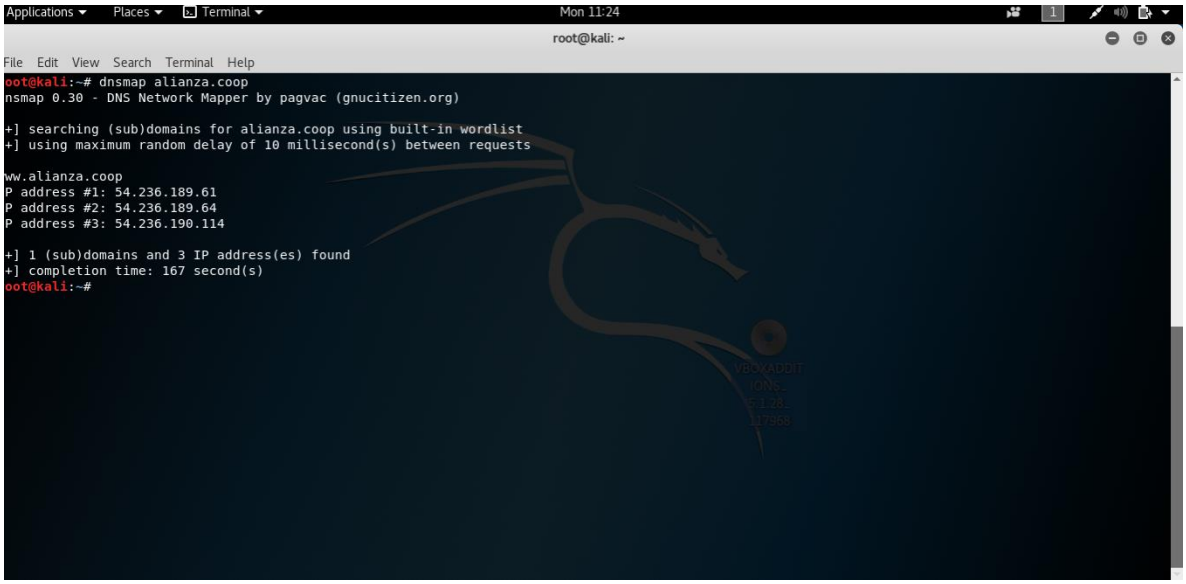
Figura 9. WHOIS IP www.alianza.coop



Fuente: Cooperativa Alianza Ltda.

Utilizando la herramienta DNSMap, del sistema operativo Kali, la cual se encarga de validar los subdominios asociados al dominio principal alianza.coop, en la Figura 10 se puede observar que no existe ningún subdominio asociado al dominio principal.

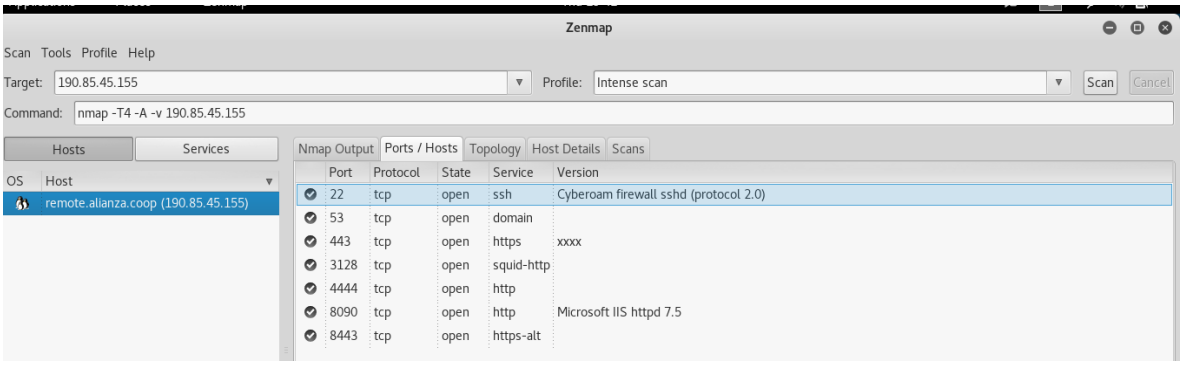
Figura 10. DNSMap



Fuente: Cooperativa Alianza Ltda.

Nmap es una funcionalidad del sistema operativo Kali, el cual permite hacer un barrido de puertos a un host determinado, utilizando la aplicación Zenmap, gráficamente realizamos el mismo procedimiento de nmap, como se puede observar en la Figura 11, verificando los puertos abiertos actualmente en el servidor web donde se aloja el sitio www.alianza.coop.

Figura 11 . Resultados Zenmap www.alianza.coop



Fuente: Cooperativa Alianza Ltda.

A través del listado *Port Vulnerability Reference* (PVR)[63] se verifican los puertos abiertos encontrados y las posibles vulnerabilidades asociadas a estos puertos,

[63] OUAH.ORG. Port Vulnerability Reference (PVR). [En línea], [consultado el 21 de abril de 2016]. Disponible en: http://www.ouah.org/PVR.htm.

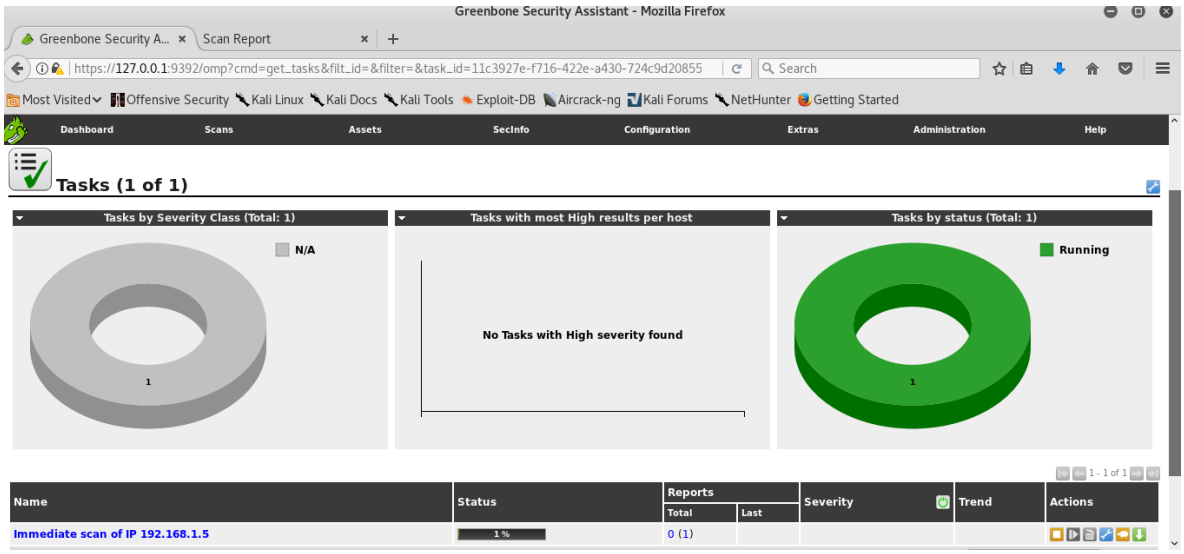
como se puede verificar en la tabla 12, en la etapa de análisis de riesgos, se definirá el impacto al tener estos puertos abiertos.

Tabla 12. *Puertos Abiertos Cooperativa Alianza*

Puerto	Servicio Asociado
22	*SSH, scp, SFTP – Remote Login Protocol*
53	*Domain Name System (DNS)*
443	*HTTPS*
3128	*SQUID – HTTP*
4444	*HTTP*
8090	*HTTP*
8443	*HTTPS-ALT*
Fuente: Elaboración propia con datos de Cooperativa Alianza	

Utilizando la herramienta OPENVAS, se lanzan los diferentes análisis de vulnerabilidades a los equipos core indicados por la organización, el primer análisis se realiza a la ip 192.168.1.5 como se observa en la Figura 12 el inicio del análisis.

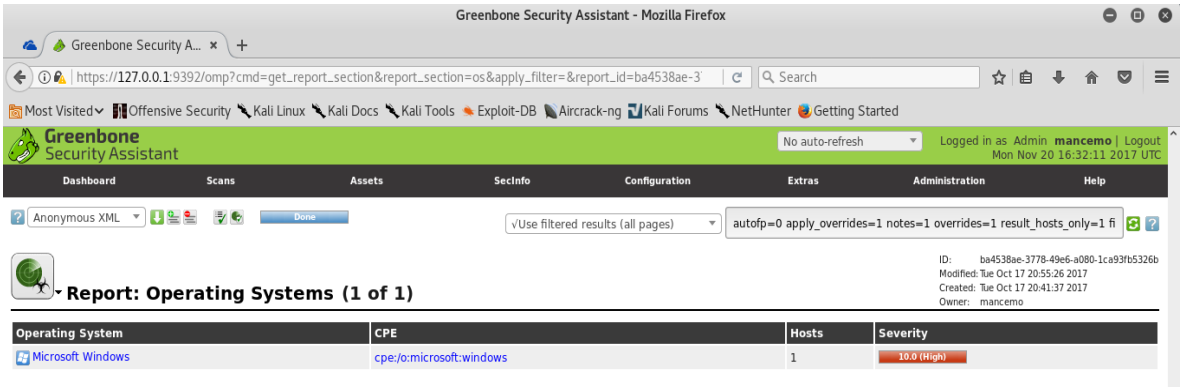
Figura 12. OPENVAS 192.168.1.5



Fuente: autor con datos de Cooperativa Alianza

A través de las herramientas de análisis, se pudo identificar que el sistema operativo del equipo es un sistema Microsoft Windows como se puede observar en la Figura 13.

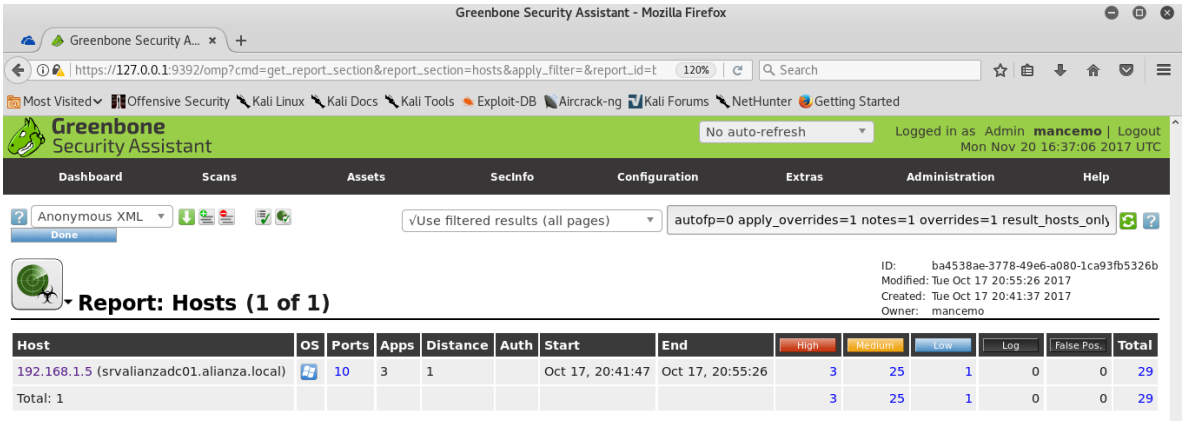
Figura 13. OPENVAS S.O.



Fuente: autores con datos de Cooperativa Alianza

Así mismo, en la Figura 14 se puede observar un resumen del análisis desplegado, en donde se encontró 3 vulnerabilidades con impacto alto, 25 con impacto medio y 1 con impacto bajo, 10 puertos abiertos los cuales se compararán con el listado PVR.

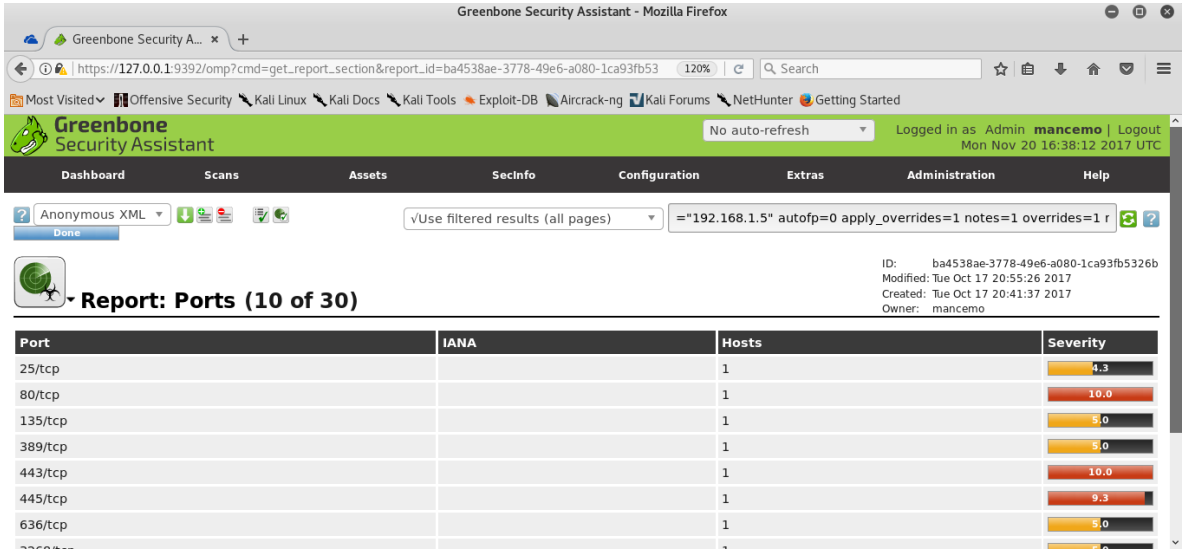
Figura 14. OPENVAS Resumen 192.168.1.5



Fuente: autor con datos de Cooperativa Alianza

Los puertos abiertos en este host se observan en la Figura 15

Figura 15. Puertos abiertos 192.168.1.5

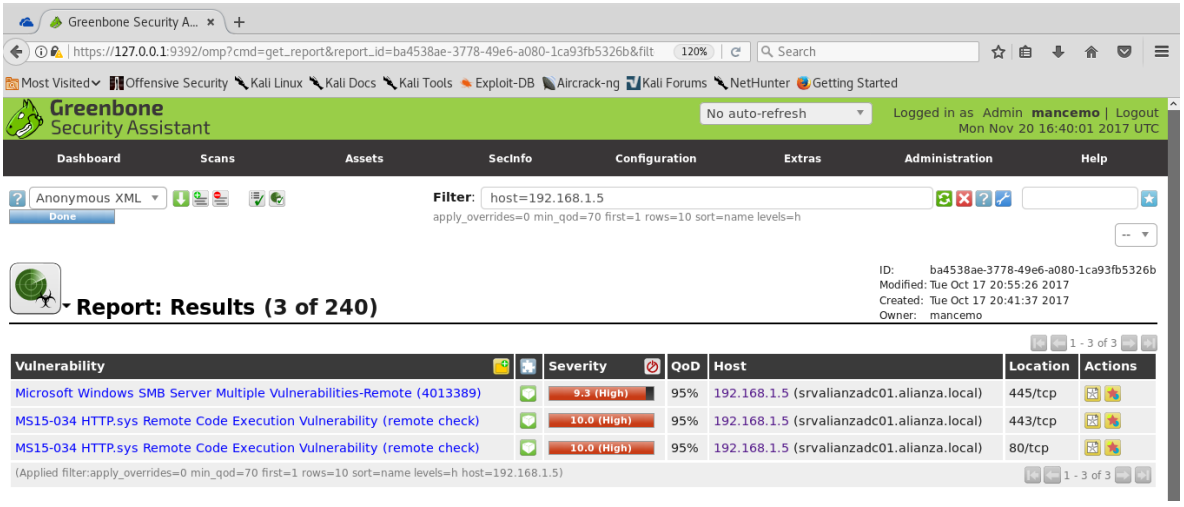


Fuente: autor con datos de Cooperativa Alianza

Los servicios marcados como alta severidad en este informe corresponden a los puertos 80, 443 y 445 donde se presentará en el análisis de riesgos el impacto a la organización.

Se encontraron 3 vulnerabilidades catalogadas con impacto alto, como se observa en la Figura 16, las cuales serán tratadas en el informe de riesgos.

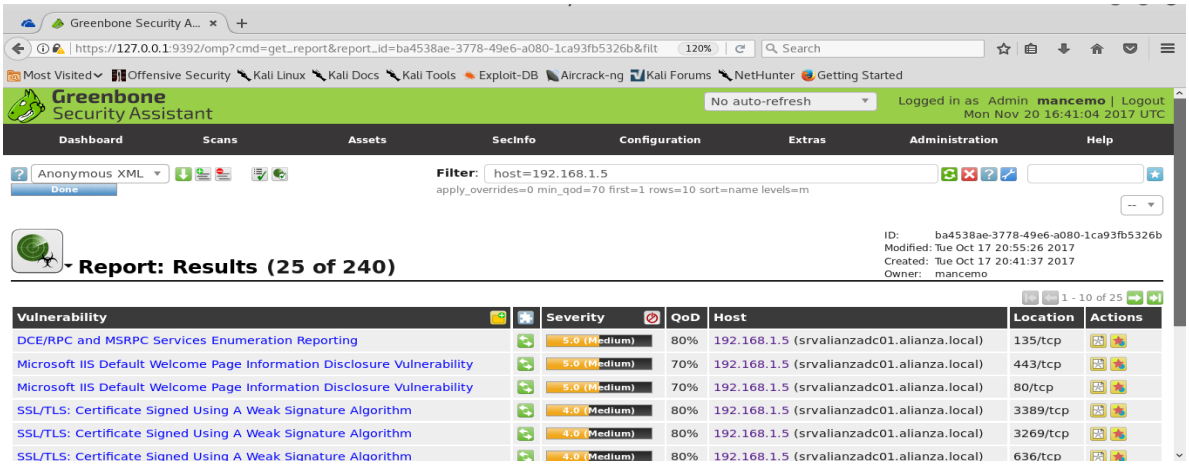
Figura 16. OPENVAS Vulnerabilidades 192.168.1.5



Fuente: autor con datos de Cooperativa Alianza

Se encontraron 25 vulnerabilidades catalogadas con impacto medio, como se observa en la Figura 17, las cuales serán tratadas en el informe de riesgos.

Figura 17. OPENVAS Vulnerabilidades 192.168.1.5



Fuente: autor con datos de Cooperativa Alianza

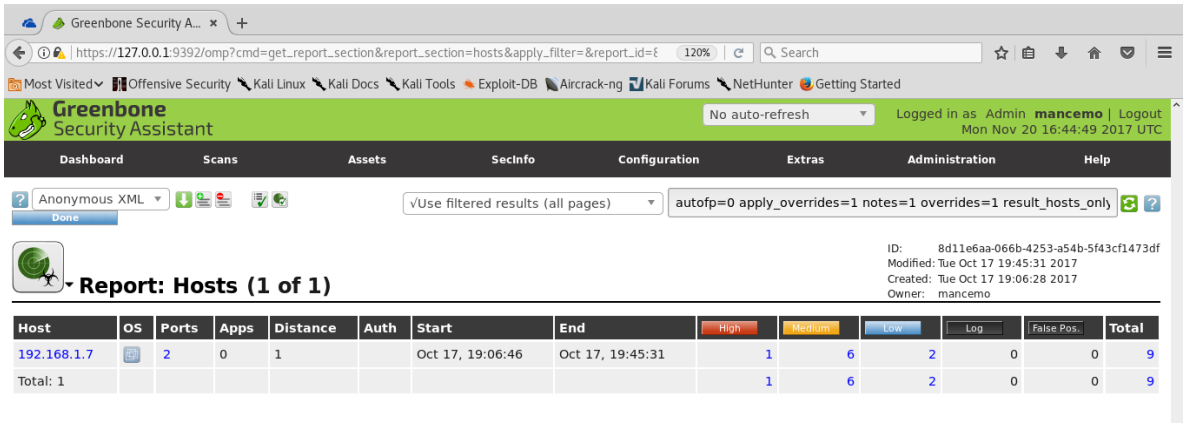
Se realiza el análisis al equipo 192.168.1.3, en la Figura 18 se observa el resumen del análisis efectuado, en donde se observa que no se logra identificar ninguna vulnerabilidad a este dispositivo a través de la herramienta OPENVAS.

Figura 18 . Resumen OPENVAS 192.168.1.3

Fuente: Elaboración propia con datos de Cooperativa Alianza

Se realiza el análisis al equipo 192.168.1.7, en la Figura 19 se observa el resumen del análisis efectuado, en donde se observa que el sistema operativo de ese equipo es un VMWARE ESXI, encontrando 2 Puertos abiertos,1 vulnerabilidades de impacto alto, 6 vulnerabilidades de impacto medio y 2 vulnerabilidades con impacto bajo.

Figura 19. OPVENVAS 192.168.1.7



Fuente: autor con datos de Cooperativa Alianza

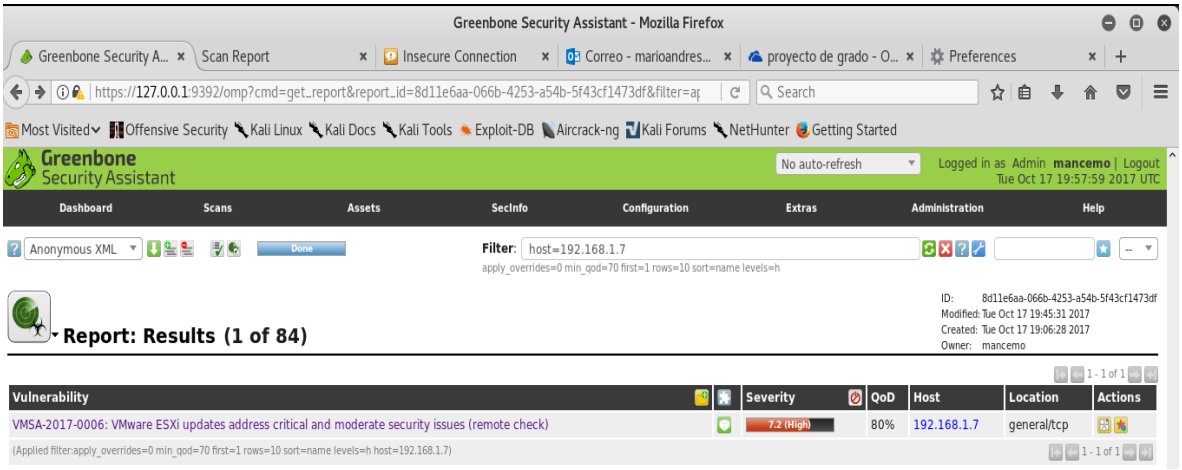
En la Figura 20 se pueden verificar los puertos abiertos en este host.

Figura 20. OPENVAS puertos 192.168.1.7

Fuente: autor con datos de Cooperativa Alianza

En la Figura 21 se observan las vulnerabilidades catalogadas con un impacto alto, en el análisis de riesgos se dará una explicación más detallada de la vulnerabilidad y el plan de acción a ejecutar.

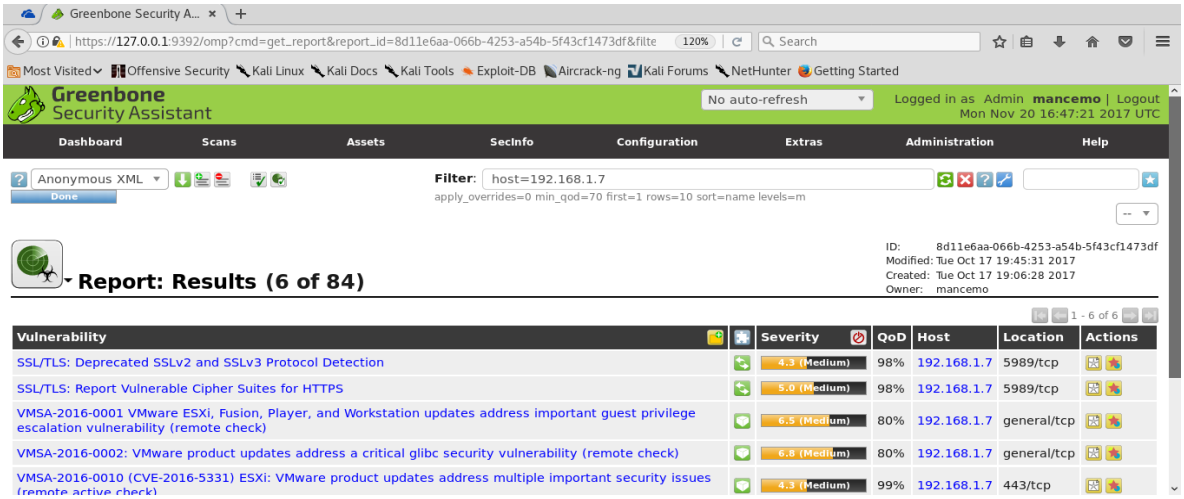
Figura 21. OPENVAS Vulnerabilidad impacto alto 192.168.1.7



Fuente: autor con datos de Cooperativa Alianza

En la Figura 22 se puede observar las vulnerabilidades detectadas con un impacto medio, así como las de impacto bajo detectadas.

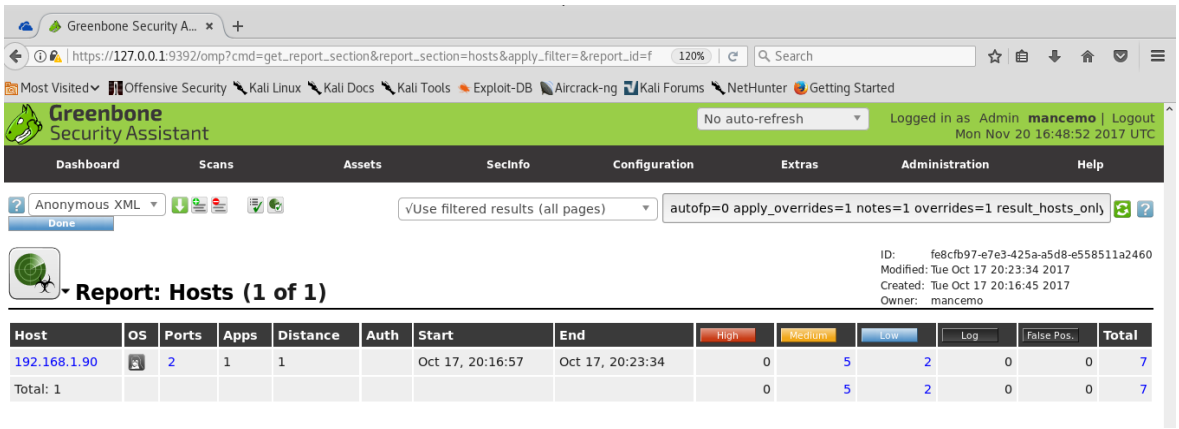
Figura 22. OPENVAS Vulnerabilidades media y baja 192.168.1.7



Fuente: autor con datos de Cooperativa Alianza

Se realiza el análisis al equipo 192.168.1.90, en la Figura 23 se observa el resumen del análisis efectuado, en donde se observa que el sistema operativo de ese equipo es un LINUX, encontrando 2 Puertos abiertos, 5 vulnerabilidades de impacto medio y 2 vulnerabilidades con impacto bajo.

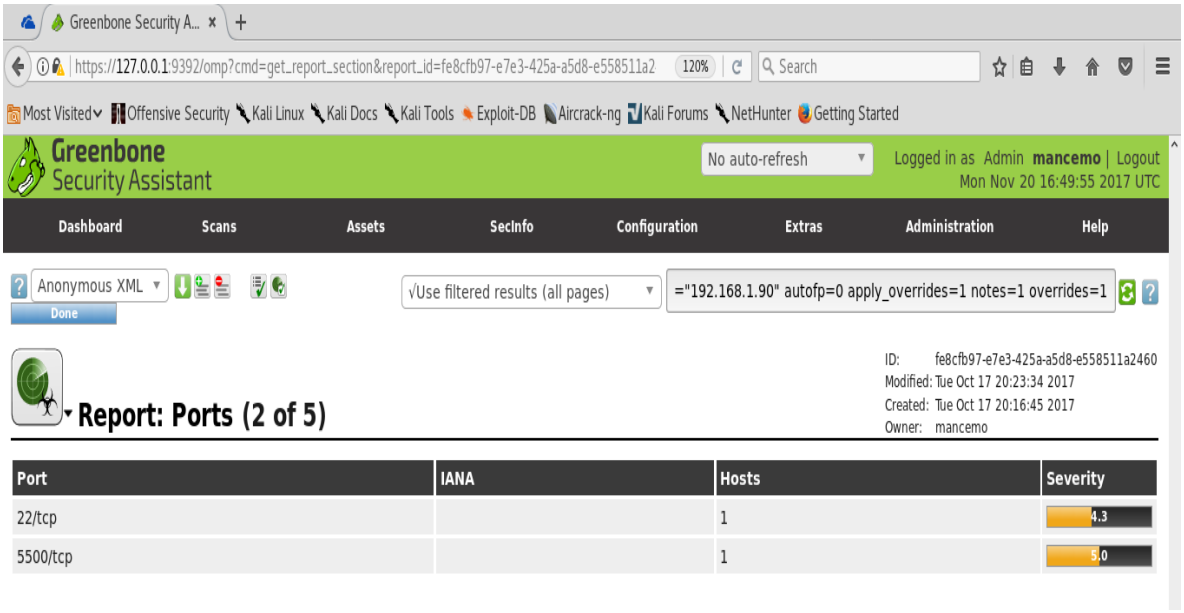
Figura 23. OPENVAS 192.168.1.90



Fuente: autor con datos de Cooperativa Alianza

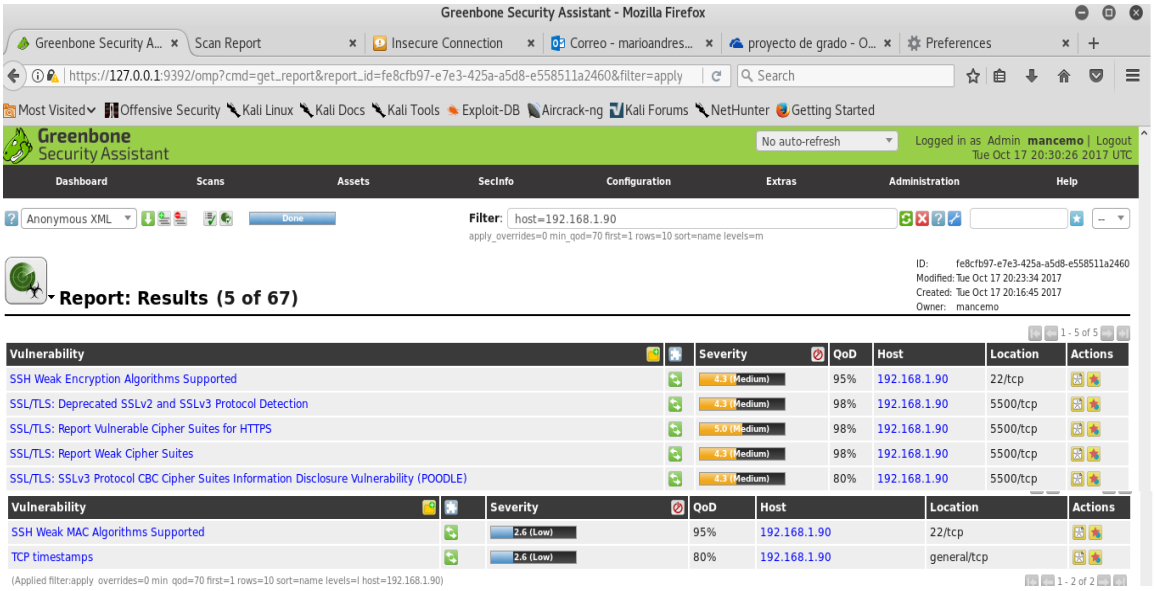
En la Figura 24 se observan los dos puertos abiertos en este host, y en la Figura 25 se observan y catalogan las vulnerabilidades referidas.

Figura 24 . OPENVAS Puertos abiertos 192.168.1.90



Fuente: autor con datos de Cooperativa Alianza

Figura 25. OPENVAS Vulnerabilidades 192.168.1.90



Fuente: autor con datos de Cooperativa Alianza

4.4 ANÁLISIS DE RIESGOS

La metodología de gestión de riesgos y privacidad de la información se tendrán en cuenta los lineamientos descritos en la norma técnica colombiana NTC-ISO/IEC 31000, así como los controles y seguridad definida a cada riesgo identificado se tendrá en consideración los controles informados en el Anexo A de la Norma Técnica Colombiana NTC-ISO/IEC 27001:2013, así como la metodología de análisis y medición de riesgos definida por la Cooperativa en su documento Matriz de SIAR (Sistema Integral de Administración de Riesgos)[64]

4.4.1 Definiciones.

Los siguientes términos y definiciones están basados en la norma ISO/IEC 31000[65]

Riesgo: Efecto de la incertidumbre sobre los objetos

Gestión del Riesgo: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Establecimiento del contexto: definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo, y establecimiento del alcance y los criterios de riesgo.

Valoración del riesgo: proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo.

Identificación del riesgo: Proceso para encontrar, reconocer y describir el riesgo.

Fuente del riesgo: elemento que solo o en combinación tiene el potencial intrínseco de originar un riesgo.

Evento: presencia o cambio de un conjunto particular de circunstancias.

Consecuencia: resultado de un evento.

---

[64] COOPERATIVA ALIANZA. Matriz de análisis propuestas SIAR (SARC, SARL, SARO), [En línea], [consultado el 21 de abril de 2016]. Disponible en: www.cooperativaalianza.com 2016.

[65] NORMA TÉCNICA COLOMBIANA NTC. ISO 31000 Cartilla Versión 2011-02-22. [En línea], [consultado el 21 de abril de 2016]. Disponible en: https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf

Probabilidad: Oportunidad de que algo suceda.

Perfil de riesgo: descripción de cualquier conjunto de riesgos.
Análisis del riesgo: proceso para comprender la naturaleza del riesgo.

Criterios del riesgo: Términos de referencia frente a los cuales se evalúa la importancia de un riesgo.

Nivel de riesgo: magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su probabilidad.

Evaluación del riesgo: proceso de comparación de los resultados del análisis de riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerantes.

Tratamiento del riesgo: proceso para modificar el riesgo.

Control: proceso que modifica al riesgo.

Riesgo residual: riesgo remanente después del tratamiento del riesgo.

4.4.2 Metodología de análisis de riesgo.

Para este análisis de riesgos se adoptó una metodología basado en el modelo propuesto de gestión de riesgos (Matriz de SIAR (Sistema Integral de Administración de Riesgos)) que la Cooperativa tiene definido actualmente.[66]

El impacto definido para la cooperativa, de determina en base a la consecuencia de la explotación de las amenazas sobre los activos de información, se clasificaron según la consecuencia como se indica en la tabla 13.

Tabla 13. Consecuencias explotación riesgos

Consecuencia	Descripción
Pérdida Financiera	Determina una pérdida de dinero

[66]COOPERATIVA ALIANZA. Op. Cit. p.70,

Consecuencia	Descripción
	para la cooperativa.
Seguridad de la Información	Determina una afectación a los servicios de confidencialidad e integridad de la información.
Demandas y/o Sanciones	Determina incumplimientos de orden legal generando riesgos de demandas por los asociados y/o usuarios, o sanciones por parte de los entes regulatorios.
Tabla 15. (Continuación)	
Fallas en los sistemas tecnológicos y de comunicación	Determina la no disponibilidad de los recursos tecnológicos que soportan la operación de la cooperativa. Afectando además el principio de disponibilidad de la información.
Deterioro imagen de la Cooperativa ante asociados y el estado	Determina el riesgo de desprestigio y pérdida de confianza por parte de los asociados y/o usuarios, así como de las entidades de regulación y el estado.
Número de Procesos afectados	Riesgo validado en la cantidad de procesos disponibles para el desarrollo de las actividades de la Cooperativa.
Fuente: autor con datos de Cooperativa Alianza	

Para cada consecuencia, es necesario definir una matriz que determine el nivel de impacto determinado para la cooperativa como se observa en la tabla 14 a la 19.

Tabla 14. Matriz de impacto pérdida financiera

Pérdida Financiera		
Insignificante	Pérdida financiera Baja. Del 0 al 1% de los Ingresos promedio registrados el último año (cierre fiscal)	No genera pérdida financiera o su efecto es marginal
Menor	Pérdida financiera Media. Pérdida mayor al 1% y menor o igual al 2% de los Ingresos promedio registrados el último año (cierre fiscal)	Genera pérdida financiera menor que no impacta la viabilidad de la Cooperativa
Moderado	Pérdida financiera Alta. Pérdida mayor al 2% y menor o igual al 7,5% de los Ingresos promedio registrados el último año (cierre fiscal)	Genera pérdida financiera moderada que restringe el presupuesto y puede impactar marginalmente sobre algunas áreas, procesos, procedimientos

Pérdida Financiera		
		y/o servicios
Mayor	Pérdida financiera Alta. Pérdida mayor al 7,5% y menor o igual al 10% de los Ingresos promedio registrados el último año (cierre fiscal)	Genera pérdida financiera alta que restringe el presupuesto e impacta sobre algunas áreas, procesos, procedimientos y/o servicios
Grave	Pérdida financiera Enorme. Más del 10% de los Ingresos promedio registrados el último año (cierre fiscal)	Genera pérdida financiera alta que restringe el presupuesto e impacta sobre algunas áreas, procesos, procedimientos y/o servicios, comprometiendo la viabilidad de la Cooperativa
Fuente: autor con datos de Cooperativa Alianza		

Tabla 15. Matriz de impacto seguridad de la información

Seguridad de la información	
Insignificante	No hay Pérdida de confidencialidad y/o propiedad de la información
Menor	Pérdida de confidencialidad y/o propiedad de la información – Pública
Moderado	Pérdida de confidencialidad y/o propiedad de la información - Uso Interno
Mayor	Pérdida de confidencialidad y/o propiedad de la información – Confidencial
Grave	Pérdida de confidencialidad y/o propiedad de la información – Secreta
Fuente: autor con datos de Cooperativa Alianza	

Tabla 16. Matriz impacto demandas y/o sanciones

Demandas y/o Sanciones		
Insignificante	No tiene la potencialidad de generar demandas y/o sanciones institucionales para la Cooperativa. – Requerimientos	No afecta
Menor	Podría generar demandas y/o sanciones institucionales para la Cooperativa de bajo impacto (afectación menor al 0,5% de los ingresos mensuales de la entidad)	Afectación marginal

Demandas y/o Sanciones		
Moderado	Podría generar demandas y/o sanciones institucionales para la Cooperativa de impacto moderado (afectación menor al 1% de los ingresos mensuales de la entidad)	Afectación moderada
Mayor	Podría generar demandas y/o sanciones institucionales para la Cooperativa de gran impacto (afectación mayor al 1% y menor al 10% de los ingresos mensuales de la entidad), sanciones que impidan la prestación de alguno de los servicios de la Cooperativa	Afectación significativa
Grave	Podría generar demandas y/o sanciones institucionales graves para la Cooperativa (afectación menor al 10% de los ingresos mensuales de la entidad), sanciones que impidan la prestación del servicio.	Afectación grave
Fuente: autor con datos de Cooperativa Alianza		

Tabla 17. Matriz impacto Fallas en los sistemas tecnológicos

Fallas en los sistemas tecnológicos y de comunicación		
Insignificante	Software: Falla en los sistemas que no afectan los sistemas core; Hardware: Falla del hardware que no soportan los sistemas core, Fallas en los canales de comunicación que no afectan los sistemas core, Redes: Fallas menores al 10% en los canales de comunicaciones que soportan los sistemas core	Fallas tecnológicas insignificantes cuya afectación en la operación es marginal
Tabla 17. (Continuación)		
Menor	Software: Fallas menores al 10% de los sistemas core, Hardware: Fallas menores al 10% en el hardware que soporta los sistemas core, Redes: Fallas menores al 10% en los canales de comunicaciones que soportan los sistemas core	Fallas tecnológicas menores, cuya afectación en la operación es percibida pero no la detiene

Fallas en los sistemas tecnológicos y de comunicación		
Moderado	Software: Fallas entre el 10% y el 25% de los sistemas core; Hardware: Fallas entre el 10% y 25% del hardware que soporta los sistemas core, Redes: Fallas entre el 10% y 25% de los canales de comunicación que soportan los sistemas core.	Fallas tecnológicas, cuya afectación en la operación es percibida y puede detener la operación por un período corto de tiempo o generar reprocesos
Mayor	Software: Fallas entre el 25% y 50% de los sistemas core, Hardware: Fallas entre el 25% y 50% del hardware que soporta los sistemas core, Redes: Fallas entre el 25% y 50% de los canales de comunicación que soportan los sistemas core	Fallas tecnológicas, pudiendo detener la operación por un período significativo de tiempo, generar reprocesos y/o deteriorar significativamente la prestación del servicio
Grave	Software: Falla en el 50% o más de los sistemas core; Hardware: Falla en el 50% o más del hardware que soporta los sistemas core; Redes: Falla en el 50% o más de los canales de comunicación que soportan los sistemas core.	Fallas tecnológicas graves, pudiendo detener la operación por un período significativo de tiempo, generar reprocesos y/o deteriorar significativamente la prestación del servicio. Generan secuelas en el tiempo
Fuente: autor con datos de Cooperativa Alianza		

Tabla 18. Matriz impacto deterioro imagen

Deterioro imagen de la Cooperativa ante asociados y el estado		
Insignificante	No afecta la imagen de la Cooperativa ante las autoridades, los asociados y el público en general	No afecta

Deterioro imagen de la Cooperativa ante asociados y el estado		
Menor	Respecto de la organización y sus prácticas de negocio, puede afectar marginalmente la entidad generando desprestigio o mala imagen de la Cooperativa ante las autoridades, los asociados y el público en general - Incremento hasta un 5% de las quejas.	Afectación marginal
Moderado	Respecto de la organización y sus prácticas de negocio, puede afectar moderadamente la entidad, generando desprestigio o mala imagen de la Cooperativa ante las autoridades, los asociados y el público en general - Incremento hasta un 10% de las quejas.	Afectación moderada
Mayor	Respecto de la organización y sus prácticas de negocio, puede afectar significativamente la entidad, generando desprestigio o mala imagen de la Cooperativa ante las autoridades, los asociados y el público en general - Incremento hasta un 15% de las quejas.	Afectación significativa
Grave	Respecto de la organización y sus prácticas de negocio, puede afectar gravemente la entidad, generando desprestigio o mala imagen de la Cooperativa ante las autoridades, los asociados y el público en general - Incremento mayor al 20% de las quejas.	Afectación grave
Fuente: autor con datos de Cooperativa Alianza		

Tabla 19. Matriz impacto número de procesos afectados

Número de Procesos afectados		
Insignificante	No genera reprocesos	No genera reprocesos

Menor	Puede generar reprocesos y/o interrupción en la ejecución de los procesos de 5 a 15 minutos.	Genera reprocesos en áreas o actividades que no son críticas ni comprometen el desarrollo de la operativa
Moderado	Genera un reproceso en los procesos estratégicos y/o afecta la ejecución de 1 proceso soporte. Genera interrupciones de 15 a 20 minutos.	Genera reprocesos en áreas o actividades que son sensibles, pero no comprometen el desarrollo de la operativa
Mayor	Genera más de un reproceso de los procesos estratégicos y/o afectos la ejecución de 2 o más procesos soporte de manera temporal de 20 y 40 minutos.	Genera reprocesos en áreas o actividades que son sensibles y afectan el desarrollo de la operativa
Grave	No se pueden ejecutar las actividades de los procesos estratégicos por más de 1 hora (Comercial, Crédito y Aportes y Ahorro) de la Cooperativa, poniendo en riesgo la operatividad del negocio.	Genera reprocesos en áreas o actividades que son sensibles e impiden el desarrollo de la operativa
Fuente: autor con datos de Cooperativa Alianza		

Para poder realizar una valoración de cada impacto, se define un estándar para cada nivel, como se puede observar en la tabla 22.

Tabla 20. Ponderación del nivel de impacto

Impacto	Ponderación del Impacto
Grave	50
Mayor	40
Moderado	30
Menor	20
Insignificante	10
Fuente: Elaboración propia con datos de Cooperativa Alianza	

También se determina el nivel de probabilidad que pueden tener las amenazas dentro de la organización, como se observa en la tabla 21.

Tabla 21. Matriz nivel de probabilidad

Probabilidad	Descriptor	
Casi Certeza	Se espera la ocurrencia del evento en la mayoría de las circunstancias. Eventualidad frecuente. Su probabilidad de ocurrencia es del 95% al 100%. El evento se ha presentado en el último mes.	Se espera que el evento ocurra casi con seguridad
Probable	El evento ocurrirá en casi cualquier circunstancia. Significativa probabilidad de ocurrencia. Su probabilidad de ocurrencia se encuentra entre el 65% al 95%. El evento se ha presentado en el último semestre.	El evento probablemente ocurrirá en la mayoría de las circunstancias
Posible	El evento ocurrirá en algún momento. Mediana probabilidad de ocurrencia. Su probabilidad de ocurrencia se encuentra entre el 20% al 65%. El evento se ha presentado en los últimos dos años.	El evento puede ocurrir en algún momento
Raro	El evento puede ocurrir en algún momento. Baja probabilidad de ocurrencia. Su probabilidad de ocurrencia se encuentra entre el 5% al 20%. El evento se ha presentado en los últimos cinco años.	El evento puede ocurrir en algún momento
Improbable	El evento puede ocurrir solo bajo circunstancias excepcionales. Muy baja probabilidad de ocurrencia. Su probabilidad de ocurrencia se encuentra entre 0% al 5%. El evento nunca se ha presentado.	El evento puede ocurrir solo en circunstancias excepcionales
Fuente: autor con datos de Cooperativa Alianza		

Para poder realizar una valoración de cada probabilidad, se define un estándar para cada nivel, como se puede observar en la tabla 22.

Tabla 22. Matriz evaluación probabilidad

Probabilidad	Ponderación de la probabilidad

Certeza	25
Probable	20
Posible	15
Raro	10
Improbable	5
Fuente: autor con datos de Cooperativa Alianza	

Basándose en el impacto y la probabilidad de la amenaza, se definen los niveles de riesgo para la Cooperativa como se puede observar en la tabla 23.

Tabla 23. Matriz niveles de riesgo

Nivel de Riesgo	**Valor Asignado**		**Acción Requerida**
	Mínimo	**Máximo**	
Extremo	750	1250	Evitar el riesgo empleando controles que busquen reducir el nivel de probabilidad. Reducir el riesgo empleando controles orientados a minimizar el impacto si el riesgo se materializa. Compartir o transferir el riesgo mediante la ejecución de pólizas.
Alto	450	749	Evitar o mitigar el riesgo mediante medidas adecuadas y aprobadas, que permitan llevarlo a la zona de riesgo moderado. Compartir o transferir el riesgo.
Moderado	250	449	Mitigar el riesgo mediante de medidas momentáneas y efectivas del proceso que permitan prevenirlo o llevarlo a la zona de riesgo bajo. Asumir el riesgo.
Bajo	50	249	Asumir el riesgo. Mitigar el riesgo con actividades propias del proceso y por medio de acciones detectivas y preventivas.
Fuente: autor con datos de Cooperativa Alianza			

Teniendo en cuenta la matriz anterior, se diseña un mapa de riesgo para Cooperativa Alianza, como se observa en la Figura 26, mediante el cual se da información a la administración gráficamente, para poder determinar los planes de acción a seguir.

Figura 26. Mapa de calor niveles de riesgo Cooperativa Alianza

Matriz de calificación de riesgo inherente

Ponderación	Probabilidad	Impacto				
		Insignificante	Menor	Moderado	Mayor	Grave
		10	20	30	40	50
25	Certeza	Moderado (250)	Alto (500)	Extremo (750)	Extremo (1000)	Extremo (1250)
20	Probable	Bajo (200)	Moderado (400)	Alto (600)	Extremo (800)	Extremo (1000)
15	Posible	Bajo (150)	Moderado (300)	Alto (450)	Alto (600)	Extremo (750)
10	Raro	Bajo (100)	Bajo (200)	Moderado (300)	Moderado (400)	Alto (500)
5	Improbable	Bajo (50)	Bajo (100)	Bajo (150)	Bajo (200)	Moderado (250)

Zona de riesgo		Puntaje	
		Mínimo	Máximo
	Extremo	750	1250
	Alto	450	749
	Moderado	250	449
	Bajo	50	249

Fuente: autor con datos de Cooperativa Alianza

Teniendo en cuenta las definiciones anteriores, se diseña una matriz en la cual se representarán los riesgos detectados en el análisis anterior, se puede observar en la Figura 27 la matriz definida.

Figura 27. Matriz riesgos Cooperativa Alianza

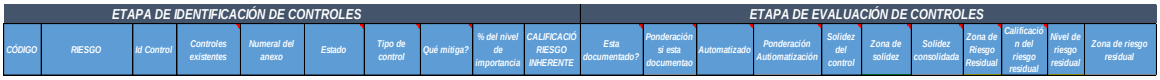
ETAPA DE IDENTIFICACIÓN DE RIESGOS								ETAPA DE MEDICIÓN						
CÓDIGO	RIESGO	EVENTO / CAUSA	DESCRIPCION DE LA CAUSA	FACTOR	ÁMBITO	CONSECUENCIAS	DESCRIPCIÓN DE LA CONSECUENCIA	PROBABILIDAD	VALOR PROBABILIDAD	IMPACTO	VALOR IMPACTO	CALIFICACIÓ RIESGO INHERENTE	NIVEL RIESGO INHERENTE	ZONA DE RIESGO INHERENTE

Fuente: autor con datos de Cooperativa Alianza

Esta definición de riesgo es el denominado riesgo inherente, es el riesgo intrínseco de cada actividad, sin tomar en cuenta los controles definidos para la mitigación de la probabilidad o el impacto asociados a cada actividad. Por esta razón es necesario hacer una valoración de los controles existentes o no dentro de cada proceso para determinar el riesgo residual, riesgo que aún persiste luego de la implementación de los controles, este es el riesgo que debe tratar la organización. Estos controles deben estar enmarcados dentro del anexo A de la norma colombiana NTC-ISO-IEC 27000.

Se define la siguiente plantilla para la identificación y clasificación de los controles como se observa en la figura 28.

Figura 28. Matriz definición de controles



Fuente: autor con datos de Cooperativa Alianza

Para la determinación de la eficiencia del control, en la tabla 24 se observan las variables y ponderaciones que determinen la eficiencia del control.

Tabla 24. Matriz ponderación controles por su diseño

Diseño	Valor
Documentado	100
No Documentado	0
Fuente: autor con datos de Cooperativa Alianza	

Igualmente teniendo en cuenta la operatividad del control, se define la tabla 25

Tabla 25. Matriz ponderación con roles por su operatividad

Diseño	Valor
Automatizado	4
Semi Automatizado	3
Manual	2
Fuente: autor con datos de Cooperativa Alianza	

Para poder determinar la solidez del control, se definen las siguientes zonas de aceptación para los controles como se observa en la tabla 26.

Tabla 26. Zonas de aceptación de los controles

Solidez	Puntaje
Alta/Zona de revisión periódica	400
Media/Zona de mejoramiento de controles	300
Baja/Zona de mejoramiento de controles	200
Muy baja/Zona de reingeniería de controles	0
Fuente: autor con datos de Cooperativa Alianza	

4,4,3 Medición Riesgo Inherente.

Luego de verificar los controles, se obtiene un nuevo mapa de calor con los niveles de riesgo residual, el cual es el que se presentara a la administración de la organización a fin de tomar las medidas necesarias de corrección o remediación a las vulnerabilidades y/o amenazas detectadas.

Al diligenciar la matriz de riesgos, se lograron identificar 28 vulnerabilidades en los equipos a los que se realizó el escaneo, encontrando que las vulnerabilidades según la clasificación de impacto y probabilidad descritas anteriormente como se observa en la Figura 29.

Figura 29. Mapa de Calor Cooperativa Alianza

	Zona de Riesgo Inherente				
	Insignificante	Menor	Moderado	Mayor	Grave
	10	20	30	40	50
Certeza (25)	0	0	3	0	0
Probable (20)	0	0	0	1	0
Posible (15)	0	0	2	1	0
Raro (10)	0	7	4	10	0
Improbable (5)	0	0	0	0	0

Fuente: autor con datos de Cooperativa Alianza

Se observan 4 riesgos en la zona extremo, como se observa en la tabla No. 27 donde se muestra una relación de los riesgos clasificaos en la zona extremo.

Tabla 27. Riesgos clasificados zona extremo

RIESGO	*EVENTO / CAUSA*	*DESCRIPCIÓN DE LA CAUSA*	*FACTOR*	*ÁMBITO*	*CONSECUENCIAS*

RIESGO	*EVENTO / CAUSA*	*DESCRIPCIÓN DE LA CAUSA*	*FACTOR*	*ÁMBITO*	*CONSECUENCIAS*
Acceso no autorizado a los sistemas de información	Actualización del Sistema Operativo	El equipo no cuenta con las últimas actualizaciones de seguridad según los boletines Microsoft MS17-010.	Tecnología	Interno	Seguridad de la Información
Acceso no autorizado a los sistemas de información	Actualización del Sistema Operativo	El host para la virtualización del servidor de dominio no cuenta con las últimas actualizaciones del sistema operativo en cuanto a seguridad liberadas por el fabricante.	Tecnología	Interno	Seguridad de la Información
Acceso no autorizado a los sistemas de información	Actualización del Sistema Operativo	El servidor host que virtualiza el servidor de dominio no cuenta con las últimas actualizaciones del sistema operativo en cuanto a seguridad liberadas por el fabricante	Tecnología	Interno	Seguridad de la Información
Acceso no autorizado a los sistemas de información	Puertos Abiertos	Riesgo de ataque por fuerza bruta a través de los puertos 22, y 5500 abierto en el servidor de bases de datos.	Tecnología	Externo	Seguridad de la Información
Fuente: autor con datos de Cooperativa Alianza					

En la tabla 28 se observan los 3 riesgos clasificados dentro de la zona alta.

Tabla 28. Riesgos clasificados zona alta

RIESGO	*EVENTO / CAUSA*	*DESCRIPCIÓN DE LA CAUSA*	*FACTOR*	*ÁMBITO*	*CONSECUENCIAS*
Acceso no autorizado a los sistemas de información	Puertos Abiertos	Riesgo de ataque por fuerza bruta a través de los puertos 22, 53 y 4444 abierto en el firewall	Tecnología	Externo	Seguridad de la Información
Riesgo de acceso utilizando el servicio DCE / RCP	Fallas Tecnológicas	El equipo no cuenta con las últimas actualizaciones de seguridad según boletín Microsoft MS17-010.	Infraestructura	Interno	Seguridad de la Información
Acceso no autorizado a los sistemas de información	Actualización del Sistema Operativo	El sistema Operativo del host para la virtualización del servidor de dominio no tiene las últimas actualizaciones de seguridad recomendadas por el fabricante	Tecnología	Externo	Seguridad de la Información
Fuente: autor con datos de Cooperativa Alianza					

En la tabla No. 29 se observan los 14 riesgos clasificados dentro de la zona moderada.

Tabla 29 Riesgos clasificados zona moderada

RIESGO	*EVENTO / CAUSA*	*DESCRIPCIÓN DE LA CAUSA*	*FACTOR*	*ÁMBITO*	*CONSECUENCIAS*
Acceso no autorizado a los sistemas de información	Fallas de Configuración	Riesgo de denegación del servicio a través de los puertos 443 y 3128 abierto en el firewall	Infraestructura	Externo	Fallas en los sistemas tecnológicos y de comunicación
Acceso no autorizado a los sistemas de información	Fallas de Configuración	Riesgo de denegación del servicio a través de los puertos 8090 y 8443 abierto en el firewall	Infraestructura	Externo	Fallas en los sistemas tecnológicos y de comunicación
Violación de los sistemas de seguridad debido a la utilización de mecanismos de encriptación débil.	Fallas de Configuración	El servicio asociado al puerto 3389 (RDP), 3269,636, 443 y 25 está utilizando una cadena de certificados SSL / TLS que se ha firmado utilizando un algoritmo de hashing criptográficamente débil.	Infraestructura	Interno	Seguridad de la Información
Violación de los sistemas de seguridad debido a la utilización de protocolos de encriptación muy antiguos.	Actualización del Sistema Operativo	Está en uso el protocolo SSLV2 y el servicio recomendado es SSLV3 a través de los servicios 3269, 636, 443 y 5.	Tecnología	Interno	Seguridad de la Información

Tabla 29. (Continuación)

RIESGO	*EVENTO / CAUSA*	*DESCRIPCIÓN DE LA CAUSA*	*FACTOR*	*ÁMBITO*	*CONSECUENCIAS*
Los servicios de directorio activo presentan información de configuración.	Fallas de Configuración	Es posible obtener información sobre la configuración del Directorio Activo.	Tecnología	Interno	Seguridad de la Información
Los servicios de directorio activo presentan información de configuración.	Fallas de Configuración	Es posible obtener información sobre la configuración del Directorio Activo	Tecnología	Interno	Fallas en los sistemas tecnológicos y de comunicación
Acceso no autorizado a los sistemas de información	Fallas de Configuración	Riesgo de denegación del servicio a través de los puertos 443 y 5989 en el equipo host donde se encuentra virtualizado el servidor de dominio.	Infraestructura	Externo	Fallas en los sistemas tecnológicos y de comunicación
Violación de los sistemas de seguridad debido a la utilización de protocolos de encriptación muy antiguos.	Actualización del Sistema Operativo	Está en uso el protocolo SSLV2 y el servicio recomendado es SSLV3 a través de los servicios 5989 en el servidor host de virtualización para el servidor de dominio.	Tecnología	Interno	Seguridad de la Información
Violación de los sistemas de seguridad debido a la utilización de protocolos de encriptación muy antiguos.	Actualización del Sistema Operativo	El servidor remoto SSH está configurado para permitir algoritmos de cifrado débiles	Tecnología	Interno	Seguridad de la Información
Tabla 29. (Continuación)					

RIESGO	*EVENTO / CAUSA*	*DESCRIPCIÓN DE LA CAUSA*	*FACTOR*	*ÁMBITO*	*CONSECUENCIAS*
Violación de los sistemas de seguridad debido a la utilización de protocolos de encriptación muy antiguos.	Actualización del Sistema Operativo	Está en uso el protocolo SSLV2 y el servicio recomendado es SSLV3 a través de los servicios 5500 del servidor de bases de datos.	Tecnología	Interno	Seguridad de la Información
Los servicios SSL/TLS presentan información detallada de su configuración	Fallas de Configuración	Esta rutina informa todos los conjuntos de cifrado SSL / TLS aceptados por un servicio donde los vectores de ataque solo existen en los servicios HTTPS en el servidor de bases de datos.	Tecnología	Interno	Fallas en los sistemas tecnológicos y de comunicación
Los servicios SSL/TLS presentan información detallada de su configuración	Fallas de Configuración	A través de una rutina, es posible obtener una relación de los servicios y puertos asociados a las aplicaciones disponibles en el servidor de bases de datos.	Tecnología	Interno	Fallas en los sistemas tecnológicos y de comunicación
Los servicios SSL/TLS presentan información detallada de su configuración	Fallas de Configuración	A través de una rutina, es posible obtener una relación de los servicios y puertos asociados a las aplicaciones disponibles en el servidor de bases de datos.	Tecnología	Interno	Fallas en los sistemas tecnológicos y de comunicación
Acceso no autorizado a los sistemas de información	Fallas de Configuración	El servidor SSH remoto está configurado para permitir algoritmos MAC débiles MD5 y / o 96 bits	Tecnología	Interno	Seguridad de la Información
Fuente: autor con datos de Cooperativa Alianza					

En la tabla 30 se observan los 7 riesgos clasificados dentro de la zona baja.

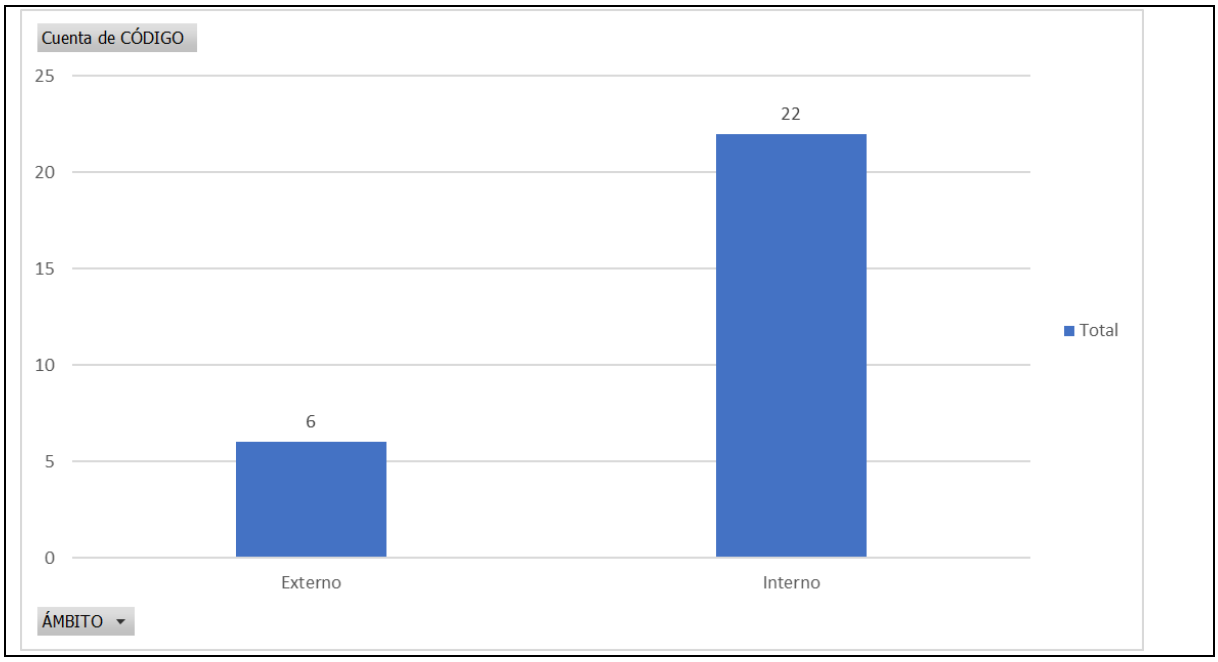
Tabla 30. Riesgos clasificados dentro de la zona baja

RIESGO	***EVENTO / CAUSA***	***DESCRIPCIÓN DE LA CAUSA***	***FACTOR***	***ÁMBITO***	***CONSECUENCIAS***
Acceso no autorizado a los sistemas de información	Fallas de Configuración	Riesgo de denegación del servicio a través de los puertos 25, 80, 135, 389, 443, 445,636, 3268, 3269 y 3389 abiertos en el servidor de dominio.	Tecnología	Interno	Fallas en los sistemas tecnológicos y de comunicación
Los servicios web presentan información detallada de su configuración	Fallas de Configuración	A través de una serie de comandos es posible obtener información detallada sobre las configuraciones de IIS.	Infraestructura	Interno	Fallas en los sistemas tecnológicos y de comunicación
Los servicios SSL/TLS presentan información detallada de su configuración	Fallas de Configuración	Esta rutina informa todos los conjuntos de cifrado SSL / TLS aceptados por un servicio donde los vectores de ataque solo existen en los servicios HTTPS.	Tecnología	Interno	Fallas en los sistemas tecnológicos y de comunicación
Los servicios SSL/TLS presentan información detallada de su configuración	Fallas de Configuración	A través de una rutina, es posible obtener una relación de los servicios y puertos asociados a las aplicaciones disponibles	Tecnología	Interno	Fallas en los sistemas tecnológicos y de comunicación
Tabla 30. (Continuación)					
Los servicios	Fallas de	A través de una	Tecnología	Interno	Fallas en los

RIESGO	*EVENTO / CAUSA*	*DESCRIPCIÓN DE LA CAUSA*	*FACTOR*	*ÁMBITO*	*CONSECUENCIAS*
SSL/TLS presentan información detallada de su configuración	Configuración	rutina, es posible obtener una relación de los servicios y puertos asociados a las aplicaciones disponibles			sistemas tecnológicos y de comunicación
Es posible determinar las marcas de tiempo.	Fallas de Configuración	Dentro de los equipos se implementa las marcas de tiempo TCP y, por lo tanto, permite calcular el tiempo de actividad. Vulnerabilidad presentada en el equipo host de virtualización del servidor de dominio, en el servidor de dominio y en el servidor de bases de datos.	Infraestructura	Interno	Fallas en los sistemas tecnológicos y de comunicación
Los servicios SSL/TLS presentan información detallada de su configuración	Actualización del Sistema Operativo	A través de una rutina, es posible obtener una relación de los servicios y puertos asociados al protocolo SSL en el servidor host de virtualización para el servidor de dominio.	Tecnología	Interno	Fallas en los sistemas tecnológicos y de comunicación
Fuente: autor con datos de Cooperativa Alianza					

Se puede observar que de las 28 vulnerabilidades encontradas dentro de los servidores a los que se corrió el análisis, 6 provienen de un ámbito externo a la organización equivalente al 21.43 % de las vulnerabilidades según se observa en la Figura 30.

Figura 30. Vulnerabilidades según su ámbito



Fuente: autor con datos de Cooperativa Alianza

4.4.3 Medición Riesgo Residual.

Luego del análisis de riesgo inherente, se corrió el análisis para verificar el riesgo residual de la Cooperativa Alianza, sobre el cual se diseñarán los planes de acción para la mitigación de estas vulnerabilidades.

En la Figura 31 se presenta el mapa de calor para el riesgo residual.

Figura 31 Mapa de riesgo residual

	Zona de Riesgo Inherente				
	Insignificante	Menor	Moderado	Mayor	Grave
	10	20	30	40	50
Certeza (25)	0	0	3	0	0
Probable (20)	0	0	0	1	0
Posible (15)	0	0	1	0	0
Raro (10)	0	6	2	9	0
Improbable (5)	0	1	3	2	0

Fuente: autor con datos de Cooperativa Alianza

Se puede observar que una vez establecidos los controles se observa una disminución considerable en los riesgos clasificados como altos, pasando de 3 a 1, lo mismo los riesgos clasificados en moderados pasando de 14 a 11 identificando que los controles logran minimizar el riesgo de exposición de Cooperativa Alianza, en la tabla 31 se observa un resumen de las zonas de riesgos sin aplicar los controles y luego aplicando los controles:

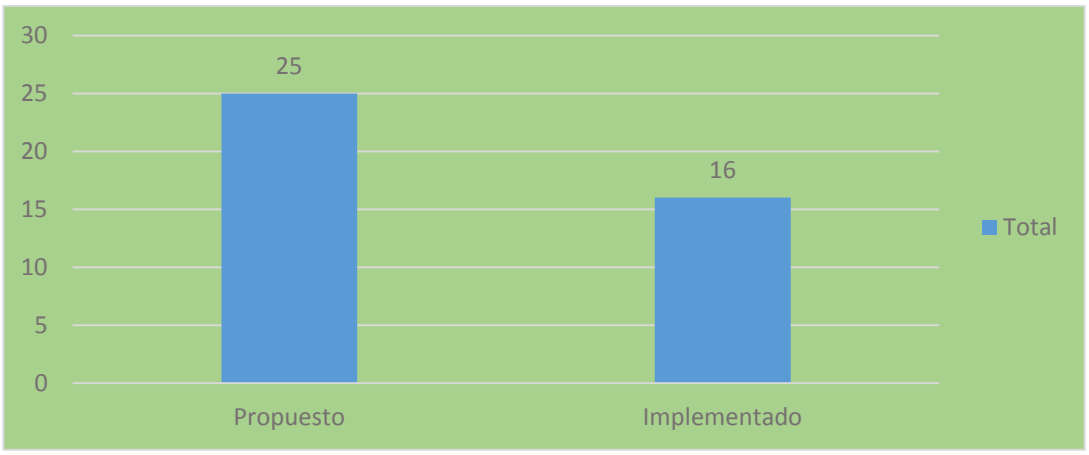
Tabla 31 Comparación zonas de riesgo

Nivel de Riesgo	Riesgo Inherente	Riesgo Residual	Variación
Extremo	4	4	0%
Alto	3	1	-200%
Moderado	14	11	-27%
Bajo	7	12	42%
Fuente: autor con datos de Cooperativa Alianza			

Se observa que los controles definidos, cumplen con el objetivo de disminuir las zonas de riesgo definidas, clasificando riesgos en la zona baja riesgos que se encontraban en alto y moderado.

De los 40 controles propuestos en este análisis, se encuentran implementados 16, como se puede observar en la Figura 32, es necesario que la Cooperativa Alianza determine la implementación de los controles propuestos.

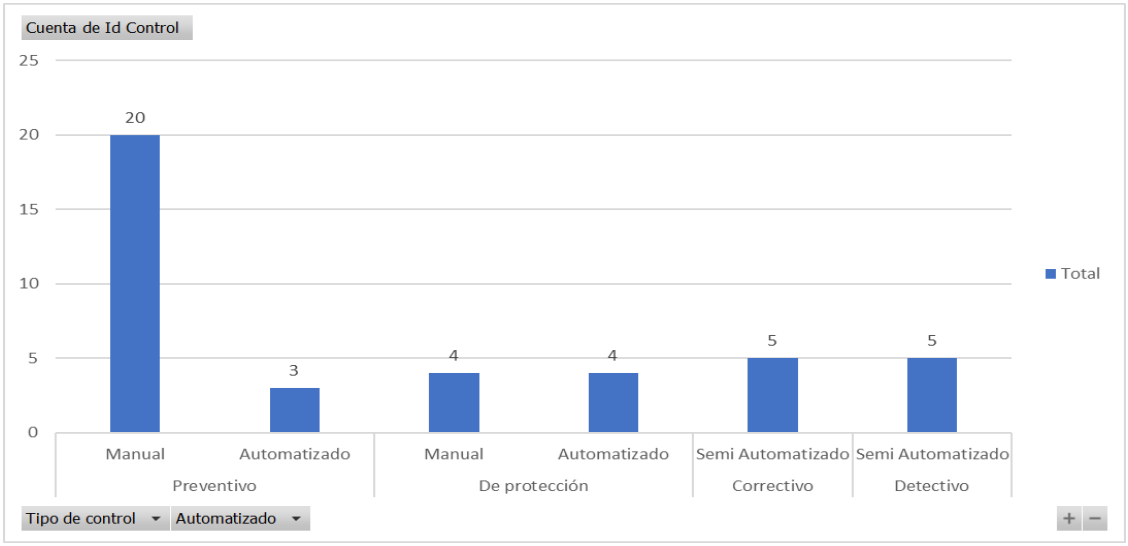
Figura 32. Controles implementados



Fuente: autor con datos de Cooperativa Alianza

De los controles definidos, se puede identificar que el 56.16% son controles de tipo preventivo como se puede observar en la Figura 33, de estos controles preventivos el 87% no se encuentran automatizados, es necesario identificar según la medición continua que conlleva un sistema de seguridad como automatizar los controles propuestos.

Figura 33 Tipos de controles



Fuente: autor con datos de Cooperativa Alianza

En la tabla 32 se observa la relación de los controles propuestos para Cooperativa Alianza

Tabla 32 Relación de los controles propuestos para Cooperativa Alianza

CÓD.	***RIESGO***	***Id Control***	***Controles existentes***	***Numeral del anexo***	***Estado***	***Tipo de control***	***¿Qué mitiga?***
1	Acceso no autorizado a los sistemas de información	1	Bloqueo Contraseña después de 3 intentos errados en la digitación de la misma	A.9 - Control de Acceso	Implementado	De protección	Probabilidad
		2	Políticas de Definición y entrega de contraseñas, así como la vigencia de las mismas	A.9.2 - Gestión de acceso de usuarios. A.9.3. - Responsabilidad de usuarios A.9.4. Control de acceso a sistemas y aplicaciones	Implementado	Preventivo	Probabilidad
2	Acceso no autorizado a los sistemas de información	3	Bloqueo Contraseña después de 3 intentos errados en la digitación de la misma	A.9 - Control de Acceso	Implementado	De protección	Probabilidad
		4	Políticas de Definición y entrega de contraseñas, así como la vigencia de las mismas	A.9.2 - Gestión de acceso de usuarios. A.9.3. – Responsabilidad de usuarios A.9.4. Control de acceso a sistemas y aplicaciones	Implementado	Preventivo	Probabilidad

CÓD.	*RIESGO*	*Id Control*	*Controles existentes*	*Numeral del anexo*	*Estado*	*Tipo de control*	*¿Qué mitiga?*
Tabla 32. Continuación							
3	Acceso no autorizado a los sistemas de información	5	Bloqueo Contraseña después de 3 intentos errados en la digitación de la misma	A.9 - Control de Acceso	Implementado	De protección	Probabilidad
		6	Políticas de Definición y entrega de contraseñas, así como la vigencia de las mismas	A.9.2 - Gestión de acceso de usuarios. A.9.3. – Responsabilidad de usuarios A.9.4. Control de acceso a sistemas y aplicaciones	Implementado	Preventivo	Probabilidad
4	Acceso no autorizado a los sistemas de información	7	Bloqueo Contraseña después de 3 intentos errados en la digitación de la misma	A.9 - Control de Acceso	Implementado	De protección	Probabilidad
		8	Políticas de Definición y entrega de contraseñas, así como la vigencia de las mismas	A.9.2 - Gestión de acceso de usuarios. A.9.3. – Responsabilidad de usuarios A.9.4. Control de acceso a sistemas y aplicaciones	Implementado	Preventivo	Probabilidad
5	Acceso no autorizado a los sistemas de información	9	Implementar un servicio desde el servidor que controle la dispersión de las actualizaciones y aplique automática mente las actualizaciones de seguridad WSUS	A.11.2.4 - Mantenimiento de Equipos	Propuesto	Preventivo	Probabilidad

CÓD.	*RIESGO*	*Id Control*	*Controles existentes*	*Numeral del anexo*	*Estado*	*Tipo de control*	*¿Qué mitiga?*
Tabla 32.	Continuación						
6	Riesgo de acceso utilizando el servicio DCE / RCP	10	Diseñar una plantilla que verifique los parámetros que se habilitan por default al instalar un nuevo servicio, deshabilitando los que no sean estrictamente necesarios.	A.12.5.1 - Instalació de software e sistemas operativos	Propuesto	Preventivo	Impacto
7	Riesgo de no disponibilidad de servicio por un ataque de DOS	11	Diseñar una plantilla que verifique los parámetros que se habilitan por default al instalar un nuevo servicio, deshabilitando los que no sean estrictamente necesarios.	A.12.5.1 - Instalació de software e sistemas operativos	Propuesto	Preventivo	Impacto

CÓD.	*RIESGO*	*Id Control*	*Controles existentes*	*Numeral del anexo*	*Estado*	*Tipo de control*	*¿Qué mitiga?*
Tabla 32.	Continuación						
8	Violación de los sistemas de seguridad debido a la utilización de mecanismos de encriptación débil	12	Implementar periódicamente un análisis de vulnerabilidades para identificar fallas en los sistemas operativos	A.12.6 - Gestión de l vulnerabilidad técnica	Propuesto	Detectivo	Impacto
		13	Plantilla de verificación a los sistemas operativos que entren a producción que cuenten con las últimas versiones de los mecanismos de encriptación	A.10.1 - Controle criptográficos A.12.5.1 - Instalació de software e sistemas operativos	Propuesto	Correctivo	Probabilidad
9	Violación de los sistemas de seguridad debido a la utilización de protocolos de encriptación muy antiguos.	14	Implementar periódicamente un análisis de vulnerabilidades para identificar fallas en los sistemas operativos	A.12.6 - Gestión de l vulnerabilidad técnica	Propuesto	Detectivo	Impacto
		15	Plantilla de verificación a los sistemas operativos que entren a producción que cuenten con las últimas versiones de los mecanismos de encriptación	A.10.1 - Controle criptográficos A.12.5.1 - Instalació de software e sistemas operativos	Propuesto	Correctivo	Probabilidad

CÓD.	*RIESGO*	*Id Control*	*Controles existentes*	*Numeral del anexo*	*Estado*	*Tipo de control*	*¿Qué mitiga?*
Tabla 32.	Continuación						
10	Riesgo de no disponibilidad de servicio por un ataque de DOS.	16	Diseñar una plantilla que verifique los parámetros que se habilitan por default al instalar un nuevo servicio, deshabilitando los que no sean estrictamente necesarios.	A.12.5.1 - Instalació de software e sistemas operativos	Propuesto	Preventivo	Impacto
11	Los servicios SSL/TLS presentan información detallada de su configuración	17	Diseñar una plantilla que verifique los parámetros que se habilitan por default al instalar un nuevo servicio, deshabilitando los que no sean estrictamente necesarios.	A.12.5.1 - Instalació de software e sistemas operativos	Propuesto	Preventivo	Impacto
12	Los servicios SSL/TLS presentan información detallada de su configuración	18	Diseñar una plantilla que verifique los parámetros que se habilitan por default al instalar un nuevo servicio, deshabilitando los que no sean estrictamente necesarios.	A.12.5.1 - Instalació de software e sistemas operativos	Propuesto	Preventivo	Impacto

CÓD.	*RIESGO*	*Id Control*	*Controles existentes*	*Numeral del anexo*	*Estado*	*Tipo de control*	*¿Qué mitiga?*
Tabla 32.	Continuación						
13	Riesgo de no disponibilidad de servicio por un ataque de DOS.	19	Diseñar una plantilla que verifique los parámetros que se habilitan por default al instalar un nuevo servicio, deshabilitando los que no sean estrictamente necesarios.	A.12.5.1 - Instalació de software e sistemas operativos	Propuesto	Preventivo	Impacto
14	Riesgo de no disponibilidad de servicio por un ataque de DOS.	20	Diseñar una plantilla que verifique los parámetros que se habilitan por default al instalar un nuevo servicio, deshabilitando los que no sean estrictamente necesarios.	A.12.5.1 - Instalació de software e sistemas operativos	Propuesto	Preventivo	Impacto
15	Riesgo de no disponibilidad de servicio por un ataque de DOS	21	Diseñar una plantilla que verifique los parámetros que se habilitan por default al instalar un nuevo servicio, deshabilitando los que no sean estrictamente necesarios.	A.12.5.1 - Instalació de software e sistemas operativos	Propuesto	Preventivo	Impacto

CÓD.	*RIESGO*	*Id Control*	*Controles existentes*	*Numeral del anexo*	*Estado*	*Tipo de control*	*¿Qué mitiga?*
Tabla 32. Continuación							
16	Acceso no autorizado a los sistemas de información	22	Bloqueo Contraseña después de 3 intentos errados en la digitación de la misma	A.9 - Control d Acceso	Implementado	De protección	Probabilidad
		23	Políticas de Definición y entrega de contraseñas, así como la vigencia de las mismas	A.9.2 - Gestión d acceso de usuario A.9.3. Responsabilidad d usuarios A.9.4. Control d acceso a sistemas aplicaciones	Implementado	Preventivo	Probabilidad
17	Acceso no autorizado a los sistemas de información	24	Implementar un servicio desde el servidor que controle la dispersión de las actualizaciones y aplique automáticamente las actualizaciones de seguridad (WSUS)	A.11.2.4 Mantenimiento d Equipos	Propuesto	Preventivo	Probabilidad

CÓD.	*RIESGO*	*Id Control*	*Controles existentes*	*Numeral del anexo*	*Estado*	*Tipo de control*	*¿Qué mitiga?*
Tabla 32. Continuación							
18	Violación de los sistemas de seguridad debido a la utilización de protocolos de encriptación muy antiguos.	25	Implementar periódicamente un análisis de vulnerabilidades para identificar fallas en los sistemas operativos	A.12.6 - Gestión de l vulnerabilidad técnica	Propuesto	Detectivo	Impacto
		26	Plantilla de verificación a los sistemas operativos que entren a producción que cuenten con las últimas versiones de los mecanismos de encriptación	A.10.1 - Controle criptográficos A.12.5.1 - Instalació de software e sistemas operativos	Propuesto	Correctivo	Probabilidad
19	Los servicios SSL/TLS presentan información detallada de su configuración	27	Diseñar una plantilla que verifique los parámetros que se habilitan por default al instalar un nuevo servicio, deshabilitando los que no sean estrictamente necesarios.	A.12.5.1 - Instalació de software e sistemas operativos	Propuesto	Preventivo	Impacto

CÓD.	*RIESGO*	*Id Control*	*Controles existentes*	*Numeral del anexo*	*Estado*	*Tipo de control*	*¿Qué mitiga?*
Tabla 32. Continuación							
20	Acceso no autorizado a los sistemas de información.	28	Implementar un servicio desde el servidor que controle la dispersión de las actualizaciones y apli que automáticamente las actualizaciones de seguridad (WSUS)	A.11.2.4 Mantenimiento d Equipos	Propuesto	Preventivo	Probabilidad
21	Acceso no autorizado a los sistemas de información	29	Bloqueo Contraseña después de 3 intentos errados en la digitación de la misma	A.9 - Control d Acceso	Implementado	De protección	Probabilidad
		30	Políticas de Definición y entrega de contraseñas, así como la vigencia de las mismas	A.9.2 - Gestión d acceso de usuario A.9.3. Responsabilidad d usuarios A.9.4. Control d acceso a sistemas aplicaciones	Implementado	Preventivo	Probabilidad

CÓD.	*RIESGO*	*Id Control*	*Controles existentes*	*Numeral del anexo*	*Estado*	*Tipo de control*	*¿Qué mitiga?*
Tabla 32.	Continuación						
22	Acceso no autorizado a los sistemas de información	31	Bloqueo Contraseña después de 3 intentos errados en la digitación de la misma	A.9 - Control d Acceso	Implementado	De protección	Probabilidad
		32	Políticas de Definición y entrega de contraseñas, así como la vigencia de las mismas	A.9.2 - Gestión d acceso de usuario A.9.3. Responsabilidad d usuarios A.9.4. Control d acceso a sistemas aplicaciones	Implementado	Preventivo	Probabilidad
23	Violación de los sistemas de seguridad debido a la utilización de protocolos de encriptación muy antiguos.	33	Implementar periódicamente un análisis de vulnerabilidades para identificar fallas en los sistemas operativos	A.12.6 - Gestión de l vulnerabilidad técnica	Propuesto	Detectivo	Impacto
		34	Plantilla de verificación a los sistemas operativos que entren a producción que cuenten con las últimas versiones de los mecanismos de encriptación	A.10.1 - Controle criptográficos A.12.5.1 - Instalació de software e sistemas operativos	Propuesto	Correctivo	Probabilidad

CÓD.	*RIESGO*	*Id Control*	*Controles existentes*	*Numeral del anexo*	*Estado*	*Tipo de control*	*¿Qué mitiga?*
Tabla 32. Continuación							
24	Violación de los sistemas de seguridad debido a la utilización de protocolos de encriptación muy antiguos.	35	Implementar periódicamente un análisis de vulnerabilidades para identificar fallas en los sistemas operativos	A.12.6 - Gestión de l vulnerabilidad técnica	Propuesto	Detectivo	Impacto
		36	Plantilla de verificación a los sistemas operativos que entren a producción que cuenten con las últimas versiones de los mecanismos de encriptación	A.10.1 - Controle criptográficos A.12.5.1 - Instalació de software e sistemas operativos	Propuesto	Correctivo	Probabilidad
25	Los servicios SSL/TLS presentan información detallada de su configuración	37	Diseñar una plantilla que verifique los parámetros que se habilitan por default al instalar un nuevo servicio, deshabilitando los que no sean estrictamente necesarios.	A.12.5.1 - Instalació de software e sistemas operativos	Propuesto	Preventivo	Impacto

CÓD.	*RIESGO*	*Id Control*	*Controles existentes*	*Numeral del anexo*	*Estado*	*Tipo de control*	*¿Qué mitiga?*
Tabla 32. Continuación							
26	Los servicios SSL/TLS presentan información detallada de su configuración	38	Diseñar una plantilla que verifique los parámetros que se habilitan por default al instalar un nuevo servicio, deshabilitando los que no sean estrictamente necesarios.	A.12.5.1 - Instalación de software en sistemas operativos	Propuesto	Preventivo	Impacto
27	Los servicios SSL/TLS presentan información detallada de su configuración	39	Diseñar una plantilla que verifique los parámetros que se habilitan por default al instalar un nuevo servicio, deshabilitando los que no sean estrictamente necesarios.	A.12.5.1 - Instalació de software e sistemas operativos	Propuesto	Preventivo	Impacto
28	Acceso no autorizado a los sistemas de información	40	Bloqueo Contraseña después de 3 intentos errados en la digitación de la misma	A.9 - Control d Acceso	Implementado	De protección	Probabilidad
		41	Políticas de Definición y entrega de contraseñas, así como la vigencia de las mismas	A.9.2 - Gestión d acceso de usuario A.9.3. Responsabilidad d usuarios A.9.4. Control d acceso a sistemas aplicaciones	Implementado	Preventivo	Probabilidad
Fuente: autor con datos de Cooperativa Alianza							

4.4.4 Socialización con la gerencia general.

Se realizó una reunión con el señor Juan Carlos Borda Fernández gerente general de Cooperativa Alianza, Cesar Bermúdez coordinador de riesgos y procesos, donde se socializaron los resultados obtenidos en el análisis de vulnerabilidades, y la Cooperativa tomo la decisión de incluir los riesgos planteados referentes a los controles sobre actualizaciones de seguridad de los fabricantes, y configuraciones por default de los diferentes sistemas de información dentro de la matriz de riesgos tecnológicos de la entidad, así como implementar en el menor tiempo posible la funcionalidad que permita controlar las actualizaciones de los equipos Windows a través del controlador de dominio, garantizando siempre la instalación de actualizaciones importantes, así mismo implementar un control en el área de TI que garantice una correcta administración de la reglas de filtrado en el Firewall.

Con esta reunión y compromisos de la Cooperativa, se da por finalizado el análisis de vulnerabilidades.

5. CONCLUSIONES

Luego de verificar el riesgo residual de Cooperativa Alianza, haciendo un análisis de las vulnerabilidades reportadas, se puede concluir que Cooperativa alianza cuenta con un ambiente de seguridad de la información satisfactorio en cuanto a los sistemas que sirvieron de muestra en el presente análisis, después de aplicados los controles se evidenciaron 4 riesgos catalogados en nivel extremo, todos enfocados en un riesgo de Acceso no autorizado a los sistemas de información y la remediación es ejecutar las diferentes actualizaciones pendientes por parte de los fabricantes, así como implementar el mecanismo de control definido en el presente análisis.

Implementar los controles expuestos en el presente análisis, los cuales se adaptan a la norma ISO 27001, permitirá que Cooperativa Alianza cada vez más reduzca los niveles de exposición a riegos, aunque lograr un sistema perfecto en seguridad de la información es un reto casi imposible de conseguir, con las valoraciones realizadas sobre los sistemas críticos de la organización, se evidencia un cumplimiento aceptable de sus políticas y niveles de seguridad.

Desde el área de tecnología, es necesario llevar un registro de incidentes de seguridad, que permitirá contar con información detallada para elaborar los planes de acción requeridos, realizando un seguimiento, control y ajuste a las políticas definidas por la organización.

6. RECOMENDACIONES

Luego de verificar el riesgo residual de Cooperativa Alianza, haciendo un análisis de las vulnerabilidades reportadas, se puede recomendar:

- Desarrollar un plan de trabajo que permita descargar las actualizaciones de seguridad que están pendientes en los diferentes servidores de la cooperativa.

- Implementar un sistema de control y monitoreo sobre las actualizaciones liberadas por los distintos fabricantes, para equipos con sistema operativo Windows, se puede implementar desde el controlador de dominio una herramienta denominada Wsus, la cual permite centralizar y gestionar las actualizaciones automáticamente y liberarlas dentro de los equipos vinculados al dominio.

- Implementar un plan de trabajo que permita verificar las configuraciones por default que tienen los servicios verificados en este análisis, para garantizar que no se evidencie información no pertinente a personas no autorizadas.

- Diseñar un esquema de control, para realizar un análisis de vulnerabilidades sobre los servidores que van a ingresar a producción, esto para determinar características como instalaciones y configuraciones de los servicios por default, puertos abiertos innecesariamente, vigencia de los sistemas de seguridad y encriptación, entre otros, esto permitirá tener un mayor control de los servicios puestos en producción mitigando vulnerabilidades por defecto de estos servicios.

- Se recomienda realizar un análisis de vulnerabilidades anualmente, a los servicios críticos de la organización, y por lo menos 1 vez cada dos años a los computadores clientes.

- Diseñar un control que permita evidenciar el monitoreo que realiza el sistema antivirus corporativos, desplegando con alguna frecuencia un análisis de todas las máquinas para garantizar el correcto funcionamiento del antivirus y una protección eficaz en las maquinas clientes.

- Diseñar un mecanismo de control, que permita evidenciar las modificaciones que se realicen sobre las reglas de filtrado del firewall, tener un backup de esta configuración valida y llevar un control sobre las modificaciones realizadas.

- Realizar un plan de sensibilización a los funcionarios de Cooperativa Alianza, para reforzar las medidas de seguridad y protección teniendo en cuenta que el

recurso humano es el eslabón más débil de la cadena de seguridad de la información.

BIBLIOGRAFÍA

ABARTIATEAM. ¿Qué es antispam?. [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: www.abartiateam.com/antispam-antivirus

ALIANZA COOPERATIVA. Misión y Visión. [En línea], [consultado el 20 de agosto de 2017]. Disponible en: www.alianza.coop

AVAST. ¿Qué son rootkit? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.avast.com/es-es/c-rootkit

BACA URBINA, Gabriel. Introducción a la seguridad informática, México: Grupo Editorial Patria, 2016.

CNET. ¿Qué es un bot? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.cnet.com/es/como-se-hace/que-es-un-bot/

COOPERATIVA ALIANZA. Misión, Visión y valores corporativos. [En línea], [consultado el 21 de abril de 2016]. Disponible en: www.alianza.coop

Planeación Estratégica 2014 – 2018. [En línea], [consultado el 20 de agosto de 2017]. Disponible en: https://www.aciamericas. coop/IMG/ pdf/plan_estrategico_ 2017_2020 _v4.pdf

Quienes somos. [En línea], [consultado el 21 de abril de 2016]. Disponible en: www.alianza.coop

CYIDIGITAL. ¿Qué es amenaza? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.cyldigital.es/articulo/amenazas-en-internet

OUAH.ORG. Port Vulnerability Reference (PVR). [En línea], [consultado el 21 de abril de 2016]. Disponible en: http://www.ouah.org/PVR.htm.

CULTURACIÓN. ¿Qué es encriptación? [En línea], [consultado el 3 de septiembre de 2017]. en: culturacion.com/que-es-encriptación-o-cifrado-de-archivos/

DHAVE SECURITY. ¿Qué es vector de ataque a WPA2? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.facebook.com/ DhavidSegundo/photos/a. ../1444726995576688/?type=3

DEFINICIONES ABC. ¿Qué significa antivirus? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.definicionabc.com/tecnologia/ antivirus.php

DEFINICION. Spyware. [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://definicion.de/spyware/

ECURED. ¿Qué son amenazas polimorfas? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.ecured.cu/ Amenazas _polimorfas

ECURED. ¿Qué es caballo de troya? Qué es Botnet? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://techlandia.com/definicion-del-virus-informatico-caballo-troya-sobre_54996/

¿Que son redes punto a punto? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.ecured.cu/Redes_punto_a_punto

ENTER.CO. ¿Qué es ingeniería social? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/

EL UNIVERSAL. ¡Qué es economía clandestina? [En línea], [consultado el 3 de septiembre de 2017]. en: interactivo.eluniversal.com.mx/online/PDF.../PDF-ECONOMÍA CLANDESTINA.pdf

FACEBOOK. ¿Qué significa Toolkit? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.facebook.com/toolkitfotografia/

FOCA, Informática 64. [En línea], [consultado el 20 de agosto de 2017]. Disponible en: http://www.informatica64.com/

GENBETA.COM. ¿Qué significa Malware? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.genbeta.com/.../malwarebytes-quiere-reemplazar-tu-antivirus-de-siempre.

HOSTING MONTEVIDEO. Greylisting o lista gris. [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.hostingmontevideo. com/ clientes/index. php?rp=/.../82/ Greylisting.html

INFOSEGUR. ¿Qué es Vulnerabilidad? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://infosegur.wordpress.com/tag/ vulnerabilidades/

INFOSPYWARE. ¿Qué son los virus informáticos? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.infospyware.com/articulos/¿que-son-los-virus-informaticos/

¿Qué es el phishing? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.infospyware.com/articulos/que-es-el-phishing/

¿Qué es software de seguridad fraudulento? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www. infospyware. com/ articulos/rogue-software-fakeav/

ISECOM.ORG. Open Source Security Testing Methodology Manual [En línea], [consultado el 20 de agosto de 2017]. Disponible en: http://www.isecom. org/research/

KAPERSKY. ¿Qué son gusanos cibernéticos? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.kaspersky.es/resource-center/threats/viruses-worms

MALWAREBYTES. ¿Que son variantes? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://es.malwarebytes.com/pdf/white-papers/es/DefeatingRansomware.pdf

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN. ¿Qué son Aplicaciones engañosas? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: www.mintic.gov.co/ portal/ 604/w3-article-18745.html.

¿Qué son ataques multi-etapas? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: www.mintic.gov.co/portal/ 604/w3-article-18750.html

¿Qué es Blacklisting o lista negra? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: www.mintic.gov. co/portal/ 604/w3-article-18749.html.

¿Qué es Keystroke Logger o Programa de captura del teclado? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: www.mintic.gov.co/portal/604/w3-article-18802.html

¿Qué es, mecanismo de propagación? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: www.mintic.gov.co/portal/604/w3-article-18804.html

¿Qué son Exploits o Programas intrusos? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: www.mintic.gov.co/portal/604/w3-article-18797.html

NORMA TÉCNICA COLOMBIANA NTC. ISO 31000 Cartilla Versión 2011-02-22. [En línea], [consultado el 21 de abril de 2016]. Disponible en: https:// sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf

ONIUP.COM. ¿Qué es lista blanca o whitelisting? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://oniup.com/que-es/white-list/

OWASP. Web Application Penetration Testing. [En línea], [consultado el 20 de agosto de 2017]. Disponible en: https://www.owasp.org/index.php/Web_ Application_Penetration_Testing

PANDA SECURITY. ¿Qué es **PROTECCIÓN HEURÍSTICA?** [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.panda security.com/enterprise/ downloads/ docs/product/...00.../582.htm

Sistema de prevención de intrusos. [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.pandasecurity.com/usa-es/support/ card?id= 31452

PATERVA.COM. ¿Qué es Maltego?, [En línea], [consultado el 20 de agosto de 2017]. Disponible en: https://www.paterva.com/web7/buy/maltego-clients/maltego-ce.php

PENTEST STANDARD.ORG. The Penetration Testing Execution Standard. [En línea], [consultado el 20 de agosto de 2017]. Disponible en: http://www.pentest-standard.org/ index. php/Main_Page

REDES TELECOM. Seguridad basada en la reputación. [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: www.redestelecom.es › Noticias › Informática Profesional

REVISTA DE SEGURIDAD UNAM. ¿Qué son Ataques WEB? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://revista. seguridad.unam.mx/numero-05/ataques-web

¿Qué es Firewall? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://revista.seguridad.unam.mx/numero-18/firewall-de-bases-de-datos

SEGURIDAD INFORMÁTICA. ¿Qué es Carga destructiva? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://seguinfo.wordpress. com/2009/04/06/¿carga destructiva?/

¿Qué es Crimeware? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://seguinfo.wordpress.com/2009/04/06/¿que-es-crimeware/

SALLIS Ezequiel, CAACCIOLO Claudio, RODRIGUEZ Marcelo. Ethical Hacking Argentina: Alfaomega, 2010.

SEO. ¿Qué es ciberdelitos? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: www.seo-posicionamientoweb.com/ciberdelitos-definicion-tipos-frecuentes

SMARTERWORKSPACES. ¿Qué es virus? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://smarterworkspaces.kyocera.es/blog/8-tipos-virus-informaticos-debes-conocer/

SOFTDOIT. ¿Qué es Botnet? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.softwaredoit.es/definicion/definicion-botnet.html

SPYWARE. ¿Qué es adware? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.segu-info.com.ar/malware/spyware.htm

SYMANTEC. ¿Qué es pharming? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en:www.symantec.com/region/mx/avcenter/cybercrime/ pharming.html

TIBCO SOFTWARE. **Filtrado de datos.** [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://docs.tibco.com/.../GUID-6CF74B7C-9425-4BDE-B8C4-F9F45B1F1710.html

VALOR TOP. ¿Qué es Spam? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: www.valortop.com/blog/que-significa-spam

VELAVERDE, Mario. Sistema de detección de intrusos. [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: www.aslan.es/ boletin/ boletín 41/ ironport.shtml

WEBSECURITY. ¿Qué es un ataque de negación de servicio? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: www.websecurity.es/que-es-un-ataque-denegaci-n-servicio

WELIVESECURITY. ¿Qué significa firma antivirus? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: https://www.welivesecurity.com/la-es/2014/.../cumplimos-10000-faq-firmas-antivirus/

¿Cómo gestionan la seguridad las empresas en Latinoamérica? [En línea], [consultado el 21 de abril de 2016]. Disponible en: http://www.welivesecurity.com/la-es/2016/04/21/como-gestionan-seguridad-empresas-de-latinoamerica/

WIKISEGURIDAD. ¡Qué es descarga inadvertida? [En línea], [consultado el 3 de septiembre de 2017]. Disponible en: wikiseguridad.org/descarga-inadvertida

WIKIPEDIA. Google Hacking, [En línea], [consultado el 20 de agosto de 2017]. Disponible en: https://es.wikipedia.org/wiki/Google_Hacking