UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
PROPUESTA METODOLÓGICA DE BUENAS PRÁCTICAS PARA APLICAR ETHICAL HACKING EN INSTITUCIONES FINANCIERAS DE LA ECONOMÍA POPULAR Y SOLIDARIA
Línea de Investigación:
Sistemas de Información e Informática
Campo amplio de conocimiento:
Tecnologías de la Información y Comunicación (TIC)
Autor:
Quezada Ochoa Leandro Damian
Tutor:
Mg. Recalde Varela Pablo Marcel

Quito – Ecuador

2023

APROBACIÓN DEL TUTOR

Yo, PABLO MARCEL RECALDE VARELA con C.I: 1711685055 en mi calidad de Tutor del proyecto de investigación titulado: PROPUESTA METODOLÓGICA DE BUENAS PRÁCTICAS PARA APLICAR ETHICAL HACKING EN INSTITUCIONES FINANCIERAS DE LA ECONOMÍA POPULAR Y SOLIDARIA.

Elaborado por: LEANDRO DAMIAN QUEZADA OCHOA, de C.I: 0105073175, estudiante de la Maestría: SEGURIDAD INFORMÁTICA, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2023

Firmado electrónicamente por:
PABLO MARCEL
RECALDE VARELA

Firma

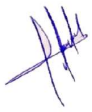
ORCID: 0000-0001-7256-2836

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, LEANDRO DAMIAN QUEZADA OCHOA con C.I: 0105073175, autor del proyecto de titulación denominado: PROPUESTA METODOLÓGICA DE BUENAS PRÁCTICAS PARA APLICAR ETHICAL HACKING EN INSTITUCIONES FINANCIERAS DE LA ECONOMÍA POPULAR Y SOLIDARIA.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., septiembre de 2023



_____

Firma

ORCID: 0009-0001-2974-1828

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

La seguridad informática ha ganado popularidad en los últimos años y ha pasado de ser considerada como un incremento en los gastos operativos, a ser vista como una inversión por parte de los directivos de las empresas y organizaciones a nivel mundial.

Contextualización del tema

En algunos países esto ha sucedido de forma acelerada, en otros el paso ha sido más lento; pero en última instancia todos han convergido en un mundo digital en el que la información es el activo intangible más valioso; y por consiguiente debe ser protegido de posibles pérdidas, robos, mal uso, etc. (Suarez, 2020).

Según (OEA, 2018) El sector financiero, ha sido uno de los sectores con mayores índices de digitalización. Cada día un mayor número de clientes del sector financiero son usuarios de servicios electrónicos, realizan transacciones por internet o pagos a través de dispositivos móviles. Esta adaptación de los modelos de negocio y la explotación de canales digitales pretenden aprovechar las ventajas de las tecnologías, que tiene como contrapartida la aparición de nuevos riesgos que se deben prevenir con el fin de mitigar los posibles ataques y situaciones de fraude a los que está expuesto actualmente el sector y, por supuesto sus usuarios.

En Ecuador, al igual que en muchos otros países de América Latina, los sistemas informáticos, incluyendo los servidores y servicios que brindan las instituciones financieras, están en constante riesgo de ser vulnerados y atacados. Con el avance de nuevas tecnologías y técnicas, las amenazas a estos sistemas aumentan cada año. Por lo tanto, es fundamental considerar qué es lo que se debe proteger y de quién, y definir las políticas de seguridad adecuadas para garantizar una red segura. Estas políticas deben incluir estrategias claras para proteger los sistemas y evitar vulnerabilidades (Ojeda y otros, 2020).

Es esencial garantizar la protección de los equipos informáticos para evitar riesgos que puedan poner en peligro la estabilidad de la organización. Hay que tener en cuenta que la seguridad informática está estrechamente relacionada con la gestión de riesgos. Invertir en la protección de los sistemas informáticos no solo mejora la rentabilidad, sino que también demuestra un compromiso sólido hacia el futuro de las entidades financieras.

Las instituciones financieras de la economía popular y solidaria en el Ecuador tienen regulaciones específicas de seguridad informática que deben cumplir como son las Resoluciones: SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-009, y la SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002 de la Superintendencia de Economía Popular y Solidaria (SEPS).

Problema de investigación

Todas las instituciones financieras con el propósito de prestar sus servicios están obligadas a recopilar información sensible de las personas, las mismas deben estar debidamente protegidas; en este proceso juega un papel importante el tipo de controles infraestructura/seguridad que utilicen y quien esté encargado de la misma. Con el objeto de no sufrir ningún ataque o robo por personas no autorizadas y puedan contar con mayor confianza dentro del mercado al que se dedican.

Muchas empresas actualmente no cuentan con herramientas y procesos ante ataques de seguridad informática, no reconocen la importancia de implementar medidas de protección de la información, ya que se suele creer que su única tarea es prestar servicios financieros. Sin embargo, es fundamental que comprendan que la seguridad informática es un tema crítico para salvaguardar la integridad de sus activos y la información (Gutierrez, 2022).

En octubre del 2021 la superintendencia de bancos del Ecuador, confirmó que una de las instituciones financieras más importante del Ecuador fue víctima de un ciberataque, cometido por delincuentes informáticos internacionales, esto generó la indisponibilidad principalmente de canales electrónicos, y también generó desconfianza entre sus clientes (Harán, 2021).

En la actualidad, la seguridad informática se ha convertido en un tema crítico para las instituciones financieras, ya que deben proteger su activo más valioso: la información. En este sentido, es fundamental implementar medidas que resguarden la información y eviten vulnerabilidades de cualquier tipo (Malagon, 2023).

Es por eso que las entidades de control reguladoras como lo es la Superintendencia de Economía Popular y Solidaria genera la resolución SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-009, donde consta en la sección V de los respaldos y auditoria, «Artículo 32: Auditoría de seguridad. - Las entidades deberán establecer y

ejecutar procedimientos de auditoría de seguridad en sus canales electrónicos, por lo menos, una vez al año» (SEPS, 2023).

Si una empresa sufre un ataque informático, puede enfrentar grandes costos por la recuperación de datos, la reparación de sistemas y otros gastos asociados. Al realizar Ethical Hacking, se pueden identificar y corregir vulnerabilidades antes de que se produzca un ataque, lo que puede ahorrar dinero y recursos.

¿Realizar un Ethical hacking ayuda a identificar vulnerabilidades, mejorar la seguridad, proteger sus finanzas y cumplir normativas?

Objetivo general

Diseñar una metodología que fomente buenas prácticas para la aplicación de Ethical Hacking en las instituciones financieras de la economía popular y solidaria.

Objetivos específicos

- Proporcionar un marco contextual de los conceptos fundamentales del Ethical Hacking, Pentesting y herramientas que serán empleadas en el proceso.
- Analizar la aplicabilidad de las herramientas de Ethical Hacking en varias plataformas y sistemas operativos.
- Diseñar un guía de buenas prácticas para realizar Ethical Hacking.
- Valorar el uso de la guía en varias instituciones financieras.

Vinculación con la sociedad y beneficiarios directos:

La presente metodología tiene como objetivo contribuir al cumplimiento de los Objetivos de Desarrollo Sostenible (ODS), especialmente el noveno ODS centrado en la industria, innovación e infraestructura. Esta metodología busca promover la adopción de nuevas tecnologías, facilitar el comercio y fomentar el uso eficiente de los recursos.

Los beneficiarios directos se encuentran el personal del área de seguridad informática de las entidades financieras, que son los que van verificar y aplicar estas herramientas, con el fin de identificar áreas de mejora en los procesos y procedimientos de seguridad, y mejorar la conciencia de seguridad entre los usuarios y el personal de una organización.

Los beneficiarios indirectos son todos los socios o clientes que consumen los servicios, puesto que con la ayuda de las herramientas se minimiza el riesgo cuando utilizan los servicios transaccionales.

Como un beneficiario adicional son los profesionales de la seguridad informática y los docentes de Ethical Hacking ya que podrán utilizar una metodología flexible, y para la aplicación práctica se incluye una amplia gama de herramientas y utilidades de seguridad informática.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

Las instituciones financieras del segmento de la economía popular y solidaria en Ecuador deben considerar el hacking ético como una herramienta para comprender a fondo las fortalezas y debilidades de sus sistemas informáticos, mientras que la industria de la seguridad informática continúa en crecimiento para salvaguardar y proteger los datos de sus usuarios.

1.1. Contextualización general del estado del arte

Hoy en día, los ciberataques se han convertido en una forma de robo muy común debido a los avances en la tecnología y los procesos de internet en las empresas, organizaciones y principalmente las entidades financieras, infiltrándose directamente en la seguridad de todo tipo de corporaciones en Ecuador y el mundo (Rubio, 2019).

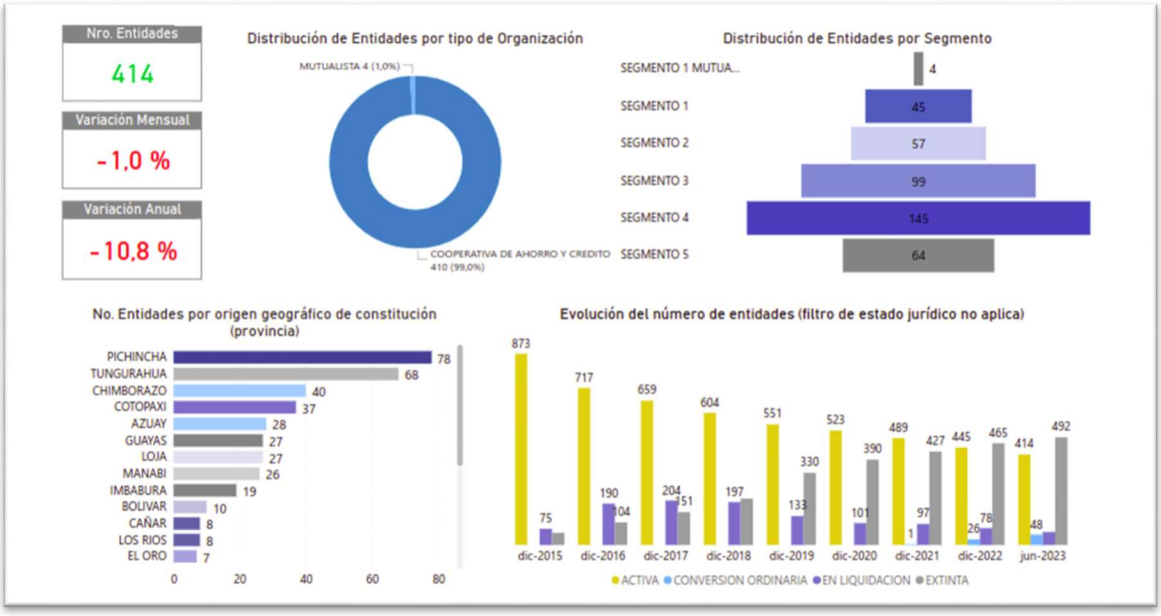
Los ciberdelincuentes utilizan su ingenio para ingresar al sistema a través de softwares especialmente elaborados con este propósito a través de múltiples formas de acceder a datos personales de los usuarios y causar revuelo en las empresas, gobiernos e instituciones financieras y comerciales (Guerra, 2022).

Según cifras del Observatorio de Ciberseguridad de la multinacional GMS, empresa especializada en seguridad informática, el ranking de los sectores que han sido víctimas de ciberataques efectivos está liderado por las entidades públicas con un 20%, seguido por la industria de alimentos con el 16%, en tercer lugar, las empresas de retail también con el 16% y en cuarto puesto el sector financiero y el de seguros y salud con el 12% (GMS, 2022).

En base a la recopilación de datos de la Superintendencia de Economía Popular y Solidaria en Ecuador, se registran 410 Cooperativas de Ahorro y Crédito y 4 Mutualistas bajo su supervisión. La creciente cantidad de entidades amplía la superficie de riesgo para posibles ataques cibernéticos por parte de delincuentes informáticos.

Figura 1.

Instituciones Financieras de la Economía Popular y Solidaria en el Ecuador



Nota: Sistema de Gestión de Organizaciones del Sector Financiero, adaptado a la propuesta. Tomado de Superintendencia de Economía Popular y Solidaria, 2023.

1.2. Proceso investigativo metodológico

Para el presente proyecto se utilizó varios tipos de investigación que se describe a continuación:

En primera instancia se utilizó la investigación bibliográfica, según (Codina, 2020), proporcionan un marco teórico necesario para afrontar la investigación, así mismo indica que es la primera demostración del investigador que sabe manejar, analizar e interpretar información científica.

Dentro del proceso se utilizó también la investigación científica y el método comparativo, como indica (Léon, 2016), es buscar las ventajas que ofrecen cada modelo y sistematizar la información para adoptar la mejor solución.

Para complementar el proyecto, se empleó la investigación explicativa, cuyo principal propósito consiste en la aplicación práctica de los conocimientos y resultados obtenidos durante la investigación.

1.3. Análisis de resultados

Como resultado del presente proyecto, se presentan los fundamentos teóricos y conceptuales de diversas herramientas esenciales para el desarrollo. El objetivo es ofrecer una metodología entendible y fácil de usar o seguir, que incluye herramientas efectivas para aplicar el Ethical Hacking. Además, se proporcionará una imagen Open Virtual Appliance (OVA), que contendrá un conjunto de recursos tecnológicos preconfigurados y empaquetados, lo que facilitará su distribución y uso siguiendo las mejores prácticas.

El proyecto ofrece una guía estructurada en fases, complementada con una imagen OVA que incluirá los instructivos necesarios para el adecuado uso de las herramientas, así como formatos para la elaboración de informes y recomendaciones sobre la aplicación del Ethical Hacking. De esta manera, se busca proporcionar una metodología integral que permita a los usuarios maximizar el potencial de las herramientas y asegurar la eficacia de sus prácticas.

La imagen OVA y los instructivos deben ser utilizados como recursos complementarios para una comprensión más profunda de la metodología, las herramientas y sus aplicaciones contribuirá de manera positiva a mejorar la seguridad informática de las instituciones.

CAPÍTULO II: PROPUESTA

En este capítulo se aborda el desarrollo de la metodología propuesta, que se explica en diversas fases. Para complementar y respaldar su aplicabilidad, se incluyen en los anexos. De esta manera, se ofrece una perspectiva más completa y verificable de la metodología.

2.1 Fundamentos teóricos aplicados

Ethical Hacking

Es una técnica de seguridad informática que se emplea para detectar y solucionar vulnerabilidades en sistemas y redes informáticas. El objetivo principal de esta práctica es mejorar la seguridad de los sistemas y prevenir intrusiones malintencionadas. Normalmente, empresas de seguridad informática o profesionales independientes son los encargados de llevar a cabo esta actividad. No obstante, es crucial tener en cuenta que el Ethical Hacking sólo puede ser llevado a cabo con el permiso explícito del propietario del sistema que se va a analizar (Arango, 2023).

Tabla 1.

Tipos de Ethical Hacking

Tipo	Descripción
Caja negra	Se trata de una técnica de pruebas de penetración en la que el evaluador o "hacker ético" posee un conocimiento limitado acerca del sistema que se está evaluando. En otras palabras, el ataque se lleva a cabo sin disponer previamente de detalles sobre la estructura interna del sistema, como su diseño o su configuración (Rodriguez, 2020).
Caja gris	Se trata de una técnica de pruebas de penetración en la que el evaluador o "hacker ético" cuenta con un conocimiento limitado acerca del sistema que está evaluando. En otras palabras, el hacker tiene acceso parcial a la información sobre la estructura interna del sistema objetivo, como su diseño o configuración (Rodriguez, 2020).
Caja blanca	Se trata de una técnica de pruebas de penetración en la que el evaluador o "hacker ético" cuenta con un conocimiento completo y detallado acerca del sistema que está evaluando. En otras palabras, el hacker tiene acceso total a la información sobre la estructura interna del sistema objetivo, incluyendo su diseño, su configuración y su código fuente (Rodriguez, 2020).

Nota: Desarrollo propio

Sistemas Operativos Ethical Hacking

Hay varios sistemas operativos que son populares entre los profesionales de Ethical Hacking y que están diseñados específicamente para fines de seguridad y pruebas de penetración. Entre los más usados son los siguientes:

Tabla 2.

Sistemas Operativos para Ethical Hacking

Sistema Operativo	Derivación	Descripción
Kali Linux	Linux basada en Debian	Es un Sistema Operativo Linux, diseñado para temas de seguridad muy variados, como análisis de redes, ataques inalámbricos, análisis forenses y otros que más adelante citaremos. Contiene herramientas para llevar a cabo todas estas pruebas de seguridad y análisis (Altube, 2021).
Parrot OS	Linux basada en Debian	Es un Sistema Operativo Linux que actúa como un laboratorio completo y portable para realizar operaciones acerca de ciberseguridad, pentesting y análisis forense (Altube, 2021).
BlackArch Linux	Linux basada en Arch Linux	Es un sistema operativo de código abierto desarrollado voluntariamente por un grupo de programadores expertos. Este reúne más de dos mil ochocientas herramientas para hacking (KeepCoding, 2023).
BackBox	Linux basada en Ubuntu	Es una distro de hacking ético con un escritorio XFCE, diseñada para facilitar al máximo todo tipo de tareas de seguridad, desde llevar a cabo ataques de pentesting para medir la seguridad de una red hasta realizar un estudio avanzado de las vulnerabilidades de cualquier sistema operativo o infraestructura (Velasco, 2020).

Nota: Desarrollo propio

Herramientas Tecnológicas de Ethical Hacking

Las herramientas de Ethical Hacking ayudan a identificar posibles vulnerabilidades en sistemas y aplicaciones, permitiendo que los profesionales de seguridad puedan tomar medidas para corregir estas vulnerabilidades antes de que sean explotadas por atacantes malintencionados, también puede ayudar con el cumplimiento normativo y estándares de seguridad.

Tabla 3.

Herramientas para Ethical Hacking

Herramientas	Descripción
TheHarvester	Es una herramienta para recolectar información pública en la web. Aprende cómo funciona para anticiparse a ataques de Ingeniería Social (Perez, 2015).
Subfinder	Es una herramienta de descubrimiento de subdominios, que descubre subdominios válidos para sitios web mediante el uso de fuentes pasivas en línea (blog.segu-info, 2019).
Spoofcheck	Esta herramienta permite verificar una serie de condiciones para demostrar si un dominio es spoofeable o no (flu-project.com, 2016).
Frida-server	Es una herramienta de instrumentación dinámica y flexible. Esta aplicación puede inyectar instrucciones en procesos en ejecución a múltiples plataformas: Android, iOS, Windows, Mac y QNX (Plaza, 2019).
Genymotion	Es un emulador multiplataforma específico para soportar Android, que ejecuta de forma fluida y rápida distintos tipos de dispositivos móviles (Teléfonos y Tabletas), a los cuales se le pueden instalar ROMs, Aplicaciones y Juegos de Android (desdelinux.net, 2018).
Mobile-Security-Framework-MobSF	Es una herramienta de código abierto escrita en Python para analizar aplicaciones móviles (Android / iOS) capaz de realizar el análisis estático y dinámico automatizado (elhacker.net, 2021).
Google Dorks	Es una técnica de hackeo de búsqueda que utiliza consultas de búsqueda avanzadas para acceder a información oculta en Google. Los Google dorks, o Google hacks, son los comandos de búsqueda específicos (incluyendo parámetros especiales y operadores de búsqueda) que cuando se introducen en la barra de búsqueda de Google revelan

Herramientas	Descripción
	partes ocultas de los sitios web. (Freda, 2022).
wafw00f	Es una herramienta que nos permite identificar diferentes tipos de WAF a partir de sus huellas (Vadmin, 2017).
metasploit-framework	Es una herramienta desarrollada en Perl y Ruby en su mayor parte, que está enfocada a auditores de seguridad y que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración (Rizaldos, 2018).
CRACKMA-PEXEC	Es una herramienta diseñada para la post-explotación, su principal característica es que permite hacer movimientos laterales dentro una red local (adastra, thehackerway, 2022).
Rubeus	Es una herramienta que permite ejecutar diversos tipos de ataques contra el protocolo Kerberos (adastra, 2021).
Nmap	Es una herramienta de código abierto para exploración de red y auditoría de seguridad.
OpenVas	Es un escáner de vulnerabilidades de código abierto multiplataforma que cuenta con una aplicación web que nos permite realizar búsquedas de vulnerabilidades en uno o varios equipos dentro de una red (Columna, 2020).
Mimikatz	Es una herramienta de código abierto que se utiliza para recuperar contraseñas y credenciales de seguridad almacenadas en sistemas operativos Windows (Keepcoding, 2023).
BloodHound	Es una herramienta visor gráfico que tiene como objetivo realizar un mapeo de todas las relaciones, configuraciones en un Dominio de Windows siendo utilizando tanto del lado del atacante para identificar las rutas que pueden ser complejas para identificar, falencias de configuración de usuarios y políticas (Snifer, 2021).
Sliver	Es un marco de equipo rojo/emulación de adversarios multiplataforma de código abierto que pueden utilizar organizaciones de todos los tamaños para realizar pruebas de seguridad (github, 2023).
Wappalyzer	Es una extensión para navegadores basados en Chromium y Firefox, la cual permite de forma gráfica y simple visualizar las tecnologías que

Herramientas	Descripción
	está usando una página web individual que visites (colddsecurity, 2023).
FoxyProxy	Es una extensión para Firefox y Chrome que te permite gestionar los proxys de forma rápida y sencilla. Esta extensión le permite configurar varios servidores para que cambien rápidamente de uno a otro en caso de que falle la conexión predeterminada (Cahuana, 2021).
Burpsuite	Es una herramienta de seguridad de software de código abierto que se utiliza para hacer pruebas de pentesting y descubrir vulnerabilidades en aplicaciones web (Estrada, 2023).
Wireshark	Es un analizador de protocolos de red o un sniffer de paquetes. Es capaz de capturar paquetes en una conexión entre dos PCs, un servidor y una PC, o una LAN e internet (Manjaly, 2023).
Sonarqube	Es una plataforma de código abierto para la inspección continua de la calidad del código a través de diferentes herramientas de análisis estático de código fuente. Proporciona métricas que ayudan a mejorar la calidad del código de un programa permitiendo a los equipos de desarrollo hacer seguimiento y detectar errores y vulnerabilidades de seguridad para mantener el código limpio. (Sentrio, 2021).
Gophish	Es herramienta para la simulación de ataques de phishing y con ella podrás realizar entrenamiento de técnicas de Phishing (derechodelared, 2022).
Textmaker	Es un editor gratuito distribuido bajo la licencia GPL para escribir documentos de texto, multiplataforma, que integra muchas herramientas necesarias para desarrollar documentos con LaTeX, en una sola aplicación.

Nota: Desarrollo propio

2.2 Descripción de la propuesta

El presente proyecto tiene como objetivo proponer una metodología para llevar a cabo Ethical Hacking en instituciones financieras, mediante un enfoque práctico que facilite el trabajo de los profesionales de seguridad informática. Se basa en una cuidadosa recopilación de buenas prácticas y herramientas.

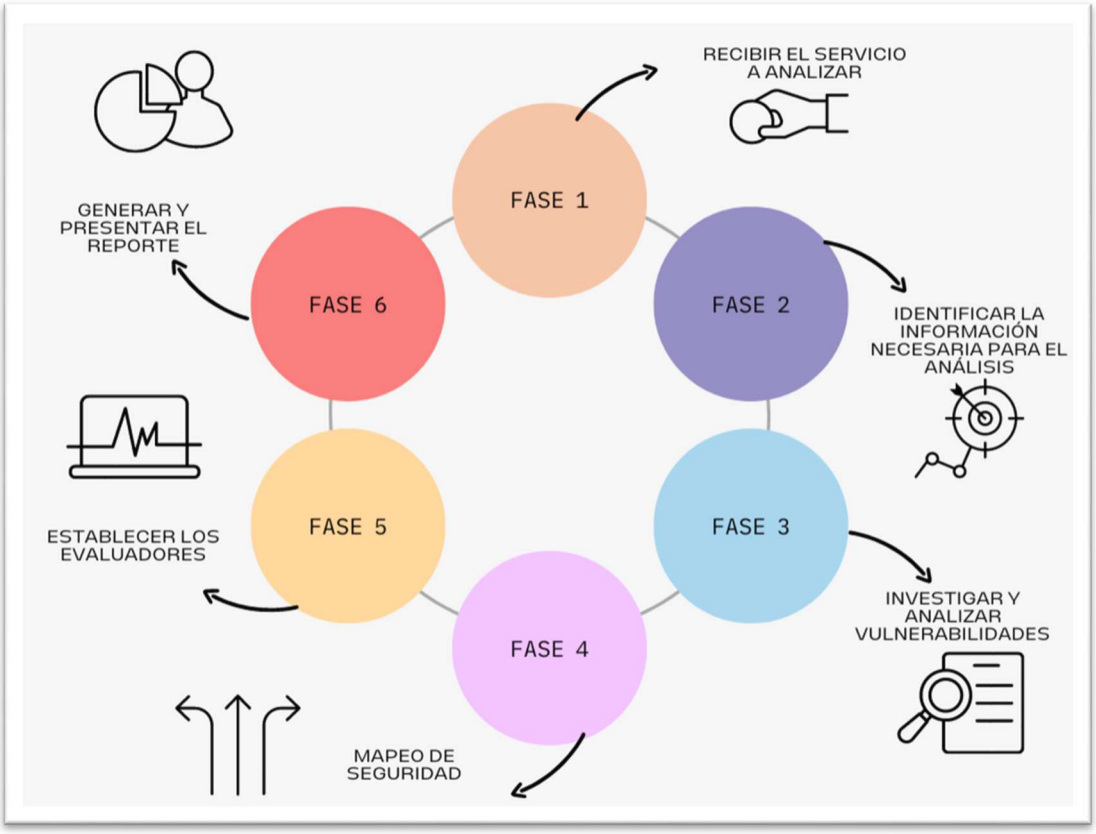
En este proyecto, se documenta y se pone a disposición del público el libre uso de la metodología, permitiendo así una mayor accesibilidad y colaboración en la comunidad de expertos en seguridad informática.

a. Estructura general

Para diseñar la metodología, se han recopilado buenas prácticas de varios modelos existentes, tales como el *Open Source Security Testing Methodology Manual* (OSSTMM) y el *Open Web Application Security Project* (OWASP). Estos modelos son analizados y adaptados para su inclusión en el sector financiero ecuatoriano. La metodología se encuentra definida en 6 fases, que detallan las actividades y herramientas a utilizar en cada una de ellas, como se muestra en la siguiente Figura.

Figura 2.

Modelo para Ethical Hacking



Nota. Elaboración propia

b. Aplicación del aporte

Esta metodología aborda diversas fases con un enfoque estructurado que tiene como objetivo ayudar a las instituciones a identificar y corregir posibles vulnerabilidades en sus servicios. La implementación de esta metodología permitirá fortalecer la seguridad informática de las instituciones financieras, protegiéndolas de posibles amenazas cibernéticas.

Las fases de la metodología se han diseñado para seguir un proceso sistemático y completo, garantizando una evaluación integral de los sistemas y servicios financieros. Mediante la aplicación de técnicas de Ethical Hacking, se simulan ataques controlados para detectar falencias en la seguridad y proponer soluciones efectivas.

A continuación, se detallan cada una de las fases que componen esta metodología, brindando una guía clara y efectiva para desarrollar evaluaciones de seguridad informática de manera ética y proactiva.

Con esta metodología de Ethical Hacking adaptada a las necesidades específicas de las instituciones financieras, se busca crear un entorno más seguro y confiable, aumentando la protección de datos y activos financieros. Al implementar este enfoque estructurado, las instituciones podrán estar mejor preparadas para enfrentar posibles amenazas cibernéticas y garantizar la confianza de sus clientes en un entorno digital cada vez más complejo.

Fases

- Recibir el servicio a analizar
- Identificar información necesaria para el análisis.
- Investigar y analizar vulnerabilidades.
- Mapeo de seguridad.
- Establecer evaluadores.
- Generar y presentar informes.

Figura 3.

Fases Propuesta Metodológica

Nota. Elaboración propia

c. Modelo propuesto

Es importante resaltar que la presente metodología incluye las herramientas para el desarrollo práctico que se podrá descargar del siguiente link.
https://bit.ly/3OxvewJ

En base al resumen anterior, se describen cada una las fases a seguir.

Fase 1 Recibir el servicio a analizar

Durante la fase inicial de recepción del servicio, se establece el primer contacto con los responsables de cada área de la institución financiera para recopilar las necesidades y objetivos de seguridad. En esta etapa, la institución proporcionará información detallada sobre los sistemas o aplicaciones que desean someter a evaluación. Esta comunicación inicial sienta las bases para el proceso de análisis y evaluación de seguridad que se llevará a cabo posteriormente.

El siguiente paso es firmar un Acuerdo de Confidencialidad con la institución y el profesional que llevará a cabo la evaluación de seguridad. Este acuerdo asegura que cualquier información sensible o datos relacionados con los sistemas o redes de la

institución financiera estén protegidos adecuadamente. Es fundamental que este documento esté en conformidad con las leyes de protección de datos vigentes en el Ecuador, asegurando el cumplimiento normativo y la seguridad de la información confidencial. Al establecer una base legal sólida, se garantiza la confianza y la protección de los activos digitales de la institución financiera durante todo el proceso de análisis y evaluación.

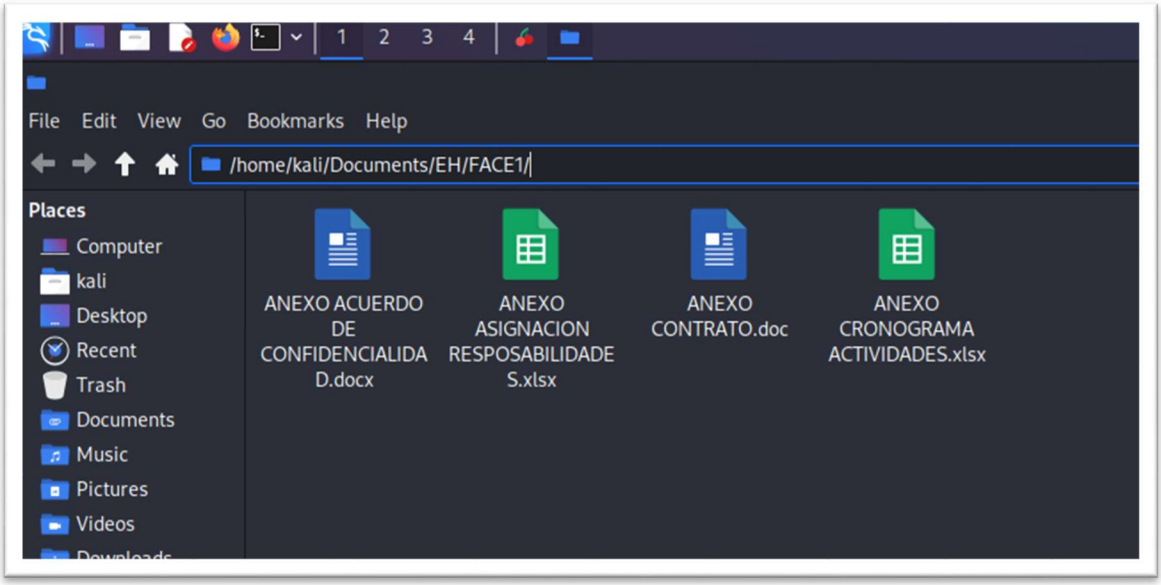
En la siguiente etapa de esta fase, se procede a establecer un cronograma de actividades que guiará el desarrollo del proyecto. Para ello, es necesario seguir varios pasos clave:

- Identificar tareas y estimar tiempos: Se enumeran todas las tareas requeridas en el proyecto, y se estima el tiempo necesario para completar cada una de ellas. Esto ayuda a tener una visión clara de la duración total del proyecto.
- Priorizar según requerimientos: Las tareas se priorizan en función de los requerimientos y objetivos específicos de la institución financiera. Aquellas de mayor relevancia o con fechas límite más cercanas se atienden en primer lugar.
- Definir fechas límite: Se establecen fechas límite realistas para cada tarea y para el proyecto en su conjunto. Estas fechas deben tener en cuenta cualquier restricción de tiempo o evento crítico.
- Asignar personal y responsabilidades: Se designa al personal adecuado para llevar a cabo cada tarea, y se les asignan responsabilidades claras. Esto garantiza que todos los aspectos del proyecto estén cubiertos y que cada miembro del equipo sepa qué se espera de él.
- Crear un calendario o matriz de seguimiento: Se presenta el cronograma en un formato claro y accesible, como un calendario o una matriz. Esto facilita el seguimiento del progreso del proyecto y permite identificar rápidamente cualquier desviación o retraso.

Esta primera fase se crea como anexo los documentos que se encuentra en la ruta /home/kali/Documents/EH/FASE1/, de la imagen máquina virtual o a su vez se podrán descargar de la siguiente ruta: https://bit.ly/3OH0Fpy

Figura 4.

Modelo de Documentos Fase 1



Nota. Elaboración propia

Fase 2 Identificar información necesaria para el análisis

Para la segunda fase de la metodología, es importante coordinar los lineamientos a seguir, con los responsables de cada servicio que se va a evaluar.

Durante este proceso, se solicita documentación relacionada con los procesos y, en el caso de llevar a cabo un Ethical hacking de caja blanca, se pide acceso a los servidores y aplicaciones pertinentes. Con la información recopilada, se procede a verificar los datos generales que se mencionan a continuación:

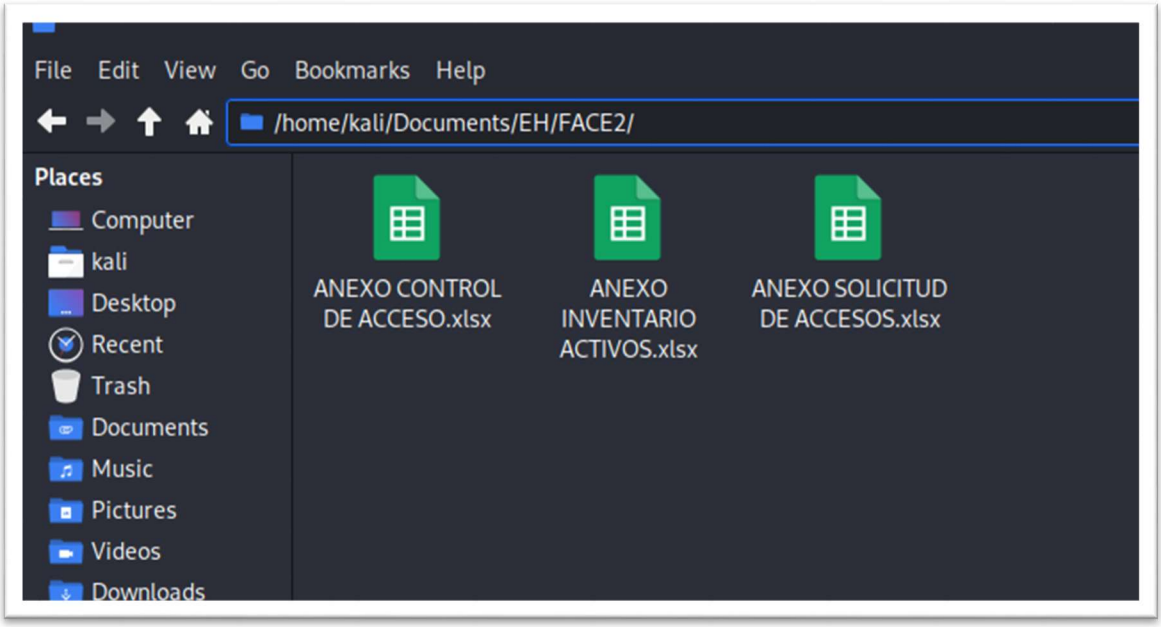
- Dominios
- Aplicaciones móviles
- Certificados
- Arquitectura del servicio
- Código fuente de ser el caso

Una vez recopilada la información, se procede a analizarla y establecer los alcances dentro de la evaluación de los sistemas o servicios. Es crucial definir los límites de lo que se realizará y no se realizará durante la ejecución del Ethical Hacking. Esto asegura el cumplimiento de las normas éticas y garantiza un enfoque responsable en el proceso de evaluación.

Para esta fase se crea como anexo los documentos que se encuentra en la ruta /home/kali/Documents/EH/FASE2/, de la imagen máquina virtual o a su vez se podrán descargar de la siguiente ruta: https://bit.ly/3OIB7sq

Figura 5.

Modelo de Documentos Fase 2



Nota. Elaboración propia

Fase 3 Investigar y analizar vulnerabilidades

La tercera fase de la metodología consiste en el trabajo técnico realizado por los responsables de las evaluaciones, quienes llevan a cabo un minucioso proceso de investigación y análisis en busca de vulnerabilidades o posibles fallos de seguridad en sistemas, redes y aplicaciones.

Para esta fase se presenta las siguientes etapas a seguir:

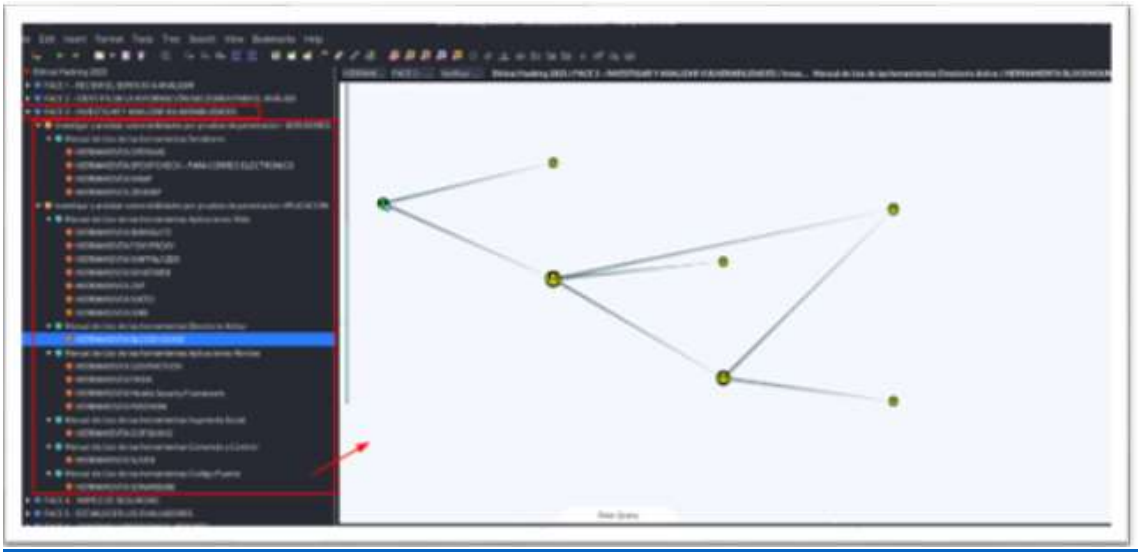
- Recopilación de información: Se recopilan datos sobre el sistema, la aplicación o la red que se va a evaluar. Esto puede involucrar identificar la versión del software, la arquitectura del sistema, los servicios y puertos abiertos, entre otros detalles.
- Análisis de código y configuración: Se examina el código fuente o la configuración de la aplicación o sistema en busca de posibles errores, fallas de diseño o configuraciones inseguras.

- Pruebas de penetración: Se realizan pruebas de intrusión para simular ataques controlados y descubrir vulnerabilidades explotables. Esto puede incluir ataques de fuerza bruta, inyecciones de código, falsificación de identidad, entre otros.
- Evaluación de vulnerabilidades conocidas: Se comparan las características del sistema con una base de datos de vulnerabilidades conocidas para detectar posibles problemas de seguridad que hayan sido previamente reportados y corregidos.
- Identificación de nuevas vulnerabilidades: En algunos casos, los investigadores pueden descubrir vulnerabilidades desconocidas, llamadas "zero-days", que aún no han sido reportadas o solucionadas por el fabricante.

Para esta fase se crea como anexo los manuales que se encuentra en la ruta /home/kali/Documents/EH/Ethical Hacking 2023.ctx/, y las herramientas preconfigurases en la imagen de la máquina virtual, o a su vez se podrán descargar de la siguiente ruta: https://bit.ly/3OG4VFP

Figura 6.

Manuales de Uso Fase 3



Nota. Elaboración propia

Fase 4 Mapeo de seguridad.

En esta fase, se pondrá especial atención en examinar los equipos de seguridad perimetral, como el Firewall, WAF, en caso de estar presente, y las configuraciones de red para evaluar minuciosamente el rendimiento y la eficiencia de la red institucional. A continuación, se describen las actividades que se llevarán a cabo durante este proceso:

- Recopilación de información: Se obtiene información sobre la topología de la red, sus componentes, direcciones IP, servidores, enrutadores, firewall y cualquier otro dispositivo relevante.
- Análisis de tráfico: Se examina el tráfico de red para identificar patrones, congestiones y posibles problemas de rendimiento.
- Pruebas de rendimiento: Se llevan a cabo pruebas de velocidad y rendimiento para evaluar la eficiencia y capacidad de la red para manejar la carga de trabajo.
- Análisis de paquetes: Se capturan y analizan los paquetes de datos que circulan por la red para identificar problemas de tráfico y detectar posibles ataques.
- Auditoría de permisos y acceso: Se revisan los permisos y niveles de acceso de usuarios y dispositivos para asegurarse de que solo tengan acceso a los recursos necesarios.
- Evaluación de la configuración de seguridad: Se revisan las configuraciones de firewall, enrutadores y otros dispositivos de seguridad para garantizar que estén adecuadamente configurados.
- Análisis de calidad de servicio (QoS): Se evalúa cómo se está manejando el ancho de banda y se asegura que las aplicaciones críticas reciban la prioridad adecuada.
- Evaluación de redundancia y tolerancia a fallos: Se verifica la redundancia en la red y cómo se comporta frente a fallos para garantizar una alta disponibilidad.
- Análisis de protocolos: Se inspecciona el uso y la eficiencia de los protocolos de red implementados.
- Análisis de redes wifi: se analiza las configuraciones y evalúa posibles vulnerabilidades.

Durante esta fase del análisis, es imprescindible contar con la participación y guía del responsable de cada servicio para evitar interrupciones no deseadas en la disponibilidad de los mismos. Cabe destacar que todas las evaluaciones se llevarán a cabo en entornos de producción, lo que enfatiza la importancia de llevar a cabo un trabajo minucioso y preciso para prevenir cualquier incidencia que pueda afectar los servicios.

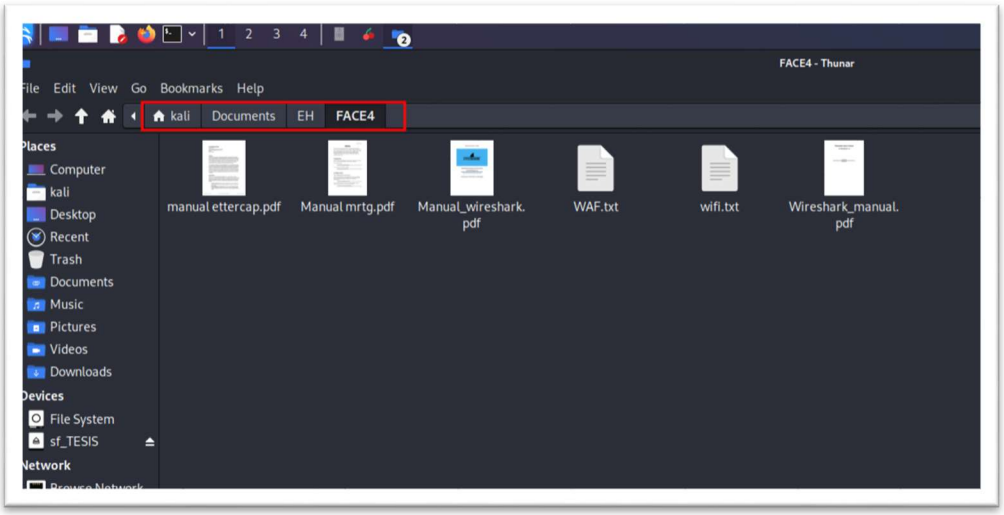
El enfoque principal será garantizar la continuidad de los servicios mientras se ejecutan las actividades de evaluación de seguridad y rendimiento en la red institucional. Al finalizar esta fase, se espera contar con un análisis completo y recomendaciones

sólidas para mejorar la eficiencia y proteger adecuadamente la infraestructura de la red sin comprometer la operatividad de los servicios.

Para esta fase se crea como anexo las actividades a detalle por servicio que se encuentra en la ruta /home/kali/Documents/EH/FASE4/, y las herramientas preconfiguradas en la imagen de la máquina virtual, o a su vez se podrán descargar de la siguiente ruta: https://bit.ly/3qfu54L

Figura 7.

Manuales de Uso Fase 4



Nota. Elaboración propia

Fase 5 Establecer los evaluadores

En esta fase, se lleva a cabo un minucioso análisis de los resultados obtenidos tanto en la fase 3 (Investigar y analizar vulnerabilidades) como en la fase 4 (mapeo de seguridades). Durante este proceso, se evalúan exhaustivamente los resultados de las pruebas de penetración, registrando todos los hallazgos relevantes y señalando aquellas áreas que requieren mejoras en términos de seguridad.

Además, se asigna una métrica a cada hallazgo de acuerdo con los siguientes criterios:

- Priorización de vulnerabilidades: Se clasifican las vulnerabilidades identificadas según su gravedad y su impacto potencial en la seguridad de los sistemas. Esto ayuda a enfocar los esfuerzos en abordar las vulnerabilidades más críticas primero.

- Análisis de exploits exitosos: Si se logró explotar con éxito una vulnerabilidad, se analizan detalladamente los exploits utilizados para comprender cómo funcionaron y determinar cómo mitigar eficazmente esos vectores de ataque.
- Análisis de riesgos: Se evalúan los riesgos asociados con cada vulnerabilidad identificada, considerando el contexto de la organización y el posible impacto financiero, de reputación o legal de una explotación exitosa.
- Evaluación de defensas y mitigaciones: Se examinan las defensas y contramedidas existentes para determinar su efectividad en la detección y prevención de ataques.

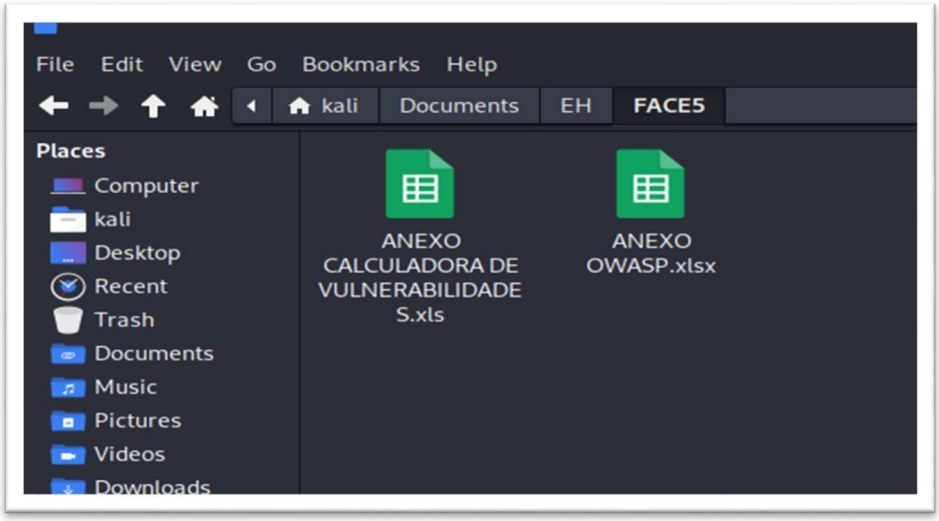
Esto puede incluir soluciones de seguridad como firewalls, sistemas de detección de intrusiones (IDS) o prevención de intrusiones (IPS), entre otros.

La asignación de métricas y la priorización de las vulnerabilidades permiten a la organización centrar sus esfuerzos en abordar los problemas más críticos primero, fortaleciendo así su postura de seguridad y protegiéndose mejor contra posibles amenazas cibernéticas.

Para esta fase se adjunta una matriz modelo para generar la severidad de las vulnerabilidades la misma que se encuentra en la ruta /home/kali/Documents/EH/FASE5/, o a su vez se podrán descargar de la siguiente ruta: https://bit.ly/3q7F948

Figura 8.

Modelo de Documentos Fase 5

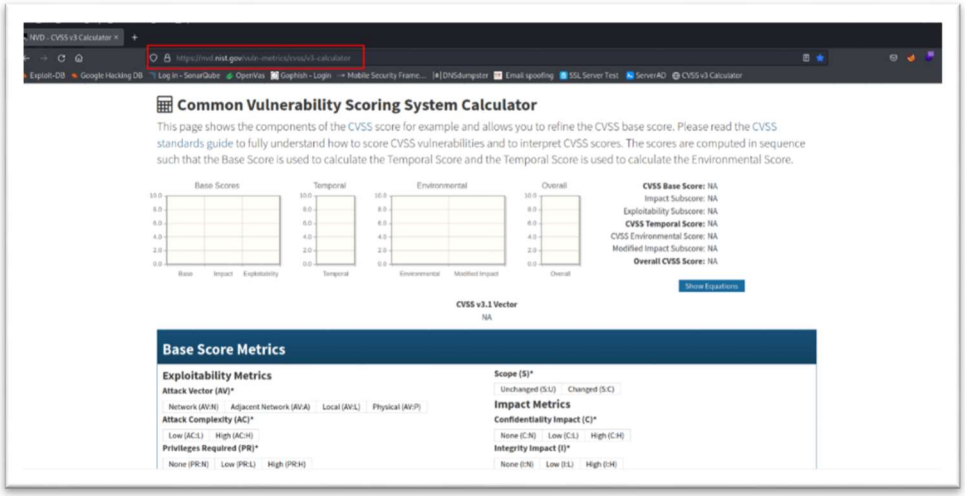


Nota. Elaboración propia

Adicional se pone a consideración el uso de la calculadora de puntuación de vulnerabilidades de NIST, que se puede ingresar desde el siguiente link. https://bit.ly/3OwNl5M

Figura 9.

Calculadora de Vulnerabilidades NIST



Nota. Métricas de vulnerabilidades, adaptado la metodología. Tomado de *NIST*, 2023.

Fase 6 Generar y presentar el reporte

En esta fase final de la metodología, es crucial elaborar los reportes o informes de manera objetiva y profesional. Estos informes deben ser redactados de forma clara y comprensible tanto para el personal administrativo como para el técnico de la institución. Además, es de suma importancia reconocer la criticidad del informe, ya que contiene información sensible sobre las vulnerabilidades encontradas en la organización y, por lo tanto, debe tratarse con total confidencialidad.

El informe debe presentar de manera detallada los hallazgos de las pruebas de penetración, incluyendo las vulnerabilidades identificadas, su gravedad y el impacto potencial en la seguridad de la institución. Asimismo, es esencial proporcionar recomendaciones claras y específicas para abordar cada vulnerabilidad y mejorar la postura de seguridad.

La redacción del informe debe ser imparcial y sin jerga técnica excesiva, para que pueda ser comprendido por todos los interesados, desde los responsables de la toma de decisiones hasta los técnicos encargados de la implementación de las

correcciones. Asimismo, se debe resaltar la importancia de actuar rápidamente para mitigar los riesgos identificados y fortalecer la seguridad de la institución.

Por último, es vital asegurar que el informe se comparta solo con las partes autorizadas y se maneje con la confidencialidad necesaria para proteger la integridad de la información sensible que contiene. El objetivo final del informe es proporcionar una visión clara y completa del estado de seguridad de la institución, para que se puedan tomar decisiones informadas y se implementen las medidas correctivas adecuadas. Para generar el reporte se debe tener en cuenta los siguientes criterios:

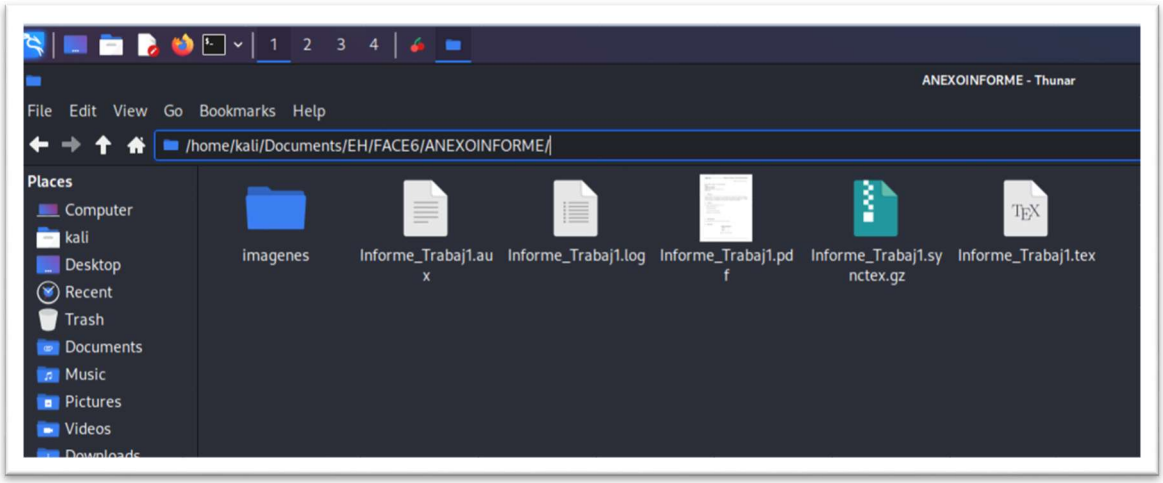
- Número de informe
- Fecha
- A quién va dirigido
- Asunto
- Objetivos
- Alcance: Detalla el alcance de las pruebas de penetración, incluyendo los sistemas, redes o aplicaciones que fueron evaluados.
- Limitaciones: cualquier aspecto relevante relacionado con el proceso de pentesting.
- Resumen: proporcionar un resumen breve pero claro de los hallazgos más importantes y las recomendaciones principales para mejorar la seguridad de la organización. Es una sección crítica para que los directivos y responsables de la seguridad puedan obtener rápidamente una visión general de los resultados.
- Desarrollo: Hallazgos de vulnerabilidades: Enumera y describe detalladamente todas las vulnerabilidades encontradas durante las pruebas de penetración, incluyendo su gravedad, probabilidad de explotación, impacto potencial y la forma en que fueron descubiertas. Evidencia de los hallazgos: Proporciona pruebas sólidas de las vulnerabilidades encontradas, como capturas de pantalla, registros de eventos, resultados de escaneos y cualquier otro dato relevante que respalde los hallazgos. Recomendaciones de mitigación: Ofrece recomendaciones claras y específicas para corregir cada vulnerabilidad, junto con las medidas correctivas y contramedidas adecuadas para mejorar la seguridad.
- Conclusiones Presenta conclusiones y reflexiones finales sobre los resultados del Ethical hacking, destacando la importancia de abordar las vulnerabilidades identificadas y fortalecer la postura de seguridad de la organización.

- Firmas de responsabilidad.

Para esta fase se crea como anexo el modelo de informe el mismo se encuentra en la ruta /home/kali/Documents/EH/FASE6/ o a su vez se podrán descargar de la siguiente ruta: https://bit.ly/3QnSkbA, importante mencionar que el reporte esta generado en la herramienta latex, y, esta preconfigurado en la máquina virtual.

Figura 10.

Modelo Informe Fase 6



Nota. Elaboración propia

2.3 Valoración de la propuesta

Para la valoración de la aplicabilidad de la presente metodología se utiliza el método Delphi o juicio de experto como lo indica (García, 2013), es una metodología estructurada para recolectar sistemáticamente juicios de expertos sobre un problema, procesar la información y a través de recursos estadísticos, construir un acuerdo general de grupo. Permite la transformación durante la investigación de las apreciaciones individuales de los expertos en un juicio colectivo superior.

Situación

Para llevar a cabo este estudio, se ha consultado a expertos del ámbito financiero que desempeñan roles en diversas instituciones del sector. Se ha presentado la propuesta en persona y posteriormente administrado una encuesta diseñada para evaluar su percepción acerca de la viabilidad y aplicabilidad de la misma en el contexto de sus respectivas organizaciones financieras. La herramienta empleada para la encuesta fue kobotoolbox, y en este informe se exponen detalladamente los resultados obtenidos a través de dicho proceso.

Tabla 4.

Participantes para la evaluación de la metodología

Participante	Institución Financiera	Cargo que Ocupa
Mg. Paul Zhañay.	COAC Jardín Azuayo.	Responsable de Seguridad Informática.
Ing. Francisco Mocha.	COAC Señor de Girón.	Oficial de Seguridad de la Información.
Ing. Yina Jaramillo.	COAC Once de Junio	Oficial de Seguridad de la Información.
Mg. Hugo Bastidas.	Coopac Austro Ltda.	Subgerente de TI

Nota. Elaboración propia

Preguntas de la encuesta aplicación de la metodología

Con el propósito de verificar la eficacia y aplicabilidad de nuestra metodología, se llevó a cabo una encuesta entre los participantes. Esta propuesta incluyó una serie de preguntas destinadas a evaluar el uso y la implementación de la metodología.

- Nombres y Apellidos.
- Institución Financiera en la que Labora.
- Segmento a la que pertenece la institución en la SEPS.
- Cargo que Desempeña.
- Años de experiencia en el sector financiero.
- ¿Cómo calificarías la efectividad de la metodología en términos de alcanzar tus objetivos o resultados deseados? (“Siendo 1 Muy ineficaz y 5 Muy efectiva")
- ¿Hubo algún aspecto de la metodología que encontraste especialmente útil o innovador? (“Descríbelo brevemente”)
- ¿Experimentaste alguna dificultad o desafío al aplicar la metodología? (SI/NO) (“En el caso que sea afirmativo, por favor descríbelo brevemente”)
- ¿Hubo alguna situación en la que consideraste que la metodología no era aplicable o no se adaptaba a tus necesidades? (SI/NO) (“En caso afirmativo, ¿por qué?”)
- ¿Recomendarías esta metodología a otros profesionales o colegas? (SI/NO)
- ¿Cuál es tu nivel de satisfacción general con la metodología? (“Siendo 1 Muy insatisfecho y 5 Muy satisfecho”)

- ¿Tienes alguna sugerencia para mejorar la metodología? (“Descríbelo brevemente”)

Resultados

En la encuesta presentada se recopila los comentarios constructivos y valiosos sobre la efectividad y la aplicabilidad de la metodología que hemos desarrollado. También nos ayudarán a evaluar si la metodología cumple con sus expectativas, si es clara, comprensible y aplicable en las instituciones financieras. Una vez recopilados los datos de la encuesta, se realiza el análisis y tabulación de los resultados, los cuales se presentan a continuación de manera detallada.

La primera pregunta en la valoración de la propuesta metodológica tiene el siguiente propósito: garantizar la identificación única y la autenticidad de los participantes. Esto asegura la integridad de los datos al prevenir respuestas duplicadas. Además, la inclusión de esta información refuerza la confianza y credibilidad del estudio. Los detalles completos se encuentran presentados en la tabla siguiente.

Tabla 5.

Encuesta pregunta 1

Nombres y Apellidos	Frecuencia	Porcentaje
Francisco Mocha.	1	25.00%
Paul Zhañay Ledesma.	1	25.00%
Hugo Bastidas Mendieta.	1	25.00%
Yina Jaramillo.	1	25.00%

Nota. Elaboración propia

La encuesta fue llevada a cabo con profesionales especializados en seguridad informática pertenecientes a instituciones financieras. Estos expertos desempeñaron un papel fundamental al validar nuestra propuesta metodológica.

La segunda pregunta en la valoración de la propuesta metodológica tiene el siguiente propósito: validación de datos, al incluir en la institución donde labora se puede adicionar un control de calidad adicional para asegurar que los datos sean reales. Los detalles completos se encuentran presentados en la tabla siguiente.

Tabla 6.

Encuesta pregunta 2

Institución Financiera en la que Labora.	Frecuencia	Porcentaje
COAC Señor de Girón.	1	25.00%
COAC Jardín Azuayo.	1	25.00%
Coopac Austro Ltda.	1	25.00%
COAC Once de Junio	1	25.00%

Nota. Elaboración propia

Las instituciones financieras escogidas para la valoración de la metodológica cuentan con gran acogida y reconocida reputación en el sector de la Economía Popular y Solidaria.

La tercera pregunta en el proceso de valoración de la propuesta metodológica tiene el siguiente propósito: determinar el segmento al que pertenecen las instituciones financieras, esta información nos ayuda para un análisis detallado de la adaptabilidad y la cobertura de la metodología en función de las necesidades únicas de cada segmento. Los detalles completos de esta pregunta se encuentran presentados en la tabla siguiente tabla y figura.

Tabla 7.

Encuesta pregunta 3

Segmento a la que pertenece la institución en la SEPS.	Frecuencia	Porcentaje
Segmento 1	2	50%
Segmento 2	2	50%
Segmento 3	0	0%
Segmento 4	0	0%
Segmento 5	0	0%

Nota. Elaboración propia

Figura 11.

Encuesta pregunta 3

Nota. Elaboración propia

De las instituciones financieras donde se validó la propuesta, el 50% pertenecen al segmento 1 de la SEPS. y el 50% pertenece al segmento 2 de la SEPS.

La cuarta pregunta en el proceso de valoración de la propuesta metodológica tiene el siguiente propósito: análisis según su función laboral, este enfoque nos permite discernir las variaciones en las respuestas según las diferentes funciones desempeñadas. Adicionalmente, esta pregunta proporciona una perspectiva valiosa sobre cómo diversas funciones perciben la aplicabilidad de la metodología. Los detalles completos de esta pregunta se encuentran presentados en la tabla siguiente tabla.

Tabla 8.

Encuesta pregunta 4

Cargo que Desempeña	Frecuencia	Porcentaje
Oficial de Seguridad de la Información	2	50.00%
Responsable de Seguridad Informática	1	25.00%
Subgerente de Tecnología	1	25.00%

Nota. Elaboración propia

Los cargos de los profesionales que validaron la propuesta, en la mayoría de casos son oficiales de seguridad de la información, responsables del área de seguridad informática y el área administrativa de las instituciones financieras.

La quinta pregunta en el proceso de valoración de la propuesta metodológica el siguiente propósito: análisis de conocimiento, mediante esta pregunta, se busca validar la metodología mediante la evaluación de expertos en el sector. Esta etapa asegura que la metodología sea sometida a una revisión detallada por parte de quienes cuentan con un profundo conocimiento en la materia. Los detalles completos de esta pregunta se encuentran presentados en la tabla siguiente tabla.

Tabla 9.

Encuesta pregunta 5

Años de experiencia en el sector financiero	**Frecuencia**	**Porcentaje**
7 años	1	25.00%
12 años	1	25.00%
13 años	1	25.00%
11 años	1	25.00%

Nota. Elaboración propia

Los profesionales que validaron la propuesta cuentan con varios años de experiencia en el sector financiero, el promedio es 10.75 años de experiencia.

La sexta pregunta en el proceso de valoración de la propuesta metodológica el siguiente propósito: evaluar la efectividad, esto permite determinar qué tan bien está funcionando en la práctica, proporciona una medida cuantitativa de su eficacia. Los detalles completos de esta pregunta se encuentran presentados en la tabla siguiente tabla.

Tabla 10.

Encuesta pregunta 6

¿Cómo calificarías la efectividad de la metodología en términos de alcanzar tus objetivos o resultados deseados? (“Siendo 1 Muy ineficaz y 5 Muy efectiva")			
Media	Mediano	Modo	Desviación estándar
4.67	5	5	0.58

Nota. Elaboración propia

Los profesionales que evaluaron la metodología califican la propuesta como muy efectiva, para alcanzar los resultados deseados con una media de 4.76 sobre 5.

La séptima pregunta en el proceso de valoración de la propuesta metodológica tiene el siguiente propósito: reconocer el feedback positivo, con esta información que nos proporcionen podemos evaluar la satisfacción y aspectos positivos de la metodología, así como también una retroalimentación. Los detalles completos de esta pregunta se encuentran presentados en la tabla siguiente tabla.

Tabla 11.

Encuesta pregunta 7

¿Hubo algún aspecto de la metodología que encontraste especialmente útil o innovador?	**Frecuencia**	**Porcentaje**
Metodología es objetiva y precisa.	1	25.00%
Contar con una metodología dentro de un proceso interno con estandarización de herramientas.	1	25.00%
Uso de herramientas open source cubren de manera íntegra el proceso de detención de vulnerabilidades.	1	25.00%
Metodología descrita en fases acompañadas de las herramientas para su comprobación.	1	25.00%

Nota. Elaboración propia

La octava pregunta en el proceso de valoración de la propuesta metodológica tiene el siguiente propósito: identificar problemas, con la información proporcionada detectaremos posibles falencias o limitaciones en la metodología. Los detalles completos de esta pregunta se encuentran presentados en la tabla siguiente tabla y figura.

Tabla 12.

Encuesta pregunta 8

¿Experimentaste alguna dificultad o desafío al aplicar la metodología?	**Frecuencia**
SI	0
NO	4

Nota. Elaboración propia

Figura 12.

Encuesta pregunta 8

Nota. Elaboración propia

De los profesionales encuestados el 100% no experimentaron ninguna dificultad en aplicar la metodología.

La novena pregunta en el proceso de valoración de la propuesta metodológica tiene el siguiente propósito: identificar limitaciones, con la información proporcionada podemos identificar situaciones donde existen puntos débiles de la metodología. Los detalles completos de esta pregunta se encuentran presentados en la tabla siguiente tabla y figura.

Tabla 13.

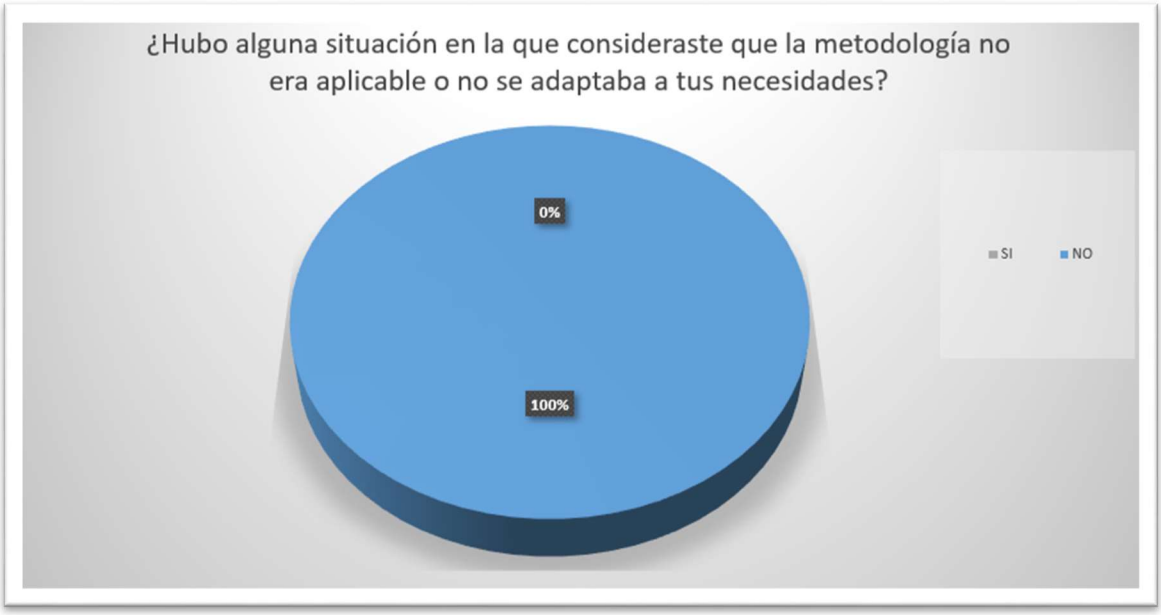
Encuesta pregunta 9

¿Hubo alguna situación en la que consideraste que la metodología no era aplicable o no se adaptaba a tus necesidades?	**Frecuencia**
SI	0
NO	4

Nota. Elaboración propia

Figura 13.

Encuesta pregunta 9



Nota. Elaboración propia

De los profesionales encuestados el 100% consideran la metodología es aplicable y se adapta a las necesidades de la institución.

La décima pregunta en el proceso de valoración de la propuesta metodológica tiene el siguiente propósito: medir la confianza de la propuesta, con la información proporcionada podemos reflejar la perspectiva de los participantes en sus resultados y beneficios de la metodología. Los detalles completos de esta pregunta se encuentran presentados en la tabla siguiente tabla y figura.

Tabla 14.

Encuesta pregunta 10

¿Recomendarías esta metodología a otros profesionales o colegas?	**Frecuencia**
SI	4
NO	0

Nota. Elaboración propia

Figura 14.

Encuesta pregunta 10

Nota. Elaboración propia

De los profesionales encuestados, el 100% recomendaría el uso de la metodología a otros colegas o profesionales.

La undécima pregunta en el proceso de valoración de la propuesta metodológica tiene el siguiente propósito: evaluar la percepción global. Con esta información obtendremos una visión general de los participantes como ven la metodología en términos de satisfacción. Los detalles completos de esta pregunta se encuentran presentados en la tabla siguiente tabla.

Tabla 15.

Encuesta pregunta 11

¿Cuál es tu nivel de satisfacción general con la metodología? (“Siendo 1 Muy insatisfecho y 5 Muy satisfecho”)			
Media	Mediano	Modo	Desviación estándar
4.33	4.00	4.00	0.58

Nota. Elaboración propia

De los profesionales encuestados, el nivel de satisfacción general de la propuesta es satisfecho.

La duodécima pregunta en el proceso de valoración de la propuesta metodológica tiene el siguiente propósito: identificar información para futuras actualizaciones o mejoras, con la información recopilada se puede dirigir o recomendar para nuevos trabajos de investigación en base a las necesidades presentadas. Los detalles completos de esta pregunta se encuentran presentados en la tabla siguiente tabla.

Tabla 16.

Encuesta pregunta 12

¿Tienes alguna sugerencia para mejorar la metodología? (“Descríbelo brevemente”)	**Frecuencia**	**Porcentaje**
Realizar un alcance para contemplar infraestructura e hipervisores.	1	25.00%
Generalizar ciertos puntos para que sean aplicables a cualquier realidad de operación en cada institución donde se desea aplicar.	1	25.00%
Complementar con una fase de remediación(apoyo).	1	25.00%
Ninguna recomendación.	1	25.00%

Nota. Elaboración propia

2.4 Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

Tabla 17.

Matriz de Articulación

	Ejes o partes principales del proyecto	Breve descripción de los resultados de cada parte	Sustento teórico que se aplicó en la construcción del proyecto	Metodologías, herramientas técnicas y tecnológicas que se emplearon
1	Fase 1 propuesta metodológica Recibir el servicio a analizar: Se establece el primer contacto para recopilar necesidades y objetivos de seguridad.	Análisis de costos y factibilidad Tomas de decisiones en base a acuerdos. Acuerdos de Confidencialidad Cronograma de actividades	Gestión de proyectos Gestión de tiempos Estimación y planificación Jurisdicción y ley aplicable Asesoramiento legal	Entrevistas Investigación bibliográfica Herramientas de ofimática Formatos anexo 2
2	Fase 2 propuesta metodológica. Identificar información necesaria para el análisis: Coordinar lineamentos a seguir.	Solicitud de documentación Análisis de procesos Definir límites y alcances	Comunicación y coordinación Teoría de complejidad	Comunicación efectiva Reuniones presenciales Formatos anexo 3
3	Fase 3 propuesta metodológica, Investigar y analizar vulnerabilidades: Trabajo especializado por los responsables de evaluar los sistemas.	Investigar vulnerabilidades Pruebas de penetración Análisis de código fuente	Protocolos de comunicación Ejecución de exploit Configuración y administración de software especializado Herramientas preconfiguradas en el sistema operativo Kali Linux	Investigación científica Comparativa de herramientas y sistemas Anexo 4 Manuales de las herramientas

	Ejes o partes principales del proyecto	Breve descripción de los resultados de cada parte	Sustento teórico que se aplicó en la construcción del proyecto	Metodologías, herramientas técnicas y tecnológicas que se emplearon
4	Fase 4 propuesta metodológica, Mapeo de seguridad: Evaluación de equipos de seguridad, acompañado por los responsables de cada servicio.	Examinar configuración de equipos de seguridad Análisis de red interna Pruebas de rendimiento Análisis de redes wifi	Listas de acceso Equipos de seguridad perimetral Configuraciones inseguras malas prácticas.	Análisis estratégico Anexo 5 Manuales de herramientas
5	Fase 5 propuesta metodológica, Establecer los evaluadores: Asignación de métricas a cada vulnerabilidad encontrada.	Evaluar los resultados Registrar hallazgos Asignar métricas	Comparación de estándares Recopilación de datos Priorización Clasificación	Análisis de Métricas y datos Anexo 6 modelo de calculadoras de vulnerabilidad
6	Fase 6 propuesta metodológica Generar y presentar el reporte: proporcionar visión clara y completa del estado de seguridad de la institución.	Redactar informes Presentar informes	Estructura lógica Gráfico y visualizaciones Comprensión del usuario	Investigación, análisis, estadísticas Anexo 7 Modelo de Informe

Nota. Elaboración propia

2.5 Análisis de resultados.

Presentación y discusión.

Después de haber desarrollado la metodología con la documentación necesaria y las herramientas incluidas en este trabajo, se procedió a presentarla y consultar su aplicabilidad en varias instituciones financieras. Como resultado de esta evaluación, se pudo concluir que la metodología propuesta fue aceptada de manera satisfactoria y demostró ser aplicable en dichas instituciones financieras.

La metodología propuesta ha demostrado ser una herramienta valiosa y adecuada para fortalecer la seguridad y proteger la información sensible en las instituciones financieras. Su aceptación y aplicabilidad satisfactoria en varias entidades respaldan su capacidad para contribuir significativamente a la mejora de las prácticas de Ethical Hacking y la gestión de riesgos cibernéticos en el sector financiero.

La continua colaboración y retroalimentación con las instituciones implicadas asegurarán que la metodología siga evolucionando y manteniéndose actualizada en un entorno tecnológico en constante cambio.

CONCLUSIONES

Si bien la implementación de esta metodología requerirá un compromiso por parte de las instituciones financieras, el potencial para mejorar la resiliencia ante los ataques cibernéticos y reforzar su postura en seguridad cibernética es considerable. A medida que se adopten y adapten estas prácticas en el contexto específico de cada organización, se podrá construir una infraestructura más segura y confiable, en consonancia con los estándares más elevados de seguridad en la era digital actual.

La contextualización adecuada de estos temas sienta las bases para una implementación efectiva de prácticas de Ethical Hacking y Pentesting en el ámbito de la ciberseguridad, garantizando la protección y confianza en las infraestructuras tecnológicas de las organizaciones, y asegurando la privacidad y seguridad.

El análisis de herramientas efectivas para Ethical Hacking en varios sistemas operativos ha proporcionado una perspectiva valiosa para la mejora de las prácticas de ciberseguridad. La correcta selección, implementación y actualización de estas herramientas en consonancia con los sistemas operativos específicos resulta esencial para fortalecer la seguridad de las organizaciones y proteger la confidencialidad, integridad y disponibilidad de sus activos digitales.

El diseño de esta guía de buenas prácticas representa un valioso aporte a la comunidad de profesionales de Ethical Hacking y a las organizaciones que buscan mejorar su postura en seguridad cibernética. Al seguir esta guía con diligencia y compromiso, se puede lograr una mayor robustez en la infraestructura tecnológica, minimizando los riesgos de posibles ataques y fortaleciendo la confianza de los usuarios y clientes en los servicios proporcionados.

La valoración del uso de la guía de buenas prácticas en varias instituciones financieras ha demostrado ser un paso crucial hacia la mejora de la ciberseguridad en este sector altamente sensible.

RECOMENDACIONES

Se recomienda que exista coordinación y colaboración continua entre expertos en seguridad, directivos y el personal involucrado, para mantenerse a la vanguardia en la protección de los activos financieros con la aplicabilidad de la presente metodología. El personal involucrado en distintos niveles y departamentos de la organización juega un papel fundamental en la protección de los activos financieros. La concienciación sobre las prácticas de seguridad, el uso seguro de la tecnología y la rápida detección de posibles incidentes son elementos cruciales para una estrategia de ciberseguridad exitosa.

Se recomienda mantener una constante preparación y capacitación, ya que tanto el conocimiento teórico como práctico son esenciales para garantizar la protección y confianza en las infraestructuras tecnológicas de las organizaciones. En el ámbito de la ciberseguridad, la evolución rápida y constante de las amenazas y técnicas maliciosas hace que el conocimiento esté en un estado de constante cambio. Por lo tanto, es fundamental que los profesionales de seguridad estén actualizados con los últimos avances y tendencias en el campo.

Se recomienda considerar la inversión en la adquisición de las herramientas en sus versiones completas, siempre que esté dentro del presupuesto de las instituciones, con el fin de fortalecer los procesos y la seguridad en su organización. Al adquirir las versiones completas de las herramientas, se obtiene acceso a todas las funcionalidades y características que pueden ser esenciales para abordar de manera efectiva los desafíos de ciberseguridad.

Se recomienda continuar gestionando el conocimiento de la presente metodología de Ethical Hacking, la cual se basa en buenas prácticas, pero puede ser refinada y adaptada a las necesidades específicas de cada institución, teniendo en cuenta sus realidades y requerimientos particulares.

BIBLIOGRAFÍA

adastra. (20 de 05 de 2021). Obtenido de https://thehackerway.com/2021/05/20/post-explotacion-en-sistemas-windows-con-ghostpack-parte-3-de-3/#:~:text=Rubeus,ataques%20contra%20el%20protocolo%20Kerberos.

adastra. (05 de 10 de 2022). *thehackerway*. Obtenido de https://www.elladodelmal.com/2020/05/crackmapexec-una-navaja-suiza-para-el.html

Altube, R. (05 de 11 de 2021). Obtenido de https://openwebinars.net/blog/kali-linux-que-es-y-caracteristicas-principales/

Altube, R. (12 de 11 de 2021). *openwebinars*. Obtenido de https://openwebinars.net/blog/parrot-os-que-es-y-caracteristicas-principales/

Arango, O. (2023). *El ABC de la seguridad informática: guía práctica para entender la seguridad digital.* https://doi.org/http://repositorio.itm.edu.co/handle/20.500.12622/5901

blog.segu-info. (20 de 05 de 2019). Obtenido de https://blog.segu-info.com.ar/2019/05/subfinder-herramienta-de-descubrimiento.html?m=0#:~:text=SubFinder%20es%20una%20herramienta%20de,para%20las%20pruebas%20de%20penetraci%C3%B3n.

Cahuana, J. L. (21 de 11 de 2021). Obtenido de https://www.nettix.com.pe/documentacion/varios/usando-proxy-ssl-con-foxy-proxy/#:~:text=Foxy%20Proxy%20es%20una%20extensi%C3%B3n%20para%20Firefox%20y%20Chrome%20que,que%20falle%20la%20conexi%C3%B3n%20predeterminada.

Codina, L. (01 de 06 de 2020). CÓMO HACER REVISIONES BIBLIOGRÁFICAS TRADICIONALES O SISTEMÁTICAS UTILIZANDO BASES DE DATOS ACADÉMICAS. pág. 15. https://doi.org/https://doi.org/10.14201/orl.22977

colddsecurity. (15 de 01 de 2023). Obtenido de https://www.colddsecurity.com/que-es-wappalyzer/

Columna, P. (2020). *kolibers*. Obtenido de kolibers: https://kolibers.com/blog/openvas.html

derechodelared. (25 de 04 de 2022). Obtenido de https://derechodelared.com/gophish/

desdelinux.net. (06 de 06 de 2018). Obtenido de desdelinux.net: https://blog.desdelinux.net/genymotion-emulador-android-gnu-linux/

elhacker.net. (03 de 02 de 2021). Obtenido de elhacker.net: https://blog.elhacker.net/2021/01/herramienta-analisis-app-apk-android-malware-automatizada-mobsf-mobile-security-framework.html

Estrada, A. (06 de 02 de 2023). Obtenido de https://albertoestrada.es/hacking/burp-suite-que-es/

flu-project.com. (08 de 2016). Obtenido de https://www.flu-project.com/2016/08/simpleemailspoofer-y-spoofcheck.html

Freda, A. (14 de 10 de 2022). *avg*. Obtenido de avg: https://www.avg.com/es/signal/google-dorks

García, M. (2013). El método Delphi para la consulta a expertos en la. *Revista Cubana de Salud Pública, 39(2), 253-267*, pág. 15. https://doi.org/253-267

Gavidia Córdova, J. V. (2022). Modelo de seguridad informática en el control de accesos del Sistema Integrado de Gestión Estratégica de la Universidad Israel, aplicando ISO 27002 y CSF de NIST. *Universidad Israel*, 53. https://doi.org/http://repositorio.uisrael.edu.ec/handle/47000/3360

github. (2023). Obtenido de https://github.com/BishopFox/sliver

GMS. (14 de 10 de 2022). *CriteriosDigital.* Obtenido de https://criteriosdigital.com/sub-portada/gmsseguridad/ataques-de-ciberseguridad-crecen-en-un-400/

Guerra, E. (22 de 06 de 2022). Ecuador es uno de los países más vulnerables para los ciberdelincuentes. Obtenido de https://prensa.ec/2022/06/22/ecuador-es-uno-de-los-paises-mas-vulnerables-para-los-ciberdelincuentes/

Gutierrez, N. (17 de 02 de 2022). Obtenido de https://preyproject.com/es/blog/30-estadisticas-seguridad-informatica

Harán, J. M. (14 de 10 de 2021). Obtenido de https://www.welivesecurity.com/la-es/2021/10/14/banco-pichincha-sufrio-ataque-informatico/

imaginaformacion.com. (s.f.). Obtenido de https://imaginaformacion.com/diccionario-informatico/que-es-kali-linux

isecom. (14 de 12 de 2010). Obtenido de https://www.isecom.org/OSSTMM.3.pdf

Keepcoding. (27 de 04 de 2023). *keepcoding*. Obtenido de keepcoding: https://keepcoding.io/blog/como-funciona-mimikatz/

KeepCoding. (10 de 04 de 2023). *keepcoding.oi*. Obtenido de https://keepcoding.io/blog/que-es-blackarch-linux/

Léon, C. (02 de 05 de 2016). MÉTODO COMPARATIVO. Obtenido de http://eprints.uanl.mx/9943/

Malagon, J. (10 de 07 de 2023). Análisis de las técnicas de ingeniería social que amenazan la seguridad informática de usuarios de entidades financieras. https://doi.org/https://repository.unad.edu.co/handle/10596/55080

Manjaly, S. (23 de 03 de 2023). Obtenido de https://blog.invgate.com/es/wireshark

OEA. (2018). Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe.

Ojeda, F., Moreno, V. P., & Torres, M. M. (2020). Gestión del riesgo y la ciberseguridad en el sector financiero popular y solidario del Ecuador. https://doi.org/https://doi.org/10.35381/cm.v6i2.366

Perez, I. (08 de 04 de 2015). Obtenido de https://www.welivesecurity.com/la-es/2015/04/08/the-harvester-riesgo-nformacion-publica/

Plaza, P. (03 de 10 de 2019). *ironhackers*. Obtenido de https://ironhackers.es/tutoriales/introduccion-a-frida-pentesting-android-parte-1/#:~:text=Frida%20es%20una%20herramienta%20de,%2C%20Windows%2C%20Mac%20y%20QNX.

Rizaldos, H. (22 de 10 de 2018). *openwebinars*. Obtenido de openwebinars: https://openwebinars.net/blog/que-es-metasploit/

Rodriguez, A. (2020). Herramientas fundamentales para el hacking ético. https://doi.org/2020:12(1)116-131

Rubio, J. (2019). Técnicas de ciberataque y su relación con el espionaje industrial y económico. https://doi.org/https://repository.unad.edu.co/handle/10596/31843

Sarango Narváez, D. F. (2023). PROPUESTA METODOLÓGICA PARA LA IMPLEMENTACIÓN DE LA SEGURIDAD EN REDES INALÁMBRICAS DE ÁREA LOCAL. *Universidad Israel* , 44. https://doi.org/http://repositorio.uisrael.edu.ec/handle/47000/3561

Sentrio. (15 de 12 de 2021). Obtenido de https://sentrio.io/blog/que-es-sonarqube/

SEPS. (2022). *www.seps.gob.ec.* Obtenido de www.seps.gob.ec: https://www.seps.gob.ec/wp-content/uploads/SEPS-IGS-IGT-IGJ-IGDO-INGINT-INTIC-INSESF-INR-DNSI-2022-002.pdf

SEPS. (14 de 04 de 2023). *seps.gob.ec.* Obtenido de seps.gob.ec: https://www.seps.gob.ec/wp-content/uploads/Resol-SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-009-NORMA_DE_CANALES_ELECTRONICOS.pdf

Snifer. (31 de 07 de 2021). *sniferl4bs*. Obtenido de sniferl4bs: https://sniferl4bs.com/2021/07/bloodhound-i-que-es-instalaci%C3%B3n-de-neo4j-bloodhound-e-ingestors/#:~:text=Bloodhound%20es%20una%20herramienta%20visor,configuraci%C3%B3n%20de%20usuarios%20y%20pol%C3%ADticas.

Suarez, J. L. (2020). Importancia de la seguridad informática y ciberseguridad en el mundo actual.

Vadmin. (01 de 06 de 2017). *foro.vozidea*. Obtenido de https://foro.vozidea.com/d/58-wafw00f-aplicacion-para-identificar-firewall-waf

Velasco, R. (15 de 05 de 2020). *softzone.es*. Obtenido de https://www.softzone.es/noticias/open-source/backbox-linux-7/

Villacis Peralvo, J. C. (2022). Propuesta de una metodología forense para dispositivos móviles con sistema operativo Android. *Universidad Israel*. https://doi.org/http://repositorio.uisrael.edu.ec/handle/47000/3370

ANEXOS

Anexo 1. Formato encuesta

Encuesta

* **Nombres y Apellidos.**

* **Institución Financiera en la que Labora.**

* **Segmento a la que pertenece la institución en la SEPS.**

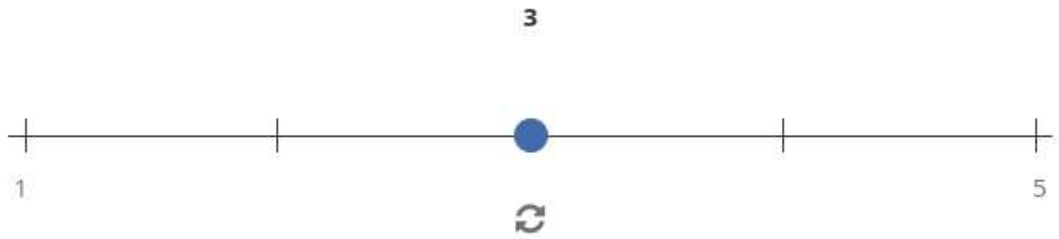
- [ ] 1
- [ ] 2
- [ ] 3
- [ ] 4
- [ ] 5

* **Cargo que Desempeña.**

* **Años de experiencia en el sector financiero.**

* **¿Cómo calificarías la efectividad de la metodología en términos de alcanzar tus objetivos o resultados deseados?**

Siendo 1 Muy ineficaz y 5 Muy efectiva



* **¿Hubo algún aspecto de la metodología que encontraste especialmente útil o innovador?**

* **¿Experimentaste alguna dificultad o desafío al aplicar la metodología?**

- [ ] SI
- [ ] NO

En el caso que sea afirmativo, por favor descríbelo brevemente.

* **¿Hubo alguna situación en la que consideraste que la metodología no era aplicable o no se adaptaba a tus necesidades?**

- [ ] SI
- [ ] NO

En caso afirmativo, ¿por qué?

* **¿Recomendarías esta metodología a otros profesionales o colegas?**

- [ ] SI
- [ ] NO

* **¿Cuál es tu nivel de satisfacción general con la metodología?**

Siendo 1 Muy insatisfecho y 5 Muy satisfecho

3

* **¿Tienes alguna sugerencia para mejorar la metodología?**

Guardar borrador

Enviar

Anexo 2 Certificados de aplicabilidad de la metodología

JARDÍN AZUAYO | COOPERATIVA DE AHORRO Y CRÉDITO JARDÍN AZUAYO
CONTROLADA POR LA SUPERINTENDENCIA DE ECONOMÍA POPULAR Y SOLIDARIA

Cuenca, 21 de agosto de 2023.

CERTIFICADO

Mediante el presente certifico que el Ing. Leandro Damian Quezada Ochoa realizó la presentación del tema de tesis **"PROPUESTA METODOLÓGICA DE BUENAS PRÁCTICAS PARA APLICAR ETHICAL HACKING EN INSTITUCIONES FINANCIERAS DE LA ECONOMÍA POPULAR Y SOLIDARIA"** misma que fue llevada a cabo el día 7 de agosto de 2023, en las instalaciones de la Cooperativa de Ahorro y Crédito Jardín Azuayo, entidad que es controlada por la Superintendencia de Economía Popular y Solidaria (SEPS) y pertenece al segmento 1 de Cooperativas.

Luego de haber analizado la propuesta se concluye:

1. La contextualización de las herramientas va acorde a la propuesta metodológica, sistematizada de manera correcta y adecuada.

2. Las fases de la propuesta están estructuradas de manera cohesiva, proporcionando una guía comprensible que facilita su aplicabilidad. Esto contribuye a establecer un estándar de trabajo efectivo y gestionable.

3. La selección de las herramientas se ajusta al entorno financiero, lo que contribuye a la mitigación de riesgos y a la detección temprana de posibles vulnerabilidades en los sistemas.

4. La propuesta es aplicable en la Cooperativa Jardín Azuayo, donde no solo respalda el cumplimiento normativo, sino que también se encuentra en sintonía con los objetivos de seguridad informática establecidos.

Este documento queda a disposición del destinatario para su utilización en los fines pertinentes.

Atentamente,

HENRY PAUL ZHANAY LEDESMA

Ing. Paul Zhañay Ledesma, MSc
RESPONSABLE DE SEGURIDAD INFORMÁTICA
COOPERATIVA JARDÍN AZUAYO

www.jardinazuayo.fin.ec
Dir.: Benigno Malo 9-75 entre Gran Colombia y Simón Bolívar | **Teléfono PBX:** 07 2 833 255 / Cuenca - Ecuador

SEÑOR DE GIRÓN
COOPERATIVA

Girón, 21 de agosto 2023

CERTIFICADO DE APLICABILIDAD DE LA METODOLOGÍA PARA ETHICAL HACKING UTILIZANDO SISTEMAS OPEN SOURCE

Por la presente, se certifica que la metodología de Ethical Hacking, desarrollada por el Ingeniero Leandro Damián Quezada Ochoa, ha sido evaluada y considerada aplicable para su implementación en los sistemas informáticos, y/o servicios de la Cooperativa de Ahorro y Crédito Señor de Girón.

La metodología propuesta es una aproximación ética y controlada a la identificación y resolución de vulnerabilidades en los sistemas informáticos, con el propósito de fortalecer la seguridad y salvaguardar la integridad de los datos y la infraestructura tecnológica.

La Cooperativa de Ahorro y Crédito Señor de Girón reconoce la importancia de mantener un entorno digital seguro y protegido, tanto para sus propios activos como para la confianza de los socios y clientes. Con la implementación de la metodologia presentada por el Ing. Leandro Damián Quezada Ochoa de Ethical Hacking utilizando herramientas Open Source, la cooperativa puede:

Realizar auditorías regulares y controladas de seguridad informática para identificar posibles vulnerabilidades en los sistemas y redes de la cooperativa.

Evaluar el grado de riesgo asociado a las vulnerabilidades descubiertas y establecer prioridades para su mitigación y definirlas en la matriz de riesgos institucional considerando medidas preventivas y correctivas para abordar las vulnerabilidades identificadas antes de que puedan ser explotadas.

La metodología presentada se ajusta a los principios y valores de la Cooperativa de Ahorro y Crédito Señor de Girón, garantizando la confidencialidad, integridad y disponibilidad de la información, asi como el respeto a la privacidad de los socios y clientes. Y esto permitirá un ciclo de mejora continua en la seguridad de la información.

De esta manera y en base a la evaluación realizada, se concluye que la metodología de Ethical Hacking presentada por el Ing. Leandro Damián Quezada Ochoa es adecuada y aplicable para la Cooperativa de Ahorro y Crédito Señor de Girón.

Sírvase el presente documento hacer uso para los fines pertinentes

Atentamente,

Ing. Martha Cobos M.
GERENTE GENERAL
COAC SEÑOR DE GIRÓN

Ing. Francisco Mocha S.
OFICIAL DE SEGURIDAD DE LA INFORMACIÓN
COAC SEÑOR DE GIRÓN

SEÑOR DE GIRÓN COOPERATIVA | Seguridad de la Información

Matriz Girón:
Calle Antonio Flor y Calderón
(07) 227-6592

www.coacgiron.fin.ec
Girón - Ecuador

COOPAC AUSTRO LTDA.
Cooperativa de Ahorro y Crédito
Protegiendo tu Futuro con Solidez y Confianza

www.coopacaustro.fin.ec

Cuenca, 24 de agosto de 2023

CERTIFICADO

Por la presente certificamos que el Ing. Leandro Damián Quezada Ochoa realizo la presentación de su **"PROPUESTA METODOLÓGICA DE BUENAS PRÁCTICAS PARA APLICAR ETHICAL HACKING EN INSTITUCIONES FINANCIERAS DE LA ECONOMÍA POPULAR Y SOLIDARIA"** misma que fue expuesta para la Cooperativa de Ahorro y Crédito "Coopac Austro" Ltda entidad que pertenece al segmento 2 de Cooperativas y que es regulada por la Superintendencia de Economía Popular y Solidaria.

Se han analizado las 6 fases que componen dicha metodología con las siguientes conclusiones:

1. La metodología es aplicable para la cooperativa "Coopac Austro" Ltda. pues toma en consideración las mejores prácticas de modelos probados como el Open Source Security Testing Methodology Manual (OSSTMM) y el Open Web Application Security Project (OWASP).
2. Se hace uso de herramientas Open Source lo cual lo hace accesible para cualquier institución del sector financiero, se debe considerar sin embargo que se debe mantener cierto nivel de conocimiento previo sobre dichas herramientas para sacar el mayor provecho.
3. La metodología presenta un orden estructurado y organizado lo cual facilita su aplicación por parte de los encarados de la seguridad de la información dentro la institución.
4. Sirve de apoyo en cumplimiento de la normativa vigente SEPS para canales electrónicos pues se alinea a lo solicitado por los entes de control.

El referido podrá hacer uso del presente documento para los fines pertinentes.

Atentamente,

COOPAC AUSTRO LTDA.
DEPARTAMENTO DE TECNOLOGÍA

COOPAC AUSTRO LTDA.
Cooperativa de Ahorro y Crédito
Ing. Orlando Tapia
OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

Mg. Hugo Bastidas
Subgerente de Tecnología de la Información y Comunicación
Coopac Austro Ltda

Ing. Orlando Tapia
Oficial de Seguridad de la Información
Coopac Austro Ltda

Creciendo Contigo

ONCE DE JUNIO
COOPERATIVA

Machala, 04 de septiembre de 2023

CERTIFICADO

Por medio del presente certificamos que el Ing. Leandro Damián Quezada Ochoa realizó la presentación de su **"PROPUESTA METODOLÓGICA DE BUENAS PRÁCTICAS PARA APLICAR ETHICAL HACKING EN INSTITUCIONES FINANCIERAS DE LA ECONOMÍA POPULAR Y SOLIDARIA"** misma que fue expuesta para la Cooperativa de Ahorro y Crédito "Once de Junio" Ltda., entidad que pertenece al Segmento 1 de Cooperativas y que es regulada por la Superintendencia de Economía Popular y Solidaria.

Se aplicaron las 6 fases que componen la metodología con las siguientes conclusiones:

1. La metodología es aplicable para la Cooperativa Once de Junio, pues toma en cuenta buenas prácticas de modelos existentes, tales como el Open Source Security Testing Methodology Manual (OSSTMM) y el Open Web Application Security Project (OWASP).
2. Se hace uso de herramientas Open Source lo cual lo hace accesible para cualquier institución del sector financiero; sin embargo, se debe considerar que es necesario mantener cierto nivel de conocimiento previo sobre dichas herramientas para sacar el mayor provecho.
3. La metodología brinda a los responsables de seguridad de la información una guía clara y efectiva para el desarrollo de las evaluaciones de seguridad de manera ética y proactiva dentro de la institución.
4. Al implementar este enfoque estructurado, la institución está mejor preparada para enfrentar posibles amenazas cibernéticas y garantizar la confianza de nuestros socios y clientes.
5. Ayuda a identificar vulnerabilidades, mejorar la seguridad y sirve de apoyo en cumplimiento de la Resolución Nro. SEPS-IGT-IGS-INSESF-INR-INGINT-INSEPS-009 Norma de control de seguridad en el uso de canales electrónicos para las entidades financieras controladas por la SEPS.

Es todo cuanto podemos certificar en honor a la verdad, pudiendo el interesado utilizar el presente documento como bien creyere conveniente.

Atentamente,

PIEDAD MARIA CABEZAS CHICA
Firmado digitalmente por PIEDAD MARIA CABEZAS CHICA
Fecha: 2023.09.04 16:01:15 -05'00'

Ing. Piedad Cabezas Chica
JEFE DE LA UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN

YINA MARITZA JARAMILLO ZAMBRANO
Firmado digitalmente por YINA MARITZA JARAMILLO ZAMBRANO
Fecha: 2023.09.04 15:52:45 -05'00'

Ing. Yina Jaramillo Zambrano.
JEFE DE LA UNIDAD DE SEGURIDAD DE LA INFORMACIÓN