UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Modelo para el Análisis de Vulnerabilidades Digitales en una entidad pública de Lima, 2021

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Ingeniería de Sistemas con mención en Tecnologías de Información

AUTOR:

Huamantingo Navarro, Ricardo Richard (ORCID: 0000-0002-0300-4184)

ASESOR:

Dr. Martínez López, Edwin Alberto (ORCID: 0000-0002-1769-1181)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LIMA - PERÚ

2022

DEDICATORIA

A mis abuelos Estefa y Felix, quienes desde el más allá, siguen presentes y siendo una fortaleza y motivación.

AGRADECIMIENTO

Agradezco a Dios; a mis padres, por la formación y apoyo; a Alondra, por la motivación constante; a Ivonne y familia, por el apoyo desinteresado.

Índice de contenidos

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS Y FIGURAS

RESUMEN

En la presente investigación, se determina un modelo para el análisis de vulnerabilidades digitales, dicho modelo es adaptable y está desarrollado para que sea implementado en cualquier entidad pública; fue diseñado con el enfoque cualitativo y teniendo en cuenta el paradigma interpretativo, de igual modo, el tipo de investigación que se ha utilizado de acuerdo con el propósito de la misma es de tipo básica, con el diseño investigación – acción, ya que este diseño resulta viable para poder mitigar las amenazas y mantener seguro cada sistema de información, aplicaciones, servicios y las redes de comunicación del ministerio público.

La unidad de estudio se enfoca en la unidad de Seguridad de Información; se utilizó técnicas para la recolección de datos y los resultados se obtuvieron mediante la técnica de la triangulación. Como conclusión se llegó a que el modelo para el análisis de vulnerabilidades tiene tres pilares fundamentales que son la gestión de vulnerabilidades, la metodología para el análisis y las tecnologías defensivas, que a su vez, se subdividen en componentes necesarios para un buen análisis, que contribuirá a reducir la probabilidad de ataques exitosos a entidades públicas, asimismo se tuvo en cuenta las tendencias internacionales respecto a seguridad y ciberseguridad.

Palabras claves: Vulnerabilidades, análisis de vulnerabilidades, gestión de vulnerabilidades, ciberseguridad.

Abstract

In the present investigation, a model is determined for the analysis of digital vulnerabilities, said model is adaptable and is developed to be implemented in any public entity; It was designed with a qualitative approach and taking into account the interpretive paradigm, in the same way, the type of research that has been used according to its purpose is of a basic type, with the research - action design, since this design It is feasible to mitigate threats and keep the information systems, applications, services and communication networks of the public ministry.

The unit of study focuses on the Information Security unit; Data collection techniques were also used and the results were obtained by means of the triangulation technique. As a conclusion, it was reached that the model for vulnerability analysis has three fundamental pillars that are vulnerability management, analysis methodology and defensive technologies, which in turn are subdivided into components necessary for a good analysis, which will help reduce the probability of successful attacks on public entities, international trends regarding security and cybersecurity were taken into account.

Keywords: Vulnerabilities, vulnerability analysis, vulnerability management, cybersecurity.

I. INTRODUCCIÓN

En cuanto a la seguridad de cada sistema de información y de todos los activos, es muy importante tanto a nivel nacional y mundial, así como para las empresas y las entidades públicas, ya que ningún sistema puede considerarse 100% seguro, debido a los ataques y amenazas latentes en el ciberespacio, que pueden terminar en un costo para la organización, aprovechándose de las vulnerabilidades digitales existentes, estas deben descubrirse y analizarse, para reducir las probabilidades de los ataques. Es por ello que resulta primordial que las actividades preventivas como el análisis de vulnerabilidades pasen a ser actividades prioritarias para todos los sectores en especial el sector público.

En el mundo globalizado que se vive actualmente, según la proyección de la compañía CISCO (2020), para el 2023 los usuarios de internet serán el 66% de la población mundial y para entonces los dispositivos conectados a internet serán 29,300 millones, asimismo Frost & Sullivan (2021) mencionan que para el 2026 los dispositivos de IoT conectados serán más de 66 mil millones. Con el crecimiento de los dispositivos conectados, también incrementan las vulnerabilidades y por ende las amenazas, la compañía Check Point (2021), dice que, en este primer semestre a nivel mundial los ciberataques incrementaron en un 29%. Por otro lado. Kaspersky (2021) tras una investigación y análisis, afirma que los ciberataques se incrementaron en un 24% en América Latina. Por ello es necesario medidas de seguridad, en especial las preventivas como el análisis de vulnerabilidades.

Existen vulnerabilidades que al no ser identificadas y mitigadas terminaron en ciberataques, tal es el caso de la vulnerabilidad CVE-2017-0143, también conocido como EternalBlue, como mencionan Walkowski et al. (2021) dicha vulnerabilidad fue aprovechada para que los piratas informáticos desarrollaran el ransonware WannaCry, el cual cifró miles de terabytes de datos causando pérdidas financieras en corporaciones internacionales como Nissan y FedEx. Los gobiernos estatales no son ajenos a estos sucesos, como se menciona en el canal CNN Español (2021), se explotaron vulnerabilidades digitales de 150 agencias del gobierno de EE.UU. De igual forma Europa Press (2021) y BBC News (2021) señalan que muchas organizaciones de EE.UU que usan Microsoft Exchange, resultaron perjudicadas tras exponer las vulnerabilidaes de esos servidores.

En España se impulsan medidas preventivas en el sector público, que se verifican mediante auditorias, ya que se hicieron públicas muchas vulnerabilidades y es el tercer país más atacado dentro de la Unión Europea (The Economy Journal, 2021). En el Estado Australiano, Queensland Government (2018) desarrolló su propia Directriz de Gestión de Vulnerabilidades, para que las organizaciones comprendan mejor cuáles están creando riesgos innecesarios. El Reino Unido creó su Centro de Ciberseguridad Nacional que se encarga de dar respuestas a las vulnerabilidades existentes (HM Government, 2021). También menciona la agencia ENISA (2021) que la Unión Europea ha implementado su equipo de respuestas ante incidentes de seguridad de productos denominado PSIRT que se encarga de gestionar las vulnerabilidades de los productos y servicios.

Las políticas gubernamentales de divulgación pública de vulnerabilidades, resultan necesarias para la implementación de estándares de transparencia de los gobiernos para su manejo y divulgación de vulnerabilidades, Herpig (2018) menciona que mediante el Transatlantic Cyber Forum se pretende adoptar dichas políticas en Alemania y EE.UU., con un enfoque de “cuándo y cómo”. En esa línea EE.UU. mediante el Instituto NIST (2021), implementó su propia base de datos, con la finalidad de automatizar la gestión de vulnerabilidades. Por otro lado Taylor (2021) afirma que los sistemas de TI de gobiernos locales y entidades públicas del Reino Unido, son más vulnerables por su infraestructura de TI obsoleta y sin actualizaciones. El intercambio de información con respecto a las vulnerabilidades trae buenos resultados, ya que permite mitigar a tiempo las amenazas.

Las entidades públicas a diferencia del sector privado, cuenta con pocos profesionales y áreas encargadas de la ciberseguridad, debido a ello, como mencionan Gutierres et al. (2020), en el 2019, Ecuador sufrió 40 millones de ciberataques a 300 entidades públicas, con el fin de paralizar sus servicios públicos. Según el reporte de ciberseguridad del Banco Interamericano de Desarrollo (2020), el gobierno federal de Brazil posee un marco para la divulgación de vulnerabilidades, que sirve para elaborar informes y abordar dichos incidentes; en Haití tanto el sector público como el privado plantean realizar auditorías tecnológicas para detectar vulnerabilidades; en Paraguay, mediante el Ministerio de Tecnología se ofrece auditorías de vulnerabilidades a los sistemas gubernamentales.

Ahora bien con respecto a Perú, el Banco Interamericano de Desarrollo (2020) menciona que aún no tiene una estrategia nacional de ciberseguridad, en consecuencia tampoco dispone de una gestión de vulnerabilidades adecuado, pero cuenta con un CSIRT, que es el equipo de respuesta a incidentes de seguridad, de entidades públicas; además, entre el 2016 y 2020 ha tenido un crecimiento regular en estos temas. Así mismo el diario Gestión (2018) indica que el sector energético es el más vulnerado después del financiero, con un costo de $ 17.20 millones al año, el cual se podría evitar prediciendo y gestionando las vulnerabilidades en su entorno digital e industrial.

Al ser un país en desarrollo, la infraestructura e implementación tecnológica en Perú, traerá consigo vulnerabilidades evidentes que tienen que ser identificadas y mitigadas a tiempo; como menciona Ormachea (2019), también se debe plantear políticas públicas y la base jurídica para responder ante estos eventos. Bustamante et al. (2021) hacen énfasis que en las municipalidades se introducen vulnerabilidades por instalaciones de software no autorizados, estás provocan fugas de información, por ello se debe definir bien el cómo gestionar las vulnerabilidades. Con una perspectiva más clara MIDIS (2020) busca garantizar la identificación oportuna de vulnerabilidades digitales y brindar una efectiva respuesta con medidas adecuadas para solucionar el riesgo conjunto, mediante su Procedimiento para gestionar las vulnerabilidades y las incidencias de seguridad de la Información.

En el Ministerio Público se vive una realidad similar a todo lo expuesto anteriormente, ya que se enfrenta a constantes amenazas por las vulnerabilidades de sus sistemas informáticos, se puede apreciar mediante MPFN (2017) y el Plan de Gobierno Digital 2021 – 2023, uno de los proyectos informáticos fue para el análisis de vulnerabilidades, con un costo de 170 mil nuevos soles, dicho proyecto consistía en la identificación, corrección y monitoreo de controles de seguridad, para luego mitigar las vulnerabilidades y riesgos identificados. Asimismo con MPFN (2018), se verifica la implementación de múltiples sistemas informáticos, pero no incluye un análisis o gestión de vulnerabilidades, cabe mencionar que hay un esfuerzo en mantener actualizado los softwares, pero la implementación de un nuevo sistema trae consigo inherentemente vulnerabilidades que deben ser identificadas a tiempo, para evitar ataques y pérdida de información.

Según la realidad problemática expuesta, esta investigación tiene como problema general: ¿Cómo se desarrolla un modelo para el análisis de vulnerabilidades digitales en un ministerio público de Lima, 2021?, de ahí, se plantean los problemas específicos siguientes: (a) ¿Cómo es la gestión de un Modelo para el Análisis de Vulnerabilidades Digitales en un ministerio público de Lima, 2021?, (b) ¿Cómo es la metodología en el Modelo para el Análisis de Vulnerabilidades Digitales en un ministerio público de Lima, 2021? y (c) ¿Cómo es la tecnología defensiva en el Modelo para el Análisis de Vulnerabilidades Digitales en un ministerio público de Lima, 2021?.

Referente a los objetivos, se plantea como objetivo general: Proponer un modelo para el análisis de vulnerabilidades digitales en un ministerio público de Lima, 2021; de igual forma se establecen los objetivos específicos siguientes: (a) Determinar la gestión de un Modelo para el Análisis de Vulnerabilidades Digitales en un ministerio público de Lima, 2021; (b) Determinar la metodología en el Modelo para el Análisis de Vulnerabilidades Digitales en un ministerio público de Lima, 2021; (c) Determinar la tecnología defensiva en el Modelo para el Análisis de Vulnerabilidades Digitales en una entidad pública de Lima, 2021.

En cuanto a la justificación de la presente investigación, predomina su intención teórica, puesto que, facilitará el conocimiento necesario y actualizado, así como también contribuirá a las teorías existentes sobre el análisis y gestión de vulnerabilidades digitales y servirá como base teórica para futuras investigaciones con temas relacionados. También tiene una intención metodológica, porque la investigación ayudará a proponer un modelo, que resulta necesario implementar en las entidades públicas, para evitar los ciberataques, además puede ser usado por otras investigaciones.

La investigación en cuestión también tiene una justificación práctica, ya que el modelo para el análisis de vulnerabilidades digitales es conveniente porque reducirá la probabilidad de los ciberataques, permitiendo la identificación, rectificación y prevención, con tiempo suficiente para volver invulnerables estos sistemas informáticos, asimismo contibuirá a mantener y por ende a mejorar la integridad, confidencialidad y disponibilidad en la seguridad de la información del Ministerio Público, ya que las entidades públicas suelen ser víctimas y blancos de hackers, por la información que poseen.

II. MARCO TEÓRICO

Con respecto a los trabajos e investigaciones previas revisadas en el entorno nacional, referentes a las vulnerabilidades digitales existentes, se tiene a Ormachea (2019) quien concluyó que, una de las pricipales brechas es la gran carencia de adecuadas tecnologías, que contienen programas y equipos obsoletos, con gran presencia de vulnerabilidades, el cual conlleva a que haya poca articulación e integración con las nuevas tecnologías que se pretende implementar. Así mismo Bustamante et al (2021), sostuvo que, para mantener la información segura, se implantó un modelo con políticas seguras y/o de seguridad, que dio resultados positivos en la gestión de la seguridad de la información, y se recomiendan el uso de dicho modelo dentro de muncipalidades, previa identificación de su realidad.

Por otro lado Niño (2018), en el INEI con sede en Lambayeque, plantea un modelo de seguridad de la información, quien concluye que un análisis para determinar los riesgos nos permite identificar y conocer las amenazas que son producidos por vulnerabilidades tecnológicas en ciertos casos y afectan a los activos de la entidad, debido a ello se listaron todos los activos para identificar sus vulnerabilidades explotables por amenazas, asimismo mencionó que frente a vulnerabilidades que afectan la disponibilidad de sus activos de información, no contaban con medidas de seguridad para su preservación.

Con referencia a las investigaciones previas revisadas en el contexto internacional, sobre el análisis y gestión de vulnerabilidades digitales, se tiene a Mugavero et al. (2018) quienes mencionan que los informes de vulnerabilidad proporcionan conocimiento adecuado y permiten desarrollar sus contramedidas, también que la gestión de vulnerabilidades debe brindar soporte a la arquitectura y sistemas heredados, hasta que los protocolos de seguridad sean universales, asimismo hacen enfasis en que, al invertir presupuesto en la gestión proactiva de vulnerabilidades, se eleva el costo de los ataques, es decir los actores de las amenazas deberán invertir más recursos en la identificación del eslabón más débil; Chen et al. (2019) refirieron que saber si existe y cuándo se explotará una vulnerabilidad, más aún si se supiera la gravedad de la vulnerabilidad, esto ayudaría al personal de seguridad a idear los parches correspondientes.

De manera semejante Kenner (2020) en su investigación, refiere que para identificar las vulnerabilidades en una infraestructura de red, se debe utilizar los escáneres y determinar la superficie de ataque visible, esto incluye, identificación de puertos accesibles, protocolos, servicios alojados y servicios prestados, dicha información se puede recopilar mediante OpenVass o Nessus, de esa manera, se identifica y se pone a disposición las vulnerabilidades, para que los profesionales encargados de la seguridad evaluen y lo solucionen; Li, Wang, et al. (2022) plantean un nuevo método para determinar la vulnerabilidad de la red, ya que los métodos convencionales no son efectivos para algunos tipos específicos de vulnerabilidades que generan fallas de enlace.

Prosiguiendo con los trabajos previos, se destaca a Morales et al. (2020), quienes refirieron que para el analisis de vulnerabilidades de los sistemas, se verifica por medio de las herramientas de escaneo como: Acunetix, Shodan y Nessus, las cuales permiten el escaneo de IPs públicas o sus enlaces web, cuyo resultado otorga la clasificación de las vulnerabilidades, cabe mencionar que manejaron tres segmentos: Redes, Información y Aplicaciones. La explotación del control de acceso es el más recurrido, por ello Muyón y Montaluisa (2020) junto a Reis et al. (2021), afirman que el acceso no autorizado se da cuando el programador no configura adecuadamente la accesibilidad al software y esto genera las vulnerabilidades de acceso, también que existen amenazas y vulnerabilidades en los servicios web, ya que estos se diseñan para estar interoperables y abiertos.

Continuando, a nivel internacional se tiene a Kapellmann & Washburn (2019) que afirman que la gestión de vulnerabilidades es un desafío para las organizaciones, el personal de seguridad debe hacer oportunamente evaluaciones de vulnerabilidad e implementar controles, actualizaciones y parches. Tambien Nakajima et al. (2019) en su investigación refieren que, muchos gobiernos han iniciado las investigaciones sobre la regulación de vulnerabilidades, su gestión y su ciclo de vida (que puede clasificarse en dos grupos: pre y post descubrimiento), sacando leyes y normas. Lee et al. (2020), aportan que para la detección estandarizada de vulnerabilidades de seguridad, se debe hacer uso de las vulnerabilidades y exposiciones comunes (CVE) junto con su base de datos sobre las vulnerabilidades nacional (NVD) de EE.UU.

Con respecto a las teorías de la presente investigación, iniciaremos aclarando el término “vulnerabilidad digital”, que según el contexto de la investigación se define como una debilidad o fallo que hace posible una amenaza; Romero et al. (2018), define que, una vulnerabilidad es un fallo de diseño del sistema, asimismo afirma que un riesgo es la probabilidad de que una determinada vulnerabilidad sea aprovechada por una amezaza en concreto; también Nguyen-Duc et al. (2021) lo define como un atributo de calidad de un sistema que si se activa de forma accidental o se explota intencionalmente, provoca una falla de seguridad; todo esto puede originarse por errores de configuración, un diseño deficiente o técnicas de programación/codificación inseguras o inadecuadas, por ello una vulnerabilidad identificada debe abordarse para mitigar la amenaza. Una vulnerabilidad es inherente a todas las redes y dispositivos informáticos.

Ahora bien, el análisis de vulnerabilidades digitales son aquellas pruebas nada intrusivas, no debe afectar la disponibilidad, confidencialidad e integridad o la de los servicios que se analizan; Imperva (2021) precisa que el proceso de análisis de vulnerabilidades normalemente consta de Identificación, Análisis, Evaluación de Riesgo y Remediación, tal como se muestra en la Figura 1; Li et al. (2021) dice que, permite la detección de vulnerabilidades (fallos de sistema) y que para ello se debe usar la herramienta adecuada; Arfaj et al. (2022) nos afirma que, al incluir las pruebas de penetración este proceso se vuelve intrusivo; ya que tras el análisis, suele haber una alta tasa de falsos positivos, es decir, vulnerabilidades detectadas por la herramienta de escaneo que realmente no existen, para descartarlos se aplica las pruebas de penetración o penetration testing en inglés.

Las redes suelen estar plagadas de al menos una de las tres principales vulnerabilidades o debilidades que son: (a) debilidades tecnológicas, las tecnologías y las redes tienen debilidades intrínsecas como: debilidades de protocolo, del sistema operativo y de equipos de red; (b) debilidades de configuración, debido a las malas configuraciones de los dispositivos de red, contraseñas débiles, cuentas de usuarios no aseguradas y servicios de internet mal configurados; y (c) debilidades de la política de seguridad, puede darse por falta de una politica escrita, falta de continuidad y controles de acceso sin aplicar (Romero et al., 2018) y (Egloff, 2021). Todas estas pueden traer riesgos de seguridad para la red y los sistemas, más aún, si los usuarios no siguen las politicas de seguridad.

Figura 1

Vulnerability Analysis Process

Nota. En la figura se muestra el proceso de analisis de vulnerabilidades, Adaptado de Imperva (2021)

El proceso de analisis de vulnerabilidades digitales debe ser llevado a cabo trimestralmente, después de la integración de un nuevo sistema de información o luego de un cambio significativo, esto debido a que se le considera como una actividad preventiva, tal como afirma Romero et al. (2018) estos mecanismos preventivos son los más olvidados y se ve como un tiempo perdido, la administración por lo general lo considera un costo adicional innecesario; además el escaneo de vulnerabilidades internas debe ser realizado por el personal de la entidad con conocimiento demostrado de seguridad y debe ser relativamente corto y automatizado, se aplica las mismas condiciones para una prueba de penetración, excepto que es de mayor duración, más detallado y se debe ejecutar anualmente. En esa línea, se puede evitar los ataques informáticos o al menos reducir el impacto, haciendo uso de los mecanismos preventivos.

La apodción de un modelo para el análisis de vulnerabilidades digitales en la entidad pública como actividad preventiva primordial, contribuirá a reducir la probabilidad de los ataques y por ende a mejorar la seguridad de los sistemas, identificando a tiempo los fallos y mitigando cualquier amenaza, esto se logrará mediante la (a) gestión de vulnerabilidades, (b) la metodología para el análisis, (c) la auditoria de seguridad y finalmente con la (d) tecnología defensiva, cabe mencionar que, los escaneos de vulnerabilidades son esecialmente técnicos y se orientan a la identificación y detección, cada uno de los cuatro componentes son los pilares fundamentales para el diseño del modelo propuesto, que a continuación se irán describiendo.

Para definir un modelo para el análisis de vulnerabilidades, es muy importante hablar de la gestión de vulnerabilidades o vulnerability management traducida al idioma inglés, que desarrollada y aplicada adecuadamente resulta ser la única manera de garantizar una respuesta rápida al descubrimiento de vulnerabilidades; Mugavero et al. (2018) dice que debe incluir la práctica cíclica de identificar, clasificar, remediar y mitigar vulnerabilidades en la red, software y firmware, juntamente con el desarrollo de políticas de seguridad y capacitaciones al personal de la organización, pero debido a que el comportamiento de los intrusos es impredecible, no es posible brindar documentos con instrucciones claras para combatir las amenazas, por ello es necesario hacer uso de la experiencia previa y mentalizar las posibles contramedidas en base a los ataques más comunes.

Cabe resaltar que la gestión de vulnerabilidades es un proceso ciclico y continuo, que implica más que una simple ejecución de una herramienta de análisis, sin embargo, la elección de un conjunto de herramientas de alta calidad mejora drásticamente el éxito de este proceso; Dissanayaka et al. (2020) mencionan que un sistema de gestión de vulnerabilidades protege los sistemas contra la explotación y el robo de datos, esto hace que sea vital en la gestión de riesgos de TI, por tres razones: 1. Amenazas persistentes (ataques que aprovechan las vulnerabilidades), 2. Regulaciones (las regulaciones gubernamentales exigen prácticas rigurosas de gestión de vulnerabilidades); por ello cuando se organiza y se ejecuta bien es proactivo, es decir se anticipa a las amenazas, esto permite que no solo se oriente al area de TI, sino que también se oriente a los negocios.

Así como cualquier otro marco de gestión, la gestión de vulnerabilidades tiene un ciclo de vida y la mayor parte de las políticas de seguridad que existen se crearon bajo la idea de que hay cuatro procesos de alto nivel: (a) descubrimiento, (b) realización de informes, (c) priorización y (d) respuesta, (Mugavero et al., 2018); el descubrimiento o identificación de vulnerabilidades puede variar entre un sistema y otro, un descubrimiento manual proporciona solo algunos posibles vectores de ataque, en cambio, los conjuntos de herramientas de evaluación de vulnerabilidades automatizadas (Nessus, OpenVAS, Acunetix, Languard, etc.) sirven para realizar una descripción general del estado de seguridad del sistema, pero la desventaja de estas herramientas es que la gran cantidad de resultados, son falsos positivos que se generan durante la auditoría.

Una vez que las vulnerabilidades son detectadas de forma manual o automatizada, se deben archivar en el informe de evaluación de vulnerabilidades siguiendo las buenas prácticas (OWASP o ISSAF); Lala et al. (2021) sugieren que se debe enumerar según el OWASP top ten, es decir, las 10 vulnerabilidades principales de OWASP; en este caso se debe usar el OWASP top ten 2021, ya que hay una variación significativa con respecto a las vulnerabilidades del 2017 (Fredj et al., 2021); en el cual lidera como vulnerabilidad número uno “Broken Access Control” o “Control de Acceso Roto”; además, según los estándares y procedimientos de seguridad internos establecidos en la organización, se debe informar al departamento o área de seguridad y a la alta dirección de la entidad, sobre las vulnerabilidades detectadas, para su posterior actualización de seguridad.

Uno de los aspectos claves es la priorización dentro de cualquier proceso de gestión de vulnerabilidades o gestión de riesgos, asimismo las vulnerabilidades pueden ser explotables y no explotables, tanto del lado del servidor como del lado del cliente. También se pueden clasificar según Mugavero et al. (2018) como: (a) Crítico, (b) Importante, (c) Moderado y (d) Bajo; de igual manera Schweikert et al. (2021) nos mencionan que, es importante la priorización de las vulnerabilidades según el riesgo identificado y las consecuencias de dichas fallas de seguridad. La priorización de una vulnerabilidad recién descubierta es fundamental para desarrollar una respuesta adecuada, mitigar los riesgos y remediar las amenazas potenciales, debidamente desarrollada debe asignarse para la instalación priorizada durante el próximo mantenimiento programado.

Finalmente, la respuesta a las vulnerabilidades puede requerir o no acciones inmediatas, según su clase, disponibilidad del desarrollo del parche, versión del firmware y el tipo de procedimiento de instalación de la actualización de seguridad; cabe resaltar que, una vulnerabilidad crítica, que puede causar DDoS remoto o ejecución remota de código, debe tratarse como una amenaza inmediata, esto da lugar a mantenimientos y parches no planificados; Mugavero et al. (2018) nos sugiere que, se debe aplicar la actualización lo antes posible o posponer la actualización (como máximo) hasta el próximo mantenimiento planificado; cada nueva característica, parche o actualización de seguridad, aplicada a un firmware, puede resultar en una vulnerabilidad potencial, y el ciclo debe considerarse como un proceso continuo de gestión de vulnerabilidades dentro de una entidad.

Las prácticas de seguridad modernas promueven metodologías genéricas que abarcan y cubren muchas necesidades, normalmente una organización puede adaptarse a una determinada metodología, pero no siempre y más aún en una entidad pública, que no cuenta con recursos y personal para acomodarse a una metodología, es por eso que es necesario una metodología acorde a la realidad; entonces, determinar una metodología para el análisis de vulnerabilidades es primordial, para reducir la probabilidad de ataques y mitigar las amenazas que se encuentran en los sistemas de la organización, para ello se establece un conjunto de pasos: (a) Acuerdo de confidencialidad, (b) Recolección de información, (c) Análisis interno y (d) Análisis externo, estos se describen con más detalle parráfos abajo.

Es necesario la explicación de cada paso que se debe realizar para poder hacer un análisis de vulnerabilidades de forma adecuada y lo más importante sin tener inconvenientes en la ejecución, es importante conocer el procedimiento a seguir en la detección de fallos al ser parte del equipo de seguridad, cuyo objetivo consiste en dar a conocer el real estado de la red actual, las amenazas potenciales y los riesgos que corren; Romero et al. (2018) nos propone, establecer las reglas de juego, es decir, antes de realizar el proceso de análisis de vulnerabilidades, se debe definir cuáles serán las actividades a desarrollar y los límites de estos, así como las obligaciones y los permisos que se seguirán; por ejemplo, cuando se relice el análisis, se debe mantener al mínimo la información de esta actividad, para que el uso de la red por parte del personal sea normal.

Referente al acuerdo de confidencialidad o también conocido como acuerdo de no divulgación, es una de las principales actividades que se debe corroborar, entre la entidad y el analista de seguridad, es necesario dicho acuerdo entre las partes involucradas en el análisis de vulnerabilidades, porque, como nos comenta Ramsauer et al. (2020) en el proceso de descubrimiento, es posible que se obtenga información sumamente crítica para la entidad en cuestión, como contraseñas, nombres de usuarios, documentos expuestos en la red, puertas traseras, entre otros; esto generalmente se comenta en un grupo privado pequeño y todo se usa para fines informativos, seguridad y mejoras de servicio, no puede divulgarse a terceros o personas que no estén involucradas en el análisis, asimismo el acuerdo de confidencialidad brinda un marco legal y un respaldo formal.

Otro punto a verificar es la recolección de información, que inicia dentro del análisis de vulnerabilidades cuando se obtiene la información del o los objetivos, en este punto se determina el uso de un test de caja negra o caja blanca como mencionana Arcuri (2021) y Hamza & Hammad (2019), un black box test es un proceso similar a la que sigue un atacante, se puede obtener direcciones, correos, nombres de dominios, para ello se puede usar la técnica OSINT que tiene 6 fases para la recolección de información, como se muestra en la Figura 2, por otra lado un white box test, ayuda a recopilar la información en mayor cantidad, como; dirección del servidor, nombre e IDs de usuarios, passwords, servicios, topologías de red, privilegios, entre otros.

Figura 2

Proceso OSINT

Nota. En la figura se muestra el proceso de analisis, Adaptado de Imperva (2021)

Previo al análisis de vulnerabilidades, se debe todavía realizar un test o análisis interior, que sirve para determinar hasta dónde se permitirá acceder con los privilegios usuales de un usuario en la red y sistemas de la organización, quien proporcionará un dispositivo con usuario y contraseña, de un usuario típico; un análisis interno contiene múltiples pruebas que según Thapa et al. (2021) y Laghrissi et al. (2021) pueden ser: (a) test de aplicativos de internet, (b) la revisión de la privasidad, (c) test de sistema de detección, (d) descifrado de contraseñas, (e) test de medidas de contingencia, (f) test de denegación de servicios y (g) evaluación de las políticas de seguridad; con estas pruebas garantizamos una mejor ejecución del análisis de vulnerabilidades.

Luego de lo anterior, continuamos con el análisis exterior que consisten en, acceder a los servidores de la entidad de manera remota y lograr conseguir permisos y/o privilegios que naturalmente no deberían estar accesibles; Khlobystova & Abramov (2022) sugieren que, se debe iniciar con técnicas de ingeniería social, para conseguir información y acceder, el análisis exterior consta de: (a) revisión de la inteligencia competitiva, (b) revisión de la privacidad, (c) análisis de solicitud y (d) análisis de sugerencia direccionada; luego se debe hacer las pruebas de sondeo de red, identificar los servicios de sistemas, buscar y verificar las vulnerabilidades, test de relaciones de confianza y verificar las redes inalámbricas bajo el estándar 802.11; al finalizar se debe elaborar un informe detallado de lo realizado, especificando la lista de vulnerabilidades que se probaron y detectaron, también los dispositivos y servicios que son vulnerables.

Es muy importante determinar la herramienta que se utilizará en el análisis de vulnerabilidades, entre las más usadas y con buenas prestaciones, tal como muestra Qasaimeh et al. (2018) se tiene los siguientes: (a) Nessus: es una buena solución de administración de vulnerabilidades y ayuda a reducir la superficie de ataque; (b) Acunetix: permite pruebas automatizadas, para reducir el aumento de ataques en la capa de aplicaciones web, (c) Languard: es un software de seguridad que se diseñó para explorar la red, permite escanear los equipos y gestionar los parches de seguridad; (d) Nexpose: internacionalmente conocida, su descubrimiento dinámico se integra con su infraestructura actual; (e) OWASP ZAP: permite comprobar la seguridad de la web para evitar vulnerabilidades que pongan en riesgo los datos y el servidor; y (f) BurpSuite: permite hacer auditorías de seguridad a aplicaciones web y es conocido como la navaja suiza del pentester.

Una vez que se identifican las vulnerabilidades, descartando los falsos positivos, para reducir las probabilidades de los ataques, mitigar las amenazas y evitar el robo de información, es necesario determinar las tecnologías defensivas que se pueden implementar; normalmente al hablar de este punto se viene a la mente “los antivirus”, pero existe más elementos de tecnología defensiva que se pueden implementar en una entidad (Daffalla et al., 2021); además se tiene que tener mucho cuidado con la gestión administrativa ya que puede involucrar el departamento de TI y las áreas de seguridad de la información, que tienen funciones diferentes, también se debe establecer una defensa en profundidad.

Al referirnos a las soluciones defensivas, hablamos de implementar barreras o controles, para evitar que las vulnerabilidades sean explotadas, las capas de una defensa en profundidad según Romero et al. (2018) constan de: (a) Sistema Operativo, (b) Aplicaciones, (c) Segmento de Red y (d) Red Perimetral, se debe tener en cuenta que cada una de ellas involucra recursos y se encarga de mitigar los riesgos, estas soluciones implementadas en cada capa, normalmente tienen la finalidad de evitar la explotación de las vulnerabilidades y se recomienda que se hagan del interior hacia el exterior, dentro de las técnicas de seguridad, se tiene el mantenimiento de los equipos, que va de la mano con los parches de seguridad, esta actividad aparentemente no tiene relevancia, pero si es posible que se elimine una vulnerabilidad en el equipo ya no sería necesario una capa exterior.

Otra actividad necesaria es, instalar y mantener actualizado el software de antivirus en los servidores y en cada estación de trabajo, estos programas se centran en la detección de malware, analizando las posibles amenazas antes de que se ejecuten y de esa manera prevenir ataques (Sreerag et al.,2022); en caso no se tenga recursos para adquirir programas costosos se debe activar Windows Defender en cada equipo; los sistemas de protección y detección en punto final suelen ser más avanzados gracias a que trabajan en modo cliente – servidor, esto permite tener reportes junto a un sistema de gestión centralizado, brindan detección en ejecución y emiten alertas de incidentes; cabe mencionar que el software antivirus brinda protección contra el malware, pero habrá fallas de configuración que podrían dejar los sistemas expuestos a ataques.

Proporcionar seguridad de red en la actualidad es una gran preocupación, ya que estos entornos están expuestos a diversos tipos de riesgos, amenazas y ataques de seguridad, para ello se debe hacer, de acuerdo con Guru Prasad et al. (2022) y Romero et al. (2018), la implementación de medidas de seguridad en: (a) Segmentación de redes, (b) Proxies, (c) Firewalls, (d) Sistemas de prevención y detección de intrusiones: Intrusion Prevention System (IPS), Intrusion Detection System (IDS), y (e) Security Information and Event Management (SIEM) del inglés, que es una solución híbrida entre la gestión de información de la seguridad y respectivamente la gestión de eventos; hay que tener en cuenta que no debemos centrar toda la defensa en la red perimetral, ya que si el ataque supera este nivel no habría más protección, por eso hay que defender en cada nivel de profundidad.

Debido a que los entornos administradores de justicia se están convirtiendo en entornos cada vez más complejos en los que una gran cantidad de dispositivos y sistemas de información están vinculados entre sí para prestar servicios, requieren medidas de seguridad especiales, resguardando la integridad de los datos administrados y la privacidad, en esa línea los firewalls se consideran la primera línea de defensa para proteger las redes y abordar las amenazas, ataques y riesgos en general, como nos menciona Anwar et al. (2021), se aplican a diferentes niveles en las redes y van desde los convencionales basados en servidor hasta los firewalls basados en la nube; comprender los tipos, los servicios ofrecidos y el análisis de las vulnerabilidades subyacentes son consideraciones de diseño importantes que deben abordarse antes de implementar un firewall.

Desde la alta dirección y los jefes de cada área tienen un rol importante dentro de la seguridad tecnológica y su infraestructura, porque es necesario que coperen los jefes en identificar los riesgos que impidan el cumplimiento de sus funciones, asimismo deben permitir la implementación de estas medidas de seguridad de manera eficiente, como menciona Romero et al. (2018), como líderes deben dar lugar a un plan de seguridad siguiendo las estrategias y objetivos de la entidad, para ello se debe ver los siguientes puntos: (a) Riesgos: amerita identificar y evaluar los riesgos, luego planificar un plan de mitigación, siempre en coordinación con el jefe de TI y el área de seguridad; (b) Implantación de sistemas: tiene que ir de la mano con estándares de seguridad de la ISO 27000; y (c) Cumplimiento legal: seguir con las normas y leyes del gobierno peruano.

Contextualizando el dicho, la seguridad será tan fuerte como su eslabón más débil, en este caso el usuario es el punto más débil, se puede implementar un sistema de seguridad muy complejo, pero no se puede tener el control de las personas y es ahí dónde surge una de las mayores vulnerabilidades de toda organización, como afirma Romero et al. (2018), un usuario puede actuar involuntaria o voluntariamente para causar daño, un atacante fácilmente puede tener el control de un usuario o personal de la entidad por medio de la técnica de ingeniería social, terminando este en un enemigo interno; Diamantopoulou et al. (2020) menciona, involucrar a los usuarios en los controles de la ISO 27002; por todo lo mencionado, resulta imprescindible la concienciación de usuarios, se les debe involucrar activamente en las prácticas de seguridad.

Desarrollar una cultura de seguridad institucional en el que se involucre todo el personal es esencial, juntamente con buenas prácticas y hábitos de trabajo seguro; se debe tener extremo cuidado al eliminar documentación confidencial, hay que establecer un procedimiento seguro que incluya por ejemplo los destructores de papel, otro hábito seguro es bloquear la sesión cuando se deje solo el equipo de cómputo, practicar la política de escritorio limpio, identificar las fuentes de procedencia de los correos, proteger la reputación digital y el uso de contraseñas seguras, sumado a otros hábitos seguros, son parte de la prevención y reducción de amenazas, ataques y riesgos; es importante hacer énfasis en el fortalecimiento de las contraseñas, ya que la contraseña, junto al nombre del usuario son las llaves de acceso a los sistemas, se debe promover el uso de contraseñas robustas.

Finalmente, una buena práctica de seguridad en estos momentos, para proporcionar información sobre la priorización y respaldar el análisis predictivo, es haciendo uso de: Common Vulnerabilities and Exposures (CVE), que traducido es, Las vulnerabilidades y exposiciones comunes; y a través de la National Vulnerability Database (NVD) traducido como Base de datos nacional de vulnerabilidades, que es el repositorio de vulnerabilidades del gobierno de EE.UU (Jiang et al., 2021); dichos repositorios públicos permiten una forma de estandarizar y compartir información actualizada sobre vulnerabilidades, con el propósito de mejorar la conciencia de la seguridad cibernética, por otro lado, otros servicios públicos, como Shodan y Microsearch, proporcionan la plataforma para la generación de informes de vulnerabilidades y el desarrollo de exploits de prueba, para ir mitigando las amenazas y reparando las vulnerabilidades descubiertas.

III. METODOLOGÍA

En la línea del planteamiento cualitativo, se sabe dónde se empieza, pero no dónde se concluirá, se caracteriza esencialmente porque en el transcurso de la investigación se van viendo modificaciones y por ello en estas investigaciones se debe estar preparado para adaptarse a los cambios que van surgiendo producto de la misma investigación; debido a ello, la investigación en cuestión, es con un enfoque “Cualitativo”, como menciona Hernández y Mendoza (2018), este enfoque tiene como finalidad la expansión y profundización de los datos e información, en este caso el conocimiento sobre el análisis de vulnerabilidades, ya que a partir de la observación de los participantes se reconstruye una realidad tal cual es percibida, sin la necesidad de generalizar, su importancia radica en entender el fenómeno a partir del punto de vista de aquellos que lo experimentan.

Asimismo, como método, esta investigación se basa en el paradigma interpretativo, que de acuerdo con Escudero y Cortez (2018) busca profundizar los conocimientos y el entendimiento del porqué de un determinado contexto, con una mirada holística que en este peculiar caso se centra alrededor del análisis de vulnerabilidades digitales, siguiendo el principio de que cualquier escenario e individuo es susceptible de un estudio y también resulta interpretativa a la hora de pretender encontrar sentido a los hechos y fenómenos según los significados dado por las personas involucradas en dicha realidad.

3.1. Tipo y diseño de investigación

Tipo de investigación

La investigación en cuestión, viene a ser de tipo básica, debido a que las investigaciones de este tipo, surgen de la necesidad de profundizar, reafirmar e incrementar las teorías referentes a las vulnerabilidades digitales, tal cual cómo se intenta realizar con el modelo a proponer, según menciona Escudero y Cortez (2018), este tipo de investigación se orienta al descubrimiento de los principios básicos y profundizar las definiciones y conceptos del análisis de vulnerabilidades digitales; cuyo propósito radica en la formulación de nuevo conocimiento o la modificación de las teorías ya existentes, la clave es la reflexión continua que

permitirá la transformación y uso óptimo de la tecnología, cabe mencionar que la investigación básica es la base y genera un previo antecedente para una investigación de tipo aplicada, que tiene como objeto, estudiar e investigar el problema destinado a la acción, asimismo se tiene la intención de llevar posteriormente a la práctica las teorías generales plasmadas a lo largo de toda la investigación.

Diseño de investigación

En el trabajo de investigación se ha hecho uso del diseño "investigación – acción", porque es un camino viable para mitigar las amenazas y mantener más seguros cada sistema de información, aplicativos y la red de comunicación del ministerio público, mediante el modelo de análisis de vulnerabilidades digitales. De Ñaupas et al. (2018) se rescata que, este diseño permite que la persona o el investigador sea considerado como objeto de estudio y como resultado, el investigador es protagonista de transformar su propia realidad, por otro lado Hernández y Mendoza (2018), hace énfasis en que el diseño de investigación acción debe conducir a cambiar e integrarlo en el mismo proceso de investigación, es por eso que el diseño se ajusta a esta investigación, ya que se busca resolver y comprender la problemática de las vulnerabilidades digitales en el sector público.

3.2. Categorías, Subcategorías y matriz de categorización:

Para diseñar un modelo óptimo para el análisis de vulnerabilidades digitales, se ha desagregado y/o determinado tres componentes o categorías fundamentales, cada uno de ellos con su correspondiente subcategoría, tomando como referencia a Mugavero et al. (2018) para la categoría de Gestión, junto con sus cuatro subcategorías, en el cual se determina como debe ser la gestión de vulnerabilidades; y Romero et al. (2018) para las categorías de Metodología para el análisis con cuatro subcategorías, en el que se determina los pasos a seguir y las herramientas a utilizar; y la Tecnología defensiva con cuatro subcategorías, ya que es importante determinar los métodos seguros a emplear luego de descubrir las vulnerabilidades digitales, se puede ver de manera conjunta las categorías que se presentan en la Tabla 1.

Tabla 1

Categorías y subcategorías de la investigación

Categorías	Subcategorías
Gestión	Descubrimiento
	Informes
	Priorización
	Respuesta
Metodología para el análisis	Acuerdo de confidencialidad
	Recolección de información
	Análisis interior
	Análisis exterior
Tecnología defensiva	Seguridad en red
	Administración en la defensa
	Conciencia de usuarios
	Contraseñas robustas

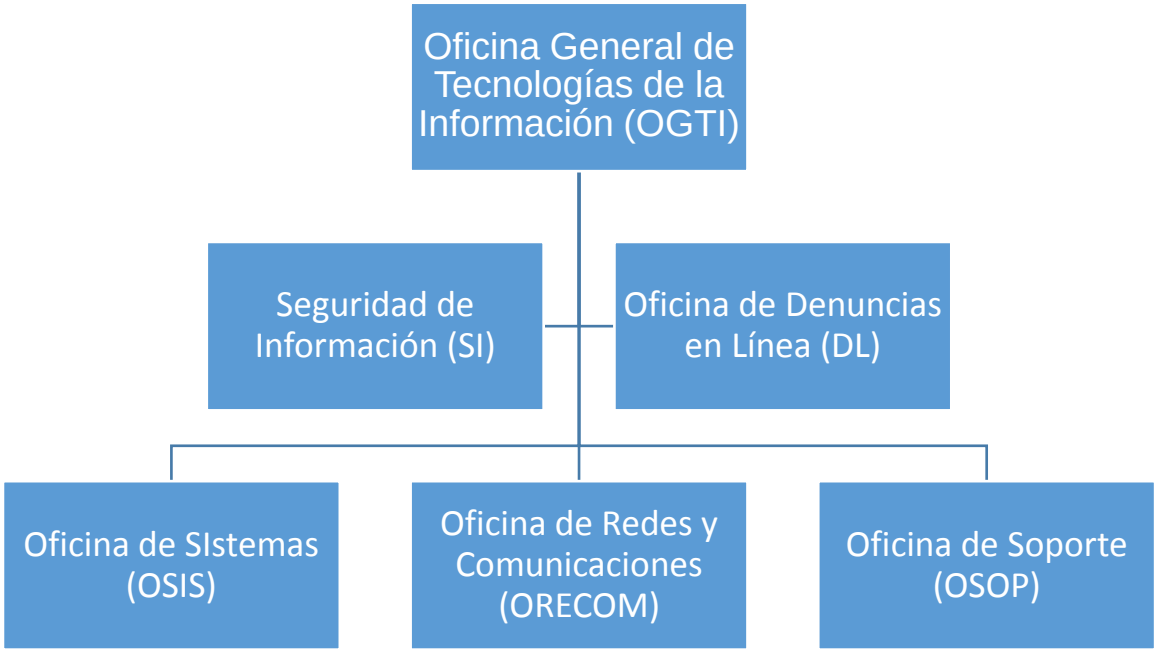
3.3. Escenario de estudio

Como escenario de estudio, se tiene a la Oficina General de Tecnologías de la Información (OGTI) de la sede central, principalmente la unidad de Seguridad de Información, como se puede apreciar en la Figura 3, la sub división de Seguridad de Información (SI), es una unidad orgánica que no está incluida en el MOF de la OGTI, pero debido a la necesidad se ha creado y asignado funciones y tareas de este ámbito; ubicado en el décimo piso, en la sede central de la entidad pública en cuestión, en la ciudad de Lima, esta unidad es liderado por el Oficial de Seguridad de la Información, las otras oficinas son: Oficina de Sistemas (OSIS), Oficina de Redes y Comunicaciones (ORECOM) y la Oficina de Soporte (OSOP), cuyo organigrama es tal como se presenta en la Figura 3, de los cuales existe personal que realiza trabajo remoto debido a la pandemia por la que se atraviesa actualmente, la oficina central también se encarga de la Oficina de Denuncias en

Línea y de la central telefónica, es importante mencionar que en la oficina laboran alrededor de 150 trabajadores de las cuales 3 son responsables directos de los temas de seguridad.

Figura 3

Organigrama de la OGTI



Fuente: Manual de Organización y funciones de la OGTI

3.4. Participantes

Los profesionales participantes en este estudio son los encargados de dirigir la unidad de Seguridad de la Información, a cargo del Oficial de Seguridad como líder, y los Analistas de Seguridad, este personal es responsable de gestionar la seguridad en todos sus niveles, también está incluido el personal de gerencia, que forman parte de la Gerencia u Oficina General de Tecnologías de la Información del Ministerio Público, los que se encuentran en la sede central. Estas personas fueron elegidos según el nivel jerárquico y naturalmente el dominio del tema, debido a que cargan con la responsabilidad de velar por la seguridad tecnológica en general y de implementar las tecnologías defensivas junto a las políticas de seguridad, también por el hecho, que son parte de la realidad problemática de esta

investigación y quienes manejan el tema de vulnerabilidades digitales, los mencionados participantes.

3.5. Técnicas e instrumentos de recolección de datos

Dentro del mar de técnicas disponibles, fueron empleadas en esta investigación, para poder recolectar los datos; primeramente se usó la entrevista semi-estructurada, que tiene como instrumento la guía de entrevista, que no es tan estricta y formal; mediante el cual permite al investigador y/o entrevistador aumentar preguntas con la finalidad de aclarar más el tema y ampliar la información, como menciona Ñaupas et al. (2018), las preguntas no necesariamente están definidas para seguirse tal cual, se puede ir introduciendo según la necesidad del investigador en profundizar el tema; es por esta característica que resulta la técnica e intrumento más adecuado para recabar información.

En la recolección de datos, es importante que el investigador no induzca las respuestas ni el comportamiento de los sujetos o participantes, por ello otra técnica que se usó es la observación, que según Hernández y Mendoza (2018), la observación es un registro sistemático y válido de información, asimismo el investigador debe estar preparado para observar, lo cual involucra la exploración y la descripción de ambientes y a los participantes en cuestión, entender y analizar los procesos que siguen cotidianamente, todo esto es más que simple ver los acontecimientos del escenario de estudio; como instrumento de la mencionada técnica se tiene la guía de observación, la cual fue aplicada en la entidad dónde se llevó a cabo la investigación a la cual pertenece el investigador.

Como última técnica se utilizó el análisis documental o recopilación documental que de acuerdo con Ñaupas et al. (2018), la técnica mencionada sirve para recabar información relevante y altamente veraz de medios documentales; por otra parte Escudero y Cortez (2018), menciona que un análisis documental es catalogar, indagar y seleccionar las fuentes informativas o documentos para luego extraer la información pertinente para la investigación, estas fuentes suelen ser de carácter institucional, personal o documental; como instrumento de esta técnica se tiene la ficha de análisis documental.

3.6. Procedimientos

Una investigación es considerada de calidad, cuando se cumplen con ciertos requisitos técnicos y sobre todo éticos, estos proporcionan credibilidad y significado a los resultados y al proceso en sí de la investigación (Escudero y Cortez, 2018); como prueba de ello en esta investigación se utilizó las entrevistas, observaciones y análisis documental a la unidad de estudio, posterior a esto se pasó a triangular los datos para la validación y contrastación de la información obtenida sobre el análisis de las vulnerabilidades digitales con los instrumentos y técnicas de recojo de datos, elegidas en la investigación en mención; asimismo la investigación tiene credibilidad, ya que se aseguró la obtención de muchos datos, revisando documentos, observando y entrevistando; de igual forma cumple con la transferibilidad, debido a que el modelo y todo lo plasmado en este trabajo es transferible y aplicable a otros contextos; la constancia interna es garantizada mediante la triangulación y en cuanto a la fiabilidad se cumple porque el investigador fue imparcial en el análisis, sin involucrar ideologías personales, realizando interpretaciones sensatas con juicio profesional.

3.7. Rigor científico

En la presente investigación, se han respetado los componentes del rigor científico, los cuales pueden ser corroborados con el uso de las técnicas e instrumentos seleccionados para obtener los datos y su posterior interpretación, para empezar se obtuvo las mejores referencias, evidencias y antecedentes disponibles de los cuatro últimos años, casi en su mayoría de revistas indexadas como scopus, ello brinda credibilidad y validez a la investigación en cuestión, además que, la información se obtuvo de expertos en el tema que con su experiencia acumulada junto a la del investigador, el modelo a proponer será aplicable a los diferentes entornos públicos, de esta manera se evita caer en la subjetividad; a esto se suma los valores del investigador y su transparencia durante el estudio de esta investigación, con todo ello se valida el rigor científico.

3.8. Método de análisis de la información

En cuanto al análisis de información se hizo uso del método inductivo, que según Escudero y Cortez (2018), para responder y dar solución a los problemas planteados, este método permite que el investigador interactue con los participantes de la unidad de estudio, es decir, la Oficina Central de Tecnología , y así generar los datos necesarios a partir de las entrevistas a profundidad con ayuda de la guía de entrevista, las observaciones siguieron los lineamientos de la guía de observación y complementariamente, durante toda la investigación se acudió constantemente al análisis documental con su respectiva ficha para el análisis documental, todo esto junto a la triangulación de los datos recabados otorgan validez científica a la investigación.

3.9. Aspectos éticos

El trabajo de investigación en cuestión, es de autoría propia, que es respaldada mediante una declaración jurada, tal como lo establece la universidad, así mismo se ha respetado la propiedad intelectual, por ello las citas y referencias se aplicaron según lo indicado en las normas APA en su séptima versión, también se ha mantenido, respetado y protegido la identidad de los profesionales a los que se les entrevistaron y a la unidad de estudio. Adicionalmente, se ha hecho uso del Turnitin, el cual es una herramienta para probar la originalidad de la investigación; siguiendo las normativas de la universidad, se ha tenido en cuenta la resolución del vicerrectorado de investigaciones N° 011-2020-UCV y el respectivo código de ética de la universidad, particularmente de la escuela de posgrado.

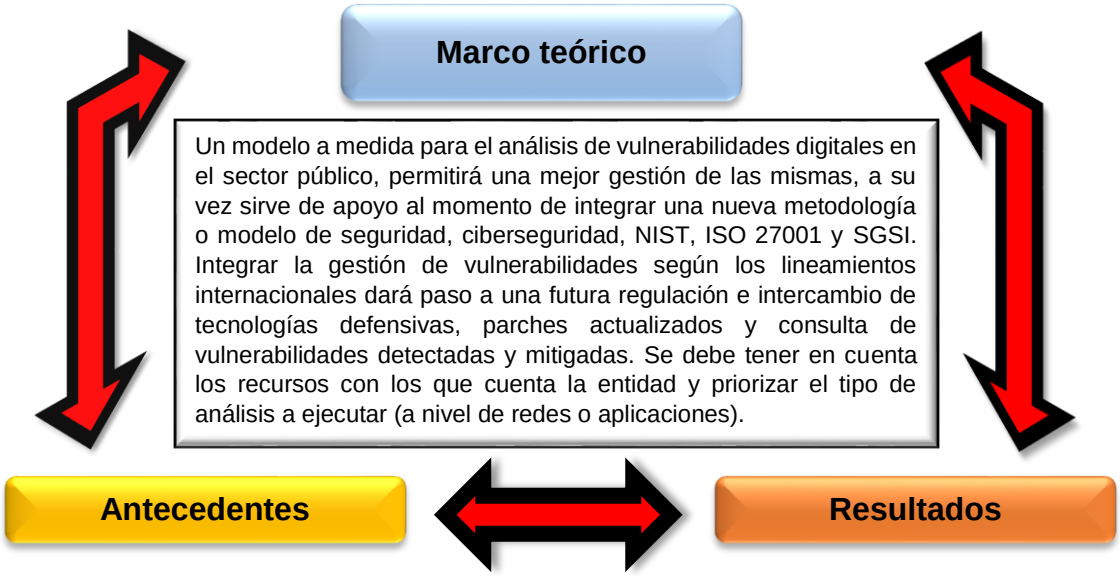
IV. RESULTADOS Y DISCUSIÓN

En cuanto a la obtención de los resultados, se hizo la triangulación del marco teórico, los antecedentes y los resultados, este último obtenido a partir de las técnicas de recolección de datos, como se puede observar en la Figura 5.

Figura 4

Triangulación de marco teórico, antecedentes y resultados.

De acuerdo con Romero et al. (2018) y Mugavero et al. (2018), se determina que el modelo para el análisis de vulnerabilidades debe tener en cuenta la gestión de las vulnerabilidades, que se desglosa en: descubrimiento, informes, priorización y respuestas; la metodología para el análisis, se desglosa en: acuerdo de confidencialidad, recolección de información, análisis interior y exterior; y las tecnologías defensivas, que se divide en: seguridad en red, administración en la defensa y concienciación de usuarios.



El sector público cuenta con programas y equipos tecnológicos obsoletos, con presencia de vulnerabilidades (Ormachea, 2019), por otro lado Bustamante et al. (2021) hace énfasis en un modelo de políticas de seguridad. Chen et al. (2019) y Kenner (2020), mencionan que es necesario conocer las vulnerabilidades e idear los parches respectivos, por el personal de seguridad. Invertir presupuesto en la gestión proactiva de vulnerabilidades, hace que los atacantes inviertan más recursos en identificar el eslabón más débil y por ende se reduce la probabilidad de los ataques (Mugavero et al., 2018). Nakajima et al. (2019) refiere que los gobiernos están investigando la regulación de las vulnerabilidades, su gestión y su ciclo de vida.

Es necesario un modelo a medida para el análisis de vulnerabilidades digitales dentro de las entidades públicas, la cual debe tener en cuenta la planificación de la actividad de análisis, la gestión de eventos, gestión de incidentes y gestión de riesgos, dentro de la gestión de vulnerabilidades, priorizar los sistemas, usar Owasp Zap, hacer pruebas de penetración priorizadas y para la defensa, aplicar medidas de seguridad en cada capa del modelo OSI. Este análisis se debe hacer trimestralmente y cada vez que haya un cambio significativo, también mejorar la documentación e informes para manejar un registro histórico de vulnerabilidades mitigadas.

De la triangulación anterior, los antecedentes muestran a manera de evidencia la importancia de un análisis de vulnerabilidad, cuyo hecho es contrastado por los entrevistados, como muy importante, cabe mencionar que se carece de antecedentes nacionales, ya que no se hicieron investigaciones al respecto, los trabajos previos internacionales dan una perspectiva más innovadora, pero la realidad del sector público en Perú es muy diferente, pero para tener un modelo que cumpla con las expectativas, se incluyó la gestión de vulnerabilidades con los lineamientos manejados en EE.UU; con el marco teórico se respalda y se valida los componentes que tendrá este modelo para el análisis de vulnerabilidades.

De acuerdo a la pregunta general, que tiene relación con el objetivo general: ¿Cómo se desarrolla un modelo para el análisis de vulnerabilidades digitales en una entidad pública de Lima, 2021?, el modelo se desarrolla primeramente teniendo en cuenta la realidad de la entidad pública, identificando los recursos con los que dispone; el modelo para el análisis de vulnerabilidades, debe componerse de tres pilares fundamentales: Gestión de vulnerabilidades; Metodología de análisis y tecnología defensiva; estos componentes se acomodan a cualquier entidad y lo más importante es que sirven de soporte para la implementación de la ISO 27001, ciberseguridad y el Sistema de Gestión de Seguridad de la Información, también ayuda a lograr un buen nivel de madurez en la gestión de vulnerabilidades.

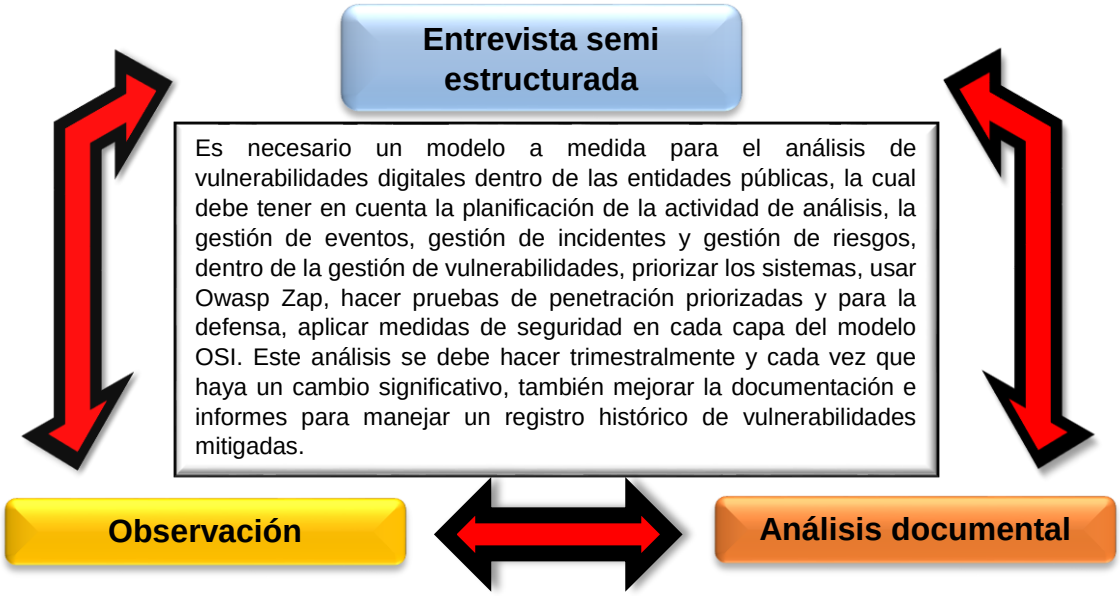
Un análisis de vulnerabilidades, debe realizarse periódicamente, así como, evaluar las vulnerabilidades, para implementar oportunamente controles, actualizaciones, parches y medidas de seguridad; todo esto es un desafío para una organización, en ese sentido, se concuerda con Kapellmann & Washburn (2019), además, se coincide en que se debe encontrar un equilibrio entre la protección y la divulgación de información confidencial, es decir, la divulgación de vulnerabilidades, por eso es necesario políticas de divulgación gubernamentales, para ello se puede seguir los lineamientos propuestos en las investigaciones de Nakajima et al. (2019) y Lee et al. (2020). Por otra parte, se concuerda con Ormachea (2019), en que los equipos antiguos son un foco de vulnerabilidades y un potencial riesgo para una entidad, pero también se debe considerar que hay entidades como el MPFN, que tienen proyectos de data center de última tecnología y por eso el modelo debe también adecuarse a ambos escenarios.

En la investigación, se utilizaron técnicas para recolectar los datos, tales como, la observación participante, la entrevista semi estructurada y su respectivo análisis documental, los cuales fueron aplicadas cada uno con su correspondiente instrumento, orientados al logro y validación de los objetivos. A continuación se hará la triangulación de estás tres técnicas para obtener los resultados.

Figura 5

Triangulación de las técnicas de recolección de datos.

Es muy importante contar con un modelo a medida para el análisis de vulnerabilidades, debido a la información confidencial que se maneja, el cual permitirá identificar las fallas de la tecnología en sí, la gestión de vulnerabilidades debe estar enlazada con la gestión de eventos e incidentes, asimismo se debe incluir una evaluación de riesgos sencilla, se debe priorizar los sistemas y hacer una planificación de toda la actividad. La metodología debe incluir pruebas de penetración según la prioridad de los sistemas y es factible usar Owasp Zap como herramienta por ser código libre. Para la defensa se debe aplicar medidas en cada capa del modelo OSI y aprovechar los esfuerzos del hacker.



Solo se hace un análisis de vulnerabilidades, cuando un sistema importante que maneja información fiscal sale a producción con acceso remoto, nivel de riesgo alto, o si el área usuaria exige el servicio, debido a que no se cuenta con los recursos e involucra tiempo, dicho análisis no es un proceso estandarizado, es a criterio del profesional de seguridad, que lo realiza gracias a su experiencia, conocimiento y para salvaguardar la seguridad de la información. Es preciso resaltar que luego del análisis se hace una prueba de penetración, el cual permite explotar las vulnerabilidades y mitigar las amenazas, esta prueba de penetración debe ser incluida en la metodología del modelo.

A la fecha, la gestión de vulnerabilidades es bastante inmaduro, se debe mejorar la documentación e incluir técnicas de puntuación.

Al existir muchos sistemas desarrollados y por desarrollar sea hace más necesario actividades preventivas como el análisis de vulnerabilidades, es por eso que en MPFN se programa la contratación de externos para desarrollar esta actividad, de ahí lo más importante son los informes de vulnerabilidades mitigadas, esto sirve para futuros análisis. Mantener actualizado los equipos tecnológicos y la adquisición de software con licencia, reduce las vulnerabilidades.

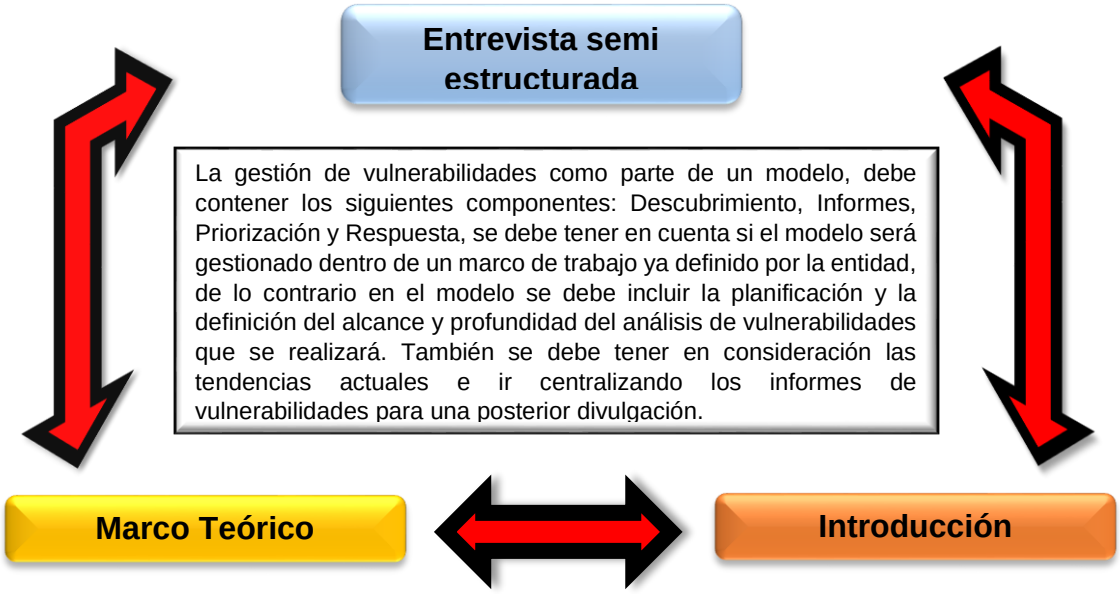
De la triangulación anterior, se puede concluir que, para reducir las amenazas, los ataques, evitar el robo de información y la caída de los servicios se debe implementar actividades preventivas; el modelo debe incluir en parte la gestión y lo técnico; como resultado se tiene la gestión de vulnerabilidades que debe estar enlazado con la gestión de eventos, incidentes y riesgos, asimismo la metodología debe iniciar con un análisis de activos, luego priorizar las aplicaciones o la tecnología a analizar, seleccionar la herramienta adecuada, elaborar el acuerdo de confidencialidad, así hasta que finalmente según la criticidad del servicio, hacer pruebas de penetración para mayor seguridad, se puede seguir los lineamientos de Owasp o NIST; la defensa se debe enfocar en aplicar medidas de seguridad en cada capa del modelo OSI (capa física, enlace de datos, red, transporte, sesión, presentación y aplicación) mediante el Security Hardening Checklist; aprovechar el esfuerzo del hacker para determinar el vector de ataque y protegerlo, lo básico radica en usar https y firewall.

En base a la información que se obtuvo de las técnicas para recolectar los datos, se verificó que un modelo a medida resulta más práctico que una metodología de ciberseguridad u otros marcos de trabajo en seguridad; generalmente se usan varios, obteniendo lo mejor de cada uno y lo que se adapta a la realidad, por ello se concuerda con Li, Wang, et al. (2022), quienes diseñaron su propio método para la evaluación de vulnerabilidades, ya que por necesidad y debido a que otras existentes no cubrían ciertos aspectos, para dicho método usaron la criticidad de Markov para que puedan identificar enlaces críticos. Se debe agregar que Niño (2018), al proponer su modelo para la seguridad de la información, hace hincapié en un análisis de riesgos, el cual permite identificar las amenazas, no se está totalmente de acuerdo con dicha proposición, ya que el escaneo de vulnerabilidades permite identificar las fallas del sistema, ahora bien, para explotar esas vulnerabilidades es necesario hacer un análisis de riesgo pequeño, para determinar el impacto y proceder a realizar la prueba de penetración, por otra parte se está de acuerdo en que no todas las entidades tienen medidas de seguridad implementadas, es más ni las consideran implementar, esa es la realidad, ya que en el sector público se da prioridad a otros aspectos.

Figura 6

Triangulación de entrevistas, marco teórico e introducción.

Los profesionales de la seguridad afirman que la gestión de vulnerabilidades debe estar amarrada con la gestión de eventos, la gestión de incidentes y la gestión de riesgos, también debe incluir lo que es la planificación, se debe determinar el alcance y la profundidad del análisis de vulnerabilidades a realizar, entre líneas confirman los componentes determinadas en el marco teórico, también se puede tener de referencia el modelo NIST (Identificar, proteger, detectar, responder y recuperar) y finalmente determinar el periodo de ejecución, en los que todos concuerdan que debe ser trimestralmente o cuando haya un cambio significativo.



Se determina la gestión de vulnerabilidades como una práctica cíclica que incluye el descubrimiento, en este punto se debe descartar los falsos positivos; la realización de informes siguiendo las buenas prácticas de OWASP; la priorización, usando niveles: critico, importante, moderado y bajo; y la respuesta según lo priorizado (Mugavero et al., 2018), a todo ello se le debe sumar el desarrollo de políticas de seguridad y capacitación al personal, se debe hacer lo posible por tener documentación con instrucciones claras, esto es complicado por la naturaleza misma de los ataques.

Muchos gobiernos desarrollan sus propias directrices con respecto a la gestión de vulnerabilidades, para que las entidades públicas identifiquen y subsanen los riesgos innecesarios, asimismo, están trabajando en la implementación de políticas gubernamentales para el manejo y la divulgación pública de las vulnerabilidades, esto es beneficioso para la elaboración de informes y la forma de abordar esos incidentes, también se trabaja en la automatización de la gestión de vulnerabilidades, en la actualidad EE.UU cuenta con una base de datos de vulnerabilidades denominada NVD.

De la triangulación anterior (Figura 6), se puede concluir que en relación al problema específico: ¿Cómo es la gestión de un Modelo para el Análisis de Vulnerabilidades Digitales en una entidad pública de Lima, 2021?, cabe precisar que “gestión” se refiere a la gestión de vulnerabilidades; en cuyo caso, se ha determinado que la gestión de vulnerabilidades como parte de un modelo, debe contener los siguientes componentes: (a) Descubrimiento, (b) Informes, (c) Priorización y (d) Respuesta; estos deben ser considerados como una práctica cíclica, debido que al ejecutar un primer ciclo con estos cuatro componentes se va

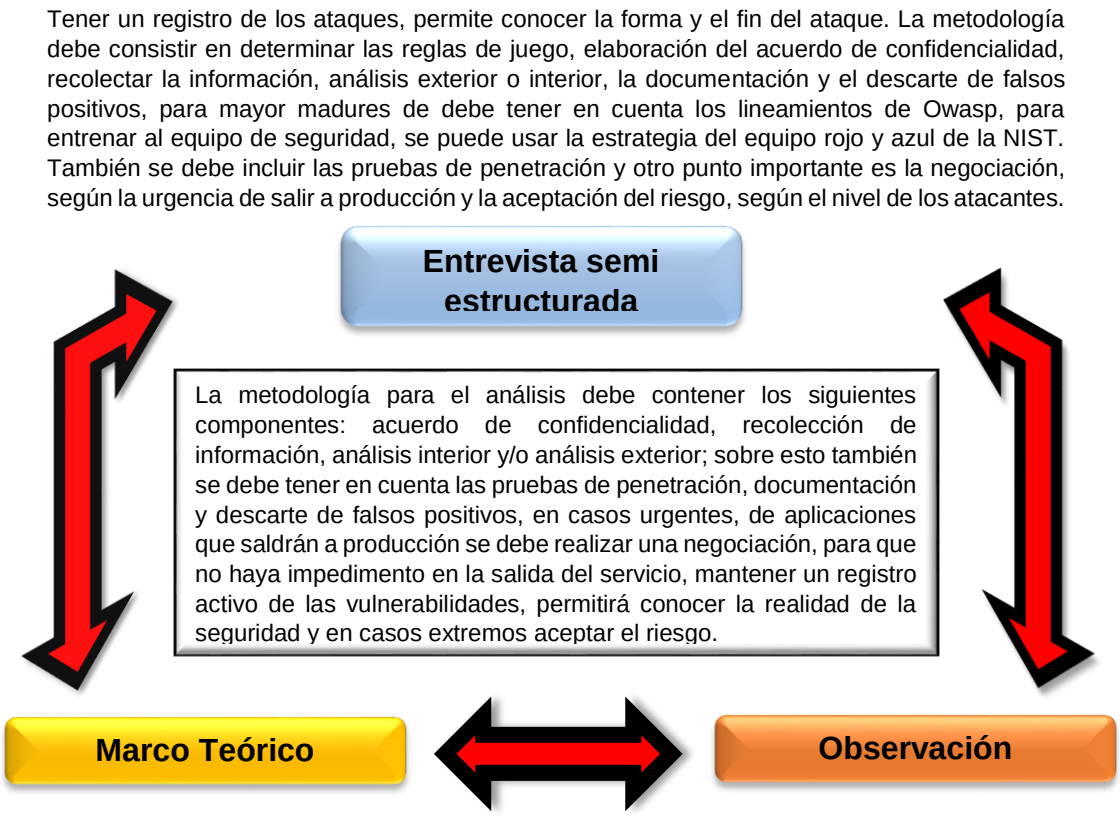
terminar dando respuesta a una vulnerabilidad, es decir, se debe implementar controles de seguridad, hacer una actualización o hacer un parche, los mismos que pueden generar otro tipo de vulnerabilidades, es por ello que se debe volver a iniciar, después de cierto tiempo, trimestralmente como ya se definió.

Producto de las entrevistas surgieron sub categorías emergentes que se deben considerar dentro de la categoría de gestión; como es la Planificación de toda la actividad y la definición del alcance y profundidad del análisis de vulnerabilidades; desde una perspectiva de proyecto, se debe planificar todos los pasos y actividades que se harán en el proceso de análisis, también se debe determinar el alcance, es decir, se debe definir qué servicios, sistemas y/o aplicaciones serán analizados, además, se debe definir el nivel de profundidad del análisis. Por otro lado cabe resaltar puntos importantes, que no necesariamente entren como sub categorías, la gestión de eventos y la gestión de incidentes, que se puede resumir en que, el evento es cuando el ataque no tiene éxito, estos se registran en gran cantidad a diario, el incidente es cuando el ataque tiene éxito y trae consecuencias como, caídas del sistema, saturación de servicios y robo de información, siendo este último el de mayor riesgo. Lo que debe considerarse como otra sub categoría emergente es la evaluación del riesgo, que debe ser con respecto al sistema seleccionado para el respectivo análisis de vulnerabilidades.

En la categoría de gestión de vulnerabilidades, se concuerda con Mugavero et al. (2018), pero no del todo, ya que la gestión de vulnerabilidades que figura en su investigación complementa a modelos y buenas practicas más estandarizadas; la realidad de las entidades públicas es muy diferente en el país, es por eso que se debe considerar las sub categorías emergentes para tener un modelo a medida, acorde con la realidad, además, la seguridad de la información no ha alcanzado la madurez y ni hablar en las entidades públicas más pequeñas, como son los gobiernos locales. También, en concordancia con Lee et al. (2020) y Nakajima et al. (2019), se debe estandarizar la detección de vulnerabilidades y empezar a tener en cuenta, por lo menos, un sistema reglamentado de divulgación de vulnerabilidades, con sus respectivas políticas de regulación.

Figura 7

Triangulación de entrevistas, marco teórico y observación.



Como resultado de la triangulación anterior (Figura 7), en relación al problema específico: ¿Cómo es la metodología en el Modelo para el Análisis de Vulnerabilidades Digitales en una entidad pública de Lima, 2021?, se determinó que la metodología para el análisis debe tener en cuenta los siguientes aspectos: (a) Acuerdo de confidencialidad, (b) recolección de información, (c) Análisis interior y/o (d) Análisis exterior; cabe resaltar que toda esta actividad debe realizarse en estricta confidencialidad y sin comprometer el uso normal de los servicios y la red,

es necesario que se establezcan reglas claras para llevar a cabo el análisis de vulnerabilidades con éxito.

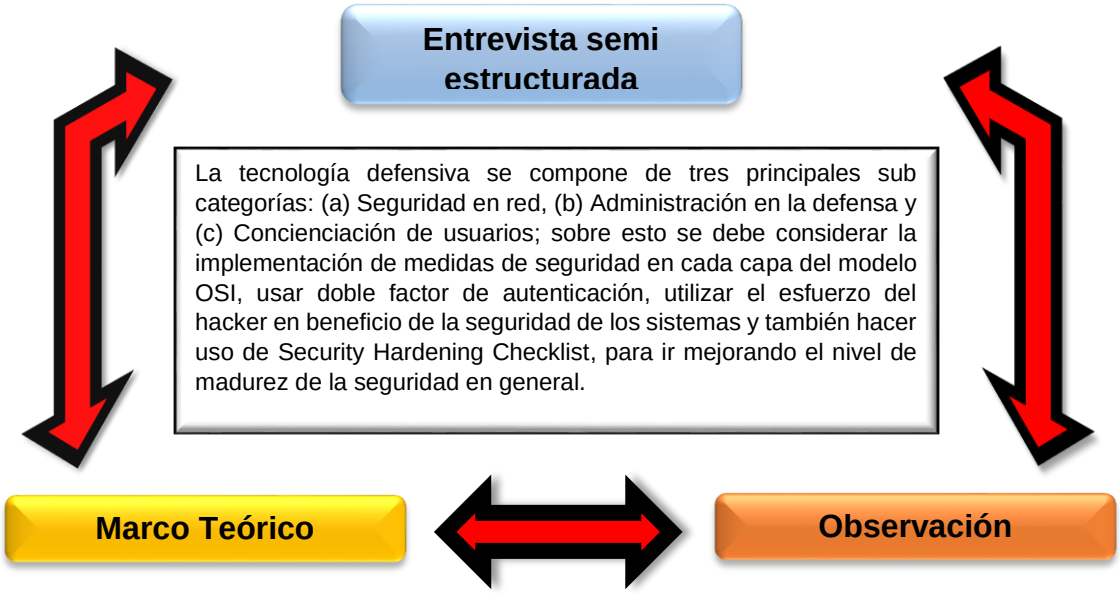
Las entrevistas sacan a relucir sub categorías emergentes, que se acomodan por su naturaleza a continuación de las ya definidas, tal es el caso de, la documentación de las vulnerabilidades encontradas en su respectivo registro para el historial; el descarte de falsos positivos, ya que es común que después del análisis, salgan muchas vulnerabilidades que realmente no lo son; las pruebas de penetración, después de haber hecho el descarte de falsos positivos, haciendo uso de la técnica de caja gris, porque es más rápido y se aprovecha el ser personal de la entidad; adicional a todo ello, se debe considerar el aspecto de negociación, aspecto que no suelen considerar otras metodologías, que consiste en, previa a la salida a producción de un servicio, aplicación y/o sistema informático, según la necesidad y la urgencia de dicha salida, por el tiempo no se puede realizar un análisis completo, entonces se debe hacer una especie de negociación con el equipo de desarrollo y el área usuaria, en el que se condicione requisitos mínimos de seguridad antes de su salida, con el compromiso de hacer un posterior análisis completo; finalmente tener en cuenta la aceptación del riesgo, gracias a las vulnerabilidades identificadas y saneadas, se puede determinar qué tan seguro son los sistemas y la arquitectura tecnológica en general, y frente a un ataque de alto nivel, ataques con hackers internacionales, se puede tomar medidas de protección aceptando el riesgo, es decir, mantener solo la red interna, sin salida al exterior o apagar los servidores temporalmente hasta que la amenaza desaparezca.

Teniendo en cuenta que, seleccionar la herramienta adecuada es fundamental en el proceso de análisis de vulnerabilidades, se está de acuerdo en parte con Morales et al. (2020), quienes refieren que las herramientas a emplear deberían ser Acunetix, Nessus y Shodan, dichos softwares son muy buenos, pero son de pago y lamentablemente en el sector público optan por otras cosas y será difícil obtener licencias para estos programas y/o servicios, entonces se puede hacer uso de Owasp Zap que es de código abierto y Shodan en su servicio gratuito y de escaneo pasivo como primera instancia, además sería bueno estar alineado con Owasp y aprovechar su top ten 2021 (las 10 vulnerabilidades principales de Owasp), tal como menciona Lala er al. (2021).

Figura 8

Triangulación de marco teórico, observación y entrevistas.

Como parte de la defensa se debe implementar medidas de seguridad en cada capa del modelo OSI, los controles de acceso con doble factor de autenticación, se puede alinear con los controles de la norma ISO 27001, concientizar a los usuarios juega un rol fundamental, ya que estos son la mayor vulnerabilidad de todo sistema. El uso de https y firewall debe ser lo mínimo en la defensa, se debe registrar los ataques, para determinar el vector y las técnicas de ataque, esto se puede simular para identificar las fallas críticas y remediarlas, es decir, utilizar el esfuerzo del hacker, realizar un análisis forense de ser posible.



Las estrategias defensivas o tecnologías defensivas, deben cubrir las siguientes capas, sistema operativo, aplicaciones, segmento de red y red perimetral; es importante resaltar que no se debe concentrar toda la defensa en la red perimetral, ya que, si el atacante pasa esa capa, ya no habrá protección, también se debe configurar muy bien el firewall, porque es la primera línea de defensa; de acuerdo con Romero et al. (2018), las tecnologías defensivas se dividen en: (a) Seguridad en red, (b) Administración en la defensa y (c) Concienciación de usuarios, estos componentes incluyen las diferentes técnicas de defensa.

Lo principal que se rescata es el uso de Security Hardening Checklist, ya que contiene todas las configuraciones seguras de las tecnologías utilizadas, es decir, cuando se detecte una vulnerabilidad por una mala configuración, se pasa la configuración segura, para que el equipo técnico modifique su configuración, el mantenimiento de los equipos es importante, ya que con esta actividad se aplica los parches de seguridad correspondientes, usar antivirus en cada equipo, la configuración segura del firewall es importante, porque es la primera barrera de defensa a la que se enfrenta el hacker.

Después de la triangulación anterior (Figura 8), en relación al problema específico: ¿Cómo es la tecnología defensiva en el Modelo para el Análisis de Vulnerabilidades Digitales en una entidad pública de Lima, 2021?, se determinó que la tecnología defensiva consta de tres grandes elementos: (a) Seguridad en red, (b) Administración en la defensa y (c) Concienciación de usuarios, estas sub categorías agrupan las diferentes técnicas, estrategias y tecnologías existentes para la defensa, cabe mencionar que este apartado dependerá mucho de los recursos con los que se cuenta y el conocimiento del personal asignado a estas actividades.

Habría que decir también, como resultado de las entrevistas y la observación realizada, salen a flote sub categorías emergentes, normalmente se podría incluir dentro de uno de los tres elementos ya mencionados, pero se incluye debido a su importancia y más que nada a su innovación, que son los siguientes; implementación de medidas de seguridad en cada capa del “modelo OSI” que consta de capa física, enlace de datos, red, transporte, sesión, presentación y aplicación; “controles” en donde se puede alinear con la norma ISO 27001, en controles de acceso se debe usar el doble factor de autenticación; tener un “plan de remediación” después de haber realizado el análisis de vulnerabilidades, es necesario; “usar el esfuerzo del hacker”, esto incluye determinar el vector de ataque y las técnicas utilizadas en esta actividad intrusiva, asimismo, conocer al atacante y realizar un análisis forense de ser posible; determinar las políticas de seguridad y concientizar a los usuarios; por último, hacer uso de Security Hardening Checklist o lista de verificación de refuerzo de la seguridad, traducido del inglés, el cual proporciona actualizaciones y configuraciones de seguridad, justamente para reforzar la seguridad, también se encuentra la forma de habilitar el firewall de manera segura.

Generalmente el control de acceso es el más recurrido para los ataques, en esa línea se coincide con Muyón y Montaluisa (2020) y Reis et al. (2021), en que el acceso no autorizado se da como consecuencia de una mala programación en la accesibilidad al sistema de información, estas vulnerabilidades crecen y se convierten en un riesgo cuando el sistema es web, es decir cuando es accesible a través de internet, estos investigadores también mencionan como parte del control de acceso, el doble factor de autenticación por defecto, en la realidad de la investigación generalmente al implementar estas medidas de seguridad innovadoras, se siente un rechazo por parte de los usuarios debido a un tema de cultura y rechazo a la nueva tecnología, por eso también es fundamental y juega un rol significativo la concienciación de los usuarios en el uso responsable de la tecnología.

V. CONCLUSIONES

Primera:

Se concluye que, de acuerdo al objetivo general y según los resultados obtenidos, un modelo para el análisis de vulnerabilidades digitales en una entidad pública, debe tener estos tres pilares que son: la gestión de vulnerabilidades, la metodología para el análisis y la tecnología defensiva; el modelo debe incluir lineamientos internacionales, con la finalidad de estandarizar el proceso de análisis en todas las entidades del sector público, para luego implementar políticas gubernamentales de manejo y divulgación de vulnerabilidades.

Segunda:

Se concluye que, de acuerdo al primer objetivo específico y según los resultados obtenidos; la gestión de vulnerabilidades debe seguir estos cuatro componentes importantes: descubrimiento, informes, priorización y respuesta, que es transversal a todo el proceso de análisis y debe ser cíclico ya que las vulnerabilidades surgen en cada integración o cambio en la tecnología, por eso se determinó también, que se debe planificar y ejecutar trimestralmente o en cada cambio significativo, cabe mencionar que esta gestión se involucra directamente con la gestión de eventos e incidentes, por ello se debe considerar un trabajo en conjunto.

Tercera:

Se concluye que, de acuerdo al segundo objetivo específico y según los resultados obtenidos, la metodología debe componerse de: acuerdo de confidencialidad, recolección de información, análisis interior y/o análisis exterior, por su importancia a esto se suma, el análisis de riesgo, en el que se evalúa de forma sencilla y práctica, el impacto del análisis de vulnerabilidades sobre el sistema, aplicación, red o arquitectura; en definitiva, este proceso tiene que ser llevado a cabo de manera confidencial y sin afectar o comprometer el uso normal de los servicios y la red en general.

Cuarta:

Se concluye que, de acuerdo al tercer objetivo específico y según los resultados obtenidos, la tecnología defensiva incluye la seguridad en la red, administración en la defensa y concienciación de usuarios, además, tiene que ser ligeramente flexible, ya que depende mucho de los recursos disponibles y el conocimiento del personal de seguridad, también, se debe implementar medidas de seguridad en cada capa del modelo OSI; se tiene que hacer uso del Security Hardening Checklist y aprovechar el esfuerzo del hacker, para determinar el vector de ataque y las técnicas utilizadas.

VI. RECOMENDACIONES

Primera:

Se recomienda al Oficial de Seguridad y a todo personal que implementará este modelo en una entidad pública, planificar bien el proceso de análisis de vulnerabilidades, priorizar el sistema o aplicación al que se hará el análisis y tener en cuenta las otras metodologías de seguridad que se estén empleando, gracias a que el modelo es adaptable, resultará fácil ubicarlo e integrarlo con cualquier otro.

Segunda:

La recomendación al personal de seguridad es que, lleve a cabo la implementación de este modelo debe contar con los conocimientos necesarios sobre seguridad, es oportuno mencionar que, se puede omitir algunos pasos del modelo, en caso de ejecutar este análisis por vez primera, se puede realizar un análisis pasivo, sin llegar al paso intrusivo, para ir identificando las vulnerabilidades de la entidad y el nivel de riesgo que trae consigo si se explotan esas vulnerabilidades en un ataque.

Tercera:

La recomendación al profesional de seguridad es que, según sus recursos y necesidades, debe seleccionar la herramienta que mejor se acomode a sus requerimientos e incluso pueden utilizar más de uno, se tiene que hacer por lo menos una vez al año según lo priorizado, una prueba de penetración que es más intrusivo, para explotar y corregir las vulnerabilidades, para mejorar las habilidades del equipo de seguridad, se puede seguir la estrategia del equipo rojo y azul de la NIST, dónde uno ataca y el otro defiende.

Cuarta:

La recomendación al experto en seguridad es que, debe ir creando un historial de vulnerabilidades descubiertas y mitigadas, asimismo, incluir los ataques, para descubrir patrones que servirán en identificar a los atacantes e implementar lo más antes posibles medidas de protección; de ser posible, se debe ir sistematizando dichos registros, teniendo en cuenta que un futuro se tendrá políticas de divulgación de vulnerabilidades, con la finalidad de hacer la tecnología más segura.

REFERENCIAS

Anwar, R., Abdullah, T., & Pastore, F. (2021). Firewall best practices for securing smart healthcare environment: A review. Applied Sciences, 11(9183). doi:10.3390/app11199183

Arcuri, A. (2021). Automated Black- And White-Box Testing of RESTful APIs with EvoMaster. IEEE Software, 38(3), 72 - 78. doi:10.1109/MS.2020.3013820

Arfaj, B., Mishra, S., & Alshehri, M. (2022). Efficacy of unconventional penetration testing practices. Intelligent Automation and Soft Computing, 31(1), 223-239. doi:10.32604/IASC.2022.019485

Banco Interamericano de Desarrollo. (2020). CIBERSEGURIDAD RIESGOS, AVANCES Y EL CAMINO A SEGUIR EN AMÉRICA LATINA Y EL CARIBE. Obtenido de https://bit.ly/2ZAHuqp

BBC News. (9 de Marzo de 2021). El "inusualmente agresivo" ciberataque del que Microsoft acusa a China (y por qué no es simplemente una nueva crisis de ciberseguridad). Obtenido de https://bbc.in/3cgDGOl

Bustamante, S., Valles, M., Cuellar, I., & Lévano, D. (2021). Políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú. Redalyc, 12(2), 69-79. doi:https://doi.org/10.29019/enfoqueute.743

Check Point. (4 de Agosto de 2021). CYBER ATTACK TRENDS Mid Year Report 2021. Obtenido de https://bit.ly/3nnHi7y

Chen, H., Liu, J., Liu, R., Noseong, P., & Subrahmanian, V. (2019). VEST: A System for Vulnerability Exploit Scoring & Timing. International Joint Conferences on Artificial Intelligence Organization (IJCAI), 6503-6505. doi:https://doi.org/10.24963/ijcai.2019/937

CISCO. (21 de Febrero de 2020). Cisco News The Americas Network. Obtenido de https://bit.ly/30xVa5V

CNN Español. (12 de Agosto de 2021). Los ciberataques a objetivos gubernamentales y empresariales en EE.UU. Obtenido de https://cnn.it/3cjXhxa

Daffalla, A., Simko, L., Kohno, T., & Bardas, A. (2021). Defensive Technology Use by Political Activists During the Sudanese Revolution. IEEE Symposium on Security and Privacy, 372-390. doi:10.1109/SP40001.2021.00055

Diamantopoulou, V., Tsohou, A., & Karyda, N. (2020). From ISO/IEC 27002:2013 information security controls to personal data protection controls: Guidelines for GDPR compliance. Lecture Notes in Computer Science, 238-257. doi:10.1007/978-3-030-42048-2_16

Dissanayaka, A., Mengel, S., Gittner, L., & Khan, H. (2020). Vulnerability Prioritization, Root Cause Analysis, and Mitigation of Secure Data Analytic Framework Implemented with MongoDB on Singularity Linux Containers. ACM International Conference Proceeding Series, 58-66. doi:10.1145/3388142.3388168

Egloff, F. (2021). Public attribution of cyber intrusions. Journal of Cybersecurity, 6(1), 1-12. doi:10.1093/CYBSEC/TYAA012

ENISA. (3 de June de 2021). New Light Shed on Capabilities in Energy & Healthcare. Obtenido de https://bit.ly/3kKjk4C

Escudero, C., & Cortez, L. (2018). Técnicas y métodos cualitativos para la investigación científica. Machala, Ecuador: UTMACH.

Europa Press. (3 de Agosto de 2021). Cybereason alerta de una campaña de ciberataques contra las 'telecos' del sudeste asiático ligada a China. Obtenido de https://bit.ly/3zQvEVI

Fredj, O., Cheikhrouhou, O., Krichen, M., Hamam, H., & Derhab, A. (2021). An OWASP top ten driven survey on web application protection methods. CRiSIS 2020: Risks and Security of Internet and Systems, 235-252. doi:https://doi.org/10.1007/978-3-030-68887-5_14

Frost & Sullivan. (7 de Julio de 2021). Frost & Sullivan The Growth Pipeline Company. Obtenido de https://bit.ly/30zCdAl

Gestión. (31 de Julio de 2018). Ciberataques al sector energético en Perú cuestan US$ 17.20 millones al año. Obtenido de https://bit.ly/2WkJL7S

Guru Prasad, U., Girija, R., Vedhapriyavadhana, S., & Jayalakshmi, S. (2022). Evaluación de herramientas y técnicas de código abierto para la seguridad de la red. Cyber Security and Digital Forensics, 289-300. doi:10.1007/978-981-16-3961-6_25

Gutierres, J., Navia, M., & Molina, G. (2020). Vulnerabilidades de sitios web gubernamentales en Ecuador: Un estudio exploratorio pre-muestral. RISTI(29), 67-78. Obtenido de http://www.risti.xyz/issues/ristie29.pdf

Hamza, Z., & Hammad, M. (2019). Web and mobile applications' testing using black and white box approaches. IET Conference Publications, 2019(CP758). Obtenido de www.scopus.com

Hernández, R., & Mendoza, C. (2018). Metodología de la Investigación: Las rutas cuantitativa, cualitativa y mixta. México: McGraw-Hill.

Herpig, S. (2018). Governmental Vulnerability Assessment Management. Berlin: Stiftung Neue Verantwortung e. V. Obtenido de https://bit.ly/3wSbV82

HM Government. (2021). ESTRATEGIA DE CIBERSEGURIDAD NACIONAL 2016-2021. Recuperado el 24 de Septiembre de 2021, de https://bit.ly/2Y0FtDL

Imperva. (2021). What is vulnerability assessment. Recuperado el 5 de Octubre de 2021, de https://bit.ly/30sq27Z

Jiang, Y., Jeusfeld, M., & Ding, J. (2021). Evaluating the Data Inconsistency of Open-Source Vulnerability Repositories. ACM International Conference Proceeding Series, 1-10. doi:https://doi.org/10.1145/3465481.3470093

Kapellmann, D., & Washburn, R. (2019). Call to Action: Mobilizing Community Discussion to Improve Information Sharing About Vulnerabilities in Industrial Control Systems and Critical Infrastructure. International Conference on Cyber Conflict, CYCON. doi:10.23919/CYCON.2019.8756895

Kaspersky. (31 de Agosto de 2021). Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021. Obtenido de https://bit.ly/3Cl4Td7

Kenner, A. (2020). Model-Based Evaluation of Vulnerabilities in Software Systems. ACM International Conference Proceeding Series, 112-119. doi:10.1145/3382026.3431246

Khlobystova, A., & Abramov, M. (2022). Time-Based Model of the Success of a Malefactor's Multistep Social Engineering Attack on a User. Lecture Notes in Networks and Systems, 216 - 223. doi:10.1007/978-3-030-87178-9_22

Laghrissi, F., Douzi, S., Douzi, K., & Hssina, B. (2021). Intrusion detection systems using long short-term memory (LSTM). Journal of Big Data, 8(65). doi:10.1186/s40537-021-00448-4

Lala, S., Kumar, A., & Subbulakshmi, T. (2021). Secure web development using OWASP guidelines. Proceedings - 5th International Conference on Intelligent Computing and Control Systems, (ICICCS) 2021, 323-332. doi:10.1109/ICICCS51141.2021.9432179

Lee, Y., Woo, S., Song, Y., Lee, J., & Lee, D. H. (2020). Practical vulnerability-information-sharing architecture for automotive security-risk analysis. IEEE Access. doi:10.1109/ACCESS.2020.3004661

Li, H.-J., Wang, L., Bu, Z., & Cao, J. (2022). Measuring the Network Vulnerability Based on Markov Criticality. ACM Transactions on Knowledge Discovery from Data, 16(2), 28:1-28:24. doi:10.1145/3464390

Li, M., Yang, Z., Wang, X., Ling, H., & Teng, Y. (2021). Research on batch detection technology of common network security vulnerabilities in IoT terminals. Paper presented at the IMCEC 2021 - IEEE 4th Advanced Information Management, Communicates, Electronic and Automation Control Conference, 1960-1962. doi:10.1109/IMCEC51613.2021.9482059

MIDIS. (3 de Setiembre de 2020). Procedimiento de Gestión de Vulnerabilidades e Incidentes de Seguridad de la Información. Obtenido de https://bit.ly/3AVoC3o

Morales, J., Avellán, N., Lectong, T., & Zambrano, M. (2020). Proceso de Ciberseguridad: Guía Metodológica para su implementación. Revista Ibérica de Sistemas e Tecnologias de Informação (RISTI)(E29), 41-50. Obtenido de https://www.scopus.com

MPFN. (2017). Plan Operativo Informático. Lima, Perú. Obtenido de https://portal.mpfn.gob.pe/descargas/transparencia/2017/148B.pdf

MPFN. (2018). Plan Operativo Informático. Lima, Perú. Obtenido de https://portal.mpfn.gob.pe/descargas/normas/r55688.pdf

Mugavero, R., Abaimov, S., Benolli, F., & Sabato, V. (2018). Cyber Security Vulnerability Management in CBRN Industrial Control Systems (ICS). International Journal of Information Systems for Crisis Response and Management (IJISCRAM), 10, 49-78. doi:10.4018/IJISCRAM.2018040103

Muyón, C., & Montaluisa, F. (2020). Métodos de seguridad de la información para proteger la comunicación y los datos de servicios web REST en peticiones HTTP utilizando JSON Web Token y Keycloak Red Hat Single Sign On. Revista Ibérica de Sistemas e Tecnologias de Informação (RISTI)(E29), 198-213. Obtenido de https://www.scopus.com/

Nakajima, A., Watanabe, T., Shioji, E., Akiyama, M., & Woo, M. (2019). Pilot Study on Consumer IoT Device Vulnerability Disclosure and Patch Release in Japan and the United States. AsiaCCS 2019 - Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security, 485-492. doi:10.1145/3321705.3329849

Nguyen-Duc, A., Do, M., Luong Hong, Q., Nguyen Khac, K., & Nguyen Quang, A. (2021). On the adoption of static analysis for software security assessment–A case study of an open-source e-government project. Computers and Security(111). doi:10.1016/j.cose.2021.102470

Niño, N. (2018). Modelo de un sistema de gestión de seguridad de información – SGSI, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el Instituto Nacional de Estadística e Informática - INEI Lambayeque. Lambayeque: (Tesis de Maestría).

NIST. (September de 2021). NATIONAL VULNERABILITY DATABASE. Obtenido de https://nvd.nist.gov/

Ñaupas, H., Valdivia, M., Palacios, J., & Romero, H. (2018). Metodología de la investigación cuantitativa - cualitativa y redacción de la tesis (5a ed.). Bogotá, Colombia: Ediciones de la U.

Ormachea, J. (2019). Estrategias integradas de ciberseguridad para el fortalecimiento de la seguridad nacional. Lima, Perú. Obtenido de https://bit.ly/3ATKVpU

Qasaimeh, M., Shamlawi, A., & Khairallah, T. (2018). Black box evaluation of web application scanners: Standards mapping approach. Journal of Theoretical and Applied Information Technology, 96(14), 4584 - 4596. Obtenido de www.scopus.com

Queensland Government. (Julio de 2018). Vulnerability management guideline. Obtenido de https://bit.ly/3nnjnoL

Ramsauer, R., Bulwahn, L., Lohmann, D., & Mauerer, W. (2020). The Sound of Silence: Mining Security Vulnerabilities from Secret Integration Channels in Open-Source Projects. CCSW 2020 - Proceedings of the 2020 ACM SIGSAC Conference on Cloud Computing Security Workshop, 147-157. doi:10.1145/3411495.3421360

Reis, S., Abreu, R., & Cruz, L. (2021). Fixing vulnerabilities potentially hinders maintainability. Empirical Software Engineering, 26(6). doi:10.1007/s10664-021-10019-z

Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., Álava, C., . . . Castillo, M. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades (Primera ed.). 3 Ciencias. doi:http://dx.doi.org/10.17993/IngyTec.2018.46

Schweikert, A., L'Her, G., & Deinert, M. (2021). Simple method for identifying interdependencies in service delivery in critical infrastructure networks. Applied Network Science, 6(44), 1-13. doi:10.1007/s41109-021-00385-4

Sreerag, M., Sethumadhavan, M., & Amritha, P. (2022). Identifying and Mitigating Vulnerabilities of Hardened Windows Operating System. Information and Communication Technology for Competitive Strategies (ICTCS 2020), 623-632. doi:https://doi.org/10.1007/978-981-16-0739-4_59

Taylor, D. (20 de May de 2021). 3 OF THE BIGGEST SECURITY CHALLENGES FACING LOCAL GOVERNMENT. Obtenido de https://bit.ly/3ih8otY

Thapa, N., Liu, Z., Shaver, A., Esterline, A., Gokaraju, B., & Roy, K. (2021). Secure cyber defense: An analysis of network intrusion-based dataset ccd-idsv1 with machine learning and deep learning models. Electronics (Switzerland), 10(1747). doi:10.3390/electronics10151747

The Economy Journal. (Septiembre de 2021). España no es más vulnerable que otros países en seguridad informática. Obtenido de https://bit.ly/3kON94e

Walkowski, M., Oko, J., & Sujecki, S. (2021). Vulnerability Management Models Using a Common Vulnerability Scoring System. Applied Sciences, 11-36. doi:https://doi.org/10.3390/app11188735

ANEXOS

Anexo 1

Matriz de Categorización

Título: Modelo para el Análisis de Vulnerabilidades Digitales en una entidad pública de Lima, 2021

Autor: Ricardo Richard Huamantingo Navarro

Problema General	Objetivo General	Categorías	Subcategorías	Técnicas	Instrumentos
¿Cómo se desarrolla un modelo para el análisis de vulnerabilidades digitales en una entidad pública de Lima, 2021?	Proponer un modelo para el análisis de vulnerabilidades digitales en una entidad pública de Lima, 2021	Gestión	▪ Descubrimiento ▪ Informes ▪ Priorización ▪ Respuesta	Entrevista Semi estructurada	Guía de Entrevista
Problemas Específicos	**Objetivos Específicos:**				
¿Cómo es la gestión de un Modelo para el Análisis de Vulnerabilidades Digitales en una entidad pública de Lima, 2021?	Determinar la gestión de un Modelo para el Análisis de Vulnerabilidades Digitales en una entidad pública de Lima, 2021	Metodología para el análisis	▪ Acuerdo de confidencialidad ▪ Recolección de información ▪ Análisis interior ▪ Análisis exterior	Observación	Guía de observación
¿Cómo es la metodología en el Modelo para el Análisis de Vulnerabilidades Digitales en una entidad pública de Lima, 2021?	Determinar la metodología en el Modelo para el Análisis de Vulnerabilidades Digitales en una entidad pública de Lima, 2021				
¿Cómo es la tecnología defensiva en el Modelo para el Análisis de Vulnerabilidades Digitales en una entidad pública de Lima, 2021?	Determinar la tecnología defensiva en el Modelo para el Análisis de Vulnerabilidades Digitales en una entidad pública de Lima, 2021	Tecnología defensiva	▪ Seguridad en red ▪ Administración en la defensa ▪ Concienciación de usuarios	Análisis documental	Ficha de análisis documental

Fuente: Romero et al. (2018) & Mugavero et al. (2018)

Anexo 2

Guía de entrevista semi-estructurada

1. ¿Qué importancia tiene el Análisis de Vulnerabilidades Digitales en una entidad pública?
2. ¿Qué se debería tener en cuenta para el diseño de un modelo para el Análisis de Vulnerabilidades Digitales en una entidad pública?
3. ¿Cómo gestionar las vulnerabilidades dentro de un modelo?
    a. ¿Cómo se debería hacer el descubrimiento dentro de un modelo de Análisis de Vulnerabilidades?
    b. ¿Cómo se deberían hacer los informes dentro de un modelo de Análisis de Vulnerabilidades?
    c. ¿Cómo se debería hacer la priorización dentro de un modelo de Análisis de Vulnerabilidades?
    d. ¿Cómo se debe implementar la respuesta dentro de un modelo de Análisis de Vulnerabilidades?
4. ¿Qué debe incluir la metodología de análisis dentro de un modelo?
5. ¿Cómo debería ser la metodología de análisis dentro de un modelo?
    a. ¿Qué importancia tiene el acuerdo de confidencialidad dentro de un modelo para el Análisis de Vulnerabilidades?
    b. ¿Qué importancia tiene la recolección de información dentro de un modelo para el Análisis de Vulnerabilidades?
    c. ¿Qué importancia tiene el análisis interior dentro de un modelo para el Análisis de Vulnerabilidades?
    d. ¿Qué importancia tiene el análisis exterior dentro de un modelo para el Análisis de Vulnerabilidades?
6. ¿Qué tecnologías defensivas es recomendable para mitigar las amenazas?
    a. ¿Cómo debería ser la seguridad en la red como parte de la tecnología defensiva?
    b. ¿Cómo debería ser la administración en la defensa como parte de la tecnología defensiva?
    c. ¿Cómo debería ser la concienciación de usuarios como parte de la tecnología defensiva?

Anexo 3

Matriz de desgravación de entrevista

N°	Preguntas	Entrevistado 1 – Oficial de Seguridad (MPFN)
1	¿Qué importancia tiene el Análisis de Vulnerabilidades Digitales en una entidad pública?	Depende del impacto, usualmente el público es cautivo por lo tanto el impacto a la imagen institucional verdaderamente no trasciende, las personas no tienen opción de ir a otras entidades, ya que estas son únicas, solo les queda protestar. Lo que sí tiene mucha importancia es el cuidado de los datos de los usuarios, entonces los ciudadanos le confieren información a entidades del estado para su cuidado por lo que debería ser muy respetuoso de que no haya filtración de esa información, por ejemplo: en ciertos tipos de instituciones, la información es más importante, que aquello que se encuentra en su página web; instituciones tales como: el instituto geofísico generalmente el aplicativo que avisa que hubo sismo o su conexión de Facebook es más importante que esté activo el servicio, esto es muy importante para ellos, sería terrible que hackeen la aplicación del sismo y envíen un sismo de magnitud a nivel Lima generando un grave pánico. Dependiendo de la información que se maneja es muy o poco importante sin llegar a ser insignificante.
2	¿Qué se debería tener en cuenta para el diseño de un modelo para el Análisis de Vulnerabilidades Digitales en una entidad pública?	Sería importante y fundamental la capacitación, formación del personal y las herramientas. La secretaría de gobierno digital está impulsando el tema de las herramientas, la PCM intenta impulsar pero es insuficiente ya que las oficinas de seguridad generalmente tienen un perfil de gestión, necesitas que te puedan hacer un análisis de vulnerabilidad ya ni hablar de la prueba de penetración, generalmente las capacitaciones que nos dicta la PCM se nota que por el nivel es muy bajo en cuanto a capacitación, es básico en sí, justo para que el personal de otras instituciones tengan referencia, porque hay instituciones que no tienen personal de seguridad y un nmap es un progreso para ellos. Entonces se complican mucho por temas básicos como puertos, servicios y no tienen como verificarlo (herramientas). Ciertamente es necesario el Oficial de Seguridad, pero no puede hacer todo, no hay manera en tema de formación, ya que es complicado que realice algo técnico, por ejemplo, no le puedes decir prepárate para presentarte ante el gerente general y a la vez prepárate para hackear una aplicación.
3	¿Cómo gestionar las	Básicamente el modelo NIST de los extremos de la ciberseguridad de la NIST porque tiene cinco fases: IDENTIFICAR, PROTEGER,

	vulnerabilidades dentro de un modelo?	DETECTAR, RESPONDER Y RECUPERAR. Lo que yo hago es ejecuto una especie de la NIST de ciberseguridad primero identificando si es un gestor empresarial, dirección de evaluación de riesgos o si se trata de un riesgo en la cadena de suministros donde analizo lo que voy a atacar. Luego tengo que proteger el control de acceso, coincidencia de información, seguridad de los datos y el proceso, procedimiento y protección de información, mantenimiento y tecnología de la información; La gestión de vulnerabilidades tiene una entrada para gestión de eventos y otra para gestión de incidentes, el evento es cuando no se logra tener éxito y el de incidentes es cuando logra tener éxito.
4	¿Qué debe incluir la metodología de análisis dentro de un modelo?	El tema metodológico es muy importante porque permite identificar y conocer, ya que los ataques más complejos no se hacen a ciegas si no sabes contra quien te estas enfrentando. Una parte básica de priorización de cuales aplicaciones o que escenarios tienen que entrar al proceso de vulnerabilidades, después de eso es el tema de riesgos para saber cuáles van a ser los vectores de ataque (ordenamiento, probar y documentarlos) y se debería priorizar las vulnerabilidades, por ejemplo: te salen 20 vulnerabilidades y puntúas para jerarquizarlas para que puedan priorizar cuales atender de nuevo y también la vía de escape, muchas veces una aplicación va a salir con vulnerabilidades por lo que se tiene que definir bajo qué condiciones se va a aceptar que la aplicación salga a pesar de tener vulnerabilidades típicamente las que sean menos transcendentes. Además llega la fase de negociación que es algo cuando una aplicación no sale en el tiempo que el usuario lo solicita (a pesar de las vulnerabilidades, la aplicación pasa a producción). Siempre en seguridad de información hay un tema de aceptación de riesgos, si te dicen que existía esa vulnerabilidad y aún no la pueden resolver pero igual tiene que entrar en producción, a veces aceptas que la aplicación salga pero no la difunden como condición porque se sabe que necesitan tiempo para arreglarla y en lo que está publicada debe ser tratada, es donde ahí entra una estrategia de comunicación.
5	¿Cómo debería ser la metodología de análisis dentro de un modelo?	Debe haber un análisis de riesgo en el proceso de análisis de vulnerabilidades. Generalmente, todas las aplicaciones tienen un análisis de riesgo que dicen cuáles son las reglas por la cual las aplicaciones van a ir, si salen a internet estará más expuestos y eso

		es un análisis de riesgo que a raíz de eso se define los controles, por un lado, tengo uno documental y el otro es más técnico. OWASP identificó varios cambios, es diferente el tema de desarrollo estándar con el desarrollo ágil, cuando desarrollas en ágil cambias tu proceso sin las actividades de control, por ejemplo: en desarrollo estándar después de sacar el QA pasa a seguridad pero no en ágil, en ágil se transfiere la actividad de seguridad al desarrollador y seguridad cumple el rol de documentar, porque de otra forma ya no da el tiempo. Ya existen formas de desarrollo seguro ágil pero fuerza que las actividades que antes se desarrollaban con el oficial de seguridad, ahora se desarrollen dentro de todo el proceso en ese sentido ya no existen las pruebas de penetración, sino de frente el desarrollador ejecuta la herramienta a partir de ello comienza a probar y seguridad solo actúa como documentador. Previamente a todo esto debe haber condiciones claras para la ejecución del análisis de vulnerabilidades. Cuando uno hace análisis de vulnerabilidades también puede jugar el tema de quipos: azul y rojo, donde divides la en dos equipos (uno que ataca y otro que defiende) eso pertenece a la NIST Como herramienta se puede hacer uso de Acunetix y NESSUS, mientras mejor sea la herramienta corresponde a mayor nivel técnico, el OWASP Zap debido a que es libre es lo más factible para una entidad pública.
6	¿Qué tecnologías defensivas es recomendable para mitigar las amenazas?	Se necesita pasar por todas las capas del modelo OSI que necesita un control por cada capa, que no accedan al centro de datos, tener controlado los puertos, etc. El tema del cableado es importante, en el tema de transporte es básico el HTPPS, el tema de SQL injection y el cierre de sesión. Como última capa sería concientizar a los usuarios para que reporten alguna vulnerabilidad, incluso por hackeo, él mismo debería informarlo que es indispensable para resolver complicaciones. A partir de gestión de incidentes te vas a dar cuenta como hackearon la aplicación por lo que necesitas hacer un pequeño análisis forense de los registros de la auditoría y la aplicación tiene que tener una cantidad infinita de registros para que sepas lo que puede pasar. En ese análisis forense puedes detectar el vector de entrada que utilizaron para hackear la aplicación, una vez conocido el vector de ataque puedes probarlo mediante una prueba de penetración o derivar al área para que pueda corregirlo, esa es la entrada cuando el riesgo se materializa que es el hackeo (parte de gestión de incidentes) por ahí viene la parte de gestión de

		vulnerabilidades, gestión de eventos que al ver en los registros del firewall aparece una serie de ataques entonces deberías hacer un pequeño análisis forense sobre las técnicas de ataque que se están utilizando, una vez realizado eso se va a poder identificar que vulnerabilidad ha descubierto el hacker, luego debes corregirlo.

N°	Preguntas	Entrevistado 2 – Analista de Seguridad
1	¿Qué importancia tiene el Análisis de Vulnerabilidades Digitales en una entidad pública?	Por lo general una entidad pública, tiene sus recursos tecnológicos desfasados, antiguos y desactualizados, esto incluye desde sistemas operativos hasta programas simples de escritorio, debido a la poca inversión en esta área tan importante, esto trae consigo un riesgo potencial, ya que está lleno de vulnerabilidades explotables por los posibles atacantes; un análisis de vulnerabilidades proporcionaría la información suficiente para evaluar y determinar los medios que se requieren para ir mitigando estas amenazas, es decir, se sabría la versión exacta del parche y se buscaría alternativas de seguridad, si es que no se cuenta con presupuesto para adquirirlos. Una entidad pública, por lo general, tiene información confidencial, que al ser expuesta y en manos equivocadas pondría en riesgo el sistema del gobierno, el riesgo es grande desde este punto de vista, pero los jefes o gerentes de estas entidades no tienen conocimiento del riesgo que involucra tener sistemas o recursos vulnerables, una vez que se dé la amenaza recién intentan tomar cartas en el asunto, pero ya es tarde, un proceso de análisis de vulnerabilidades es justamente para prevenir que se hagan realidad las amenazas.
2	¿Qué se debería tener en cuenta para el diseño de un modelo para el Análisis de Vulnerabilidades Digitales en una entidad pública?	Para diseñar un modelo para el análisis de vulnerabilidades, primero se debe tener en cuenta, si el personal cuenta con los conocimientos suficientes para llevar a cabo este proceso, ya que es necesario descubrir y mitigar estas amenazas, es decir, solucionar estos fallos de sistemas. También se debe tener en cuenta la parte administrativa, es decir la gestión del proyecto, para su primera implantación, posteriormente se debe tener en cuenta como punto esencial la planificación de estas actividades, esto incluye determinar cada cuánto tiempo se hará un análisis de vulnerabilidades y a qué tecnología, esto se entiende, qué sistemas o módulos, a las redes de comunicación, a los equipos informáticos (hardware) o las políticas de seguridad.

3	¿Cómo gestionar las vulnerabilidades dentro de un modelo?	El análisis de vulnerabilidades al ser una actividad, esta involucra recursos humanos y materiales, las cuales deben ser gestionados previamente, además previo a iniciar el proceso de análisis, debe haber una planificación en el cual se vea los tiempos, cronogramas y los recursos necesarios. También se debe tener muy en cuenta la priorización, no de priorizar las vulnerabilidades detectadas, si no, aún nivel macro; en el caso del ministerio público, ya que cuenta con 105 sistemas en producción hasta el momento y muchos otros en desarrollo, se debe priorizar con qué sistemas empezar y en cuales finalizar, de igual forma con los otros componentes como conexiones de red, servidores y equipos informáticos de usuarios finales. Es esencial definir el alcance del análisis de vulnerabilidades, qué se va cubrir y hasta qué nivel de profundidad se va legar.
4	¿Qué debe incluir la metodología de análisis dentro de un modelo?	La metodología nos debe decir cuáles son los pasos que se debe seguir, ojo que, previo a que se ejecute, ya se debe contar con todos los recursos como haber seleccionado adecuadamente el software de análisis y para ello se debe tener en cuenta los beneficios, ventajas y capacidades de cada software existente en el mercado, escoger entre licencias abiertas o cerradas. También se debe realizar un análisis de activos de la entidad en la cual se aplicará la actividad, esto permitirá generar un inventario de activos para luego clasificarlos. El acuerdo de confidencialidad debe evidenciar de forma clara todos los acuerdos con ambas partes.
5	¿Cómo debería ser la metodología de análisis dentro de un modelo?	Se debe tener bien claro las reglas de juego, es decir, se debe determinar de manera clara cuáles serán las actividades, los limites, las obligaciones y los permisos que se les darán por parte de la entidad al equipo que hará el análisis de vulnerabilidades, a pesar de que sea personal de la entidad, más si es de fuera, se debe hacer un compromiso de confidencialidad estricto, detallado y sancionador en caso de que se filtre información al respecto o no se cumpla con las reglas establecidas previamente, cuando se les otorgue permisos al equipo de análisis, solo debe ser con propósito de análisis y descubrimiento, más no de manipulación de datos, una vez culminado el proceso, se debe proceder a quitar estos permisos ipso facto. Finalmente es imprescindible realizar la documentación, reportes e informes de lo descubierto y lo realizado en general, de manera detallada, ya que esto servirá para posteriores análisis.
6	¿Qué tecnologías defensivas es	Como medidas para la defensa, adicionalmente a todas las herramientas de protección habidas y por haber, sería un plus,

	recomendable para mitigar las amenazas?	implementar algunos controles de la norma ISO 27001, como puede ser los controles de acceso, políticas de seguridad de la información y mantenimiento de los sistemas, para empezar, posteriormente ir agregando más, esto ayudaría a cualquier entidad dónde se considere en un futuro integrar la norma ISO 27001 en su totalidad o cuando se pretenda implementar un Sistema de Gestión de Seguridad de la Información. Recordemos que toda actividad preventiva suma.

N°	Preguntas	Entrevistado 3 – Experto en Seguridad (CNSD)
1	¿Qué importancia tiene el Análisis de Vulnerabilidades Digitales en una entidad pública?	Primeramente se tiene que tener claro, qué es un ataque, amenaza y vulnerabilidad, en síntesis una vulnerabilidad da lugar a una amenaza que cuando se hace realidad termina en un ataque, el cual es un riesgo para cualquier organización, la amenaza se materializa gracias a la vulnerabilidad, esto se da debido a un diseño deficiente, a errores de configuración o técnicas de configuración inseguras; todo empieza con las vulnerabilidades, por eso hacer un respectivo análisis de las vulnerabilidades sería muy importante y más en las entidades que manejan información confidencial o comprometedora; la falta de controles de seguridad también da lugar a las amenazas, se debe dar importancia a las actividades preventivas, otro punto importante es la verificación del inventario de equipos tecnológicos e identificar los equipos antiguos, ya que estos no cuentan con las últimas actualizaciones y en algunos casos ya no soportan los nuevos protocolos de seguridad. El análisis de vulnerabilidades, es muy importante porque servirá para comprobar la respuesta del equipamiento de seguridad; comprobar la capacidad de respuesta del equipo de TI, dada la vulnerabilidad, como se resolvería si surge una vulnerabilidad en una determinada tecnología; identificar las vulnerabilidades que se debe resolver, según el reporte de análisis, conocer los posibles riesgos digitales, tener mapeado los riesgos y luego aplicar controles para mitigar el riesgo.
2	¿Qué se debería tener en cuenta para el diseño de un modelo para el Análisis de Vulnerabilidades	Si se quiere desarrollar un modelo para el análisis de vulnerabilidades, se debería tener en cuenta, las debilidades tecnológicas, ya que a pesar de que se compre un software de la mejor empresa, siempre está sujeto a tener debilidades o fallos, como se dice en el mundo de la seguridad informática, ningún sistema es 100% seguro, esto puede tener fallas técnicas o por el uso humano; también se debe tener en

	Digitales en una entidad pública?	cuenta las debilidades de configuración que se le hace a la tecnología en sí (los accesos, las redes, los sistemas, lo equipos, entre otros) y también se debe considerar las debilidades de las políticas de seguridad, no hay pliticas escritas (determinar reglas para contraseñas robustas), el cual permitirá tener un buen nivel de seguridad esto también servirá de base para la implementación futura de un sistema de gestión de seguridad de la información. Se debe considerar las debilidades de los protocolos TCP / IP como HTTP, FTP e ICMP, que normalmente son inseguras; debilidades del sistema operativo y las debilidades de los equipos de red, como agujeros de cortafuegos o falta de autenticación, a veces se deja con la configuración por defecto, para ello se debe implementar directivas con los procedimientos de seguridad claros y precisos.
3	¿Cómo gestionar las vulnerabilidades dentro de un modelo?	El análisis de vulnerabilidades, son pruebas no intrusivas, es decir, no afecta la confidencialidad, la integridad o la disponibilidad de los servicios que se analizan, pero a pesar de ser algo interno, se tiene que coordinar, solicitar permisos y la autorización correspondiente, asimismo, se debe diferenciar e identificar los eventos e incidentes, hacer una planificación y priorización de los componentes a los que se les va hacer el proceso de análisis, se debe hacer la identificación y detección de los problemas en la infraestructura lógica del entorno y comparar con las bases de datos de vulnerabilidades conocidas y reportadas; al finalizar el análisis se debe hacer una revisión detallada de cada informe para detectar los falsos positivos. El análisis de vulnerabilidades debe empezar con la Identificación de vulnerabilidades, luego el análisis de esas vulnerabilidades, seguido de su gestión de riesgos y finalmente la remediación que vendrían a ser los controles de seguridad, esto es un ciclo que debe seguir cada vez que se haga un análisis de vulnerabilidades y se debe realizar de forma trimestral y también cada vez que se realice un cambio a los sistemas, cuando se saque una nueva aplicación, cuando se cambie los servidores, cuando se ponga un nuevo servicio, se debe usar mecanismos de evaluación para controlar las vulnerabilidades. Cuando se haga un escaneo interno de vulnerabilidades, debe ser realizado por personal capacitado que demuestre conocimiento en seguridad.
4	¿Qué debe incluir la metodología de	La ejecución del proceso de análisis tiene un tiempo relativamente corto, es recomendable realizarlos de manera trimestral o después de un cambio significativo. El análisis de vulnerabilidad se compone de

	análisis dentro de un modelo?	las siguientes fases: Reconocimiento, Enumeración, Análisis de vulnerabilidades automatizado y su respectiva generación de reportes, se debe tener en cuenta que en el reporte se verá falsos positivos, ya que los pasos anteriores no son intrusivos, entonces, después de los reportes se debe hacer una prueba de penetración o penetration testing, las cuales son pruebas intrusivas, ya que ahí se hacen los intentos de explotación de las vulnerabilidades encontradas, esta prueba, no solo puede ser lógica, también puede ser pruebas de ingeniería social y de accesos físicos, esta prueba de penetración es menos frecuente se puede realizar anualmente. También se debe tener en cuenta los tipos de análisis de vulnerabilidades que existen: basados en host, para analizar las vulnerabilidades de los sistemas operativos y servidores Linux, Windows, etc; basados en red, para analizar y detectar los puertos abiertos y los servicios que se ejecutan en estos; basado en base de datos; permite tener herramientas para buscar y evitar inyecciones SQL.
5	¿Cómo debería ser la metodología de análisis dentro de un modelo?	Para los escaneos de vulnerabilidades y el análisis en sí, se debe gestionar los permisos, que deben ser otorgados por la alta gerencia de la entidad, asimismo se debe elaborar un acuerdo de confidencialidad en el cual el equipo de análisis debe actuar con ética profesional y no divulgar los accesos que se les otorga, también no debe revelar por ningún motivo las vulnerabilidades que se encuentren así deje de trabajar en la entidad; es muy importante recolectar la información, para ello se puede hacer uso de las pruebas de caja negra, caja blanca o caja gris, dependiendo de cómo se haya determinado la forma de acceder a los sistemas y cómo se obtendrán los accesos; también se debe determinar si se va analizar interior o exteriormente, dependiendo si se proporcionará los permisos o se accederá de forma remota escalando los privilegios de usuario; finalmente luego de identificar las vulnerabilidades se debe hacer un descarte, ya que las herramientas suelen informar muchos falsos positivos, después del descarte se debe proceder con una prueba de penetración para cerciorarse y corroborar la vulnerabilidad, simulando un ataque.
6	¿Qué tecnologías defensivas es recomendable para mitigar las amenazas?	En cuanto a las formas de defensa o tecnologías defensivas, se debe implementar controles de acceso lógico, con doble factor de autenticación, esto debería estar por defecto, tener un equipo de respuestas ante incidentes de seguridad digital con un plan de respuestas ante los incidentes. Por lo general las entidades públicas

		tienen servidores antiguos y los atacantes aprovechan esa debilidad para ejecutar sus scripts, por ello se debe implementar un firewall delante del servidor para que contenga los ataques; realizar una auditoría de seguridad una vez al año, puede ser una auditoria interna de la ISO:27001 y también se puede implementar sus controles de seguridad. Es muy importante tener un Plan de Remediación después de haber identificado las vulnerabilidades. Otro punto fundamental es el tema de los usuarios o personas que hacen uso de los sistemas y de la tecnología en sí, ya que se ha visto mucho que el factor humano juega un papel importante y en muchos escenarios fue la vulnerabilidad o el punto de acceso a la información, aplicando ingeniería social.

Anexo 4

Matriz de codificación de la entrevista

N°	Preguntas	Entrevistado 1 – Oficial de Seguridad (MPFN)	Entrevista 1 Codificada
1	¿Qué importancia tiene el Análisis de Vulnerabilidades Digitales en una entidad pública?	Depende del impacto, usualmente el público es cautivo por lo tanto el impacto a la imagen institucional verdaderamente no trasciende, las personas no tienen opción de ir a otras entidades, ya que estas son únicas, solo les queda protestar. Lo que sí tiene mucha importancia es el cuidado de los datos de los usuarios, entonces los ciudadanos le confieren información a entidades del estado para su cuidado por lo que debería ser muy respetuoso de que no haya filtración de esa información, por ejemplo: en ciertos tipos de instituciones, la información es más importante, que aquello que se encuentra en su página web; instituciones tales como: el instituto geofísico generalmente el aplicativo que avisa que hubo sismo o su conexión de Facebook es más importante que esté activo el servicio, esto es muy importante para ellos, sería terrible que hackeen la aplicación del sismo y envíen un sismo de magnitud a nivel Lima generando un grave pánico. Dependiendo de la información que se maneja es muy o poco importante sin llegar a ser insignificante.	• Depende del impacto. • Cuidado de los datos de los usuarios. • Filtración de información. • Hackers. • Robo de información • Según el tipo de información que maneja la entidad.
2	¿Qué se debería tener en cuenta para el diseño de un modelo para el Análisis de Vulnerabilidades	Sería importante y fundamental la capacitación, formación del personal y las herramientas. La secretaría de gobierno digital está impulsando el tema de las herramientas, la PCM intenta impulsar pero es insuficiente ya que las oficinas de seguridad generalmente tienen un perfil	• Capacitación. • Formación del personal. • Herramientas de escaneo. • Las oficinas de seguridad tienen un perfil de gestión.

	Digitales en una entidad pública?	de gestión, necesitas que te puedan hacer un análisis de vulnerabilidad ya ni hablar de la prueba de penetración, generalmente las capacitaciones que nos dicta la PCM se nota que por el nivel es muy bajo en cuanto a capacitación, es básico en sí, justo para que el personal de otras instituciones tengan referencia, porque hay instituciones que no tienen personal de seguridad y un nmap es un progreso para ellos. Entonces se complican mucho por temas básicos como puertos, servicios y no tienen como verificarlo (herramientas). Ciertamente es necesario el Oficial de Seguridad, pero no puede hacer todo, no hay manera en tema de formación, ya que es complicado que realice algo técnico, por ejemplo, no le puedes decir prepárate para presentarte ante el gerente general y a la vez prepárate para hackear una aplicación.	• Análisis de vulnerabilidades y prueba de penetración. • Personal especializado. • El Oficial de Seguridad gestiona.
3	¿Cómo gestionar las vulnerabilidades dentro de un modelo?	Básicamente el modelo NIST de los extremos de la ciberseguridad de la NIST porque tiene cinco fases: IDENTIFICAR, PROTEGER, DETECTAR, RESPONDER Y RECUPERAR. Lo que yo hago es ejecuto una especie de la NIST de ciberseguridad primero identificando si es un gestor empresarial, dirección de evaluación de riesgos o si se trata de un riesgo en la cadena de suministros donde analizo lo que voy a atacar. Luego tengo que proteger el control de acceso, coincidencia de información, seguridad de los datos y el proceso, procedimiento y protección de información, mantenimiento y tecnología de la información; La gestión de vulnerabilidades tiene una entrada para gestión de eventos y otra para	• Modelo NIST. • IDENTIFICAR. • PROTEGER. • DETECTAR. • RESPONDER. • RECUPERAR. • Evaluar el riesgo. • Gestión de eventos. • Gestión de incidentes.

		gestión de incidentes, el evento es cuando no se logra tener éxito y el de incidentes es cuando logra tener éxito.	
4	¿Qué debe incluir la metodología de análisis dentro de un modelo?	El tema metodológico es muy importante porque permite identificar y conocer, ya que los ataques más complejos no se hacen a ciegas si no sabes contra quien te estas enfrentando. Una parte básica de priorización de cuales aplicaciones o que escenarios tienen que entrar al proceso de vulnerabilidades, después de eso es el tema de riesgos para saber cuáles van a ser los vectores de ataque (ordenamiento, probar y documentarlos) y se debería priorizar las vulnerabilidades, por ejemplo: te salen 20 vulnerabilidades y puntúas para jerarquizarlas para que puedan priorizar cuales atender de nuevo y también la vía de escape, muchas veces una aplicación va a salir con vulnerabilidades por lo que se tiene que definir bajo qué condiciones se va a aceptar que la aplicación salga a pesar de tener vulnerabilidades típicamente las que sean menos transcendentes. Además llega la fase de negociación que es algo cuando una aplicación no sale en el tiempo que el usuario lo solicita (a pesar de las vulnerabilidades, la aplicación pasa a producción). Siempre en seguridad de información hay un tema de aceptación de riesgos, si te dicen que existía esa vulnerabilidad y aún no la pueden resolver pero igual tiene que entrar en producción, a veces aceptas que la aplicación salga pero no la difunden como condición porque se sabe que necesitan tiempo para arreglarla y en lo que está publicada	• Conocer al atacante. • Priorización de aplicaciones. • Análisis de riesgos. • Identificación de vectores de ataque. • Priorizar las vulnerabilidades. • NEGOCIACIÓN. • Aceptación de riesgos.

		debe ser tratada, es donde ahí entra una estrategia de comunicación.	
5	¿Cómo debería ser la metodología de análisis dentro de un modelo?	Debe haber un análisis de riesgo en el proceso de análisis de vulnerabilidades. Generalmente, todas las aplicaciones tienen un análisis de riesgo que dicen cuáles son las reglas por la cual las aplicaciones van a ir, si salen a internet estará más expuestos y eso es un análisis de riesgo que a raíz de eso se define los controles, por un lado, tengo uno documental y el otro es más técnico. OWASP identificó varios cambios, es diferente el tema de desarrollo estándar con el desarrollo ágil, cuando desarrollas en ágil cambias tu proceso sin las actividades de control, por ejemplo: en desarrollo estándar después de sacar el QA pasa a seguridad pero no en ágil, en ágil se transfiere la actividad de seguridad al desarrollador y seguridad cumple el rol de documentar, porque de otra forma ya no da el tiempo. Ya existen formas de desarrollo seguro ágil pero fuerza que las actividades que antes se desarrollaban con el oficial de seguridad, ahora se desarrollen dentro de todo el proceso en ese sentido ya no existen las pruebas de penetración, sino de frente el desarrollador ejecuta la herramienta a partir de ello comienza a probar y seguridad solo actúa como documentador. Previamente a todo esto debe haber condiciones claras para la ejecución del análisis de vulnerabilidades. Cuando uno hace análisis de vulnerabilidades también puede jugar el tema de quipos: azul y rojo, donde divides la en dos equipos (uno que	• Análisis de riesgos. • Definir reglas. • Owasp. • Determinar si es desarrollo estándar o ágil. • Documentación. • Condiciones claras. • NIST: Equipo rojo y azul. • Herramientas de escaneo.

		ataca y otro que defiende) eso pertenece a la NIST Como herramienta se puede hacer uso de Acunetix y NESSUS, mientras mejor sea la herramienta corresponde a mayor nivel técnico, el OWASP Zap debido a que es libre es lo más factible para una entidad pública.	
6	¿Qué tecnologías defensivas es recomendable para mitigar las amenazas?	Se necesita pasar por todas las capas del modelo OSI que necesita un control por cada capa, que no accedan al centro de datos, tener controlado los puertos, etc. El tema del cableado es importante, en el tema de transporte es básico el HTPPS, el tema de SQL injection y el cierre de sesión. Como última capa sería concientizar a los usuarios para que reporten alguna vulnerabilidad, incluso por hackeo, él mismo debería informarlo que es indispensable para resolver complicaciones. A partir de gestión de incidentes te vas a dar cuenta como hackearon la aplicación por lo que necesitas hacer un pequeño análisis forense de los registros de la auditoría y la aplicación tiene que tener una cantidad infinita de registros para que sepas lo que puede pasar. En ese análisis forense puedes detectar el vector de entrada que utilizaron para hackear la aplicación, una vez conocido el vector de ataque puedes probarlo mediante una prueba de penetración o derivar al área para que pueda corregirlo, esa es la entrada cuando el riesgo se materializa que es el hackeo (parte de gestión de incidentes) por ahí viene la parte de gestión de vulnerabilidades, gestión de eventos que al ver en los registros del firewall aparece una serie de ataques entonces deberías	• Medidas sobre cada capa del modelo OSI. • Https. • Concientizar a los usuarios. • Usar el esfuerzo del hacker. • Análisis forense. • Identificar el vector de ataque. • Determinar las técnicas de ataque. • Web application firewall (WAF).

		hacer un pequeño análisis forense sobre las técnicas de ataque que se están utilizando, una vez realizado eso se va a poder identificar que vulnerabilidad ha descubierto el hacker, luego debes corregirlo. Se encontrarán muchos proveedores que tienen sus soluciones tipo firewall de aplicación (WAF) que también puede detectar los ataques de forma manual, verifica la vulnerabilidad y se lo pasa al desarrollador para que lo arregle, eso sería usando el esfuerzo del hacker para corregir su aplicación y cuando roban la aplicación también es necesario un análisis forense.	

N°	Preguntas	Entrevistado 2 – Analista de Seguridad	Entrevista 2 Codificada
1	¿Qué importancia tiene el Análisis de Vulnerabilidades Digitales en una entidad pública?	Por lo general una entidad pública, tiene sus recursos tecnológicos desfasados, antiguos y desactualizados, esto incluye desde sistemas operativos hasta programas simples de escritorio, debido a la poca inversión en esta área tan importante, esto trae consigo un riesgo potencial, ya que está lleno de vulnerabilidades explotables por los posibles atacantes; un análisis de vulnerabilidades proporcionaría la información suficiente para evaluar y determinar los medios que se requieren para ir mitigando estas amenazas, es decir, se sabría la versión exacta del parche y se buscaría alternativas de seguridad, si es que no se cuenta con presupuesto para adquirirlos. Una entidad pública, por lo general, tiene información	• Entidades públicas con tecnología desfasada, antigua y desactualizado. • La baja inversión en tecnología. • El análisis debe proporcionar información para evaluar, determinar y mitigar las amenazas. • Exponer la información confidencial, pone en riesgo todo el sistema del gobierno. • El proceso de análisis debe prevenir las amenazas.

		confidencial, que al ser expuesta y en manos equivocadas pondría en riesgo el sistema del gobierno, el riesgo es grande desde este punto de vista, pero los jefes o gerentes de estas entidades no tienen conocimiento del riesgo que involucra tener sistemas o recursos vulnerables, una vez que se dé la amenaza recién intentan tomar cartas en el asunto, pero ya es tarde, un proceso de análisis de vulnerabilidades es justamente para prevenir que se hagan realidad las amenazas.	
2	¿Qué se debería tener en cuenta para el diseño de un modelo para el Análisis de Vulnerabilidades Digitales en una entidad pública?	Para diseñar un modelo para el análisis de vulnerabilidades, primero se debe tener en cuenta, si el personal cuenta con los conocimientos suficientes para llevar a cabo este proceso, ya que es necesario descubrir y mitigar estas amenazas, es decir, solucionar estos fallos de sistemas. También se debe tener en cuenta la parte administrativa, es decir la gestión del proyecto, para su primera implantación, posteriormente se debe tener en cuenta como punto esencial la planificación de estas actividades, esto incluye determinar cada cuánto tiempo se hará un análisis de vulnerabilidades y a qué tecnología, esto se entiende, qué sistemas o módulos, a las redes de comunicación, a los equipos informáticos (hardware) o las políticas de seguridad.	• Personal con conocimientos para ejecutar el análisis. • Solucionar los fallos del sistema. • Gestión administrativa y de proyecto. • Planificación. • Determinar el alcance del análisis.
3	¿Cómo gestionar las vulnerabilidades dentro de un modelo?	El análisis de vulnerabilidades al ser una actividad, esta involucra recursos humanos y materiales, las cuales deben ser gestionados previamente, además previo a iniciar el proceso de análisis, debe haber una planificación en el cual se vea los tiempos, cronogramas y los	• Gestión de recursos humanos y materiales. • Planificación. • Priorizar los sistemas de la entidad.

		recursos necesarios. También se debe tener muy en cuenta la priorización, no de priorizar las vulnerabilidades detectadas, si no, aún nivel macro; en el caso del ministerio público, ya que cuenta con 105 sistemas en producción hasta el momento y muchos otros en desarrollo, se debe priorizar con qué sistemas empezar y en cuales finalizar, de igual forma con los otros componentes como conexiones de red, servidores y equipos informáticos de usuarios finales. Es esencial definir el alcance del análisis de vulnerabilidades, qué se va cubrir y hasta qué nivel de profundidad se va llegar.	• Definir el alcance del análisis de vulnerabilidades. • Determinar el nivel de profundidad del análisis.
4	¿Qué debe incluir la metodología de análisis dentro de un modelo?	La metodología nos debe decir cuáles son los pasos que se debe seguir, ojo que, previo a que se ejecute, ya se debe contar con todos los recursos como, haber seleccionado adecuadamente el software de análisis y para ello se debe tener en cuenta los beneficios, ventajas y capacidades de cada software existente en el mercado, escoger entre licencias abiertas o cerradas. También se debe realizar un análisis de activos de la entidad en la cual se aplicará la actividad, esto permitirá generar un inventario de activos para luego clasificarlos. El acuerdo de confidencialidad debe evidenciar de forma clara todos los acuerdos con ambas partes.	• Contar con los recursos necesarios. • Seleccionar el software de análisis adecuado. • Realizar un análisis de activos de la entidad. • Generar un inventario de activos y clasificar. • Acuerdo de confidencialidad claro y conciso.
5	¿Cómo debería ser la metodología de análisis dentro de un modelo?	Se debe tener bien claro las reglas de juego, es decir, se debe determinar de manera clara cuáles serán las actividades, los limites, las obligaciones y los permisos que se les darán por parte de la entidad al equipo que hará el análisis de vulnerabilidades, a pesar de que sea	• Establecer las reglas de juego. • Determinar las actividades, límites, obligaciones y permisos para el equipo de análisis.

		personal de la entidad, más si es de fuera, se debe hacer un compromiso de confidencialidad estricto, detallado y sancionador en caso de que se filtre información al respecto o no se cumpla con las reglas establecidas previamente, cuando se les otorgue permisos al equipo de análisis, solo debe ser con propósito de análisis y descubrimiento, más no de manipulación de datos, una vez culminado el proceso, se debe proceder a quitar estos permisos ipso facto. Finalmente es imprescindible realizar la documentación, reportes e informes de lo descubierto y lo realizado en general, de manera detallada, ya que esto servirá para posteriores análisis.	• Compromiso de confidencialidad estricto, detallado y sancionador. • Otorgar y quitar permisos al equipo de análisis. • Documentación, reportes e informes.
6	¿Qué tecnologías defensivas es recomendable para mitigar las amenazas?	Como medidas para la defensa, adicionalmente a todas las herramientas de protección habidas y por haber, sería un plus, implementar algunos controles de la norma ISO 27001, como puede ser los controles de acceso, políticas de seguridad de la información y mantenimiento de los sistemas, para empezar, posteriormente ir agregando más, esto ayudaría a cualquier entidad dónde se considere en un futuro integrar la norma ISO 27001 en su totalidad o cuando se pretenda implementar un Sistema de Gestión de Seguridad de la Información. Recordemos que toda actividad preventiva suma.	• Herramientas de protección. • Controles de la norma ISO 27001. • Controles de acceso • Políticas de seguridad de la información. • Mantenimiento de los sistemas.

N°	Preguntas	Entrevistado 3 – Oficial de Seguridad (CNSD)	Entrevista 3 Codificada

1	¿Qué importancia tiene el Análisis de Vulnerabilidades Digitales en una entidad pública?	Primeramente se tiene que tener claro, qué es un ataque, amenaza y vulnerabilidad, en síntesis una vulnerabilidad da lugar a una amenaza que cuando se hace realidad termina en un ataque, el cual es un riesgo para cualquier organización, la amenaza se materializa gracias a la vulnerabilidad, esto se da debido a un diseño deficiente, a errores de configuración o técnicas de configuración inseguras; todo empieza con las vulnerabilidades, por eso hacer un respectivo análisis de las vulnerabilidades sería muy importante y más en las entidades que manejan información confidencial o comprometedora; la falta de controles de seguridad también da lugar a las amenazas, se debe dar importancia a las actividades preventivas, otro punto importante es la verificación del inventario de equipos tecnológicos e identificar los equipos antiguos, ya que estos no cuentan con las últimas actualizaciones y en algunos casos ya no soportan los nuevos protocolos de seguridad. El análisis de vulnerabilidades, es muy importante porque servirá para comprobar la respuesta del equipamiento de seguridad; comprobar la capacidad de respuesta del equipo de TI, dada la vulnerabilidad, como se resolvería si surge una vulnerabilidad en una determinada tecnología; identificar las vulnerabilidades que se debe resolver, según el reporte de análisis, conocer los posibles riesgos digitales, tener mapeado los riesgos y luego aplicar controles para mitigar el riesgo.	• La vulnerabilidad materializa a la amenaza. • Diseño deficiente. • Errores de configuración. • Técnicas de configuración inseguras. • Entidades con información confidencial. • Falta de controles de seguridad. • Realizar actividades preventivas. • Identificar equipos antiguos. • Nuevos protocolos de seguridad. • Para comprobar la respuesta del equipamiento de seguridad. • Para comprobar la capacidad de respuesta del equipo de TI. • Para identificar y resolver las vulnerabilidades. • Identificar los riesgos y aplicar controles.

2	¿Qué se debería tener en cuenta para el diseño de un modelo para el Análisis de Vulnerabilidades Digitales en una entidad pública?	Si se quiere desarrollar un modelo para el análisis de vulnerabilidades, se debería tener en cuenta, las debilidades tecnológicas, ya que a pesar de que se compre un software de la mejor empresa, siempre está sujeto a tener debilidades o fallos, como se dice en el mundo de la seguridad informática, ningún sistema es 100% seguro, esto puede tener fallas técnicas o por el uso humano; también se debe tener en cuenta las debilidades de configuración que se le hace a la tecnología en sí (los accesos, las redes, los sistemas, lo equipos, entre otros) y también se debe considerar las debilidades de las políticas de seguridad, no hay pliticas escritas (determinar reglas para contraseñas robustas), el cual permitirá tener un buen nivel de seguridad esto también servirá de base para la implementación futura de un sistema de gestión de seguridad de la información. Se debe considerar las debilidades de los protocolos TCP / IP como HTTP, FTP e ICMP, que normalmente son inseguras; debilidades del sistema operativo y las debilidades de los equipos de red, como agujeros de cortafuegos o falta de autenticación, a veces se deja con la configuración por defecto, para ello se debe implementar directivas con los procedimientos de seguridad claros y precisos.	• Debilidades tecnológicas. • Sistemas sujetos a fallos • Fallas técnicas y humanas. • Debilidades de configuración. • Debilidades de las políticas de seguridad. • Debilidades de los protocolos. • Debilidades del sistema operativo. • Desarrollar directivas de procedimiento de seguridad.
3	¿Cómo gestionar las vulnerabilidades dentro de un modelo?	El análisis de vulnerabilidades, son pruebas no intrusivas, es decir, no afecta la confidencialidad, la integridad o la disponibilidad de los servicios que se analizan, pero a pesar de ser algo interno, se tiene que coordinar, solicitar permisos	• No debe afectar la confidencialidad, integridad o disponibilidad. • Coordinar, solicitar permisos y autorización.

		y la autorización correspondiente, asimismo, se debe diferenciar e identificar los eventos e incidentes, hacer una planificación y priorización de los componentes a los que se les va hacer el proceso de análisis, se debe hacer la identificación y detección de los problemas en la infraestructura lógica del entorno y comparar con las bases de datos de vulnerabilidades conocidas y reportadas; al finalizar el análisis se debe hacer una revisión detallada de cada informe para detectar los falsos positivos. El análisis de vulnerabilidades debe empezar con la Identificación de vulnerabilidades, luego el análisis de esas vulnerabilidades, seguido de su gestión de riesgos y finalmente la remediación que vendrían a ser los controles de seguridad, esto es un ciclo que debe seguir cada vez que se haga un análisis de vulnerabilidades y se debe realizar de forma trimestral y también cada vez que se realice un cambio a los sistemas, cuando se saque una nueva aplicación, cuando se cambie los servidores, cuando se ponga un nuevo servicio, se debe usar mecanismos de evaluación para controlar las vulnerabilidades. Cuando se haga un escaneo interno de vulnerabilidades, debe ser realizado por personal capacitado que demuestre conocimiento en seguridad.	• Diferenciar e identificar los eventos e incidentes. • Planificación y priorización • Detección de problemas en la infraestructura lógica. • Comparar con las bases de datos de las vulnerabilidades conocidas y reportadas. • Revisión detallada del informe y descartar falsos positivos. • Identificación. • Análisis. • Gestión de riesgos. • Remediación. • Realizar trimestralmente o cuando haya un cambio significativo. • Personal capacitado.
4	¿Qué debe incluir la metodología de análisis dentro de un modelo?	La ejecución del proceso de análisis tiene un tiempo relativamente corto, es recomendable realizarlos de manera trimestral o después de un cambio significativo. El análisis de vulnerabilidad se compone de las siguientes fases:	• Realizar trimestralmente o cuando haya un cambio significativo. • Reconocimiento. • Enumeración. • Análisis automatizado.

		Reconocimiento, Enumeración, Análisis de vulnerabilidades automatizado y su respectiva generación de reportes, se debe tener en cuenta que en el reporte se verá falsos positivos, ya que los pasos anteriores no son intrusivos, entonces, después de los reportes se debe hacer una prueba de penetración o penetration testing, las cuales son pruebas intrusivas, ya que ahí se hacen los intentos de explotación de las vulnerabilidades encontradas, esta prueba, no solo puede ser lógica, también puede ser pruebas de ingeniería social y de accesos físicos, esta prueba de penetración es menos frecuente se puede realizar anualmente. También se debe tener en cuenta los tipos de análisis de vulnerabilidades que existen: basados en host, para analizar las vulnerabilidades de los sistemas operativos y servidores Linux, Windows, etc; basados en red, para analizar y detectar los puertos abiertos y los servicios que se ejecutan en estos; basado en base de datos; permite tener herramientas para buscar y evitar inyecciones SQL.	• Generación de reportes. • Pruebas de penetración (anual). • Análisis basados en host, red, base de datos y apps.
5	¿Cómo debería ser la metodología de análisis dentro de un modelo?	Para los escaneos de vulnerabilidades y el análisis en sí, se debe gestionar los permisos, que deben ser otorgados por la alta gerencia de la entidad, asimismo se debe elaborar un acuerdo de confidencialidad en el cual el equipo de análisis debe actuar con ética profesional y no divulgar los accesos que se les otorga, también no debe revelar por ningún motivo las vulnerabilidades que se encuentren así deje de trabajar en la entidad; es muy importante recolectar la	• Gestionar los permisos. • Acuerdo de confidencialidad. • Recolección de información. • Determinar el análisis interior o exterior. • Descarte de falsos positivos. • Prueba de penetración.

		información, para ello se puede hacer uso de las pruebas de caja negra, caja blanca o caja gris, dependiendo de cómo se haya determinado la forma de acceder a los sistemas y cómo se obtendrán los accesos; también se debe determinar si se va analizar interior o exteriormente, dependiendo si se proporcionará los permisos o se accederá de forma remota escalando los privilegios de usuario; finalmente luego de identificar las vulnerabilidades se debe hacer un descarte, ya que las herramientas suelen informar muchos falsos positivos, después del descarte se debe proceder con una prueba de penetración para cerciorarse y corroborar la vulnerabilidad, simulando un ataque.	
6	¿Qué tecnologías defensivas es recomendable para mitigar las amenazas?	En cuanto a las formas de defensa o tecnologías defensivas, se debe implementar controles de acceso lógico, con doble factor de autenticación, esto debería estar por defecto, tener un equipo de respuestas ante incidentes de seguridad digital con un plan de respuestas ante los incidentes. Por lo general las entidades públicas tienen servidores antiguos y los atacantes aprovechan esa debilidad para ejecutar sus scripts, por ello se debe implementar un firewall delante del servidor para que contenga los ataques; realizar una auditoría de seguridad una vez al año, puede ser una auditoria interna de la ISO:27001 y también se puede implementar sus controles de seguridad. Es muy importante tener un Plan de Remediación después de haber identificado las vulnerabilidades. Otro	• Controles de acceso lógico. • Doble factor de autenticación. • Equipo de respuestas ante incidentes de seguridad digital. • Plan de repuestas. • Firewall, para contener los ataques. • Auditoria de seguridad ISO 27001. • Plan de remediación. • Concientización a los usuarios.

		punto fundamental es el tema de los usuarios o personas que hacen uso de los sistemas y de la tecnología en sí, ya que se ha visto mucho que el factor humano juega un papel importante y en muchos escenarios fue la vulnerabilidad o el punto de acceso a la información, aplicando ingeniería social, por ello se debe concientizar a los usuarios o trabajadores de la entidad.	

Anexo 5

Matriz de entrevistados y conclusiones

N°	Pregunta	Entrevistado 1 Oficial de Seguridad	Entrevistado 2 Analista de Seguridad	Entrevistado 3 Experto en Seguridad	Similitud	Diferencias	Conclusiones
1	¿Qué importancia tiene el Análisis de Vulnerabilidades Digitales en una entidad pública?	• Depende del impacto. • Cuidado de los datos de los usuarios. • Filtración de información. • Hackers. • Robo de información. • Según el tipo de información que maneja la entidad.	• Entidades públicas con tecnología desfasada, antigua y desactualizado. • La baja inversión en tecnología. • El análisis debe proporcionar información para evaluar, determinar y mitigar las amenazas. • Exponer la información confidencial, pone en riesgo todo el sistema del gobierno. • El proceso de análisis debe	• La vulnerabilidad materializa a la amenaza. • Diseño deficiente. • Errores de configuración. • Técnicas de configuración inseguras. • Entidades con información confidencial. • Falta de controles de seguridad. • Realizar actividades preventivas. • Identificar equipos antiguos. • Nuevos protocolos de seguridad.	Entidades con información confidencial. Tecnología antigua y desactualizada. Robo de información. Evitar ataques. Falta de políticas de seguridad.	Actividades hacktivistas. Errores de configuración. Para comprobar la capacidad de respuesta. Identificar riesgos. Falta integrar los nuevos protocolos de seguridad.	El análisis de vulnerabilidades es muy importante, porque permite proteger el activo más importante como lo es la información, más aún cuando la entidad pública maneja información confidencial y de extremo cuidado, el análisis, permite identificar las fallas de la tecnología en sí para mitigar las amenazas, reducir y evitar las probabilidades de ataques y robo de información. También permite comprobar la capacidad de respuesta del equipo de seguridad ante algún incidente y aplicar controles adecuados de seguridad.

			prevenir las amenazas.	• Para comprobar la respuesta del equipamiento de seguridad. • Para comprobar la capacidad de respuesta del equipo de TI. • Para identificar y resolver las vulnerabilidades. • Identificar los riesgos y aplicar controles.			
2	¿Qué se debería tener en cuenta para el diseño de un modelo para el Análisis de Vulnerabilidades Digitales en una entidad pública?	• Capacitación. • Formación del personal. • Herramientas de escaneo. • Las oficinas de seguridad tienen un perfil de gestión. • Análisis de vulnerabilidades y	• Personal con conocimientos para ejecutar el análisis. • Solucionar los fallos del sistema. • Gestión administrativa y de proyecto. • Planificación. • Determinar el alcance del análisis.	• Debilidades tecnológicas. • Sistemas sujetos a fallos • Fallas técnicas y humanas. • Debilidades de configuración. • Debilidades de las políticas de seguridad.	Personal capacitado. Fallas en los sistemas.	Debilidades tecnológicas. Gestión administrativa. Planificación y alcance. Directivas de seguridad. Herramientas de escaneo. Oficinas de seguridad con perfil de gestión.	Para diseñar el modelo de análisis de vulnerabilidades, se debe tener en cuenta las debilidades tecnológicas en general de la entidad pública, tener una buena planificación, determinar el alcance del análisis. Se debe tener en cuenta que la oficina de seguridad está orientada a la gestión, ya que es transversal a la entidad, también se debe considerar los

		prueba de penetración. • Personal especializado. • El Oficial de Seguridad gestiona.		• Debilidades de los protocolos. • Debilidades del sistema operativo. • Desarrollar directivas de procedimiento de seguridad.			recursos con los que se cuentan y los que se pueden obtener.
3	¿Cómo gestionar las vulnerabilidades dentro de un modelo?	• Modelo NIST. • IDENTIFICAR. • PROTEGER. • DETECTAR. • RESPONDER. • RECUPERAR. • Evaluar el riesgo. • Gestión de eventos. • Gestión de incidentes.	• Gestión de recursos humanos y materiales. • Planificación. • Priorizar los sistemas de la entidad. • Definir el alcance del análisis de vulnerabilidades. • Determinar el nivel de profundidad del análisis.	• No debe afectar la confidencialidad, integridad o disponibilidad. • Coordinar, solicitar permisos y autorización. • Diferenciar e identificar los eventos e incidentes. • Planificación y priorización • Detección de problemas en la infraestructura lógica. • Comparar con las bases de datos de las vulnerabilidades	Gestión de eventos. Gestión de incidentes. Planificación y priorización. IDENTIFICAR. DETECTAR. RESPONDER. Proteger y remediar. Gestión de riesgos.	Modelo NIST. Recursos humanos y materiales. Determinar el alcance y la profundidad. Comparar con las bases de datos. INFORMES. Descartar falsos positivos. Ejecución trimestral o en un cambio significativo.	Se concluye que la gestión de vulnerabilidades debe incluir la gestión de eventos e incidentes; se debe tener una planificación del proceso de análisis y priorizar los sistemas a analizar, se puede tener como referencia el modelo NIST, también se debe incluir la gestión de riesgos con el fin de determinar el impacto de dicho análisis, asimismo se debe establecer el periodo de ejecución de dicho análisis. En resumen, también se valida las subcategorías: Descubrimiento, informes, priorización y respuesta.

				conocidas y reportadas. • Revisión detallada del informe y descartar falsos positivos. • Identificación. • Análisis. • Gestión de riesgos. • Remediación. • Realizar trimestralmente o cuando haya un cambio significativo. • Personal capacitado.			
4	¿Qué debe incluir la metodología de análisis dentro de un modelo?	• Conocer al atacante. • Priorización de aplicaciones. • Análisis de riesgos. • Identificación de vectores de ataque.	• Contar con los recursos necesarios. • Seleccionar el software de análisis adecuado. • Realizar un análisis de activos de la entidad.	• Reconocimiento. • Enumeración. • Análisis automatizado. • Generación de reportes. • Pruebas de penetración (anual).	Herramientas de análisis. Pruebas de penetración. Generación de reportes. Reconocer al atacante. Priorización de aplicaciones.	Identificar el vector de ataque. NEGOCIACIÓN y Aceptación de riesgos. Análisis de activos. Análisis automatizado. Análisis basados en host, red, base de datos y apps	Se debe seleccionar las herramientas más adecuadas para el proceso de análisis de vulnerabilidades, se debe ir creando un historial de atacantes, se debe pensar a futuro en hacer un análisis automatizado. Un punto importante que no se menciona en otras metodologías, es la NEGOCIACION y la aceptación del riesgo. El cual tiene la finalidad

		• Priorizar las vulnerabilidades. • NEGOCIACIÓN. • Aceptación de riesgos.	• Generar un inventario de activos y clasificar. • Acuerdo de confidencialidad claro y conciso.	• Análisis basados en host, red, base de datos y apps.			de salvaguardar la información y evitar ataques inminentes.
5	¿Cómo debería ser la metodología de análisis dentro de un modelo?	• Análisis de riesgos. • Definir reglas. • Owasp. • Determinar si es desarrollo estándar o ágil. • Documentación. • Condiciones claras. • NIST: Equipo rojo y azul. • Herramientas de escaneo.	• Establecer las reglas de juego. • Determinar las actividades, límites, obligaciones y permisos para el equipo de análisis. • Compromiso de confidencialidad estricto, detallado y sancionador. • Otorgar y quitar permisos al equipo de análisis. • Documentación, reportes e informes.	• Gestionar los permisos. • Acuerdo de confidencialidad. • Recolección de información. • Determinar el análisis interior o exterior. • Descarte de falsos positivos. • Prueba de penetración.	Reglas de juego. Acuerdo de confidencialidad. Pruebas de penetración. Gestión de permisos. Seleccionar las herramientas de escaneo.	Recolección de información. Determinar el análisis interior o exterior. OWASP. NIST: equipo rojo y azul. Documentación. Descartar los falsos positivos. Determinar el equipo de análisis.	En la metodología se debe establecer las reglas de juego de forma clara, luego elaborar el acuerdo de confidencialidad, recolectar la información, determinar si se hará un análisis interior o exterior, luego hacer la documentación y descarte de falsos positivos respectivamente. También se puede seguir los lineamientos de OWASP y poner en práctica la estrategia del equipo rojo y azul de la NIST. Priorizando las aplicaciones se debe incluir una prueba de penetración.

6	¿Qué tecnologías defensivas es recomendable para mitigar las amenazas?	• Medidas sobre cada capa del modelo OSI. • Https. • Concientizar a los usuarios. • Usar el esfuerzo del hacker. • Análisis forense. • Identificar el vector de ataque. • Determinar las técnicas de ataque. • Web application firewall (WAF). • Security Hardening Checklist.	• Herramientas de protección. • Controles de la norma ISO 27001. • Controles de acceso • Políticas de seguridad de la información. • Mantenimiento de los sistemas. • Plan de repuestas.	• Controles de acceso lógico. • Doble factor de autenticación. • Equipo de respuestas ante incidentes de seguridad digital. • Firewall, para contener los ataques. • Auditoria de seguridad ISO 27001. • Plan de remediación. • Concientización a los usuarios.	Controles de acceso. Lineamientos de la ISO 27001. Plan de remediación. Auditoría de seguridad. Concientización a los usuarios. Security Hardening Checklist,	Medidas de seguridad en cada capa del modelo OSI. Https, Firewall, WAF. Usar el esfuerzo del hacker. Análisis forense. Identificar el vector y las técnicas de ataque. Políticas de seguridad. Doble factor de autenticación. Implementar el equipo de respuestas. Security Hardening Checklist.	Para la defensa es importante implementar los controles de acceso, con doble factor de autenticación, se puede seguir lo indicado en la ISO 27001 para la auditoria; concientizar a los usuarios es fundamental ya que es la mayor vulnerabilidad de todo sistema. Implementar medidas de seguridad en cada capa del Modelo OSI, https y firewall para iniciar; es importante registrar los ataques, determinar el vector y las técnicas de ataque, para ser simulados y descubrir las fallas críticas y corregirlas. Se puede hacer un análisis forense de ser posible. Usar Security Hardening Checklist, para mejorar la seguridad del entorno.

Conclusión de las Entrevistas Realizadas

En conclusión, para desarrollar un modelo para el análisis de vulnerabilidades digitales, se debe tener en cuenta primeramente contar con los recursos necesarios para desarrollar esta actividad de prevención, contar con las herramientas y el personal capacitado en el procedimiento técnico y de gestión, se debe tener en cuenta la tecnología antigua, desfasada y desactualizada a la que se va enfrentar, identificar los servicios y aplicaciones / sistemas para priorizar según el nivel de información que maneja y el nivel de riesgo asociado a esta actividad; la planificación también juega un papel importante, para poder llevar a cabo el análisis de vulnerabilidades con éxito y dentro de los plazos establecidos.

Asimismo, se debe incluir en el modelo, la gestión de eventos, gestión de incidentes y la gestión de riesgos, estos tres están relacionados directa e indirectamente con la gestión de vulnerabilidades, de igual manera se puede tomar algunos puntos relevantes del modelo NIST y de la ISO 27001; la ejecución de esta actividad preventiva se debe ejecutar periódicamente de forma trimestral y cada vez que haya un cambio significativo en la infraestructura tecnológica y los sistemas de información; un punto principal que se rescata de la entrevista al Oficial de Seguridad es la negociación y la aceptación del riesgo, ya que no se suele mencionar en otras metodologías, pero resulta fundamental para la preservación de los activos de información y la continuidad del negocio.

En cuanto a las tecnologías defensivas, se resaltan estrategias sumamente creativas e innovadoras, como usar el esfuerzo del hacker para descubrir los vectores y las técnicas de ataque, para simular, descubrir las vulnerabilidades y corregirlas, hacer uso de Security Hardening Checklist, para mejorar la seguridad del entorno, también implementar medidas de seguridad en cada capa del Modelo OSI, en el caso del MPFN, es posible realizar un análisis forense para detectar cómo accedió el hacker a la red o al sistema.

Anexo 6

Guía de Observación

Entidad	:	Ministerio Público
Ubicación	:	Av. Abancay Cdra 5 (Sede Central en Lima)
Dependencia	:	Oficina General de Tecnología de la Información
Observador	:	Ricardo Richard Huamantingo Navarro

Descripción del proceso observado, cuyos personajes principales son tres colaboradores del área de TI, dentro de la unidad de estudio, que es la unidad de Seguridad de la Información:

Previo al proceso de interés se procede a describir como se reporta un incidente de seguridad, es decir un fallo en el sistema que podría ser una vulnerabilidad no detectada, los usuarios o el área usuaria que maneja un determinado sistema o varios módulos de información, observa que su sistema tiene algunas deficiencias que pueden ser en la conexión, en la carga de datos, en la visualización de los reportes, fallos de autenticación, entre otros, el usuario reporta dicha incidencia a la oficina de soporte, estos verifican, evalúan y validan dicho incidente, si no encuentran la solución, escalan a quien corresponda, ya sea a la oficina de redes y comunicaciones, a la oficina de sistemas o al personal de seguridad, suponiendo que este último es a quien le corresponde dar solución, el Oficial de Seguridad evalúa el nivel y riesgo de dicho incidente, prioriza dentro de las actividades pendientes y asigna al personal que atenderá y dará solución, otro actividad se da cuando un usuario trae su propio equipo informático y quiere conectarse a la red de la entidad, en este caso el personal de seguridad hace un escaneo de dicho equipo para descartar posibles amenazas procedentes desde ese punto de conexión.

Se manejan un nivel de base mínimo que viene a ser el tema que se conoce como el checklist de verificación de seguridad o "hardening" que incluye las mejores prácticas en cuanto a configuración, junto al modelo de madurez de OWASP. Se manejan niveles, en el de mayor importancia, que vendría a ser las cosas que ya se publican a internet directamente con información confidencial que sale a internet con medidas de seguridad, ya se hace una verificación técnica y un análisis de vulnerabilidades, entonces no todo pasa por un análisis de

vulnerabilidades, solo las aplicaciones más importantes. Por el mismo hecho de que toma tiempo el análisis de vulnerabilidades, no es tan común y es bastante exigente, por lo que generalmente se busca que se solucione, se hace una verificación documental en otros niveles, que situaciones de bajo riesgo prefieren que se solucionen con un control documental antes de salir a producción. Las aplicaciones, una vez en producción, se ejecuta el análisis de vulnerabilidades y hacen uso de la herramienta Owasp Zap. Hay dos tipos de análisis que se suele hacer, uno que realiza el Analista de Seguridad, que es sobre servidores y uno que realiza el Oficial de Seguridad, que es sobre aplicaciones, el analista tiene acceso al servidor por lo que es más fácil ejecutar los scripts y el oficial no, por eso usa la caja gris y tiene que solicitar que le habiliten el usuario, para ejecutar el análisis de vulnerabilidades.

Ahora bien, como miembro de seguridad el Oficial de Seguridad tiene acceso a todos los controles y también sabe cómo funcionan, también cuando hace la prueba de penetración aprovecha que sabe las costumbres de los desarrolladores, para que reconozca en qué falla y alinearse de acuerdo a eso, ya que es probable que encuentre algo (por las malas prácticas de los desarrolladores que salen a la luz), los desarrolladores suelen utilizar un framework, debido a ello es poco probable que se encuentre un SQL injection, pero, porque usan un framework son muy confiados en otro tipo de ataque, los framework son de otros proveedores con una base ya establecida. El oficial de Seguridad aprovecha la confianza que tienen de los frameworks para explotar la vulnerabilidad, al hacer una prueba de penetración.

Normalmente cuando se hace pentesting o prueba de penetración, se trabaja con caja gris, todas las aplicaciones piden usuario y contraseña, entonces se solicita acceso e inicia a explorar la aplicación con la herramienta de escaneo, que de forma automática registra los errores comunes, por ejemplo: se detecta un tema de directorio, se detecta una posible dirección de IP, se detecta faltas de etiquetas, etc., entonces se procede a hacer un descarte o una verificación manual a partir del reporte. Algunas veces generan alertas pero no es transcendente, se puede hacer un cross site script pero no está publicado a internet entonces es interno por lo tanto no es transcendente. Cuando hay una verificación, a partir del reporte de la herramienta se manda a que las revisen, ya

que ahí encuentran algunas pautas. Luego se sigue el tema de la prueba de penetración donde se hace uso de las credenciales de usuario brindado, se hace la prueba como si fuese un usuario y comienza a hacer las transacciones y se observa que mensajes envía el formulario, que se está recibiendo y se trata de manipular, si la herramienta alerta un tema de SQL injection, se trata de explotar eso, generalmente lo que se trata de probar son los accesos en la elevación de privilegios, robo de sesión, que pasa si la sesión es manipulada, como se comporta si se manipula el token de sesión y si permite pasar a la sesión de otra persona. A veces como usuario se puede ingresar a un formulario y con otro usuario no, ¿qué pasa con ese usuario que no puede ingresar, envía directamente una solicitud de acceso a ese formulario?. Entonces todo eso son pruebas que no son una falla de la aplicación en sí, sino del desarrollador, por descuidos en la forma de programar, manejo de variables, manejo de la configuración de la aplicación, entre otros.

Conclusión de la Observación

En conclusión, la unidad de Seguridad de la Información, a través del Oficial de Seguridad y los Analistas de Seguridad, realizan un análisis de vulnerabilidades solo a las aplicaciones más importantes y que tendrán acceso remoto, según su nivel de riesgo o la exigencia del área usuaria en tener disponible el servicio, cabe mencionar que hay muchas aplicaciones que manejan información fiscal; este análisis de vulnerabilidades que suelen realizar no es un proceso ya establecido con lineamientos que deben seguir, sino más bien es a criterio del profesional de seguridad, que con su experiencia y conocimientos del tema ejecutan dicho análisis, con una previa evaluación de riesgos. Uno de los motivos por los que no se suele ejecutar un análisis de vulnerabilidades, es por el tiempo que demanda y la carencia de algunos recursos, mas no de conocimientos. Un punto a resaltar es que llevan a cabo pruebas de penetración o pentesting, las cuales sirven para explotar las vulnerabilidades identificadas, esto se debe integrar como parte fundamental en el modelo para el análisis de vulnerabilidades.

Anexo 7

Ficha de Análisis Documental

Entidad	:	Ministerio Público
Ubicación	:	Av. Abancay Cdra 5 (Sede Central en Lima)
Dependencia	:	Oficina Central de Tecnología de la Información
Observador	:	Ing. Ricardo Richard Huamantingo Navarro

El ministerio público, cuenta con la Oficina de Sistemas, que pertenece a la Oficina Central de Tecnología de la Información, dicha oficina se encarga del manejo, mantenimiento, seguimiento y desarrollo de los sistemas de información que se usan en todas las otras dependencias a nivel nacional, a la actualidad se cuenta con 105 sistemas en producción, las cuales son accedidas vía intranet e internet; asimismo en los POIs, que ahora fueron remplazados por el Plan de Gobierno Digital 2021 – 2023, se ve reflejado la programación de las actividades y proyectos informáticos, en ellos figuran el desarrollo y puesta en producción de múltiples sistemas de información a lo largo del año, pero en estos proyectos no se refleja la intención de realizar un análisis de vulnerabilidades luego de la integración y puesta en producción de dichos sistemas; el análisis de vulnerabilidades debería incluirse en cada nueva integración de sistemas, ya que cuando un sistema pasa de la fase de desarrollo a producción, trae consigo muchas vulnerabilidades tanto para sí mismo como para los demás sistemas y toda la arquitectura en general, cabe rescatar que hay un gran interés en mantener actualizado los servicios, ya que se programa la adquisición de licencias y parches de software.

El análisis documental permitió identificar la programación de proyectos de Análisis de Vulnerabilidades dentro de los proyectos informáticos, los cuales tienen un costo en promedio de S/. 170,000.00 Nuevos Soles, tal como figura en el POI, que tras finalizar dicho proyecto se tiene como producto final, el informe de riesgos mitigados, también figura que esta actividad beneficia a más de 18,000 usuarios entre Personal Fiscal y Administrativo a nivel nacional, en resumen, este análisis de vulnerabilidades involucra personal externo, recursos adicionales y presupuesto para poder llevarse a cabo. También se registra el inventario de softwares con los que se cuenta, ahí se observa aplicaciones para la seguridad.

Mediante las auditorías externas que se desarrollan de dos formas, una sobre el modelo de gestión y la otra con respecto a los controles que se realizan en pro del Sistema de Gestión de Seguridad de la Información, la auditoria sirve como una pre-certificación, en dicha documentación se observa que la gestión de vulnerabilidades está en inicios y se debe mejorar en los reportes para poder aumentar el nivel de madurez.

Conclusión del Análisis Documental

En conclusión, la entidad a través de la Oficina de Sistemas, seguirán desarrollando e implementando más sistemas de información, claro que un sistema puede ser desarrollado teniendo en cuenta medidas de seguridad pero a pesar de ello las vulnerabilidades siguen presentes e incluso surgen otras nuevas, al integrase el sistema desarrollado con la arquitectura tecnológica en general, es por ello que es sumamente necesario planificar un análisis de vulnerabilidades tras la integración o la puesta en producción de un nuevo sistema; con un modelo propio acorde a las necesidades de una entidad pública, permitiría ejecutarse mediante el personal de seguridad de la información, sin la necesidad de ser gestionado como proyecto una vez aprobado como parte de las actividades y funciones del área, esto reduciría los costos que demanda los proyectos.

Un punto importante identificado, tras el análisis documental, son los informes de vulnerabilidades mitigadas, este mismo debería incluirse como una subcategoría emergente dentro de la categoría de metodología, debido a lo esencial que resulta para el siguiente proceso de análisis, asimismo se rescata la intención de adquirir licencias, parches y software actualizado (nuevas versiones), tanto para el área de Tecnologías de Información en general, así como, para las área usuarias, esto como parte de las tecnologías defensivas. También se detectó, por las auditorías, que la gestión de vulnerabilidades es bastante inmaduro todavía, se debería aumentar las puntuaciones y mejorar los reportes. A pesar de tener mapeados los procesos dentro del MPFN, el cual sirve para la implementación del Sistema de Gestión de Seguridad de la Información.

Anexo 8

PROYECTOS INFORMÁTICOS 2017

N°3

I. Denominación del Proyecto:
Proyecto de Análisis de Vulnerabilidades anualizado

II. Datos Generales:

2.1Unidad Ejecutora	:	Oficina Central de Tecnologías de la Información
2.2Duración	:	12 meses / Abril -Dic 2017
2.3Costo Total	:	S/. 170,000.00Nuevos Soles

III. Del Proyecto:

3.1 Descripción del Proyecto:
El presente proyecto permitirá identificar, corregir y monitorear los controles de seguridad técnicos para mitigar los riesgos y vulnerabilidades identificadas.

3.2 Objetivo del Proyecto:
Identificar las vulnerabilidades tecnológicas que son explotables por los atacantes internos/externos al MPFN.

IV. Meta Anual:
Contar con una infraestructura tecnológica segura que permita mantener los niveles necesarios de confidencialidad, integridad y disponibilidad de la información administrada por el MPFN.

MINISTERIO PÚBLICO V°B° MG. JOEL E. VALDIVIA BACIGALUPI O.C.T.I.

V. Cobertura de Acción:
Institucional

VI. Áreas Involucradas:
Oficina Central de Tecnologías de la Información.

VII. Productos Finales:
Informe de Riesgos mitigados

Usuarios de Productos Finales:
Personal Fiscal y Administrativo del ámbito nacional. (Aprox. 18,000 beneficiarios)

Anexo 9

I. Denominación de la actividad o proyecto 1
Sistema de Carpeta Electrónica Administrativa (CEA).

Descripción del proyecto:
Implementar un Sistema de Tramite Documentario con documentos electrónicos, Software de Firma Digital y Flujo de Trabajo.

TIPO DE ORIENTACIÓN: Orientado a la Gestión Interna

II. Datos Generales
2.1 Unidad Ejecutora: Oficina de Sistemas de la OCTI
2.2 Duración: Fecha: Inicio 01/01/2018 Fecha Fin: 31/12/2018
2.3 Costo Total: S/. 579 000,00

III. Del proyecto

3.1 Descripción de la Actividad/proyecto:
Implementar un Sistema de Tramite Documentario con documentos electrónicos, Software de Firma Digital y Flujo de Trabajo.

3.2 Objetivos de la actividad/proyecto:
Reducción de los costos asociados al uso de papel, suministros y equipos de impresión; reducción de los tiempos en el acceso a los documentos.

IV. Meta Anual: 100%

V. Cobertura de Acción: Nacional.

VI. Instituciones Involucradas: Ministerio Público - Fiscalía de ña Nación.

VII. Productos Finales:
- 14 órganos administrativos con sistema implementado
- 33 Distritos Fiscales con sistema administrativo implementado.

VIII. Usuarios de Productos Finales
Personal Fiscal, Personal Administrativo y personal de Medicina Legal a nivel nacional.

I. Denominación de la actividad o proyecto 2
Implementación de la Carpeta Electrónica Fiscal Civil - En el marco del Proyecto EJE-CFE

Descripción del proyecto:
Implementar un sistema que permita impulsar el proyecto Cero Papel en el Proceso Contencioso-Administrativo.

TIPO DE ORIENTACIÓN: Orientado a la Gestión Interna.

II. Datos Generales
2.1 Unidad Ejecutora: Oficina de Sistemas de la OCTI
2.2 Duración: Fecha Inicio: 01/01/2018 Fecha Fin: 30/06/2018
2.3 Costo Total: S/. 120 000,00

III. Del proyecto

3.1 Descripción de la Actividad/proyecto:
Implementar un sistema que permita impulsar el proyecto Cero Papel en el Proceso Contencioso-Administrativo.

3.2 Objetivos de la actividad/proyecto:
Implementación de la Carpeta Electrónica Fiscal Civil

IV. Meta Anual: 100%

V. Cobertura de Acción: Distritos Fiscales de Lima Sur y Callao.

VI. Instituciones Involucradas: Ministerio Público - Fiscalía de la Nación.

VII. Productos Finales: Dos (02) Distritos Fiscales implementados (Lila Sur y el Callao).

VIII. Usuarios de Productos Finales: Personal Fiscal, Personal Administrativo y personal de Medicina Legal.

Anexo 10

- **Sistema de Gestión de Seguridad de la Información.** Busca preservar la confidencialidad, integridad y disponibilidad de la información aplicando un proceso de gestión de riesgos, manteniendo alineación estrategia institucional.

f) Marco Normativo

Criterio	Documento
Comité de Seguridad de la Información	Conformado con la RGG N 1305-2013-MP-FN-GG, siendo presidente el Gerente General y participante Secretaría General
Oficial de Seguridad de la Información	RFN N° 3283-2015-MP-FN
Política de Seguridad de la Información	Aprobado con la RFN 2895-2017-MP-FN
Metodología de Gestión de Riesgos de Seguridad de la Información	Aprobada con la RGG N° 0781-2018-MP-FN-GG
Procedimiento de Gestión de Incidentes de Seguridad de la Información	Aprobado con la RGG N° 0863-2019-MP-FN-GG-
Comité Operativo del Seguridad de la Información	Definidos en la Metodología de Gestión de Riesgos de Seguridad de la Información
Plan de Tratamiento de Riesgos	Aprobado y comunicado con Oficio N° 1810-2017-MP-FN-GG y actualizado con Oficio N° 994-2019- MP-FN-GG
Plan de Recuperación de los Servicios de TI	RGG N° 1084-2017-MP-FN-GG
Auditorías Internas	Carta S/N Prisertec
Análisis de vulnerabilidad	Carta S/N Kunak

g) Gestión del Riesgo.

En el marco de la gestión del riesgo de seguridad de la información, se realiza seguimiento a 81 escenarios de riesgos agrupados en 19 categorías.

N°	Categoría de escenario de riesgo	Nivel de riesgo
1	Toma de decisión en la inversión de TI, definición del portafolio y mantenimiento	Importante
2	Toma de decisiones de inversión en TI	Importante
3	Incidentes en la infraestructura operacional de TI	Importante
4	Problemas con la adopción y uso de Software	Importante
5	Incidentes relacionados con el Hardware	Importante
6	Incidentes relacionados con los proveedores y cadena de suministros	Importante
7	No cumplimiento	Importante
8	Programa y ciclo de vida de la gestión del proyecto	Moderado
9	Acción Industrial	Importante
10	Innovación basada en tecnología	Importante
11	Gestión del dato e información	Importante
12	Pericia, habilidades y comportamiento de TI	Moderado
13	Acciones no autorizadas	Moderado

I. Denominación del proyecto		**Código**	**PROY-012-21**
Implementación del Sistema de Gestión de Seguridad de la Información			
1.1 Justificación:			
El Ministerio Público recolecta, genera y proporciona información que tiene un alto impacto en el proyecto de vida de las personas.			
1.2 Tipo de Orientación:			
Orientado a la Gestión Interna			
1.3 Prioridad:			
Alta			
II. Datos Generales			
2.1 Unidad Ejecutora:			
OGTI - Seguridad de la Información			
2.2 Duración:			
Fecha de inicio	Ene - 2021	Fecha de culminación	Dic - 2023
2.3 Costo Total:			
S/ 900,000.00			
2.4 Fuente de Financiamiento[1]:			
R.O			
III. Del proyecto			
3.1 Descripción:			
La información fluye en los procesos de la institución para conseguir los objetivos del proceso e institucional, pero se encuentra afectada por una serie de riesgos conocidos como los riesgos de seguridad de la información, por lo que para gestionar tales riesgos se utiliza la NTP 27001:2014 que es de obligatoria aplicación, generando un modelo de gestión con responsabilidades definidas.			
3.2 Finalidad:			
Los procesos del Ministerio Público y los servicios que proporciona tratan información integra y disponible de acuerdo a su nivel de acceso.			
IV. Meta Anual			
Si bien el SGSI es un ciclo de mejora continua, la parte que se considera proyecto es la de identificación de riesgos: 2021:100% 2022: 40% 2023: 60%			
V. Cobertura de Acción			
Nivel nacional			
VI. Instituciones involucradas			
Ministerio Público - Fiscalía de la Nación			
VII. Productos Finales			
Tener integrado el Gobierno de Seguridad de la Información como parte del Gobierno Institucional.			
VIII. Usuarios de Productos Finales			
Personal Fiscal, Personal Administrativo y personal de Medicina Legal a nivel nacional.			

(1) Sujeto a cambios producto de la estrategia institucional del momento.

Anexo 11

Propuesta de Investigación

La propuesta en cuestión fue desarrollada, con la finalidad de estandarizar el proceso de análisis de vulnerabilidades, para reducir la probabilidad de ataques exitosos y mitigar las amenazas, de esta forma se tendrá sistemas y arquitecturas tecnológicas más seguras, dentro de una entidad pública, cabe mencionar que, en el marco teórico de la presente investigación es parte de la propuesta, en donde se detalla cada una de las fases (categorías y sub categorías) que se debe seguir en este modelo.

Componentes del modelo

En la investigación se determinaron y validaron los componentes necesarios para un modelo óptimo, funcional, práctico, flexible y adaptable, estos son:

- Gestión de vulnerabilidades
- Metodología para el análisis
- Tecnologías defensivas

Gestión de vulnerabilidades

Con miras a una posible política gubernamental de divulgación de vulnerabilidades, se incluye en el modelo para estar alineados a estándares internacionales; esta gestión se desagrega en: Descubrimiento, informes, priorización y respuesta, los mismos que se detallan en el Marco Teórico, para que este modelo sea más efectivo y a medida, según la realidad de cada entidad, se debe incluir las tecnologías emergentes, señalados en los resultados y discusión.

Metodología para el análisis

Aquí definimos los principales e importantes aspectos que se deben hacer necesariamente, que son: Acuerdo de confidencialidad, recolección de información, análisis interior y/o análisis exterior, según sea el alcance del análisis de vulnerabilidades; cabe mencionar que todo este proceso se debe mantener de forma confidencial y sin afectar, ni comprometer los servicios y accesos a la red normal del usuario, los dos últimos aspectos manejan el análisis de vulnerabilidades, tal cual, es donde se usa la herramienta y se hace el escaneo de vulnerabilidades, tiene su propia secuencia de pasos, todo ello se menciona con

mayor precisión en el marco teórico de la investigación, de igual forma tener en cuenta las sub categorías emergentes.

Tecnologías defensivas

Cuando se descubra las vulnerabilidades, no basta con saber cuáles son, más por el contrario se debe dar solución a dichas vulnerabilidades, luego de esto, se debe implementar estrategias defensivas, que están definidas en estos sub componentes: Seguridad en red, que cubre todas las técnicas, estrategias y herramientas para proteger y mantener segura la red; Administración en la defensa, los directivos deben de entender el propósito del proceso y brindar el apoyo necesario para la implementación de las estrategias de seguridad requeridas en toda le entidad; y otro aspecto importante es la Concienciación de usuarios, ya que estos son el eslabón más débil de la seguridad, por ello se debe difundir una cultura de seguridad institucional, en el cual estén involucrados todos los usuarios sin distinción. Considerar implementar medidas de seguridad en cada capa del modelo OSI y hacer uso del esfuerzo del hacker, para determinar del vector de ataque e identificar las técnicas de hackeo o el modus operandi, para poder armar la estrategia defensiva ideal.

Estos tres pilares del modelo para el análisis de vulnerabilidades trabajan en conjunto, siendo la gestión de vulnerabilidades transversal a todo el proceso, además todo esto en conjunto, valga la redundancia, es un proceso cíclico y se debe ejecutar de forma periódica según la disponibilidad de recursos, lo ideal es llevar a cabo de forma trimestral o cada vez que haya un cambio significativo. También es importante mencionar, si la entidad tiene algún otro modelo o metodología para el análisis de vulnerabilidades, este modelo no reemplaza ni queda relegado, más por el contrario se adapta y funciona a la par; de igual manera, este modelo ayuda a mejorar el nivel de madurez de la gestión de vulnerabilidades y la seguridad en general, colaborando con el Sistema de Gestión de Seguridad de la Información, la ciberseguridad y con la norma ISO 27001.

Figura 9

Esquema del modelo para el análisis de vulneravilidades digitales.