FACULTAD DE INGENIERÍA

Carrera de Ingeniería Informática y de Sistemas

CONTROLES DEL CENTRO DE SEGURIDAD DE INTERNET PARA LA DEFENSA CIBERNÉTICA QUE MINIMIZAN LAS VULNERABILIDADES

Tesis para optar el Título Profesional de Ingeniero Informático y de Sistemas

ROGER ALONSO PAREDES GUTIERREZ
(0000-0001-7417-3084)

FERNANDO DAVID PEREZ VALENCIA
(0000-0003-2654-9205)

Asesor:
Mg. DANIEL JESUS DIAZ ARENAS
(0000-0001-8617-0745)

Lima - Perú
2022

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

AGRADECIMIENTO

En agradecimiento a Dios Elohim. A cada uno de nuestros familiares quienes son pilares fundamentales en nuestras vidas. A nuestros amigos por apoyarnos y darnos fuerzas. A nuestros profesores y nuestro asesor de tesis quienes fueron guías esenciales en el desarrollo y culminación de esta nueva meta profesional.

DEDICATORIA

Este trabajo está dedicado a mis amigos quienes dieron su apoyo en realizar esta investigación, a mi familia, en especial a mi abuelo Eleuterio Joaquin Paredes Huarcaya y a mi abuela Elvira Villagaray Berrocal, quien se encuentra descansando en la gloria del Creador. Ellos han sido los pilares fundamentales de apoyo a la obtención de este logro profesional.

Roger Alonso Paredes Gutierrez

La presente tesis lo dedico principalmente a mi padre Juan Fernando Pérez Cárdenas, aunque ya no se encuentre en este mundo sé que desde el cielo me estará guiando y acompañando, gracias por tu paciencia y sacrificio. De igual manera dedico este trabajo a mi madre Rosario Quijandria y a mi hermana Brenda Pérez, quienes con su cariño y apoyo incondicional me han permitido llegar a cumplir una de mis metas profesionales.

Fernando David Pérez Valencia

RESUMEN EJECUTIVO

Esta investigación consiste en encontrar brechas de seguridad en el dominio público de cualquier entidad. Dicha información se encuentra públicamente en el alcance a todo usuario que navega en el Internet.

El método de la investigación se resume en que el tipo de investigación es aplicada. Por consecuente, el nivel de investigación es descriptivo con el fin de identificar el estado actual del acceso a la información pública de alguna entidad. A la vez, el enfoque de investigación es cualitativo ya que nos permite analizar y recabar los resultados obtenidos de la encuesta realizada a los ex-empleados de una entidad aleatoria. Por último, el diseño de la investigación será no experimental debido a que no se realizará manipulación de la información sensible disponible del dominio público de alguna entidad.

Se realizó un análisis en el dominio público de una entidad usando las herramientas de la fase Reconocimiento del Hacking Ético: DNSdumpster, Whois, Google Hacking. Dichas herramientas no realizan intrusión de fuerza bruta al sistema del dominio público. Gracias a ello, se tomó la decisión de aplicar los Controles de Seguridad de Internet (CIS) debido a que proponen una serie de estrategias específicas para cada tipo de vulnerabilidad encontrada en el dominio público de cualquier entidad.

Esperamos que esta investigación pueda ser de utilidad para los lectores con la finalidad de exponer la importancia de la seguridad informática.

Palabras clave: Hacking Ético, Control de Seguridad de Internet, ciberataque, ciberdefensa, CIS, hacker, DNSdumpster, Whois, Google Hacking

ABSTRACT

This investigation consists in finding security gaps in the public domain of any entity. This information is publicly available to all users who browse the Internet.

The research method is summarized in that the type of research is applied. Consequently, the level of investigation is descriptive to identify the current state of access to public information of some entity. At the same time, the research approach is qualitative since it allows us to analyze and collect the results obtained from the survey of former employees of a random entity. Finally, the design of the research will be non-experimental because there will be no manipulation of the sensitive information available in the public domain of any entity.

An analysis was carried out in the public domain of an entity using the tools of the Recognition of Ethical Hacking phase: DNSdumpster, Whois, Google Hacking. Such tools do not perform brute force intrusion into the public domain system. Thanks to this, the decision was made to apply Internet Security Controls (CIS) because they propose a series of specific strategies for each type of vulnerability found in the public domain of any entity.

We hope that this research can be useful for readers to expose the importance of computer security.

Keywords: Ethical Hacking, Internet Security Control, cyber-attack, cyber defense, CIS, hacker, DNSdumpster, Whois, Google Hacking

ESTADO DEL ARTE

Para la presente investigación, se han usado diversas fuentes que nos ayudarán a obtener los primeros acercamientos e indicios de la investigación. Asimismo, dichas fuentes se han usado como ayuda para entender de una mejor manera los términos de nuestro tema y como estos se relacionan. Por ello, se ha citado información de autores que han investigado de temas con relación al nuestro, lo cual, ayuda a aterrizar las ideas propuestas por el equipo de trabajo y esto permita al lector entender a profundidad la investigación realizada.

Según Roberto Hernández-Sampieri, en su libro denominado "Metodología de la Investigación" (2014), nos menciona que, en el desarrollo de una investigación cualitativa la hipótesis se va generando durante el proceso, se afina conforme se solicita más información, se modifica según los resultados y no se prueban estadísticamente (p.p. 357). Se entiende que estas hipótesis son supuestos basados en hechos conocidos y se pueden utilizar luego de culminar la investigación (p.p. 355). De tal manera, dicho texto nos ayuda a establecer que la hipótesis juega un papel diferente en la investigación cualitativa, ya que no se formula antes de integrar al desarrollo de la investigación, ni comienza luego de la recopilación de datos, sino se determina a medida que se recopilen y analicen más datos.

A la vez, un reporte de Redscan, llamado "NIST NVD ANALYSIS 2020", nos indica que el año 2020 se registró una mayor cantidad de vulnerabilidades a comparación de otros años, con un total de 18,103 vulnerabilidades. La tasa de cambio se refleja en el número de vulnerabilidades graves y de alta gravedad en 2020 (10,342 vulnerabilidades registradas) más que el número total de vulnerabilidades registradas en 2010 (4,639, incluidas bajas, medias, altas y graves). Esto nos demuestra la importancia de la seguridad informática visto que, si bien el aumento de nuevas vulnerabilidades es preocupante, esto es coherente con el creciente

número de dispositivos, productos y servicios digitales conectados en red que se utilizan en todo el mundo. Este crecimiento también puede atribuirse al aumento en el número de Autoridades de Numeración CVE (CNA), de las cuales más de 150 están autorizadas para crear y publicar vulnerabilidades y exposiciones comunes en todo el mundo.

Adicionando, un artículo de Felipe Daragon, llamado “Comb: The Big Password Leak” (2021), Brasil es el país con mayor número de filtraciones de registros entre los países de América Latina, con 68,535 direcciones de correo electrónico con contraseñas pertenecientes al dominio (.gov.br). Sin embargo, en Perú (.gob.pe) cuenta 6.038 contraseñas filtradas. Esto nos sirve como referencia para iniciar la investigación, porque existen herramientas como DnsDumpster, WhoIs y Google Hacking, que pueden detectar brechas de seguridad en el dominio público de cualquier entidad, donde podrían exponer información sensible de alguna entidad, empleados, etc.

Otro texto que nos será de mucha utilidad es el boletín publicado por Fortinet "Threat Intelligence Insider" (2021), en el texto establece que en el tercer trimestre del 2021 en Perú se registraron más de 31.098.216 de virus informáticos, 38.203.791 actividades de *botnets*, 3.307.661.256 de explotaciones de vulnerabilidades. Siendo las vulnerabilidades de ejecución de código remoto relacionadas a servidores “Apache”, las más detectadas con un 50.5% del total de las explotaciones de vulnerabilidades en este tercer trimestre del 2021, en Perú. Dicho texto, aporta a la investigación demostrando los diversos tipos de vulnerabilidades y sistemas que están activamente apuntando hacia Perú, donde los más recurrentes son los ataques de explotación de vulnerabilidades a servidores “Apache”. Esto último, hace énfasis porque en el dominio público de entidades tanto privadas como públicas, utilizan diversos servicios donde de no estar correctamente actualizados, las entidades podrían exponerse a múltiples tipos de vulnerabilidades.

Por otro lado, Bashar Shamma, en su tesis para optar la Maestría en Ciencias de la Seguridad del Sistema de Información de la Universidad de Houston, titulada "Implementing CIS Critical Security Controls for Organizations on a low-budget." (2018), nos indica que el enfoque de los controles CIS se centran en la capacidad de la organización para prevenir y detener ataques antes de que estos se declaren como incidentes. Los controles de CIS no se centran en proporcionar pautas detalladas para la detección, mitigación o respuesta de incidentes, sino que brindan pautas para reducir el número de incidentes al evitar infracciones y explotaciones contra la organización. Aunque existen otros marcos de seguridad desarrollados como la Organización Internacional de Normalización (ISO). Sin embargo, estos marcos requieren un gran esfuerzo para implementar y comprender a causa de la amplia gama de controles que proporcionan estos marcos. Debido a esto, nos ayuda a establecer el uso de los controles CIS puesto que éstos fueron diseñados para proporcionar a las organizaciones una menor cantidad de controles procesables para obtener resultados de seguridad efectivos, inmediatos y de alto impacto; demostrando que los controles CIS sean adecuados para cualquier organización. Esto nos demuestra que los controles CIS se pueden aplicar a cualquier tipo de entidad tanto privada como pública para poder reducir las vulnerabilidades presentes en sus dominios públicos. A su vez, nos indica que los ciberataques son cada vez más fáciles y baratos de llevar a cabo, estos ataques afectan el funcionamiento de una organización en todos los sectores, y que el riesgo potencial de una amenaza cibernética en cualquier organización es inevitable, pero las vulnerabilidades se pueden reducir significativamente mediante la implementación de controles de seguridad que eventualmente pueden conducir a una disminución del riesgo. Esta investigación nos demuestra la importancia de la seguridad informática dentro de cualquier organización.

A su vez, Vishwas Kaup Vijayananda, en su tesis para optar la Maestría en Ciencias en Sistemas de Información de la Universidad del Estado de Iowa, titulada "Implementing

CIS Cybersecurity Controls for the Department of Residence, Iowa State University.” (2018), nos indica que al implementar algunos controles del marco de seguridad CIS, se pudo cumplir con los objetivos financieros y de seguridad del proyecto, logrando reducir los costos de TI innecesarios e invertir el dinero restante en otros usos para la organización. Esto nos demuestra la efectividad de la implementación de los controles del CIS. También nos advierte que las amenazas cibernéticas se volverán más difíciles en los próximos años debidos que los ataques evolucionan y se vuelven más sofisticados, pero seguir prácticas seguras como los controles CIS ayudarán a cualquier organización a defenderse de estos ataques.

Por último, según Javier Paolo Paredes Lopez, en su tesis para obtener el título de Ingeniero de Sistemas Empresariales de la Universidad Científica del Sur, titulado “Modelo de Seguridad de Informática Perimetral para reducir los Riesgos de Ataques al RENIEC.” (2015), afirma que los ataques informáticos enfocados en las empresas, orientado en un nivel de Estado Peruano, generarían una mala reputación a la seguridad que se tiene de las entidades estatales hacia la población de usuarios de sus servicios web”. En el caso de la entidad RENIEC, nos aconseja que, con la finalidad de reforzar la seguridad perimetral, la entidad requiere ser monitoreado por especialistas de seguridad informática en todo momento, ya que constantemente se realizan ataques informáticos en la que acceden a información confidencial donde se encuentran los servidores o interrumpir el fluido y el servicio que se brinda con la denegación por ataques DDoS. A su vez, los métodos de ataque van evolucionando, transcurriendo el tiempo. La investigación que realiza el autor nos demuestra la importancia de revisar los casos de ataques informáticos dentro del dominio público de cualquier entidad.

INTRODUCCIÓN

El tema del presente trabajo o proyecto de investigación consiste en identificar las brechas de seguridad mediante los conceptos esenciales del hacking ético o *Ethical Hacking* en el cual consiste en una penetración controlada en los sistemas informáticos de una empresa, de la misma forma que lo haría un hacker o pirata informático, pero de forma ética y con previa autorización. Adicionalmente, se identificará las estrategias de Seguridad de Información según el criterio de los Controles de Seguridad para la Defensa Cibernética aprobados por el CIS (El Centro de Seguridad de Internet).

El objetivo principal es identificar las estrategias de Seguridad de Información según el criterio de los Controles de Seguridad para la Defensa Cibernética aprobados por el CIS (El Centro de Seguridad de Internet) con el fin de subsanar las brechas de seguridad.

Por este motivo es de vital importancia usar los conceptos del hacking ético para identificar vulnerabilidades dentro del dominio público de cualquier entidad, tanto privada como pública. Por esta razón, la información representa un papel muy importante dentro de cualquiera institución pues es la parte más primordial y continuamente se encuentra expuesta a sufrir modificaciones y en muchos casos a ser robada en su totalidad, es por ello la importancia de asegurar dicha información.

Por tal razón se expone a continuación una investigación que nos permitirá identificar a tiempo las vulnerabilidades existentes, brindar posibles soluciones para tratar de asegurar los servicios y por ende conseguir beneficiar a cualquier entidad, logrando brindar unos servicios seguros y de calidad especialmente a nivel de transmisión de información dentro de su base de datos.

CAPÍTULO I

REVISIÓN DE LA LITERATURA

1.1. Problema de investigación

1.1.1. Planteamiento del problema

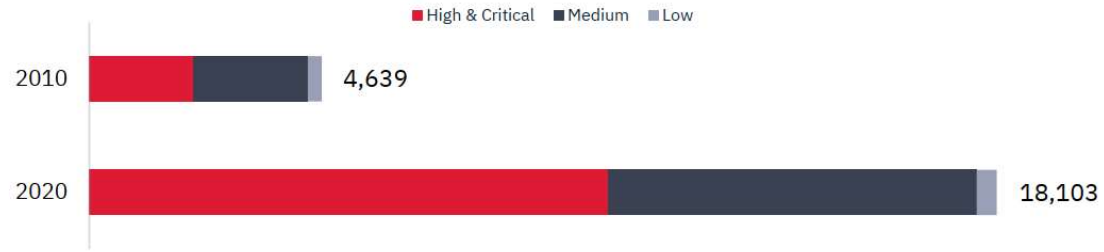
Según Herrera, J. (2021), “en marzo de 2020 la Organización Mundial de la Salud categorizó de pandemia la infección SARS-COV2 que originó la enfermedad COVID-19, para afrontar este contexto en el Perú a nivel educativo se implementó el trabajo remoto”. Sin embargo, tuvieron incidencia en el accionar de los cibercriminales. Como, por ejemplo, en el último informe de análisis de vulnerabilidades de Redscan (2021), revela que el año 2020 se reportaron 18.103 vulnerabilidades, donde en su mayoría (10.342) fueron clasificadas como de alta severidad o crítica. Además, las vulnerabilidades críticas y de alta severidad reportadas en el 2020 superaron en número a la suma total de vulnerabilidades reportadas en 2010 (ver Figura 1 y 2).

Figura 1
Número de Vulnerabilidades y exposiciones comunes (CVEs) por año: 1995-2020

Fuente: Redscan (2021)

Figura 2

Número de Vulnerabilidades y exposiciones comunes (CVEs) del 2010 en comparación con 2020



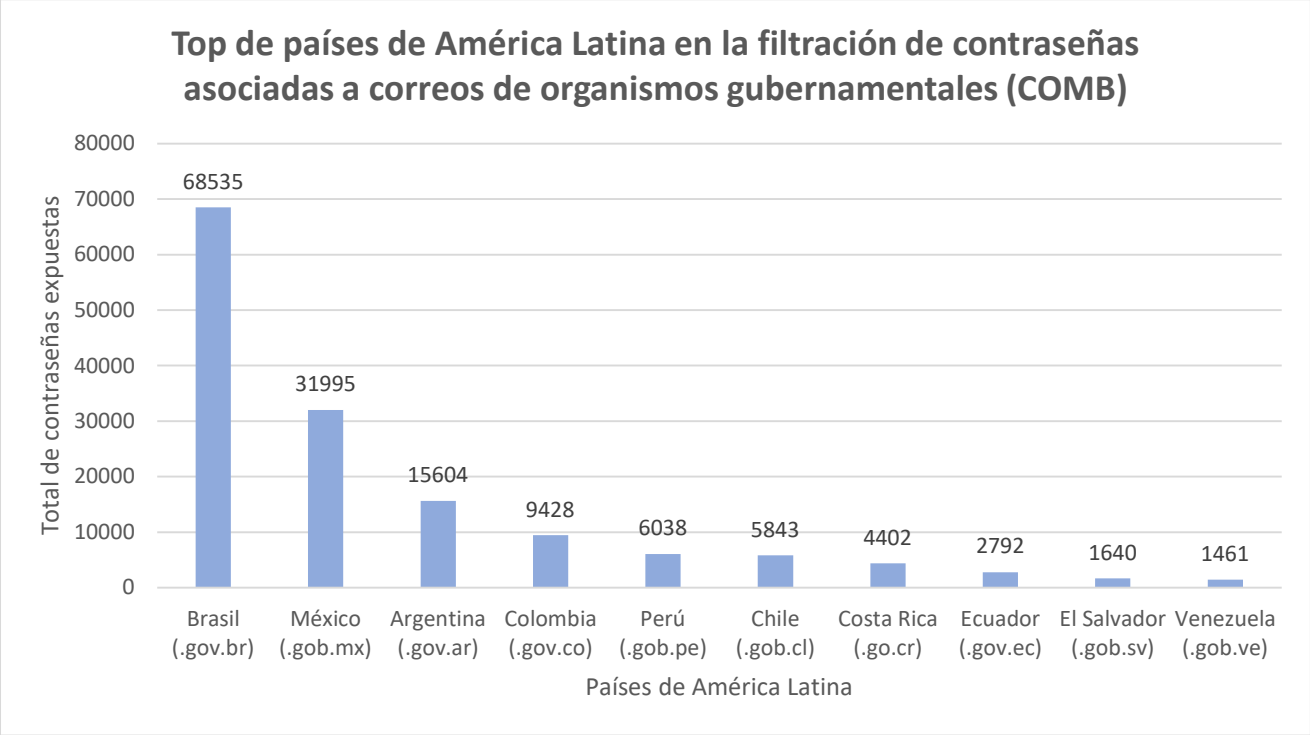
Fuente: Redscan (2021)

En una encuesta realizada por ESET Latinoamérica, se observó que el 42% de los usuarios en América Latina consideró que la empresa para la que trabaja no estaba preparada en cuanto a equipamiento y conocimiento de seguridad para hacer teletrabajo durante la pandemia según Harán (2020).

El 02 de febrero del 2021, se registró una filtración llamada COMB, donde se publicaron más de 3 millones de contraseñas asociadas a correos de organismos gubernamentales, donde varios organismos de países de América Latina forman parte de esta exposición según Meyer (2021). Brasil es el país de Latinoamérica que registra los mayores números con 68.535 contraseñas pertenecientes a direcciones de correo con el dominio (.gov.br), seguido por México con 31.995 con el dominio (.gob.mx), Argentina (.gov.ar) con 15.604, Colombia (.gov.co) con 9.428, Perú (.gob.pe) con 6.038, Chile (.gob.cl) con 5.843, Costa Rica (.go.cr) con 4.402, Ecuador (.gov.ec) con 2.792, El Salvador (.gob.sv) con 1.640 y Venezuela (.gob.ve) con 1.461 según Daragon (2021), ver Tabla 1.

Tabla 1

Top de países de América Latina en la filtración de contraseñas asociadas a correos de organismos gubernamentales (COMB) publicado el 02 de febrero del 2021



Fuente: Elaboración propia basado en Daragon (2021)

Una encuesta de Kaspersky indica que un 47% de empresas latinas usa tecnología obsoleta dentro de su infraestructura de TI, donde entre las razones para no actualizar la tecnología se destaca: la incompatibilidad con las aplicaciones desarrolladas internamente (49% de los encuestados), la resistencia de los empleados a trabajar con las nuevas versiones de *software* (47% de los encuestados), las tecnologías eran propiedad de los miembros de la junta directiva (39% de los encuestados), y que la empresa carecía de los recursos necesarios para actualizar todo a la vez (13% de los encuestados) según Diazgranados (2021).

Del 13 al 14 de noviembre del 2020, el grupo internacional de hackers Anonymous deshabilitó varios sitios del Gobierno debido al estallido de protestas a nivel nacional por la crisis política del gobierno de Manuel Merino según RPP (2020). Los sitios web del estado afectados por este ciberataque destacan: Congreso, Policía Nacional, Instituto Geográfico Nacional del Perú, Embajada de Perú en España, Comando Conjunto de las Fuerzas

Armadas, SUNAT, Tribunal Constitucional, Ministerio de Trabajo y Empleo, Gobierno Regional de Tumbes, intranet del Gobierno regional de Amazonas, Ministerio de Economía y Finanzas, etc.

Según Paredes (2015), se analizó a nivel interno y externo los principales problemas informáticos dentro de la entidad RENIEC como, por ejemplo:

> "casos de inyección de código malicioso, o la inundación de paquetes al servidor donde la generación de muchas conexiones al mismo tiempo ocasionara el colapso del servicio, o también el escaneo de vulnerabilidades, donde individuos no autorizados pueden usar para explotar y amenazar la confidencialidad, integridad y disponibilidad de este. Según los datos analizados, se sugiere elaborar un equipo de trabajo de monitoreadores especializados en seguridad informática, cubriendo las 24 horas del día y los 7 días de la semana, donde su labor será supervisar la continua conectividad de los servicios brindados por RENIEC, el cual se viene realizando ante cualquier ataque web, teniendo en cuenta que los mismo se están produciendo con mucha mayor fuerza en estos últimos años, tomando como referencia desde la creación del colectivo Anonymous, mediante sus amenazas y hechos ya realizado."

Viendo estos antecedentes, el enfoque de este proyecto a continuación se elaborará en base a las vulnerabilidades dentro del dominio público de cualquier entidad tanto pública como privada.

1.1.2. Formulación del problema

El problema general es:

"¿Cómo serán las estrategias de Seguridad de Información según el criterio de los Controles de Seguridad para la Defensa Cibernética aprobados por el CIS (El Centro de Seguridad de Internet) para subsanar las brechas de seguridad en el dominio público de una entidad?"

Por ello, en los problemas específicos tenemos:

- **Problema específico 1:** ¿Cuáles son las brechas de seguridad presentes en el dominio público de una entidad?
- **Problema específico 2:** ¿Cuáles son los Controles de Seguridad para la Defensa Cibernética aprobados por el CIS (El Centro de Seguridad de Internet) que permitan subsanar las brechas de seguridad que se encuentra en el dominio público de una entidad?

1.1.3. Justificación de la investigación

Según PricewaterhouseCoopers (2018) nos hace referencia: "Todos hemos oído hablar de la importancia de la seguridad informática y cómo esta asume un rol principal cada vez que se discuten innovaciones tecnológicas o aspectos de la era digital". (pág. 8). Esto se evidencia con la gráfica del último informe de análisis de vulnerabilidades de Redscan (2021) (Figura 1) indicándonos que desde 1995 hasta el 2020 se han ido incrementando el número de vulnerabilidades y exposiciones comunes (CVEs) mientras se crean nuevas innovaciones tecnológicas cada año.

En base a lo identificado por la plataforma *Threat Intelligence Insider Latin America* de Fortinet (2021), herramienta que recopila y analiza incidentes de ciberseguridad en varios

países, nos muestra que en el tercer trimestre del 2021 en Perú se registraron más de 31.098.216 de virus informáticos, 38.203.791 actividades de *botnets*, 3.307.661.256 de explotaciones de vulnerabilidades, siendo las vulnerabilidades de ejecución de código remoto relacionadas a servidores Apache las más detectadas con un 50.5% del total de las explotaciones de vulnerabilidades en este tercer trimestre del 2021 en Perú. Por ello, en esta investigación queremos exponer la importancia de la seguridad informática y cuáles son las consecuencias de no aplicarlo en esta era digital en la que nosotros vivimos.

En el desarrollo de investigación, se analizó la primera fase de hacking ético en una entidad aleatoria donde se observó las brechas de seguridad en información sensible expuesta en dominios público. Estas brechas pueden ser subsanadas mediante ciertos controles del Centro de Seguridad de Internet (CIS) y según el criterio como avance la investigación se tomará la decisión de elegir qué controles pueden mitigar las brechas existentes de seguridad en el dominio público de cualquier entidad privada como pública.

Con esta investigación se espera incrementar el interés del personal de cualquier entidad por las medidas actuales de ciberseguridad, cómo afrontar los desafíos a futuro de la ciberseguridad y fomentar el uso de los controles de la ciberseguridad del CIS en las entidades públicas y privadas.

1.2. Marco referencial

1.2.1. Antecedentes

1.2.1.1. Estudios o proyectos previos vinculados a nivel internacional

- En el año 2017, Hareesh Reddy Eemani elaboró una investigación titulada "*Analyzing, Implementing and Monitoring Critical Security Controls: A Case Implemented in J & B Group* - Análisis, implementación y monitoreo de controles de seguridad críticos: un caso implementado en J & B Group" (Tesis para optar la Maestría en Ciencias en Aseguramiento de la Información) de la Universidad Estatal St. Cloud.

  El objetivo general de esta investigación fue, presentar un enfoque sistemático para realizar análisis mediante la recopilación de datos, la implementación y el seguimiento de los controles de seguridad críticos, que garantice una postura de seguridad sólida para defenderse de los ciberataques con recursos mínimos y *software* de código abierto.

  El tipo de investigación fue una combinación de métodos de investigación utilizados en este artículo, mientras que parte de la investigación se basa en trabajos previos de otros (investigación aplicada) y cierta experimentación, experiencia y enseñanza se utilizan para analizar o corroborar los hallazgos (investigación pura).

  Esta investigación tuvo un tamaño poblacional donde el método principal de investigación fue a través de la web para identificar los últimos controles de seguridad, *software* de código abierto y herramientas de implementación y monitoreo. En segundo lugar, se preparó un cuestionario / plantilla estructurada con los controles de seguridad identificados y tres preguntas básicas para cada subcontrol asociado con el control. En tercer lugar, los datos recopilados se analizaron para seleccionar el control de seguridad crítico para la implementación. En cuarto lugar, el *software* de

código abierto se selecciona y se implementa en el entorno. Por último, la experiencia laboral del autor en seguridad de la información se utilizó para desarrollar reglas con lógica incorporada para correlacionar los datos con la inteligencia de indicadores de compromiso, inicios de sesión fallidos, etc.

Las conclusiones en esta investigación fueron que, con el aumento de virus, gusanos y robo de identidad, la implementación de controles de seguridad ya no es una opción, las organizaciones se están encontrando así mismas la implementación de seguridad con un costo mínimo, siguiendo este proceso descrito en este estudio, las empresas pueden mejorar la seguridad de sus sistemas y datos. Sin embargo, el nivel de detalle requerido diferirá de una organización a otra y se basará en sus niveles de riesgo.

Esta investigación nos permite que, dependiendo de los niveles de riesgo detectados en una entidad u empresa, influenciará la implementación de controles de seguridad CIS, debido que el nivel de detalle requerido diferirá de cada organización.

- En el año 2014, Sigwadi Wendy realizó la investigación titulada "*The Adoption and use of Ethical Hacking to Secure Information in Small Companies* - La adopción y el uso del hacking ético para proteger la información en pequeñas empresas" (Tesis para optar la licenciatura en Tecnología en TI: Redes de comunicación) de la Universidad Walter Sisulu.

  El objetivo general de esta investigación fue, investigar la influencia del hacking ético en las pequeñas empresas, para averiguar si la implementación del hacking ético en sus empresas ayudará a proteger la información confidencial de los ataques a la seguridad de la información.

  El tipo de investigación emplea un enfoque tanto cualitativo como cuantitativo para mejorar su confiabilidad. Los datos para esta investigación se recopilaron en forma de datos primarios y secundarios. Los datos primarios generalmente se recopilan

mediante entrevistas semiestructuradas y los datos secundarios representan publicaciones internas proporcionadas por los participantes al investigador y datos disponibles públicamente que son relevantes para el tema que se está observando.

Esta investigación tuvo un tamaño poblacional formado por cinco pequeñas empresas alrededor del este de Londres. La Muestra de esta investigación es de cinco gerentes, uno de cada una de las cinco pequeñas empresas y empleados de Administración, Marketing, Ventas, Diseño técnico y gráfico.

Las conclusiones en esta investigación fueron que, los hallazgos de este proyecto han demostrado que el hacking ético puede mejorar la eficiencia de una empresa y que las pequeñas empresas no tienen un conocimiento completo sobre el hacking ético y cómo pueden beneficiarse de su uso. Por lo tanto, esta medida de seguridad debe darse a examinar a las empresas para que puedan explotar sus beneficios, por lo que existe la necesidad de identificar mecanismos para promover esta medida de seguridad entre las pequeñas y las grandes empresas.

Esta investigación permite la adopción del hacking ético para ayudar a abordar los problemas de seguridad actuales a los que se enfrentan dentro de las empresas. El hacking ético puede proporcionar a las empresas una mejor protección de datos y productividad, lo que les permite ser más competitivas.

- En el año 2018, Vishwas Kaup Vijayananda realizó una investigación titulada "*Implementing CIS Cybersecurity Controls for the Department of Residence, Iowa State University* - Implementación de controles de ciberseguridad de CIS para el Departamento de Residencia de la Universidad Estatal de Iowa" (Tesis para optar la Maestría en Ciencias en Sistemas de Información) de la Universidad del Estado de Iowa.

El objetivo general de esta investigación fue, implementar un marco de seguridad para todo el departamento para reducir los riesgos y vulnerabilidades planteados a la infraestructura.

Esta investigación tuvo un tamaño poblacional de los diversos marcos reconocidos por la industria informática para la implementación un marco de seguridad para todo el departamento, donde: NIST Cybersecurity Framework, IS0 27001, COBIT-5 y CIS Security Controls fueron opciones diferentes que se tomaron en consideración. Aunque estos marcos tenían muchos conceptos en común, tenían sus propias formas de abordar el problema.

Las conclusiones en esta investigación fueron que, después de comparaciones y análisis cuidadosos, se decidió por el Marco de seguridad de CIS para implementar la seguridad en todo el Departamento. El marco de seguridad de CIS permitió identificar y reducir los gastos innecesarios para satisfacer las necesidades comerciales generales del Departamento.

Esta investigación nos permite que además de ser una de las formas más efectivas de crear seguridad en una infraestructura, el marco de seguridad CIS cuenta con un panorama de amenazas actual, y la facilidad de implementación.

1.2.1.2. Estudios o proyectos previos vinculados a nivel nacional

- En el año 2015, Aguilar Portilla Sergio Steven & De la Cruz Ramos Velky Gobel realizó la investigación titulada “Implementación de una Solución de Hacking Ético para mejorar la Seguridad en la Infraestructura Informática de la Caja Municipal de Sullana - Agencia Chimbote” (Tesis para optar el título profesional de Ingeniero de Sistemas e Informática) de la Universidad Nacional del Santa.

El objetivo general de esta investigación fue, “mejorar la seguridad en la Infraestructura Informática de la Caja Municipal de Sullana - Agencia Chimbote a través de la implementación de una Solución de Hacking Ético”.

“El Diseño de Investigación a Utilizar será de preprueba-posprueba” y se desarrolla a través del “método experimental que consistirá en 7 fases, con el fin de realizar una investigación más completa y precisa” de las cuales son:

- **1° Fase:** “Estudio bibliográfico sobre Hacking Ético, Seguridad informática, Infraestructura Informática y Servicios Financieros”.
- **2° Fase:** “Recopilación y análisis de la información obtenida de la Caja Municipal de Sullana - Agencia Chimbote”.
- **3° Fase:** “Análisis de la Infraestructura Informática de la empresa utilizando la metodología de Hacking”.
- **4° Fase:** “Diseño de la Solución de Hacking Ético para la infraestructura informática de la empresa”.
- **5° Fase:** “Implementación de la Solución de Hacking Ético para la infraestructura informática de la empresa”.
- **6° Fase:** “Realización de Pruebas a fin de lograr la contrastación de la Hipótesis”.
- **7° Fase:** “Desarrollo del Informe de Resultados Finales”.

Esta investigación tuvo un tamaño poblacional formado por “la infraestructura informática de la Caja Municipal de Sullana - Agencia Chimbote que está constituida por 20 Computadoras de Escritorio y 02 Servidores”. “La Muestra la constituirá el área de préstamos que comprende a 05 computadoras y los 02 servidores”.

Las conclusiones en esta investigación fueron que, “la implementación de la Solución de Hacking Ético mejora a seguridad en la Infraestructura Informática de la Caja

Municipal de Sullana - Agencia Chimbote, ya que se adelanta a posibles fallas o problemas de seguridad, previniendo desarrollar controles de seguridad con lo cual optimizan los sistemas físicos y lógicos de la entidad".

Esta investigación permite la obtención de la justificación de la implementación de una solución de hacking ético dentro de una infraestructura informática y gracias a ello, mejora la seguridad dentro de la transferencia de datos.

- En el año 2017, Bermeo Oyola Jean Carlos realizó la investigación titulada "Implementación de Hacking ético para la detección y evaluación de vulnerabilidades de red en la empresa Complex del Perú S.A.C." (Tesis para optar el grado académico de Maestro en Ingeniería de Sistemas con mención en Tecnología de Información y Comunicación) de la Universidad Católica Los Ángeles de Chimbote.

  El objetivo general de esta investigación fue, "realizar la Implementación de Hacking Ético, en la Empresa Complex del Perú S.A.C; para ayudar en la detección y evaluación de vulnerabilidades de Red".

  El tipo de investigación es cuantitativa y se desarrolla a través del método no experimental, debido a que "se basa fundamentalmente en la observación de fenómenos tal y como se dan en su contexto natural para después analizarlos" puesto que no manipula deliberadamente las variables.

  Esta investigación tuvo un tamaño poblacional formado por "24 trabajadores, que tienen relación directa con el tema de investigación sobre el manejo de la red". La Muestra de esta investigación "ha tomado la misma cantidad de la población que es 24 trabajadores, por lo tanto, no se ha realizado ninguna técnica de selección de muestreo".

  Las conclusiones en esta investigación fueron que, "se ha logrado realizar la Implementación de Hacking Ético, en la Empresa Complex del Perú S.A.C y se ha

realizado el análisis, utilizando herramientas tecnológicas de seguridad, de la actual red de datos en la empresa; por lo que se ha evaluado los problemas de vulnerabilidad a los que se encuentra expuesta la red".

Esta investigación permite la obtención de la justificación de la implementación de hacking ético en una empresa y formular una propuesta tecnológica de seguridad, teniendo como antecedente el análisis de las herramientas tecnológicas de seguridad, al detectarse posibles vulnerabilidades en la red de datos de una empresa.

1.2.1.3. Información relevante referente al contexto actual

- "Sistemas biométricos, el nuevo blanco de los ataques a instituciones financieras" (Rojas, 2019):

  Dado que los delincuentes buscan continuamente formas de derrotar las salvaguardias antifraude, intentan sustituir la huella digital real del sistema por una falsa o por los existentes robadas de la PC de otra persona.

  Este tipo de ataque muestra que los delincuentes tienen un conocimiento profundo de cómo funcionan los sistemas bancarios internos y es un verdadero desafío protegerse contra tales ataques. La mejor opción es utilizar siempre la autenticación multifactorial.

  La biometría debería resolver muchos problemas asociados con la autenticación de dos factores, pero la práctica ha demostrado que puede que no sea tan simple. Durante el año 2019, se han identificado varios casos que indican que la tecnología biométrica aún está lejos de ser perfecta.

  Ya ha habido varios ataques de prueba de concepto que utilizan datos biométricos para eludir los controles de seguridad, pero estos ataques aún podrían contrarrestarse con actualizaciones del sistema.

- “Los cinco ciberataques más frecuentes en el Perú” (Gestión, 2020):

  El Perú fue un punto fijo para los ciberdelincuentes debido a que fue objetivo de 613 millones de intentos de ciberataque desde inicio del año 2020 hasta junio del mismo año. Dicha modalidad se lo describe como “fuerza bruta” en la que significa la cantidad de intentos repetidos y sistemáticos con el fin de obtener el acceso de un sistema.

  Los ciberataques más detectados que afectaron a los usuarios fueron:

  1. **SSH.Connection.Brute.Force** (Fortiguard, 2021) indica la detección de un intento de ataque de fuerza bruta en SSH.

     “El ataque consiste en múltiples solicitudes SSH destinadas a realizar un inicio de sesión SSH de fuerza bruta, lanzado a una velocidad de aproximadamente 200 veces en 10 segundos”.
  2. **SMB.Login.Brute.Force** (Fortiguard, 2021) indica una detección de al menos 500 inicios de sesión fallidos en un minuto, lo que “señala un posible ataque de fuerza bruta en el sistema operativo de Microsoft Windows”.
  3. **W32/Bancos.CFR!tr** (Fortiguard, 2021) está clasificado como un troyano.

     “Sus actividades comúnmente incluyen establecer conexiones de acceso remoto, capturar la entrada del teclado, recopilar información del sistema, descargar/cargar archivos, colocar otro programa maligno en el sistema infectado, realizar ataques de denegación de servicio (DoS) y ejecutar/finalizar procesos.”
  4. **W32/Tibs.PACKED!tr** (Fortinet, 2021) está clasificado como un troyano, un tipo de malware que realiza actividades sin el conocimiento del usuario. Por ejemplo, “el establecimiento de conexiones de acceso remoto, capturar la entrada del teclado, recopilar información del sistema, descargar/cargar

archivos, colocar otro programa maligno en el sistema infectado, realizar ataques de denegación de servicio (DoS) y ejecutar/finalizar procesos."

5. **W32/Generic_PUA_MC.FXK** (Fortiguard, 2021) se clasifica como un infector de archivos. "Un infector de archivos es un tipo de programa maligno que tiene la capacidad de propagarse al adjuntar su código a otros programas o archivos."

- "Ciberdelincuentes hackearon el sistema del bono universal y robaron casi un millón de soles" (Grupo Electrodata, 2020):

  Un grupo de ciberdelincuentes reemplazaron las identidades de cientos de peruanos ingresando los datos personales señalados en el DNI. Estos fueron inscritos con distintos números telefónicos para conseguir la clave de seguridad que es enviada por el Banco de la Nación a través de un mensaje de texto. Luego retiraron el bono en los cajeros automáticos, donde no se requiere el DNI físico.

  Este estándar ha sido utilizado para la remuneración de los recursos públicos en el otorgamiento de las distintas contribuciones que creó el Gobierno en medio de la pandemia por el coronavirus, como el Bono Universal Familiar a través de la página web "https://bfu.gob.pe/", que es administrado por la RENIEC. En ella, se clasifica a los peruanos que han sido seleccionados para recibir el bono y comenzar los trámites de retiro en línea.

  Estos ciberdelincuentes identificaron que el sistema de la página web mostraba algunas vulnerabilidades "en el registro Capcha". Tras analizar el sistema informático, se identificaron tres puntos vulnerables:

  1. El primer error es un tema técnico, debido a que se encuentra mal programado el sistema.

2. El segundo error encontrado se localiza en el diseño del proceso, es una condición muy débil que te indica: te voy a entregar el dinero si me dices cuales son los datos personales (DNI, la fecha de emisión del documento y el nombre de los padres) que están registrados en la RENIEC.
3. Por último, el número telefónico ingresado al sistema debe estar relacionado al beneficiario del bono. Sin embargo, se ha demostrado que al ingresar cualquier número se puede realizar el cobro del bono.

Los ciberdelincuentes crearon un programa automatizado de comparación de datos de la RENIEC que obtuvieron y fueron convocando en 5 mil registros para identificar a los beneficiarios. Después de conseguir los números de DNI, averiguaban los datos personales como la fecha de expedición del documento y los nombres de los padres de los beneficiarios, es decir, los datos necesarios que el sistema web demandaba. Con el fin de recibir el mensaje de texto de confirmación, ingresaron el número telefónico de su preferencia.

- "Anonymous hackeó la web del Congreso de Perú tras la fuerte represión a las protestas por la destitución del presidente Vizcarra" (Infobae, 2020):

  Los ataques cibernéticos comenzaron en la noche del viernes 13 de noviembre del 2020 debido a la fuerte represión entre la Policía Nacional de Perú y la masiva manifestación acontecida el jueves 12 de noviembre del 2020 en el centro de Lima contra el gobierno de Manuel Arturo Merino de Lama quien asumió el Poder Ejecutivo después de que el Parlamento destituyó al mandatario Martín Alberto Vizcarra Cornejo el lunes 9 de noviembre del 2020.

  Dichos ataques dejaron sin funcionamiento el sitio web oficial del Congreso durante varias horas, pese a los intentos sin éxito de sus administradores para activarlo lo más pronto.

1.2.2. Marco teórico

Para este proyecto, se utilizó los conceptos de: seguridad informática, hacking ético, Google Hacking, metodología de hacking ético. En adición, una breve descripción de los protocolos simples para la gestión de redes junto con las herramientas necesarias de hacking ético. Finalizando con el estudio general de los controles del CIS.

1.2.2.1. Seguridad Informática

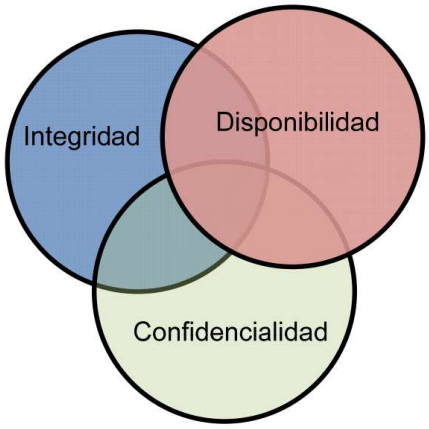
Según Tyas, A. (2021), la Seguridad Informática es la práctica de proteger la información mitigando los riesgos de la información. Esta forma parte de la gestión de riesgos de la información. Por lo general, implica prevenir o al menos reducir la probabilidad de acceso no autorizado / inadecuado a los datos, o el uso ilegal, divulgación, interrupción, eliminación, corrupción, modificación, inspección, registro o devaluación de la información.

Según Jara & Pacheco (2012, p.p. 17), indica que "si consultamos la norma ISO/IEC 27.001, esta nos dice que la seguridad de la información es aquella disciplina que tiene por objeto preservar la confidencialidad, integridad y disponibilidad de la información" (ver Figura 3); "y que puede involucrar otras propiedades, como la autenticidad, la responsabilidad o *accountability*, el no repudio y la trazabilidad."

- La **confidencialidad** se refiere a proteger la información para que no acceda a ella personas no autorizadas. En otras palabras, solo las personas que están autorizadas a hacerlo pueden acceder a datos sensibles.
- La **integridad** se refiere a garantizar la autenticidad de la información: que la información no se altere y que la fuente de la información sea genuina.
- La **disponibilidad** significa que los usuarios autorizados pueden acceder a la información.

- La **autenticidad** es el acto de probar una afirmación, como la identidad de un usuario de un sistema informático.
- La **responsabilidad** significa que cada individuo que trabaja con un sistema de información debe tener responsabilidades específicas para asegurar la información.
- El **no repudio** significa mantener un registro de todas las cosas realizadas en una red.
- La **trazabilidad** certifica todas las acciones (sea de operaciones, consultas o modificaciones de la información) que realiza cada usuario y rastrea únicamente hasta dicho usuario.

Figura 3
Principios de seguridad informática



Fuente: Baltazar, J. & Campuzano, J. (2011)

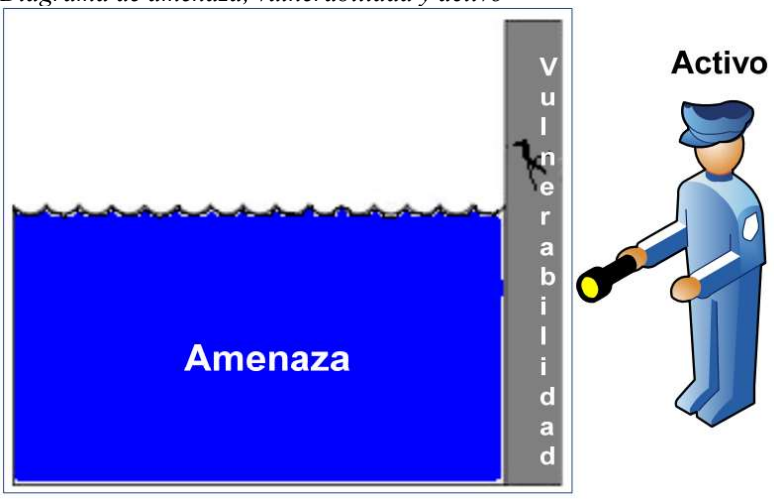
Por otro lado, Jara & Pacheco (2012, p.p. 26) nos dicen que "finalmente, no podemos dejar de conocer a qué nos referimos cuando hablamos de los siguientes conceptos: activos de información, vulnerabilidades, amenazas" (ver Figura 4), riesgos, no repudio, y controles, contramedidas o salvaguardas.

- Los **activos de información** son cualquier dato, dispositivo u otro componente del entorno que respalda actividades relacionadas con la información. Los activos generalmente incluyen *hardware*, *software* e información confidencial.

- La **vulnerabilidad** es una debilidad que puede ser aprovechada por un actor de amenazas, como un atacante, para realizar acciones no autorizadas dentro de un sistema informático.
- La **amenaza** es un acto malintencionado que tiene como objetivo corromper o robar datos o interrumpir los sistemas de una organización o toda la organización. La amenaza presenta cuatro tipos básicos de operación (ver Figura 5):
    - La interrupción se debe a la obstrucción de cualquier tipo durante el proceso de comunicación entre uno o más sistemas.
    - La intercepción consiste en que los datos o mensajes enviados por el remitente son interceptados por una persona no autorizada donde el mensaje será cambiado a una forma diferente o será utilizado por la persona para su proceso malicioso. Entonces la confidencialidad del mensaje se pierde en este tipo de ataque.
    - La modificación consiste en que el mensaje enviado por el remitente es modificado y enviado al destino por un usuario no autorizado. Este tipo de ataque pierde la integridad del mensaje.
    - La fabricación consiste en que un usuario no autorizado inserta un mensaje falso en la red como si fuera un usuario válido. Esto resulta en la pérdida de confidencialidad, autenticidad e integridad del mensaje.

Figura 4

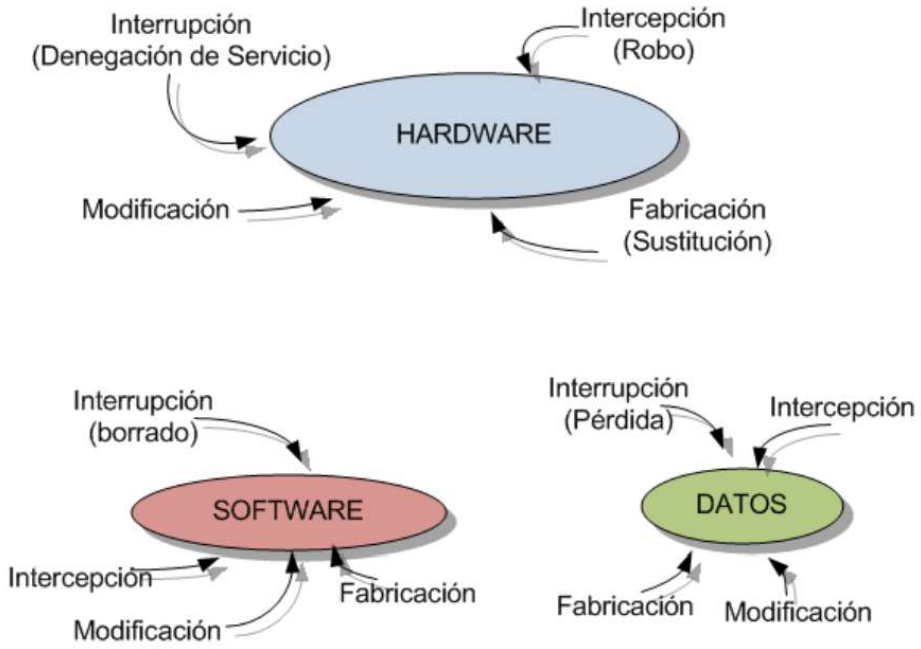
Diagrama de amenaza, vulnerabilidad y activo



Fuente: Baltazar, J. & Campuzano, J. (2011)

- El **riesgo** comprende los impactos para una organización y sus partes interesadas que podrían ocurrir debido a las amenazas y vulnerabilidades asociadas con la operación y uso de los sistemas de información y los entornos en los que operan los sistemas. Una fórmula común utilizada para describir el riesgo es: Riesgo = Amenaza x Vulnerabilidad x Consecuencia. Sin embargo, la primera parte de la fórmula del riesgo, Riesgo = Amenaza x Vulnerabilidad, también se puede considerar como probabilidad.
- El **no repudio** se refiere a un servicio que da prueba del origen de los datos y la integridad de los datos.
- Los **controles** son medidas tomadas para reducir los riesgos de seguridad de la información, como violaciones de los sistemas de información, robo de datos y cambios no autorizados en la información o los sistemas digitales.

Figura 5
Vulnerabilidades de los sistemas de cómputo



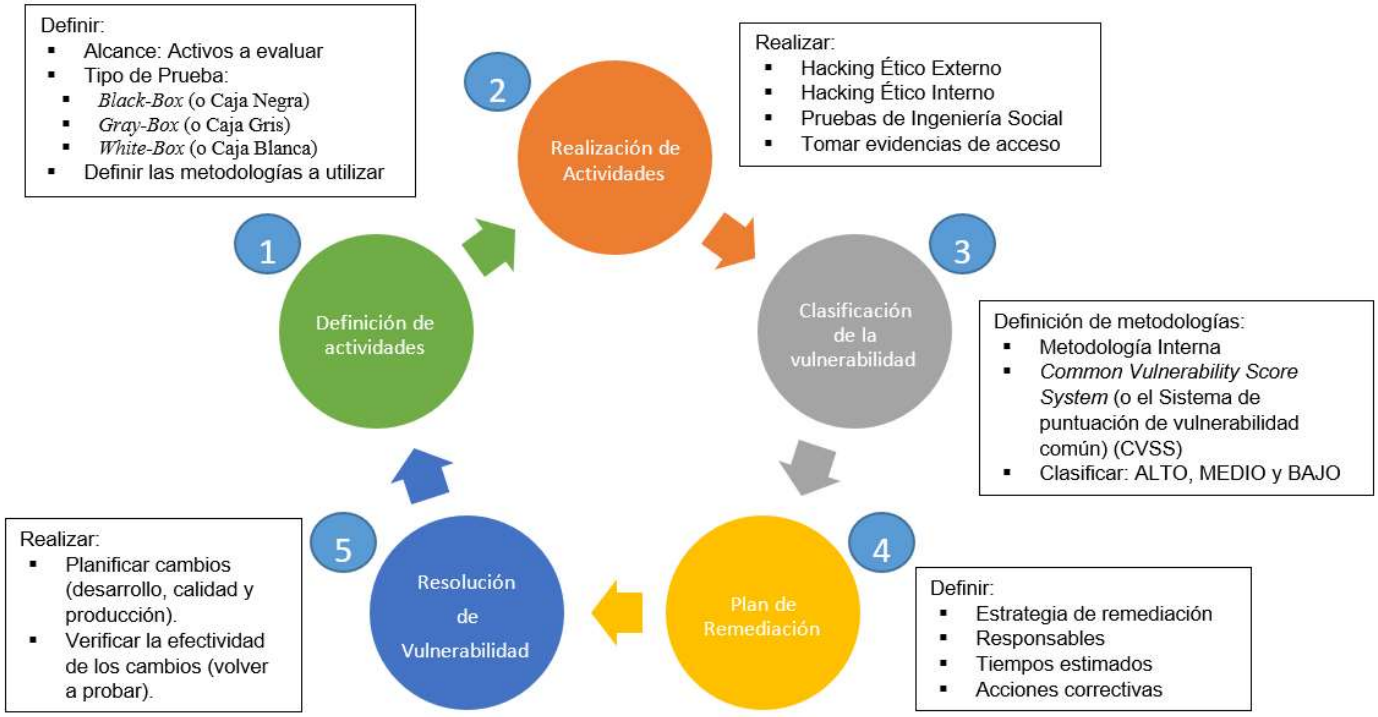
Fuente: Baltazar, J. & Campuzano, J. (2011)

1.2.2.2. Hacking Ético

Según GreyCampus (2021), *Ethical Hacking* o Hacking Ético, a veces llamado *Penetration Testing* o Prueba de Penetración, es un acto de intrusión / penetración en el sistema o las redes para descubrir amenazas, vulnerabilidades en sistemas que un atacante malintencionado puede encontrar y explotar, causando pérdida de datos, pérdidas financieras u otros daños importantes. El propósito del hacking ético es mejorar la seguridad de la red o los sistemas mediante la reparación de las vulnerabilidades encontradas durante las pruebas. Los hackers éticos pueden utilizar los mismos métodos y herramientas utilizados por los hackers malintencionados, pero con el permiso de la persona autorizada con el fin de mejorar la seguridad y defender los sistemas de los ataques de usuarios malintencionados (ver Figura 6).

Se espera que los *hackers* éticos entreguen un informe a la persona autorizada de todas las vulnerabilidades y debilidades encontradas durante el proceso.

Figura 6
Ciclo de vida de un Hacking Ético



Fuente: Palomino, O. (2018)

1.2.2.2.1. Tipos de Hackers

- ***Black hat* (o Hacker de sombrero negro) o crackers** es un hacker informático que viola la seguridad informática para beneficio personal o malicia, según Kaspersky (2021).
- ***White hat* (o Hacker de sombrero blanco)** es un experto, que se especializa en pruebas de penetración y en otras metodologías de prueba que garantizan la seguridad de los sistemas de información de una organización, según Kaspersky (2021).
- ***Grey hat* (o Hacker de sombrero gris)** es un hacker informático o un experto en seguridad informática que a veces puede violar las leyes o los estándares éticos

típicos, pero no tiene la intención maliciosa típica de un pirata informático de sombrero negro, según Kaspersky (2021).

1.2.2.2.2. Tipos de Pruebas de Penetración

Según U.S. DOI (2021), los *pentesting* (o pruebas de penetración) es una simulación de ataque controlado que ayuda a identificar la susceptibilidad a las infracciones de las aplicaciones, la red y el sistema operativo. La prueba se realiza para identificar ambas debilidades (también conocidas como vulnerabilidades), incluida la posibilidad de que partes no autorizadas obtengan acceso a las características y datos del sistema, así como las fortalezas, permitiendo un riesgo total evaluación para ser completada. Las estrategias incluyen:

- Las **pruebas de penetración interna** continúan la evaluación al ayudar a identificar qué tan lejos un atacante puede moverse lateralmente a través de una red una vez que se ha producido una infracción externa. Durante una prueba de penetración interna, el *tester* aprovechará la caja explotada de una prueba de penetración externa o utilizará una caja de prueba o una laptop en el interior de la red para realizar la evaluación. Usar una caja de prueba o una laptop es el método preferido, ya que a menudo es una ruta de prueba más estable que ejecutar herramientas a través del activo externo explotado.
- Las **pruebas de penetración externa** es una práctica que evalúa los activos externos de una organización. Durante una prueba de penetración externa, el *tester* intenta ingresar a la red interna aprovechando las vulnerabilidades descubiertas en los activos externos. Alternativamente, el *tester* puede intentar obtener acceso a datos privilegiados a través de activos externos como correo electrónico, sitios web y archivos compartidos.

- La **prueba de penetración ciega** imita un ciberataque real, además de que la empresa lo ha autorizado. La información proporcionada es limitada y el hacker ético tiene que averiguar la mayor parte de la información de la empresa.
- La **prueba de doble penetración ciega** es similar a la prueba de penetración a ciegas, aparte de que hay alguien en la organización que está al tanto de la actividad en curso. La prueba se realiza para comparar qué tan rápido y efectivo el equipo de seguridad está interesado en monitorear o responder y prepara a la empresa para un posible ataque real.

1.2.2.2.3. Modalidades de Hacking Ético

Según Poston, H. (2020):

- En una asignación de **prueba de caja negra (o *Black-Box testing*)**, el *tester* de penetración se coloca en el papel de un hacker promedio, sin conocimiento interno del sistema de destino. Los *testers* no reciben ningún diagrama de arquitectura o código fuente que no esté disponible públicamente. Una prueba de penetración de caja negra clasifica las vulnerabilidades en un sistema que se pueden explotar desde fuera de la red.
- Dentro de una asignación de **prueba de caja gris (o *Gray-Box testing*)**, el *tester* tiene los niveles de acceso y conocimiento de un usuario, potencialmente con privilegios elevados en un sistema. Los *testers* de penetración de caja gris suelen tener algún conocimiento de los componentes internos de una red, lo que puede incluir documentación de diseño y arquitectura y una cuenta interna de la red.
- Las **pruebas de caja blanca (o *White-Box testing*)** tienen varios nombres diferentes, que incluyen pruebas de caja transparente, caja abierta, auxiliares y controladas por lógica. Cae en el extremo opuesto del espectro de las pruebas de caja negra: los *testers*

de penetración tienen acceso completo al código fuente, la documentación de la arquitectura, etc. El principal desafío con las pruebas de caja blanca es examinar la enorme cantidad de datos disponibles para identificar los posibles puntos débiles, lo que la convierte en el tipo de prueba de penetración que requiere más tiempo.

1.2.2.2.4. Fases del Hacking Ético

Según Romero, G. (2019) indica que hay principalmente 5 fases en *hacking*, conocido también como el círculo del *hacking* (ver Figura 7):

1.2.2.2.4.1. Reconocimiento

Es la fase preparatoria en la que se recopila la mayor cantidad de información posible sobre el objetivo. Por lo general, recopila información sobre tres grupos (red, *host* y personas involucradas).

Existe dos tipos de reconocimiento:

- Activa: interactuar directamente con el objetivo para recopilar información sobre el objetivo.
- Pasiva: intentar recopilar la información sobre el objetivo sin acceder directamente al objetivo. Esto implica recopilar información de las redes sociales, sitios web públicos, etc.

1.2.2.2.4.2. Escaneo (Exploración)

Están involucrados tres tipos de escaneo:

- Escaneo de puertos: esta fase implica escanear el objetivo en busca de información como puertos abiertos, sistemas en vivo, varios servicios que se ejecutan en el *host*.

- Escaneo de vulnerabilidades: verificar el objetivo en busca de debilidades o vulnerabilidades que puedan explotarse. Generalmente se hace con la ayuda de herramientas automatizadas.
- Mapeo de la red: encontrar la topología de la red, *routers*, servidores de *firewall*, si los hay, e información del *host* y dibujar un diagrama de red con la información disponible. Este mapa puede servir como una valiosa información durante todo el proceso de red.

1.2.2.2.4.3. Obtener Acceso

Esta fase es donde un atacante irrumpe a nivel de Sistema Operativo/a nivel de aplicación, a nivel de red o denegar el servicio de red. Después de ingresar a un sistema, se tiene que aumentar los privilegios a nivel de administrador para poder instalar una aplicación que necesite o modificar datos u ocultar datos.

1.2.2.2.4.4. Mantener Acceso

El *hacker* puede simplemente atacar el sistema para demostrar que es vulnerable o desea mantener o persistir la conexión en segundo plano sin el conocimiento del usuario. Esto se puede hacer utilizando troyanos, *rootkits* u otros archivos maliciosos. El objetivo es mantener el acceso al objetivo hasta que finalice las tareas que planeó realizar en ese objetivo.

1.2.2.2.4.5. Borrar Huellas

Un *hacker* inteligente siempre elimina todas las pruebas para que nadie encuentre ningún rastro que lo conduzca. Esto implica modificar, corromper o eliminar los valores de

los registros, modificar los valores del registro y desinstalar todas las aplicaciones que usó y eliminar todas las carpetas que creó.

Figura 7
Círculo del Hacking

Fuente: Romero, G. (2019)

1.2.2.2.5. Beneficios del Hacking Ético

Según Edureka (2020), el repentino aumento de la demanda de hacking ético que se está notando es resultado de los avances tecnológicos que generan muchas amenazas en el ámbito tecnológico en el mundo. Comprender y acostumbrarse al hacking ético comprende profundizar en las técnicas de los *hackers* y, por lo tanto, aprender a penetrar en los sistemas mediante la identificación y evaluación de vulnerabilidades en el *software* y las redes informáticas. La persecución del hacking ético puede agregar un valor inmenso a una organización, si se practica y se ejerce de manera eficiente y correcta.

En resumen, los siguientes son los beneficios del Hacking Ético:

- Ayuda a luchar contra el ciberterrorismo y a luchar contra las violaciones de la seguridad nacional.

- Ayuda a tomar medidas preventivas contra los *hackers*.
- Ayuda a construir un sistema que evita cualquier tipo de penetración por parte de *hackers*.
- El hacking ético ofrece seguridad a los establecimientos bancarios y financieros.
- Ayuda a identificar y cerrar los agujeros abiertos en un sistema informático o red.

1.2.2.3. Google Hacking

Según López (2011, p.p. 4), "Google Hacking no es más que una técnica de fusión basada en el uso malicioso de parámetros especiales de Google, con el fin de conseguir búsquedas avanzadas y precisas, cuyo afán es obtener datos sensibles que pudiesen ver afectados a personas particulares, empresas públicas o privadas". Google Hacking implica que un atacante envíe consultas al motor de búsqueda de Google con la intención de encontrar información confidencial que reside en páginas web que han sido indexadas por Google, o encontrar información confidencial con respecto a vulnerabilidades en aplicaciones indexadas por Google. Google Hacking no se limita de ninguna manera a la búsqueda a través del motor de búsqueda de Google, sino que se puede aplicar a cualquiera de los principales motores de búsqueda.

1.2.2.4. Herramientas de Hacking Ético usadas en el dominio público

1.2.2.4.1. DNSdumpster

Según Velasco, R. (2019) define DNSdumpster como una herramienta gratuita de investigación de dominios que no permite realizar consultas online de repositorios para descubrir *hosts* relacionados con un dominio. Encontrar *hosts* visibles desde la perspectiva de los atacantes es una parte importante del proceso de evaluación de la seguridad. La compañía hackertarget.com es quien está a cargo de DNSDumpster (HackerTarget, 2019) el cual ofrece

escáneres de vulnerabilidades de seguridad de código abierto confiables y herramientas de inteligencia de red.

Por otro lado, DNSDumpster (HackerTarget, 2019) indica que una característica esencial de DNSDumpster es que no realiza listado de subdominios por métodos de fuerza bruta (método usado por la mayoría de las herramientas de reconocimiento de DNS que enumeran subdominios), el DNSDumpster realiza una búsqueda dentro de la base en datos de nuestros rastreos del 1 millón de sitios principales de Alexa, motores de búsqueda, rastreo común, transparencia de certificados, *Max Mind*, *Team Cymru*, *Shodan* y *scans.io*.

1.2.2.4.2. Whois (página web)

Según Espinosa (2019) sostiene que Whois es un protocolo TCP que se utiliza para realizar consultas en una base de datos con el fin de analizar "¿quién es?" el propietario de un dominio o de una dirección IP pública.

Además, Whois (2021) indica que se puede identificar:

- La persona y/o empresa que registró el dominio.
- La fecha de registro y la fecha de expiración del dominio.
- El correo electrónico, número telefónico y dirección, de la persona que registró el dominio.

1.2.2.5. El Centro de Seguridad de Internet

Según Cisecurity (2021), el Centro de Seguridad de Internet, Inc. (CIS®) es una organización sin fines de lucro independiente, responsable de las mejores prácticas reconocidas a nivel mundial para proteger los sistemas y datos de TI.

Desde el año 2000, el CIS se dedica a prevenir y mitigar nuevas amenazas cibernéticas, donde a través de una colaboración global, desarrolla estándares de clase mundial en forma de controles CIS y puntos de referencia CIS, junto con herramientas tecnológicas especializadas para ayudar a los profesionales de la seguridad a implementar y administrar sus defensas cibernéticas.

Actualmente, lidera una comunidad global de profesionales de TI con el fin de evolucionar continuamente estándares y proporcionar productos y servicios para proteger de manera proactiva contra las amenazas emergentes.

1.2.2.5.1. Controles del CIS

Según Cisecurity (2021) define los Controles del CIS como un conjunto de acciones priorizadas que forman un conjunto de mejores prácticas de defensa que mitigan los ataques más comunes contra sistemas y redes. Estos controles son desarrollados por una comunidad de expertos en TI que aplican su experiencia de primera mano como defensores cibernéticos para crear estas mejores prácticas de seguridad aceptadas globalmente.

Estos controles no son solo otra lista de buenas prácticas, sino un conjunto de acciones priorizadas y altamente focalizadas que tienen una red de soporte comunitario para

poder implementarlas, utilizarlas, y que sean compatibles con todos los requerimientos de seguridad gubernamental o industrial.

Según Center of Internet Security (2019) sostiene que los controles están divididos en 3 grupos, donde los controles del 1 a 6 son esenciales y deben considerarse entre las primeras cosas que se deben hacer, también considerados como "Higiene cibernética".

Controles CIS básicos

1. Inventario y control de activos de *hardware*
2. Inventario y control de activos de *software*
3. Gestión continua de vulnerabilidades
4. Uso controlado de privilegios administrativos
5. Configuración segura de *hardware* y *software* en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores
6. Mantenimiento, seguimiento y análisis de registros de auditoría

Controles CIS fundamentales

7. Protecciones de correo electrónico y navegador web
8. Defensas contra *malware*
9. Limitación y control de puertos, protocolos y servicios de red
10. Capacidades de recuperación de datos
11. Configuración segura para dispositivos de red, como cortafuegos, enrutadores y conmutadores
12. Defensa de límites
13. Protección de datos

14. Control de Acceso basado en la necesidad de saber
15. Control de acceso inalámbrico
16. Seguimiento y control de cuentas

Controles CIS organizacionales

17. Implementar un programa de capacitación y concientización sobre seguridad
18. Seguridad del *software* de aplicación
19. Respuesta y gestión de incidentes
20. Pruebas de penetración y ejercicios del equipo rojo.

1.2.2.5.1.1. Control 3: Gestión continua de Vulnerabilidades

Según Center of Internet Security (2019), se basa en adquirir, evaluar y tomar medidas continuamente para identificar vulnerabilidades, remediar y minimizar la ventana de oportunidad para los atacantes.

Este control opera en un flujo constante de nueva información sobre: las recientes actualizaciones de *software*, parches, avisos de seguridad, boletines de amenazas, etc. Los cibercriminales también tienen acceso a esta nueva información y pueden aprovechar las brechas entre la aparición de nuevos conocimientos y la corrección.

1.2.2.5.1.2. Control 9: Limitación y control de puertos, protocolos y servicios de red

Según Center of Internet Security (2019), se enfoca en gestionar, rastrear, controlar, y corregir el uso operacional continuo de puertos, protocolos y servicios en dispositivos en red para minimizar las ventanas de vulnerabilidad disponibles para los atacantes.

Este control se enfoca en casos como: servidores web mal configurados, servidores de correo, servicios de archivos e impresión y servidores de sistema de nombres de dominio (DNS) instalados por defecto, donde los paquetes de *software* instalan servicios automáticamente y los activan como parte de la instalación del paquete de *software* principal sin informar al usuario o administrador de que los servicios se han habilitado.

1.2.2.5.1.3. Control 12: Defensa de límites

Según Center of Internet Security (2019), se basa en detectar, prevenir, y corregir el flujo de información que transfieren redes de diferentes niveles de confianza con un enfoque en los datos que dañan la seguridad.

Este control se centra en las debilidades de la configuración y la arquitectura que se encuentran en los sistemas perimetrales, los dispositivos de red y las máquinas cliente con acceso a Internet para obtener un acceso inicial hacia la empresa u organización.

1.2.2.5.1.4. Control 14: Control de Acceso basado en la necesidad de saber

Según Center of Internet Security (2019), se centra en rastrear, controlar, prevenir y corregir el acceso seguro a activos críticos (información, recursos, sistemas) en base a qué personal, equipos de cómputo y *softwares* tienen la necesidad y el derecho de acceder a estos activos basados en una clasificación aprobada.

Este control es apto para las organizaciones que no identifican y separan cuidadosamente sus activos más sensibles y críticos de la información de acceso.

1.2.2.5.1.5. Control 18: Seguridad del software de aplicación

Según Center of Internet Security (2019), se basa en gestionar el ciclo de vida de la seguridad de todo el *software* desarrollado y adquirido internamente para prevenir, detectar y corregir las debilidades de seguridad.

Este control se enfoca en mitigar los ataques que aprovechan las vulnerabilidades que se encuentran en el *software* basado en la web y en otras aplicaciones, como inyecciones de *exploits* específicos, ataques de inyección SQL, etc.

1.3. Objetivos

El objetivo principal es:

"Identificar las estrategias de Seguridad de Información según el criterio de los Controles de Seguridad para la Defensa Cibernética aprobados por el CIS (El Centro de Seguridad de Internet) con el fin de subsanar las brechas de seguridad del dominio público de cualquier entidad."

Por ello, en los objetivos específicos tenemos:

- **Objetivo específico 1:** Describir las herramientas que detectan las brechas de seguridad presentes en el dominio público de alguna entidad.

- **Objetivo específico 2:** Analizar el uso de los Controles de Seguridad para la Defensa Cibernética aprobados por el CIS (El Centro de Seguridad de Internet) que permitan subsanar las brechas de seguridad que se encuentra en el dominio público de cualquier entidad.

CAPÍTULO II

MÉTODO

2.1. Tipo, nivel, enfoque y diseño de investigación

2.1.1. Tipo de investigación

Se utilizará un tipo de investigación aplicada debido a que, según Rus, E. (2021), "tiene como objetivo resolver situaciones que se presentan en la realidad. Por eso, su enfoque es claro, analizar y estudiar dichos problemas para encontrar soluciones".

2.1.2. Nivel de investigación

Se utilizará un nivel de investigación descriptiva para identificar el estado del acceso a la información pública de alguna entidad, como información de sus dominios, IPs, e información sensible disponible en el dominio público de la entidad.

Según Hernández-Sampieri, R. (2014, p.p. 98), la investigación descriptiva "busca especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis". Además, "es útil para mostrar con precisión los ángulos o dimensiones de un fenómeno, suceso, comunidad, contexto o situación".

2.1.3. Enfoque de investigación

Se utilizará un enfoque de investigación cualitativo para analizar una encuesta que puede ser utilizada por cualquier que permita interpretar el estado de la seguridad informática de la entidad.

Según QuestionPro (2021):

"La investigación cualitativa es un conjunto de técnicas de investigación que se utilizan para obtener una visión general del comportamiento y la percepción de las personas sobre un tema en particular y se centra en las interpretaciones, las experiencias y su significado.

Los datos derivados de la investigación cualitativa no son estadísticamente mensurables, deben ser interpretados subjetivamente".

2.1.4. Diseño de investigación

El diseño será una investigación no experimental debido a que no se realizará manipulación de la información sensible disponible del dominio público de alguna entidad.

Según QuestionPro (2021), "la investigación no experimental se realiza cuando, durante el estudio, el investigador no puede controlar, manipular o alterar a los sujetos, sino que se basa en la interpretación o las observaciones para llegar a una conclusión".

2.2. Variable, operacionalización

Se ha descrito la siguiente variable:

Tabla 2
Tabla de operacionalización

Variable	Definición conceptual	Definición operacional
Brechas de seguridad dentro del dominio público de cualquier entidad	Según Kaspersky (2021), "una brecha de seguridad es un incidente que permite el acceso no autorizado a datos informáticos, aplicaciones, redes o dispositivos. Es decir, permite acceder sin autorización a información".	Para medir la variable, se utilizará la encuesta conformada por las dimensiones que cuenta con su respectivo indicador y se realizarán preguntas en cada indicador.
	Dimensión	**Indicadores**
	Evaluación de la seguridad de la información dentro del dominio público.	Vulnerabilidades identificadas.
	Reforzamiento de la seguridad informática dentro del dominio público.	Controles del CIS.

Fuente: Elaboración propia

2.3. Población y Muestra

La población de la presente investigación está medida por 48 ex-empleadores informáticos de una entidad aleatoria que retiraron sus cargos entre el año 2017 y el año 2019.

La muestra es representada por 20 de los 48 ex-empleadores debido a que pudimos conseguir una respuesta por parte de ellos como apoyo a las encuestas de nuestra investigación. Nuestra muestra se limitó a esa cantidad puesto que se desconoce la situación actual del resto de los ex-empleadores; es decir, si han cambiado su número telefónico, si se encuentran bien de salud, entre otras situaciones de cada uno de ellos por la cual no respondieron las llamadas ni correos electrónicos que tuvimos de alcance.

2.4. Técnicas e Instrumentos de investigación

2.4.1. Técnicas

En la investigación se utilizó como técnica la encuesta con preguntas de escala de Likert para entender la frecuencia de ocurrencia de la cual las alternativas está definida como:

Tabla 3
Escala de Likert para responder la encuesta

0	1	2	3	4	5
no sabe	nunca	en ocasiones	tal vez sí, tal vez no	casi siempre	siempre

Fuente: Elaboración propia basado en QuestionPro (2021)

Según QuestionPro (2021):

"Las encuestas son un método de investigación y recopilación de datos utilizadas para obtener información de personas sobre diversos temas. Las encuestas tienen una variedad de propósitos y se pueden llevar a cabo de muchas maneras dependiendo de la metodología elegida y los objetivos que se deseen alcanzar".

2.4.2. Instrumentos

Hardware:

Las especificaciones mínimas de *hardware* (computadora) que se usará para el proyecto serán:

- Sistema operativo: Windows 7 o superior.
- Procesador Intel Core i3 o superior.
- Acceso a Internet.

Las herramientas DNSDumpster, los comandos de Google Hacking y Whois no necesitan ningún *software* para su ejecución, aparte del navegador web (Google Chrome, Firefox, Ophera, entre otros).

2.5. Procedimientos de recolección de datos

Inicialmente, nos comunicamos con un ex-empleado de una entidad aleatoria quien nos proporcionó una lista de sus colegas que trabajaron en la entidad, indicando sus nombres, teléfono y/o correos de cada uno.

Para la evaluación, se encuestó 20 ex-empleados de una entidad aleatoria, de entre los cuales 13 eran hombres (65% de la muestra) y 7 eran mujeres (35% de la muestra). Por otra parte, solo 8 de los ex-empleados (40% de la muestra) pertenecían al área de Informática (Networking, Base de Datos, Aplicaciones), 6 ex-empleados (30% de la muestra) pertenecían al área de Oficina (Atención al Cliente), 4 ex-empleados (20% de la muestra) pertenecían al área de Logística, y 2 ex-empleados (10% de la muestra) pertenecían al área de Recursos Humanos.

Por último, recibimos la respuesta de las encuestas. De nuestro lado, entregamos un aporte por su colaboración y tiempo en dedicación a la encuesta.

2.6. Plan de análisis

Utilizando los datos obtenidos de las encuestas, se realizó la tabulación de los resultados de cada pregunta en el programa Microsoft Excel versión 2019.

2.7. Matriz de Consistencia

Tabla 4
Matriz de Consistencia

<table>
<tr><th>Enunciado del problema</th><th>Objetivo General de la investigación</th><th>Metodología</th></tr>
<tr><td rowspan="4">¿Cómo serán las estrategias de Seguridad de Información según el criterio de los Controles de Seguridad para la Defensa Cibernética aprobados por el CIS (El Centro de Seguridad de Internet) para subsanar las brechas de seguridad del dominio público de cualquier entidad?</td><td>Identificar las estrategias de Seguridad de Información según el criterio de los Controles de Seguridad para la Defensa Cibernética aprobados por el CIS (El Centro de Seguridad de Internet) con el fin de subsanar las brechas de seguridad del dominio público de cualquier entidad.</td><td>Tipo de investigación:

Aplicada</td></tr>
<tr><td>Objetivos específicos</td><td>Nivel de investigación:

Descriptiva</td></tr>
<tr><td>1. Describir las herramientas que detectan las brechas de seguridad presentes en el dominio público de alguna entidad.</td><td>Enfoque de investigación:

Cualitativo</td></tr>
<tr><td>2. Analizar el uso de los Controles de Seguridad para la Defensa Cibernética aprobados por el CIS (El Centro de Seguridad de Internet) que permitan subsanar las brechas de seguridad que se encuentra en el dominio público de la entidad.</td><td>Diseño de investigación:

No experimental</td></tr>
</table>

Fuente: Elaboración propia

2.8. Principios Éticos

En el desarrollo de esta investigación se estima considerar de manera óptima la práctica de las herramientas del Hacking Ético que nos ayudará a identificar las brechas de seguridad presentes en el dominio público de cualquier entidad y como resultado analizar los Controles de Seguridad aprobados por el CIS.

Se reafirma que, según HackerTarget (2019) y Velasco, R. (2019), la herramienta DNSdumpster no utiliza ninguna enumeración de subdominios por fuerza bruta, como es común en las herramientas de reconocimiento de DNS que enumeran subdominios. DNSdumpster utiliza recursos de inteligencia de código abierto para consultar datos de dominio. Estos datos se obtienen mediante consultas en plataformas como Alexa Top 1 Million, motores de búsqueda (Google, Bing, etc), Common Crawl, Certificate Transparency, Max Mind, Team Cymru, Shodan y scans.io.

En adición, según Espinosa, O. (2019), Whois es un directorio público que contiene la información técnica y los datos de registro de los titulares del dominio registrado. Whois no es una base de datos única con gestión centralizada, donde los datos de registro se guardan en diferentes lugares y son administrados por múltiples registros y registradores que cumplen con los requisitos mínimos de la ICANN (Corporación de Internet para la Asignación de Nombres y Números).

A su vez, según López (2011, p.p. 4):

> "Google Hacking no es más que una técnica de fusión basada en el uso malicioso de parámetros especiales de Google, con el fin de conseguir búsquedas avanzadas y precisas, cuyo afán es obtener datos sensibles que pudiesen ver afectados a personas particulares, empresas públicas o privadas".

Asimismo, se cumple los derechos de propiedad de las fuentes electrónicas ya que nos ayudó con las definiciones de los conceptos que se implementaron en la investigación.

Además, se recogió información únicamente del ambiente público de la entidad, sin realizar ninguna vulneración de las medidas de seguridad previamente establecidas en la entidad, y sin realizar ningún tipo de cambio o modificación. Respetando la ley N° 27309 según lo publicado en el diario El Peruano (2000), Artículo 207°-A:

> "El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuentaidós a ciento cuatro jornadas.
>
> Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de la libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas".

Y el Artículo 207°-B:

> "El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multas".

Aclarando, además, que se respeta la ley N° 30096 según lo publicado en el diario El Peruano (2013), Artículo 2. Acceso ilícito:

> "El que accede si autorización a todo o parte de un sistema informático, siempre que realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menos de uno ni mayor de cuatro años y con treinta a noventa días multa.
>
> Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado".

También, el Artículo 3. Atentado contra la integridad de datos informáticos, nos indica:

> "El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa".

Y, por último, el Artículo 4. Atentado contra la integridad de sistemas informáticos, señala:

> "El que, a través de las tecnologías de la información o de la comunicación, inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa".

Finalizando, se tomaron datos exactos provenidos de encuestas para cumplir con la parte de la metodología. Es importante resaltar que se mantiene reservada la identidad de los personales que nos han apoyado a resolver las encuestas.

CAPÍTULO III

RESULTADOS

3.1. Presentación de resultados

3.1.1. Resultados de las encuestas

3.1.1.1. Indicador 01: Vulnerabilidades identificadas

Se elaboraron las siguientes preguntas:

Tabla 5
Preguntas del indicador 01

Indicador	**Preguntas**	**Rango promedio**
Vulnerabilidades identificadas	En su área de trabajo, ¿ha sido afectado por algún incidente informático?	3.2
	En su área de trabajo, ¿han recibido correos *phishing* en su correo laboral?	2.7

Fuente: Elaboración propia

3.1.1.2. Indicador 02: Controles del CIS

Se elaboraron las siguientes preguntas:

Tabla 6
Preguntas del indicador 02

Indicador	Preguntas	Rango promedio
Controles del CIS	En su área de trabajo, ¿se ejecuta alguna herramienta de análisis de vulnerabilidades automática o manualmente por algún especialista de informática?	3.1
	De ejecutarse alguna herramienta de análisis de vulnerabilidades automática o manualmente, ¿se comparan los resultados de escaneo con escaneos pasados?	2.9
	En su área de trabajo, ¿se ejecuta algún programa de aplicación de parches de software y/o sistema operativo?	2.4
	En su área de trabajo, ¿se ejecuta algún sistema de protección de red (firewall, aplicación de filtrado de puertos)?	4.1
	En su área de trabajo, ¿se ejecuta algún sistema de búsqueda y/o denegación de acceso no autorizado?	3.9
	En su área de trabajo, ¿se implementa listas de control de acceso?	3.4
	En su área de trabajo, ¿se actualiza periódicamente las aplicaciones usadas en su estación de trabajo?	2.7

Fuente: Elaboración propia

3.1.2. Análisis de Resultados

Primeramente, se resalta que el objetivo de esta encuesta no se basa en atentar contra la reputación de cualquier entidad, sino que esta exploración propia se basa en recopilar información para identificar que posibles brechas de seguridad se encuentran presente, y que controles de seguridad informática se pueden implementar para reforzar la seguridad informática en cualquier entidad mediante el uso de herramientas de la fase de reconocimiento de Ethical Hacking como DnsDumspter, Google Hacking, y WhoIs que no ejercen mecanismos de intrusión de fuerza bruta.

Mediante los resultados por parte de los ex-empleados que se puede visualizar en el Anexo N°05. Se da a comparar el respectivo análisis de resultados:

1. Según la Tabla 5 dentro del Indicador 01, a los ex-empleados encuestados se les preguntó sobre si presentaron algún incidente informático durante su periodo de trabajo, donde dicha información se puede validar mediante el uso de las herramientas WhoIs y Google Hacking. Debido que, con esta información, un hacker de sombrero negro podría hacer uso de la información sensible expuesta públicamente de la entidad.

2. Según la Tabla 6 dentro del Indicador 02, se aprecia que se formuló preguntas relacionadas a los controles del CIS para identificar qué tipo de herramientas de seguridad pueden existir en su área de trabajo y/o en el dominio público, lo cual tiene relación con la información obtenida de la herramientas DnsDumpster, WhoIs y Google Hacking, y la información obtenida de la respuesta de los ex-empleados, podemos brindar como sugerencias que controles del CIS pueden tomar para el fortalecimiento de la seguridad informática dentro del dominio público de cualquier entidad.

3.1.3. Propuesta de mejora

Se propone estrategias de Seguridad de Información brindadas por los Controles Críticos del CIS (El Centro de Seguridad de Internet) con el fin de subsanar las brechas de seguridad identificadas por las herramientas del Hacking Ético.

3.1.3.1. Antecedentes

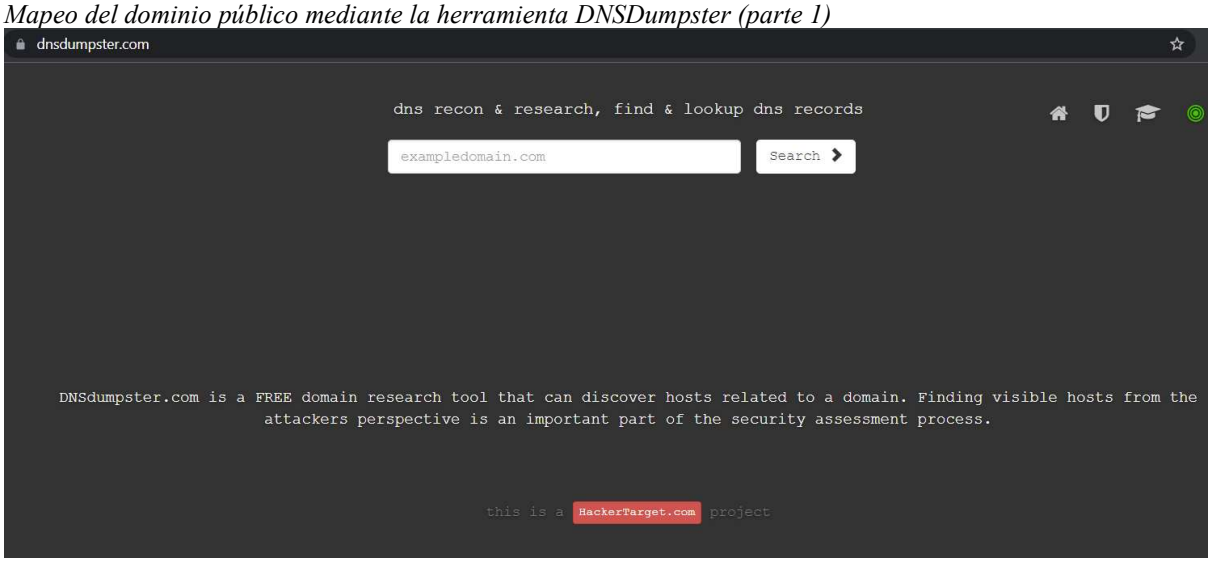
Usaremos tres herramientas que nos permitan obtener una muestra que tenga relación a la fase de Reconocimiento del Hacking Ético que se emplea en esta investigación:

1. Mediante el uso de la herramienta DnsDumpster, en la página principal nos proporciona una sección donde se puede ingresar el dominio o la IP del servidor a analizar de la entidad (ver Figura 8). Una vez ingresado el dominio o la IP del servidor a analizar, DnsDumspter muestra como resultado un listado de las direcciones IP del dominio público, DNS utilizados, aplicaciones web utilizadas, posible sistema operativo utilizado, entre otros datos. Por otra parte, DnsDumspter también nos muestra de manera gráfica la localización de donde proceden cada servidor, al igual que los dueños de los bloques de servidores. Finalmente, nos brinda la capacidad de descargar toda la información de los servidores de la entidad objetivo en un archivo de formato ".xlsx", y también permite descargar la infraestructura de red de los servidores en modo gráfico en una imagen de formato ".png".

   En base a esta información de posibles brechas de seguridad, un hacker de sombrero negro podría utilizar algunas vulnerabilidades para poder ganar acceso hacia los servidores y extraer y/o utilizar información sensible.

Figura 8

Mapeo del dominio público mediante la herramienta DNSDumpster (parte 1)



Fuente: Elaboración propia mediante la herramienta DNSDumpster

El uso de la herramienta DNSDumpster no requiere de conocimiento previo, pues solo se necesita ingresar el dominio o la IP del servidor de la entidad a analizar. También es de fácil ejecución y no toma mucho tiempo en adquirir los resultados, debido que la herramienta DNSdumpster según HackerTarget (2019) y Velasco, R. (2019), no utiliza ninguna enumeración de subdominios por fuerza bruta, DNSdumpster utiliza recursos de inteligencia de código abierto para consultar datos de dominio, obtenidos mediante consultas en plataformas como Alexa Top 1 Million, motores de búsqueda (Google, Bing, etc), Common Crawl, Certificate Transparency, Max Mind, Team Cymru, Shodan y scans.io.

DnsDumspter nos puede mostrar si los servidores mapeados cuentan con algún servicio que cuenten con versiones desactualizadas, donde de ser validado por medio de herramientas de escaneo de fuerza bruta si estos servidores cuentan con versiones obsoletas de sus aplicaciones, podrían poseer múltiples vulnerabilidades de las cuales alguna podrían ser vulnerabilidades críticas, permitiendo que un hacker de sombrero negro mediante un usuario con credenciales válidas se autentique con otro nombre de

usuario, sin pasar por las restricciones de control de acceso configuradas, permitiendo que se omitan los requisitos de autenticación,

Estas y otras vulnerabilidades le permitirían a un hacker de sombrero negro ejecutar códigos sin necesidad de utilizar usuarios con altos privilegios, ignorando las restricciones de control de acceso implementadas en los servidores de cualquier entidad (ver Figura 9).

Figura 9

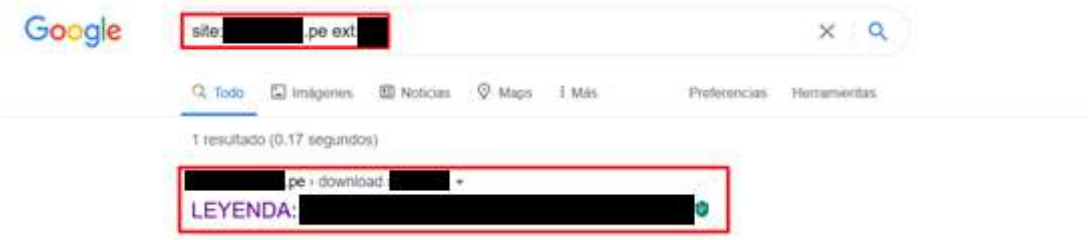
Mapeo del dominio público mediante la herramienta DNSDumpster (parte 2)

Fuente: Elaboración propia mediante la herramienta DNSDumpster

2. Mediante el uso de búsqueda avanzada (Google Hacking) se pueden encontrar archivos con información sensible, acceso a aplicaciones, etc. Para esto, se requiere conocimiento previo para ejecutar los comandos de búsqueda avanzada de Google Hacking con el fin de encontrar los accesos, agujeros de seguridad, malas

configuraciones, y archivos de la entidad objetivo que se encuentren expuestos públicamente (ver Figura 10).

Figura 10
Aplicación de los conceptos de Google Hacking en el dominio público



Fuente: Elaboración propia mediante el uso del Google Hacking

Para la aplicación de los comandos o también llamados “Dorks” o “Google Dorks”, que son la combinación de palabras para realizar el Google Haking, no existe un orden específico para ejecutar los comandos, se pueden ejecutar a voluntad los comandos específicos para detectar el tipo de brechas de seguridad deseado. Por otra parte, si se desea realizar un análisis general de las brechas de seguridad expuestas en el dominio público de una entidad objetico, se puede ejecutar por grupo de comandos para detectar los diferentes tipos de brechas de seguridad (ver Anexo N°01):

- Listado de directorios (site:dominio.com intitle:index.of)
- Archivos con información sensible (site:dominio.com ext:xml | ext:conf | ext:cnf | ext:reg | ext:inf | ext:rdp | ext:cfg | ext:txt | ext:ini)
- Archivos de Base de datos (site:dominio.com ext:sql | ext:dbf | ext:mdb | ext:ora | ext:config mysql_connect)
- Archivos de registros "logs" (site:dominio.com ext:log)
- Inyecciones o errores de código SQL (site:dominio.com intext:"sql syntax near" | intext:"syntax error has occurred" | intext:"incorrect syntax near" | intext:"unexpected end of SQL command" | intext:"Warning:

mysql_connect()" | intext:"Warning: mysql_query()" | intext:"Warning: pg_connect()")

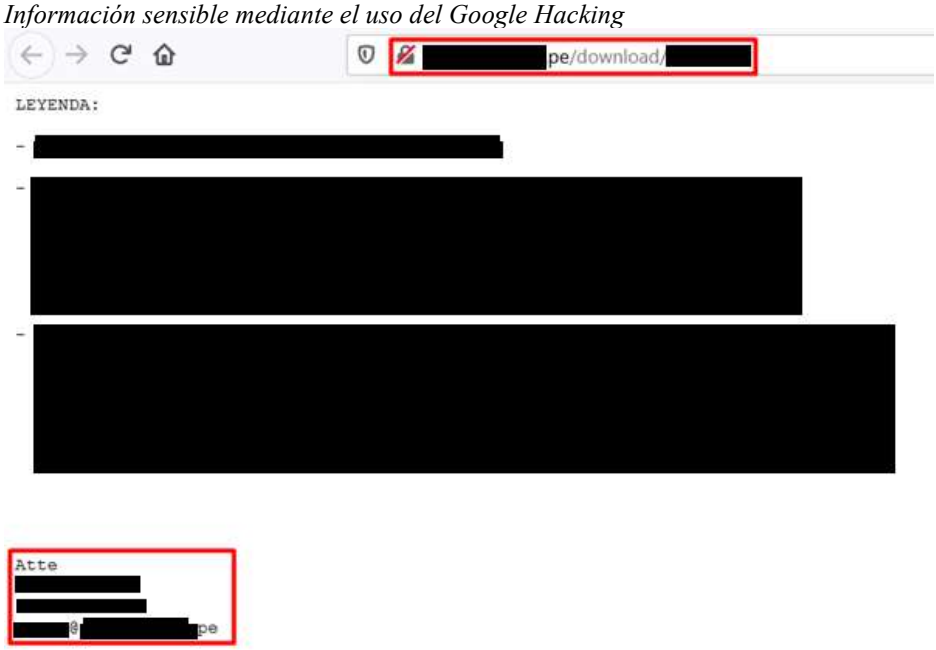
- Archivos expuestos a Internet (site:dominio.com ext:doc | ext:docx | ext:odt | ext:pdf | ext:rtf | ext:sxw | ext:psw | ext:ppt | ext:pptx | ext:pps | ext:csv)
- Archivos backup (site:dominio.com ext:bkf | ext:bkp | ext:bak | ext:old | ext:backup)

En la entidad aleatoria donde se ejecutó los comandos de Google Hacking se demostró una notable rapidez en la obtención de los resultados cuando se tiene en conocimiento los comandos o "Dorks" a ejecutar, logrando encontrar un archivo con información sensible. Dicho archivo contenía información de equipos usados en la entidad, y también contenía información de su personal.

Esto demuestra lo crucial que es detectar los archivos con información sensible, donde podría contener información de clientes, personal, aplicaciones, equipos, etc que son utilizados en cualquier entidad. Con esta información, un hacker de sombrero negro podría buscar en páginas de venta de la DarkWeb y buscar alguna vulnerabilidad o un *zero-day* de los equipos, aplicaciones y/o sistemas usados en las entidades, y con esto acceder al sistema permitiéndole al atacante utilizar la información de la entidad con el fin de realizar transacciones ilícitas, usurpación de identidad, robo y venta de información, etc. Por otra parte, el hacker de sombrero negro podría generar un diccionario de contraseñas para poder ejecutar un "ataque de fuerza bruta" que consiste en ingresar al sistema de alguna entidad mediante la repetición del uso de un diccionario que recombina palabras con miles de combinaciones diferentes en base a

la información recopilada de los archivos de información sensible expuestas públicamente (ver Figura 11).

Figura 11
Información sensible mediante el uso del Google Hacking

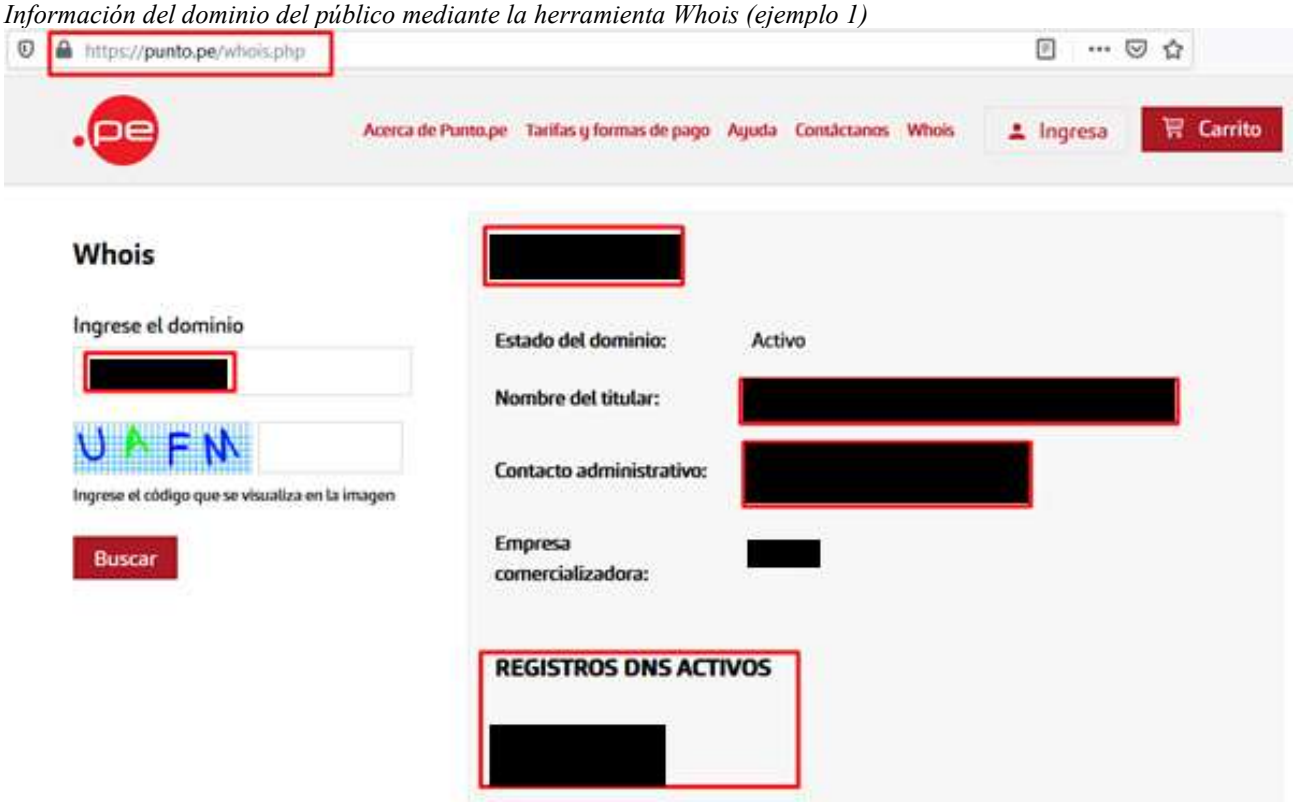


Fuente: Elaboración propia mediante el uso del Google Hacking

3. Por último, mediante el uso de la herramienta Whois, nos permite identificar de manera rápida el nombre del titular del dominio público, el estado del dominio público, los DNS registrados, información de algún contacto administrativo, y la dirección IP del dominio público de la entidad (ver Figura 12 y Figura 13). Para usar esta herramienta no requiere conocimientos previos, es fácil de ejecutar debido que solo se necesita ingresar el dominio o la IP del servidor objetivo, y en algunas páginas de WhoIs requerirá ingresar una autentificación captcha.

Figura 12

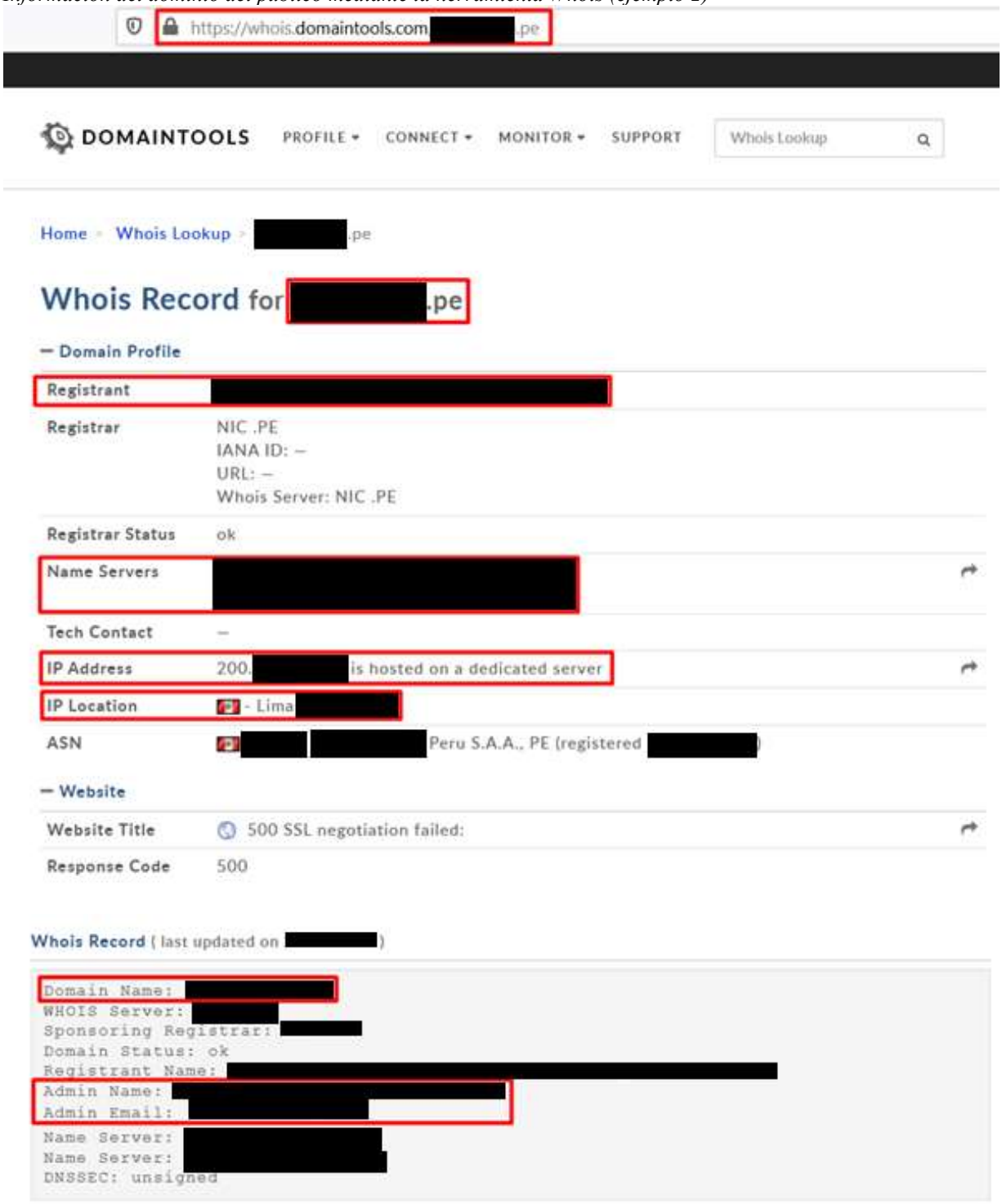
Información del dominio del público mediante la herramienta Whois (ejemplo 1)



Fuente: Elaboración propia mediante la herramienta Whois

Figura 13

Información del dominio del público mediante la herramienta Whois (ejemplo 2)

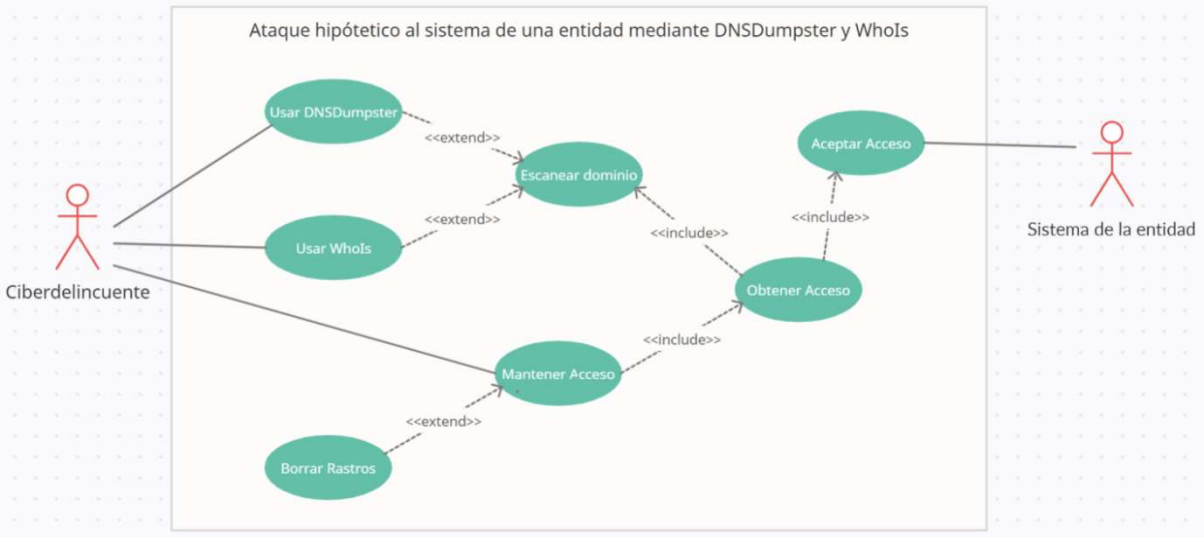


Fuente: Elaboración propia mediante la herramienta Whois

3.1.3.1.1. Diagramas de Casos de Uso - Ataques hipotéticos

Se realizó el diagrama de casos de uso para diseñar las acciones de ataques hipotéticos del ciberdelincuente (1° actor) frente al sistema de alguna entidad pública o privada (2° actor), cuyos casos de usos (al usar las herramientas DNSDumpster y WhoIs) son: Usar DNSDumpster, Usar WhoIs, Escanear dominio, Mantener Acceso, Borrar Rastros, Obtener Acceso y Aceptar Acceso (ver Figura 14).

Figura 14
Diagrama de casos de uso para diseñar las acciones de ataques hipotéticos del ciberdelincuente frente al sistema de la entidad



Fuente: Elaboración propia

A su vez, se realizó otro diagrama de casos de uso con los mismos actores de la Figura 18 cuyos casos de usos (al usar la herramienta Google Hacking) son: Usar Google Hacking, Buscar Vulnerabilidad, Escanear dominio, Mantener Acceso, Borrar Rastros, Obtener Acceso y Aceptar Acceso (ver Figura 15).

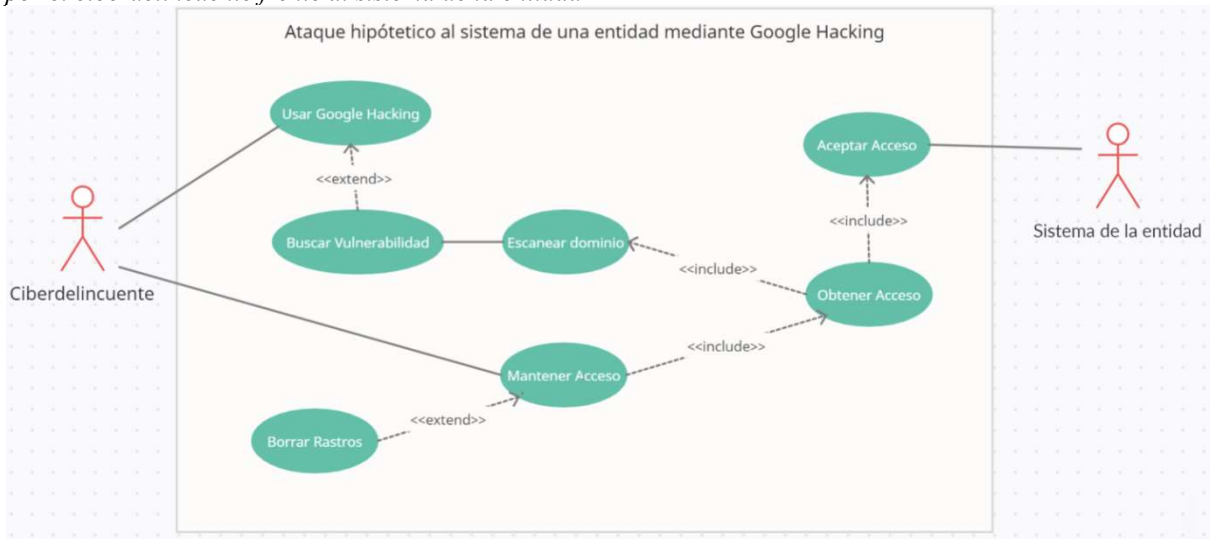
En el caso de uso “Escanear dominio” se realizará un análisis de los equipos activos en la red, y se identificará los puertos abiertos en cada equipo.

Luego en el caso de uso “Obtener Acceso” se procederá primero a identificar las vulnerabilidades que pueden ser explotadas por un eventual atacante informático, para luego ejecutar “*exploit*” que es un código escrito que aprovecha una vulnerabilidad y busca tomar el control del equipo.

Posteriormente en el caso de uso “Aceptar Acceso” se formó una conexión directa con el equipo victima (sistema de la entidad) donde el ciberdelincuente puede: obtener información sensible de la entidad, extorsionar a la entidad mediante el encriptado de su información sensible por un *malware* a cambio de un depósito de dinero, alteración de información, etc.

Por último, en el caso de uso Borrar Rastros, es donde el ciberdelincuente cerrará el acceso hacia el equipo del cliente una vez finalizado sus actos delictivos.

Figura 15
Diagrama de casos de uso para diseñar las acciones de ataques hipotéticos mediante Google Hacking hecho por el ciberdelincuente frente al sistema de la entidad



Fuente: Elaboración propia

Se realizó la documentación especificando los actores que interactuaron con los ataques hipotéticos (ver Tabla 7 y 8).

Tabla 7
Descripción del primer actor para el Diagrama de Casos de Uso

Actor	Ciberdelincuente	**Identificador:** A001
Descripción	Actor que realiza los ataques al sistema de una entidad usando las herramientas DNSDumpster, WhoIs y Google Hacking.	
Características	Persona que domina las herramientas del Hacking Ético.	
Referencias	Caso de Uso CU001: Usar DNSDumpster o Caso de Uso CU002: Usar WhoIs y Caso de Uso CU006: Mantener Acceso	

Fuente: Elaboración propia

Tabla 8
Descripción del segundo actor para el Diagrama de Casos de Uso

Actor	Sistema de la entidad	**Identificador:** A002
Descripción	Actor que recibe los ataques de "fuerza bruta" para obtener accesos a sus sistemas.	
Características	Sistema informático.	
Referencias	Caso de Uso CU009: Aceptar Acceso	

Fuente: Elaboración propia

En adición, se clasificó los actores implicados, precondiciones, postcondiciones y la descripción de los casos de uso "Usar DNSDumpster" (ver Tabla 9), "Usar WhoIs" (ver Tabla 11), "Usar Google Hacking" (ver Tabla 13), "Buscar Vulnerabilidad" (ver Tabla 15), "Escanear Dominio" (ver Tabla 17), "Mantener Acceso" (ver Tabla 19), "Borrar Rastros" (ver Tabla 21), "Obtener Acceso" (ver Tabla 23) y "Aceptar Acceso" (ver Tabla 25) con sus respectivos cursos normales de eventos (ver Tabla 10, 12, 14, 16, 18, 20, 22, 24 y 26 correspondientemente).

3.1.3.1.1.1. Usar DNSDumpster

Tabla 9
Especificación del caso de uso "Usar DNSDumpster"

Caso de Uso	Usar DNSDumpster	**Identificador:** CU001
Actores	**Ciberdelincuente**	
Tipo	Primario	
Precondición	Ninguna	

Postcondición	Escanea los dominios del sistema.
Descripción	Caso de uso en la que el ciberdelincuente escanea los dominios del sistema usando la herramienta DNSDumpster.

Fuente: Elaboración propia

Tabla 10

Curso normal de eventos del CU001

Nro.	**Ejecutor**	**Paso o Actividad**
1	Ciberdelincuente	Usa la herramienta DNSDumpster con el fin de escanear los dominios públicos del sistema.
Respuesta del sistema		
1. El Ciberdelincuente utiliza la herramienta DNSDumpster vía web.		
2. El Ciberdelincuente logra escanear los dominios públicos del sistema de la entidad.		

Fuente: Elaboración propia

3.1.3.1.1.2. Usar WhoIs

Tabla 11

Especificación del caso de uso "Usar WhoIs"

Caso de Uso	Usar WhoIs	**Identificador:** CU002
Actores	**Ciberdelincuente**	
Tipo	Primario	
Precondición	Ninguna	
Postcondición	Escanea los dominios del sistema.	
Descripción	Caso de uso en la que el ciberdelincuente escanea los dominios del sistema usando la herramienta WhoIs.	

Fuente: Elaboración propia

Tabla 12

Curso normal de eventos del CU002

Nro.	**Ejecutor**	**Paso o Actividad**
1	Ciberdelincuente	Usa la herramienta WhoIs con el fin de escanear los dominios públicos del sistema.
Respuesta del sistema		
1. El Ciberdelincuente utiliza la herramienta WhoIs vía web. 2. El Ciberdelincuente logra escanear los dominios públicos del sistema de la entidad.		

Fuente: Elaboración propia

3.1.3.1.1.3. Usar Google Hacking

Tabla 13
Especificación del caso de uso "Usar Google Hacking"

Caso de Uso	Usar Google Hacking	**Identificador:** CU003
Actores	**Ciberdelincuente**	
Tipo	Primario	
Precondición	Ninguna	
Postcondición	Escanea los dominios del sistema.	
Descripción	Caso de uso en la que el ciberdelincuente busca información dentro del sistema para encontrar vulnerabilidades usando la herramienta Google Hacking.	

Fuente: Elaboración propia

Tabla 14
Curso normal de eventos del CU003

Nro.	**Ejecutor**	**Paso o Actividad**
1	Ciberdelincuente	Usa la herramienta Google Hacking con el fin de encontrar información para buscar vulnerabilidades dentro del sistema.
Respuesta del sistema		
1. El Ciberdelincuente utiliza la herramienta Google Hacking vía web. 2. El Ciberdelincuente logra encontrar información y con ello puede ser usada para encontrar vulnerabilidades dentro de los dominios públicos del sistema de la entidad.		

Fuente: Elaboración propia

3.1.3.1.1.4. Buscar Vulnerabilidad

Tabla 15
Especificación del caso de uso "Buscar Vulnerabilidad"

Caso de Uso	Buscar Vulnerabilidad	**Identificador:** CU004
Actores	**Ciberdelincuente**	
Tipo	Primario	
Precondición	CU003: Usar Google Hacking	
Postcondición	Escanea los dominios del sistema.	
Descripción	Caso de uso en la que el ciberdelincuente busque las vulnerabilidades dentro de los dominios del sistema usando la herramienta Google Hacking.	

Fuente: Elaboración propia

Tabla 16
Curso normal de eventos del CU004

Nro.	Ejecutor	Paso o Actividad
1	Ciberdelincuente	Encuentra las vulnerabilidades de los dominios públicos del sistema.
Respuesta del sistema		
1. El Ciberdelincuente encuentra las vulnerabilidades de los dominios públicos del sistema de la entidad.		

Fuente: Elaboración propia

3.1.3.1.1.5. Escanear Dominio

Tabla 17
Especificación del caso de uso "Escanear Dominio"

Caso de Uso	Escanear Dominio	**Identificador:** CU005
Actores	**Ciberdelincuente**	
Tipo	Primario	
Precondición	CU001: Usar DNSDumpster o CU002: Usar WhoIs y Curso normal de eventos del CU008: Obtener Acceso	
Postcondición	Obtener los accesos del sistema.	
Descripción	Caso de uso en la que el ciberdelincuente escanea los dominios del sistema.	

Fuente: Elaboración propia

Tabla 18
Curso normal de eventos del CU005

Nro.	Ejecutor	Paso o Actividad
1	Ciberdelincuente	Se escanea los dominios públicos del sistema.
Respuesta del sistema		
1. El Ciberdelincuente escanea los dominios públicos del sistema usando las herramientas de Hacking Ético.		

Fuente: Elaboración propia

3.1.3.1.1.6. Mantener Acceso

Tabla 19
Especificación del caso de uso "Mantener Acceso"

Caso de Uso	Mantener Acceso	**Identificador:** CU006
Actores	**Ciberdelincuente**	
Tipo	Primario	
Precondición	Ninguna	
Postcondición	Obtener los accesos del sistema.	
Descripción	Caso de uso en la que el ciberdelincuente mantiene el acceso para obtenerlo.	

Fuente: Elaboración propia

Tabla 20
Curso normal de eventos del CU006

Nro.	Ejecutor	Paso o Actividad
1	Ciberdelincuente	Mantiene el acceso para obtenerlo.
Respuesta del sistema		
1. El Ciberdelincuente mantiene el acceso para obtenerlo.		

Fuente: Elaboración propia

3.1.3.1.1.7. Borrar Rastros

Tabla 21
Especificación del caso de uso "Borrar Rastros"

Caso de Uso	Borrar Rastros	**Identificador:** CU007
Actores	**Ciberdelincuente**	
Tipo	Primario	
Precondición	Ninguna	
Postcondición	Mantener los accesos.	
Descripción	Caso de uso en la que se borran los rastros para no ser detectado.	

Fuente: Elaboración propia

Tabla 22
Curso normal de eventos del CU007

Nro.	Ejecutor	Paso o Actividad
1	Ciberdelincuente	Borra los rastros para no ser detectado.
Respuesta del sistema		
1. El Ciberdelincuente borra sus rastros para no ser detectado por sistema de la entidad.		

Fuente: Elaboración propia

3.1.3.1.1.8. Obtener Acceso

Tabla 23
Especificación del caso de uso "Obtener Acceso"

Caso de Uso	Obtener Acceso	**Identificador:** CU008
Actores	**Ciberdelincuente**	
Tipo	Primario	
Precondición	Curso normal de eventos del CU006: Mantener Acceso	
Postcondición	Se acepta el acceso al sistema.	
Descripción	Caso de uso en la que el ciberdelincuente obtiene al acceso al sistema.	

Fuente: Elaboración propia

Tabla 24
Curso normal de eventos del CU008

Nro.	Ejecutor	Paso o Actividad
1	Ciberdelincuente	Obtiene el acceso del sistema del dominio público del sistema.
Respuesta del sistema		
1. El Ciberdelincuente obtiene el acceso del sistema del dominio público del sistema de la entidad.		

Fuente: Elaboración propia

3.1.3.1.1.9. Aceptar Acceso

Tabla 25
Especificación del caso de uso "Aceptar Acceso"

Caso de Uso	Aceptar Acceso	**Identificador:** CU009
Actores	**Sistema de la entidad/Ciberdelincuente**	
Tipo	Primario	
Precondición	Curso normal de eventos del CU008: Obtener Acceso	
Postcondición	Se acepta el acceso del sistema y por ende se puede ingresar a la información.	
Descripción	Caso de uso en la que el sistema de la entidad acepta el acceso ingresado por el ciberdelincuente.	

Fuente: Elaboración propia

Tabla 26
Curso normal de eventos del CU009

Nro.	Ejecutor	Paso o Actividad
1	Sistema de alguna entidad	Acepta el acceso ingresado por el ciberdelincuente.
2	Ciberdelincuente	Ingresa al sistema de la entidad.
Respuesta del sistema		
1. El sistema de la entidad acepta el acceso ingresado por el ciberdelincuente. 2. El ciberdelincuente ingresa al sistema de la entidad y entra obtiene la información que el ciberdelincuente desea.		

Fuente: Elaboración propia

3.1.3.2. Procedimiento

Para una eficiente seguridad informática es apto aplicar los Controles del CIS, según Center of Internet Security (2019), para formar rápidamente las medidas necesarias en base a la información sensible obtenida desde el dominio público.

Se procede a aplicar algunos de los Controles del CIS, como:

- **Control 3: Gestión continua de Vulnerabilidades:**

  Según Shamma, B. (2018), el tercer control permitiría a la organización para comprender y abordar las vulnerabilidades que pueden poseer estos activos. Este control CIS tiene siete subcontroles:

  CSC 3.1: Ejecute herramientas de análisis de vulnerabilidades automatizadas

  Es posible que identificar sus activos no sea suficiente para identificar el riesgo asociado con estos activos. Por lo tanto, una organización puede escanear sus activos en busca de vulnerabilidades en un cronograma definido y aprobado. Esto se puede lograr utilizando OpenVAS para el escaneo de redes examinando qué servicios se están ejecutando en los dispositivos y el riesgo asociado con estos servicios. Las organizaciones también pueden crear un script de Nmap para escanear el entorno y luego usar Ndiff para comparar los resultados del escaneo.

  CSC 3.2: Realizar escaneo de vulnerabilidades autenticado

  Cuando se usa un escáner de red, se puede usar una cuenta de servicio especial dedicada para autenticarse en los sistemas. El uso de un escaneo autenticado puede ayudar a proporcionar resultados más precisos con respecto a los servicios instalados y en ejecución en cada sistema. Las organizaciones pueden utilizar un proceso para configurar un análisis para que se ejecute con la cuenta de servicio designada para esta tarea a fin de cubrir este subcontrol.

CSC 3.3: Proteger cuentas de evaluación dedicadas

Para implementar este subcontrol, una organización puede configurar la cuenta de servicio especial dedicada mencionada en el subcontrol anterior con los privilegios mínimos necesarios para ejecutar análisis con éxito.

CSC 3.4: Implementar herramientas automatizadas de administración de parches del sistema operativo

Después de cada análisis, los resultados de cada uno se pueden revisar para identificar los parches necesarios para implementar en los sistemas afectados. Una organización puede tener un sistema para automatizar el envío de los parches faltantes a todos los sistemas afectados. Una organización puede analizar el programa de aplicación de parches en función de la gravedad de la vulnerabilidad. Esto se puede lograr utilizando Microsoft Windows Server Update Services (WSUS), que está disponible sin costo en todos los Windows Server 2012 y posteriores. Otras opciones pueden incluir Chef o Ansible.

CSC 3.5: Implemente herramientas de administración de parches de software automatizadas

Esto sigue los principios del subcontrol anterior. El *software* obsoleto también se puede agregar al ciclo de parcheo en función de la vulnerabilidad y la gravedad del riesgo.

CSC 3.6: Comparar análisis de vulnerabilidades consecutivos

Una organización puede identificar que los parches faltantes se hayan aplicado con éxito comparando los resultados del análisis más reciente con el análisis anterior

cuando se identificó la vulnerabilidad e iniciar un proceso para acelerar el envío de parches a cualquier sistema que no se haya parcheado correctamente.

CSC 3.7: Utilizar un proceso de calificación de riesgos

Como se analiza en el subcontrol anterior, los esfuerzos de remediación de vulnerabilidades de una organización pueden centrarse en parchear las vulnerabilidades con mayor riesgo o gravedad. Dar prioridad a los esfuerzos de remediación puede ayudar a las organizaciones a reducir su panorama de amenazas de manera más efectiva y oportuna.

- **Control 9: Limitación y control de puertos, protocolos y servicios de red**:

  Según Shamma, B. (2018), los hackers informáticos suelen iniciar su ataque buscando puertos, servicios o protocolos abiertos. Y luego comenzará a tomar huellas digitales de estos servicios para identificar cualquier vulnerabilidad. Este control ayudará a las organizaciones a comprender y proteger los puertos abiertos y los servicios en ejecución en su entorno. Este control CIS tiene cinco subcontroles:

  CSC 9.1: Asociar puertos, servicios y protocolos activos al inventario de activos

  Si una organización ha implementado con éxito el "Control 2: Inventario de Software autorizados y no autorizados", entonces este subcontrol también se puede cubrir, OpenVAS proporcionará la capacidad de asociar puertos, servicios y protocolos a sistemas y dispositivos. Si el agente Wazuh o Kolide Fleet está instalado en un sistema, también puede calcular y presentar esta información.

CSC 9.2: Asegúrese de que solo se estén ejecutando los puertos, protocolos y servicios aprobados

Una organización puede tener una política para aprobar puertos, protocolos y servicios antes de que se habiliten. También se puede colocar un proceso para abordar puertos, protocolos y servicios no aprobados que pueden requerir una terminación inmediata del servicio o aislar el sistema que lo ejecuta.

CSC 9.3: Realizar exploraciones de puertos automatizadas periódicas

Este subcontrol depende del subcontrol anterior. Para abordar puertos, protocolos y servicios no aprobados, las organizaciones deben analizarlos primero. Por lo tanto, una organización puede tener una política y un proceso para programar estos análisis de forma regular y revisar los resultados. Este subcontrol se puede cubrir con OpenVAS o Nmap.

CSC 9.4: Aplicar firewalls basados en host o filtrado de puertos

La habilitación de un *firewall* basado en *host* en los puntos finales reducirá la posibilidad del atacante de moverse lateralmente a través de la red. También reducirá la posibilidad de que un ransomware se propague por la red porque las estaciones de trabajo de los usuarios no necesitan hablar con otras estaciones de trabajo y dicha comunicación puede bloquearse. Se puede utilizar Windows Firewall para cubrir este subcontrol.

CSC 9.5: Implementar firewalls de aplicaciones

Las aplicaciones y los servidores externos suelen ser muy específicos porque ofrecen un pie en la puerta de la red de la organización. Los *firewalls* de aplicaciones web

(WAF) inspeccionan el tráfico para identificar y bloquear el tráfico anormal. ModSecurity se puede utilizar para implementar este subcontrol. ModSecurity es un WAF multiplataforma de código abierto. Se puede configurar bajo pfSense.

- **Control 12: Defensa de límites:**

  Según Shamma, B. (2018), este control se enfoca en proteger y monitorear los puntos de entrada y salida de la red. Los datos que ingresan y salen de la organización se pueden examinar para identificar anomalías y monitorear a los atacantes. Este control CIS tiene 12 subcontroles:

  CSC 12.1: Mantener un inventario de los límites de la red

  El primer subcontrol requiere que las organizaciones se mantengan al día con los dispositivos de límite de la red. Si una organización implementó el "Control 1: Inventario de Dispositivos autorizados y no autorizados", puede usar OpenVAS para rastrear e identificar los dispositivos fronterizos. Esto también se puede lograr usando un escaneo Nmap.

  CSC 12.2: Escanear en busca de conexiones no autorizadas a través de los límites de la red confiable

  Siguiendo el subcontrol anterior, las organizaciones pueden escanear el exterior y el interior de cada red para eliminar los puntos ciegos o los dispositivos que faltan detrás de un enrutador o un *firewall*. Esto también se puede lograr usando OpenVAS.

CSC 12.3: Denegar comunicaciones con direcciones IP maliciosas conocidas

Si se identificó una IP mala o maliciosa, se puede bloquear en el *firewall* perimetral para eliminar cualquier intento de ataque adicional. Este subcontrol se puede implementar utilizando las reglas del cortafuegos pfSense.

CSC 12.4: Denegar comunicación a través de puertos no autorizados

Las organizaciones pueden tener una lista de puertos y protocolos autorizados o aprobados en toda la empresa y en el perímetro. No se puede permitir que ningún puerto o protocolo no aprobado se comunique y se desconecte de inmediato. Este subcontrol también se puede implementar usando pfSense.

CSC 12.5: configurar sistemas de monitoreo para registrar paquetes de red

Este subcontrol requiere la implementación de un sistema de captura de paquetes. La captura de paquetes en vivo proporcionará una gran cantidad de información y puede ser invaluable para identificar o contener incidentes. Security Onion se puede utilizar para implementar este subcontrol. Las organizaciones también pueden implementar Moloch, que es un sistema de indexación y captura de paquetes completo de código abierto.

CSC 12.6: Implementar sensor IDS basado en red

La implementación de este subcontrol puede ayudar a las organizaciones a identificar ataques basados en la red. Los sistemas de detección de intrusiones en la red (NIDS) suelen ser ruidosos y producen una cantidad decente de alertas de falsos positivos. Las organizaciones pueden ajustar NIDS para hacerlo más eficiente. Este subcontrol se puede implementar usando Security Onion, que tiene Snort o Suricata funcionando

fuera de la caja. pfSense también tiene la capacidad de actuar como un sistema NIDS. Bro IDS también se incluye en Security Onion y también se puede utilizar para identificar comportamientos anormales del tráfico.

CSC 12.7: Implementar sistemas de prevención de intrusiones basados en red

Los sistemas de prevención de intrusiones en la red (NIPS) no solo identificarán una intrusión, sino que también bloquearán automáticamente la dirección IP atacante. Una organización puede usar NIPS cuando tiene mucha confianza en que la IP de origen es maliciosa. De lo contrario, las direcciones IP legítimas podrían bloquearse automáticamente. Este subcontrol se puede implementar mediante el uso de scripts pfSense o una llamada a la API de Snort o Suricata en Security Onion. O habilitando Snort o Suricata como parte de pfSense.

CSC 12.8: Implementar NetFlow Collection en dispositivos de límite de red

Dependiendo del tamaño de la organización, este subcontrol puede proporcionar visibilidad adicional a los dispositivos que hablan internamente si no están siendo capturados por CSC 12.5. NetFlow puede resultar muy útil para comprender el tráfico que viaja a través de los puntos finales sin salir del parámetro. ntopng se puede instalar en Security Onion para habilitar la recopilación de NetFlow. NetFlow también se puede capturar directamente desde la interfaz de monitoreo usando nfdump. Las organizaciones también pueden utilizar ElastiFlow o SOF-ELK como solución alternativa.

CSC 12.9: Implementar servidor proxy de filtrado de capa de aplicación

Como se discutió en CSC 9.5, el uso de pfSense junto con ModSecurity ayudará a analizar el tráfico y los ataques de la capa de aplicación. Otra opción disponible que se puede utilizar es OpenAppID, que se centra en el análisis de la capa de aplicación y la detección de ataques. Funciona como un módulo Snort.

CSC 12.10: Descifrar el tráfico de red en el proxy

Muchos de los subcontroles de este control resultarán inútiles si el tráfico está cifrado. Los IDS se basan en firmas y no identifican ningún ataque ya que los paquetes no son legibles. Las organizaciones pueden usar el proxy Squid para descifrar el tráfico instalando el certificado Squid en todos los puntos finales que apuntan al proxy Squid. Una organización puede colocar sensores IDS o IPS internamente antes de que el tráfico se cifre en el punto de salida.

CSC 12.11: Requerir que todos los inicios de sesión remotos utilicen la autenticación multifactor

Este subcontrol ayudará a reducir la amenaza de los atacantes que utilizan credenciales comprometidas para conectarse de forma remota a la red de una organización. Hay varias formas de implementar este subcontrol. Una organización puede utilizar pfSense, OpenVPN, RADIUS o FreeRADIUS y Windows PKI. También se puede implementar usando pfSense, OpenVPN y las soluciones mencionadas anteriormente: privacyIDEA, LinOTP y gluu.

CSC 12.12: administrar todos los dispositivos que inician sesión de forma remota en la red interna

Este subcontrol recomienda asegurarse de que los dispositivos que han salido de la red de la organización se escaneen y se identifique que estén libres de infecciones antes de que se les permita ingresar a la red. Si bien no hay OSSS para cubrir este subcontrol por completo, Wazuh se puede usar para alertar sobre una infección o un cambio de configuración y luego un administrador puede bloquear el dispositivo manualmente usando una solución de control de acceso a la red (NAC) como PacketFence.

- **Control 14: Control de Acceso basado en la necesidad de saber:**

  Según Shamma, B. (2018), este control CIS sigue el control CIS anterior para proteger los sistemas críticos y la información sensible. Este control CIS ayuda a la organización a limitar la capacidad de un atacante para acceder a datos confidenciales moviéndose lateralmente. La implementación de este control CIS también puede ayudar con el seguimiento de los cambios en los datos confidenciales. Este control CIS tiene nueve subcontroles:

CSC 14.1: Segmentar la red según la sensibilidad

El primer subcontrol fomenta la clasificación de los segmentos de la red en función de la sensibilidad de los datos dentro de la red. Este subcontrol se centra en el lado lógico de la segmentación de la red. Una organización puede utilizar una política o un proceso para garantizar que las redes estén segmentadas correctamente. Las organizaciones pueden agrupar activos con la misma función o el nivel de acceso a los datos necesarios en el mismo segmento. Este subcontrol requiere una política implementada para asegurar la cobertura.

CSC 14.2: habilitar el filtrado de firewall entre VLAN

Las reglas de *firewall* no solo son útiles en el perímetro, sino que también son muy útiles dentro de la red. Las reglas de *firewall* de pfSense se pueden usar para especificar cómo se debe permitir o denegar el tráfico de las VLAN. Un ejemplo de esta implementación sería negar cualquier tráfico de la VLAN del departamento de marketing a la VLAN de investigación y desarrollo. pfSense se puede utilizar para implementar este subcontrol.

CSC 14.3: Desactivación de la comunicación de estación de trabajo a estación de trabajo

Los mismos principios y discusión para CSC 14.2 también se aplican a este subcontrol.

CSC 14.4: cifrar toda la información confidencial en tránsito

Este subcontrol limitará la capacidad de un atacante para interceptar el tráfico mediante la escucha clandestina una vez dentro de la red. Las organizaciones pueden implementar una política o un proceso para garantizar que todo el tráfico esté encriptado mientras está en tránsito. Se puede utilizar un *software* o proceso específico según el tipo de tráfico.

CSC 14.5: Utilice una herramienta de descubrimiento activa para identificar datos confidenciales

Este subcontrol requiere identificar todos los datos confidenciales en cualquier lugar y en cualquier sistema, no solo los de la red. MyDLP se puede utilizar para implementar este subcontrol.

CSC 14.6: proteger la información a través de listas de control de acceso

Este subcontrol se centra en el uso de ACL para identificar quién puede acceder a los datos confidenciales. Este subcontrol se puede implementar en archivos almacenados en sistemas, recursos compartidos de red, bases de datos y acceso a aplicaciones. Este subcontrol recomienda a las organizaciones que otorguen acceso a los usuarios en función de sus necesidades y funciones comerciales. Aunque este subcontrol es más un proceso, Microsoft Active Directory junto con los GPO de Windows se pueden utilizar para implementar este control.

CSC 14.7: Hacer cumplir el control de acceso a los datos a través de herramientas automatizadas

Este control complementa CSC 14.5 al fomentar el uso de soluciones DLP basadas en *host*. Este subcontrol agrega otra capa de detección y protección al rastrear activamente los datos confidenciales en los puntos finales. Este subcontrol se puede cubrir instalando agentes de Windows o Linux de MyDLP en los puntos finales. El agente de Windows también se puede enviar mediante GPO de Microsoft Windows.

CSC 14.8: Cifrar información confidencial en reposo

Este subcontrol requiere agregar otra capa de protección para descifrar los datos confidenciales en reposo mediante un mecanismo de autenticación secundario no integrado en el sistema operativo. Una organización puede usar BitLocker junto con dispositivos Trusted Platform Module (TPM) o unidades USB para implementar este subcontrol.

CSC 14.9: Hacer cumplir el registro de detalles para el acceso o los cambios a datos confidenciales

El seguimiento de quién y cuándo alguien accedió o modificó información confidencial es muy importante para cualquier organización. Una organización puede usar un Wazuh para monitorear tales actividades.

- **Control 18: Seguridad del software de aplicación:**

  Según Shamma, B. (2018), este control se centra en proteger las aplicaciones desarrolladas internamente. Existe una mayor probabilidad de que una aplicación desarrollada internamente sea más vulnerable debido a la falta de recursos para las pruebas de seguridad adecuadas antes de lanzar la aplicación. Este control CIS tiene 11 subcontroles:

CSC 18.1: Establecer prácticas de codificación seguras

Este subcontrol requiere que una organización establezca una política y un proceso para garantizar que los miembros del equipo de desarrollo sigan un proceso de codificación seguro. Una organización puede consultar el Proyecto de ciclo de vida de desarrollo de *software* seguro (S-SDLC) del Proyecto de seguridad de aplicaciones web abiertas (OWASP) para examinar las pautas y las mejores prácticas.

CSC 18.2: Asegúrese de que se realice una verificación de errores explícita para todo el software desarrollado internamente

Los errores de aplicación suelen proporcionar información valiosa a los atacantes. Algunos errores pueden revelar ciertos ajustes de configuración o la ubicación de los archivos de configuración. Las organizaciones pueden implementar este subcontrol

aplicando una política y un proceso para desinfectar cualquier error de aplicación con un mensaje genérico en lugar de uno detallado.

CSC 18.3: Verifique que el software adquirido aún sea compatible

Las organizaciones pueden implementar este control utilizando una política y un proceso para identificar la versión de un *software* adquirido externamente para el soporte del proveedor.

CSC 18.4: Use solo componentes de terceros actualizados y confiables

Muchas aplicaciones desarrolladas internamente utilizarán componentes de terceros. Las organizaciones pueden implementar este subcontrol utilizando una política y un proceso para garantizar que todos los terceros tengan actualizaciones compatibles del proveedor y se actualicen tan pronto como los componentes se integren con la aplicación interna.

CSC 18.5: Utilice solo algoritmos de cifrado estandarizados y ampliamente revisados

Las organizaciones pueden implementar este subcontrol utilizando una política y un proceso para garantizar que los desarrolladores se abstengan de utilizar algoritmos internos especialmente desarrollados para aplicaciones internas. En cambio, los desarrolladores pueden usar un algoritmo popular para reducir el riesgo de romper el algoritmo.

CSC 18.6: Asegúrese de que el personal de desarrollo de software esté capacitado en codificación segura

Las organizaciones pueden implementar este subcontrol utilizando una política y un proceso para capacitar a los desarrolladores internos en la codificación segura. Dependiendo del lenguaje de programación principal utilizado para desarrollar la aplicación, una organización puede encontrar muchas pautas sobre cómo codificar de forma segura utilizando ese lenguaje de programación.

CSC 18.7: Aplicar herramientas de análisis de código estático y dinámico

Las organizaciones pueden implementar este subcontrol mediante la utilización de una política y un proceso para utilizar herramientas de análisis de código estático y dinámico al desarrollar aplicaciones. OWASP tiene una gran referencia a algunas de las herramientas que se pueden utilizar para cubrir este subcontrol. Además, la comunidad ha compilado una lista de herramientas que se pueden utilizar para cubrir este control.

CSC 18.8: Establecer un proceso para aceptar y abordar informes de vulnerabilidades de software

Las organizaciones pueden implementar este control utilizando una política y un proceso para iniciar un programa de recompensas por errores u otros programas similares para permitir que las entidades externas prueben la aplicación de una organización. Si bien no será fácil implementar este subcontrol usando OSSS, las organizaciones pueden permitir que diferentes equipos internos de Control de Calidad (QA) prueben diferentes aplicaciones que los equipos de QA nunca probaron antes.

CSC 18.9: Sistemas separados de producción y no producción

Las organizaciones pueden implementar este subcontrol utilizando una política y un proceso para obligar a los desarrolladores a usar sistemas separados e incluso redes para probar la aplicación antes de lanzarla a producción.

CSC 18.10: Implementar firewalls de aplicaciones web (WAF)

Los WAF pueden reducir significativamente el riesgo asociado con las aplicaciones web vulnerables. Los WAF tienen la capacidad de identificar la entrada del usuario y desinfectar la salida del servidor de aplicaciones web. Las organizaciones pueden implementar este subcontrol utilizando pfSense y ModSecurity.

CSC 18.11: Utilice plantillas de configuración de refuerzo estándar para bases de datos

Tal como se menciona en el "Control 5: Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores", las configuraciones seguras deben aplicarse a todos los activos de la organización, incluidas las bases de datos. Las bases de datos suelen estar dirigidas por la cantidad de datos valiosos almacenados y una amplia gama de vulnerabilidades. Las organizaciones pueden implementar este subcontrol utilizando CIS Benchmarks como guía para configurar de forma segura diferentes tipos de bases de datos. Los GPO también se pueden utilizar para garantizar que las configuraciones seguras se apliquen y no se modifiquen con el tiempo.

3.2. Discusión

Dando los seguimientos de las herramientas de reconocimiento del Hacking Ético, descritos en adición al diagrama de casos de usos, se puede llegar a encontrar información sensible en cualquier entidad privada o pública. Dicha información es un riesgo, en la que un *hacker* de sombrero negro puede realizar ataques en la que puede impactar todo el sistema del dominio público como se puede visualizar en la siguiente imagen.

En algunos casos, al usar la herramienta de la DNSDumpster sobre el dominio de una entidad, no muestra el servidor principal del dominio público de la entidad. Sin embargo, al usar la herramienta WhoIs, nos muestra la dirección IP del posible servidor principal del dominio público de la entidad, donde dicha IP al ser analizada en la herramienta DNSDumpster nos puede mostrar la información del posible servidor principal del dominio público de la entidad objetivo.

Mediante el uso de Google Hacking se puede obtener información sensible de clientes, personal, aplicaciones, accesos de la entidad objetivo. Con esta información, un hacker de sombrero negro podría crear un diccionario de contraseñas para lograr acceder al correo laboral y/u otra aplicación de la entidad con el fin de extraer información sensible de la entidad, enviar correos phishing, etc.

Mediante el uso de Google Hacking, se obtiene información sensible de los equipos, aplicaciones, etc., con la cual se podría buscar y comprar alguna vulnerabilidad o *zero-day* para algún equipo, aplicación y/o sistema específico, para así lograr acceder al sistema de la entidad.

Se propone el uso de Controles de Seguridad para la Ciberdefensa (CIS) a comparación de las 10 cláusulas de la norma del ISO 27001, según ISOTools (2021) (Objeto, Referencias normativas, Términos y definiciones, Contexto de la organización, Liderazgo, Planificación, Soporte, Operación, Evaluación del desempeño y Mejora) ya que dichas clausulas son conformados por un sistema de gestión de la seguridad de la información (SGSI). En la cual, se trata de un enfoque que permite el manejo seguro de la información confidencial de una compañía e incluye los usuarios, procesos, sistemas informáticos y la aplicación de un proceso de riesgos, que apoya a pequeñas, medianas y grandes empresas a mantener los activos de información de manera segura. Sin embargo, el ISO 27001 es solo un estándar que describe requisitos en la cual te indica lo que debes aplicar a la seguridad informática del dominio público, pero no describe a detalle de cómo hacerlo, por lo que depende de otros estándares o mejores prácticas de ISO (ISO 27002, ISO 27799, entre otros) para la implementación de ISO 27001. Por ello, optamos por el CIS, ya que tiene la ventaja de que nos brinda a detalle la aplicación de seguridad informática.

Conclusiones

- Con relación a las herramientas utilizadas de la fase de reconocimiento de Ethical Hacking: la herramienta DnsDumspter puede identificar rápidamente posibles vulnerabilidades en base a los servicios que estén operando en los servidores del dominio público de cualquier entidad, aunque dicha información debe ser corroborada mediante las herramientas de la fase de escaneo de Ethical Hacking. Por otra parte, mediante las herramientas Google Hacking, y WhoIs permiten a cualquier entidad identificar qué información sensible está expuesta públicamente, facilitando el acceso ilícito de un hacker de sombrero negro hacia la entidad objetivo. Cabe resaltar, que el uso de estas herramientas no ejerce mecanismos de intrusión de fuerza bruta, respetando los Artículo 207°-A y 207°-B de la ley N° 30096, y los Artículo N° 2, 3 y 4 de la ley N° 30096, por lo cual pueden ser utilizados por el personal de la entidad e informar lo encontrado por estas herramientas, para que un especialista de ciberseguridad de la entidad pueda analizar a estas posibles brechas de seguridad detectadas y proporcionar alguna solución.

- Con relación al Objetivo específico 1, se identificó que la herramienta más importante es Google Hacking, porque a diferencia de la herramienta DNSDumpster, la información obtenida por Google Hacking no necesita ser validada por otra herramienta de la fase de escaneo de Hacking Ético, porque Google Hacking identifica exactamente los accesos, agujeros de seguridad, malas configuraciones, y archivos de la entidad que se encuentren expuestos públicamente. A pesar de que, se requiere conocimiento previo para ejecutar los comandos, “Dorks” o “Google Dorks” de búsqueda avanzada, Google Hacking demuestra una notable rapidez en la

obtención de los resultados cuando se tiene en conocimiento los comandos o "Dorks" a ejecutar, logrando encontrar las brechas de seguridad y/o información sensible. Como consecuencia, si un hacker de sombrero negro mediante el uso de Google Hacking encontrara alguna brecha de seguridad, o algún archivo con información sensible, podría buscar en páginas de venta de la *DarkWeb* y buscar alguna vulnerabilidad o un *zero-day* de los equipos, aplicaciones y/o sistemas usados en las entidades, y con esto acceder al sistema permitiéndole al atacante utilizar la información de la entidad con el fin de realizar transacciones ilícitas, usurpación de identidad, robo y venta de información, etc. A su vez, el hacker de sombrero negro podría generar un diccionario de contraseñas para poder ejecutar un "ataque de fuerza bruta" que consiste en ingresar al sistema de alguna entidad mediante la repetición del uso de un diccionario que recombina palabras con miles de combinaciones diferentes en base a la información recopilada de los archivos de información sensible expuestas públicamente.

- Adicionalmente, dentro del Objeto especifico 1, el uso de la herramienta DnsDumpster y de WhoIs no requieren de conocimiento previo, pues solo se necesita ingresar el dominio o la IP del servidor de la entidad a analizar. También son de fácil ejecución y no toman mucho tiempo en adquirir los resultados. En el caso de la herramienta DNSdumpster puede tener una ligera demora no más de 30 segundos, dependiendo de la complejidad del dominio público de la entidad a analizar, porque DNSdumpster no utiliza ninguna enumeración de subdominios por fuerza bruta, ya que utiliza recursos de inteligencia de código abierto para consultar datos de dominio, obtenidos mediante consultas en plataformas como Alexa Top 1 Million, motores de búsqueda (Google, Bing, etc), Common Crawl, Certificate Transparency, Max Mind,

Team Cymru, Shodan y scans.io, por lo cual, toda información obtenida por la herramienta DNSDumpster debe ser corroborada mediante las herramientas de la fase de escaneo de Hacking Ético.

- En lo que respecta al Objetivo específico 2, en base a las brechas de seguridad del dominio público, se concluye que es necesario la implementación de algunos controles críticos del CIS:

    - Control 3 - Gestión continua de Vulnerabilidades: en base a los posibles servicios en los servidores del dominio público de alguna entidad, sería necesario integrar programas de escaneo de vulnerabilidades como OpenVAS, Nmap, y programas de aplicación de parches en función de la gravedad de las vulnerabilidades. Estas herramientas le permitirán a cualquier entidad analizar las versiones de los servicios instalados y en ejecución.

    - Control 9 - Limitación y control de puertos, protocolos y servicios de red: en vista que los equipos del dominio público de las entidades presentan servicios web que utilicen puertos para diferentes protocolos sería necesario el uso de *firewalls* de aplicaciones web (WAF) como ModSecurity. Esto permite inspeccionar el tráfico de red para identificar y bloquear el tráfico anormal en cualquier entidad.

    - Control 12 - Defensa de límites: basado en la información sensible que puede ser obtenida por el uso de búsqueda avanzada (Google Hacking), se requiere integrar sistemas de prevención de intrusiones en la red (NIPS) como Security

Onion. Esto les permite a las entidades, monitorear los datos que ingresan y salen del dominio público para identificar anomalías y bloquearán automáticamente la dirección IP del atacante; o integrar servidor proxy de filtrado de capa de aplicación.

- Control 14 - Control de Acceso basado en la necesidad de saber: en el caso de identificar documentos con información sensible de alguna entidad, es necesario el uso de herramientas de descubrimiento activa como MyDLP, para que cualquier entidad pueda identificar la información sensible que esté presente en el dominio público, y proteger dicha información a través de listas de control de acceso para identificar quién puede acceder a los datos confidenciales de la entidad. Por otro lado, también se requiere el uso de servicios de DNS o WhoIs privado para ocultar la información de contacto del dominio público de cualquier entidad, porque mediante el uso de la herramienta Whois se puede mostrar información del dominio público, y la dirección IP del dominio público la entidad, donde ésta al ser analizada en la herramienta DNSDumpster se puede observar que servicios podrían estar en uso, sistemas operativos, bases de datos, etc.

- Control 18 - Seguridad del software de aplicación: es recomendable analizar el ciclo de vida de la seguridad de todo el *software* desarrollado y adquirido por la entidad, con el fin de reducir las vulnerabilidades que se encuentran en el *software* basado en la web y en otras aplicaciones de los equipos del dominio público de cualquier entidad.

Recomendaciones

- Con respecto al Objetivo específico 1, se recomienda el uso de la herramienta Google Hacking debido que identifica con precisión los accesos, agujeros de seguridad, malas configuraciones, y archivos de la entidad que se encuentren expuestos públicamente. Aunque, es necesario tener conocimientos previos para ejecutar los comandos de Google Hacking, tiene una rápida respuesta de los resultados. Y al no existir un orden específico para ejecutar los comandos, se recomienda ejecutar por grupo de comandos para detectar los diferentes tipos de brechas de seguridad, de los cuales se listan los comandos más comunes:
    - Listado de directorios (site:dominio.com intitle:index.of)
    - Archivos con información sensible (site:dominio.com ext:xml | ext:conf | ext:cnf | ext:reg | ext:inf | ext:rdp | ext:cfg | ext:txt | ext:ini)
    - Archivos de Base de datos (site:dominio.com ext:sql | ext:dbf | ext:mdb | ext:ora | ext:config mysql_connect)
    - Archivos de registros "logs" (site:dominio.com ext:log)
    - Inyecciones o errores de código SQL (site:dominio.com intext:"sql syntax near" | intext:"syntax error has occurred" | intext:"incorrect syntax near" | intext:"unexpected end of SQL command" | intext:"Warning: mysql_connect()" | intext:"Warning: mysql_query()" | intext:"Warning: pg_connect()")
    - Archivos expuestos a Internet (site:dominio.com ext:doc | ext:docx | ext:odt | ext:pdf | ext:rtf | ext:sxw | ext:psw | ext:ppt | ext:pptx | ext:pps | ext:csv)
    - Archivos backup (site:dominio.com ext:bkf | ext:bkp | ext:bak | ext:old | ext:backup)

- Con respecto al Objetivo específico 1, se recomienda el uso de la herramienta DnsDumpster, debido que es una herramienta de fácil ejecución, no toma mucho tiempo en adquirir los resultados, y no requiere de conocimiento previo. En su página principal solo se debe ingresar el dominio o la IP del servidor de la entidad a analizar, mostrando como resultado un listado de las direcciones IP del dominio público, DNS utilizados, aplicaciones web utilizadas, posible sistema operativo utilizado, entre otros datos. Aunque, esta información obtenida debe ser corroborada mediante las herramientas de la fase de escaneo de Ethical Hacking, proporciona un rápido indicio de las posibles brechas de seguridad en el dominio público de cualquier entidad. Por otra parte, DnsDumspter también nos muestra de manera gráfica la localización de donde proceden cada servidor, al igual que los dueños de los bloques de servidores, y también nos brinda la capacidad de descargar toda la información de los servidores de la entidad objetivo en un archivo de formato ".xlsx", y la infraestructura de red de los servidores en modo gráfico en una imagen de formato ".png".

- Con respecto al Objetivo específico 1, se recomienda el uso de la herramienta Whois, porque no requiere conocimientos previos, es fácil de ejecutar debido que solo se necesita ingresar el dominio o la IP del servidor objetivo, identificando de manera rápida el nombre del titular del dominio público, el estado del dominio público, los DNS registrados, información de algún contacto administrativo, y la dirección IP del dominio público de la entidad. Aunque, en ciertas páginas de WhoIs requerirá ingresar una autentificación captcha, previa al resultado de la herramienta.

- Con respecto al Objetivo específico 2, se recomienda programas de escaneo de vulnerabilidades como OpenVAS, Nmap, entre otros con el fin de examinar las

versiones de los servicios presentes en los equipos del dominio público, para que, en conjunto con programas de aplicación de parches, analizar los parches necesarios a implementar en función de la gravedad de las vulnerabilidades presentes en los servicios presentes en los servidores del dominio público de cualquier entidad, en base al Control 3 de CIS.

- Con respecto al Objetivo específico 2, se recomienda comparar regularmente los resultados de escaneos de vulnerabilidades consecutivos para identificar que las vulnerabilidades se han remediado de manera oportuna, en base al Control 3 de CIS.

- Con respecto al Objetivo específico 2, se recomienda defender los puertos utilizados para los servicios de los servidores del dominio público de cualquier entidad mediante el uso de *firewalls* de aplicaciones web (WAF) como ModSecurity, que inspeccione el tráfico de red para identificar y bloquear el tráfico anormal frente a ataques informáticos, en base al Control 9 de CIS.

- Con respecto al Objetivo específico 2, se recomienda integrar sistemas de prevención de intrusiones en la red (NIPS) como Security Onion que monitoreen los datos que ingresan y salen del dominio público para identificar anomalías y bloquearán automáticamente la dirección IP del atacante; o integrar servidor proxy de filtrado de capa de aplicación, para evitar ataques informáticos, en base al Control 12 de CIS.

- Con respecto al Objetivo específico 2, se recomienda revelar la existencia de datos confidenciales que estén presentes en el dominio público, mediante el uso de herramientas de descubrimiento activa como MyDLP, en base al Control 14 de CIS.

- Con respecto al Objetivo específico 2, se recomienda analizar los Grupos de Aislamiento Base, Grupos de equipos y Grupos de acceso de red (NAG) de los equipos del dominio público para identificar el servidor que está exponiendo públicamente documentos con información sensible de la entidad, se encuentra correctamente agrupado dentro de los Grupos de Aislamiento Base, Grupos de equipos y Grupos de acceso de red (NAG), en base al Control 14 de CIS.

- Con respecto al Objetivo específico 2, se recomienda proteger toda la información almacenada en sistemas con Listas de Control de Acceso específicas para sistema de archivos, redes, aplicaciones o bases de datos, para hacer cumplir que solo las personas autorizadas puedan tener acceso a la información, en base al Control 14 de CIS.

- Con respecto al Objetivo específico 2, se recomienda implementar servicios de DNS o WhoIs privado para ocultar la información contacto del dominio público, y la dirección IP del dominio público, donde mediante el uso de herramientas como Whois y DNSDumpster se puede acceder a información sensible de cualquier entidad, en base al Control 14 de CIS.

- Con respecto al Objetivo específico 2, se recomienda actualizar los servicios presentes en los equipos del dominio público de cualquier entidad, en base al Control 18 de CIS.

Referencias

Aguilar, S. & De la Cruz, V. (2015). *Implementación de una Solución de Hacking Ético para Mejorar la Seguridad en la Infraestructura Informática de la Caja Municipal de Sullana - Agencia Chimbote* (Tesis para optar el título profesional de Ingeniero de Sistemas e Informática). Universidad Nacional del Santa. Recuperado de http://repositorio.uns.edu.pe/bitstream/handle/UNS/1964/30710.pdf?sequence=1&isAllowed=y

Baltazar, J. & Campuzano, J. (2011). *Diseño e Implementación de un Esquema de Seguridad Perimetral para Redes de Datos. Caso práctico: Dirección General del Colegio de Ciencias y Humanidades* (Tesis para obtener el título de Ingeniero de Computación). Universidad Nacional Autónoma de México. Recuperado de http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/174/Version%20Final.pdf

Bermeo, J. (2017). *Implementación de Hacking Ético para la Detección y Evaluación de Vulnerabilidades de Red en la empresa Complex del Perú S.A.C.-Tumbes; 2017* (Tesis para optar el grado académico de Maestro en Ingeniería de Sistemas con mención en Tecnología de Información y Comunicación). Universidad Católica Los Ángeles de Chimbote. Recuperado de http://repositorio.uladech.edu.pe/bitstream/handle/123456789/10386/IMPLEMENTACION_SEGURIDAD_INFORMATICA_BERMEO_OYOLA_JEAN_CARLOS.pdf?sequence=4&isAllowed=y

Center of Internet Security (2019). *CIS Controls (V7.1)*.

Cisecurity (2021). *The 20 CIS Controls & Resources*. Recuperado de https://www.cisecurity.org/controls/cis-controls-list/

CVE (2021). *CVE - CVE-2017-3167*. Recuperado de https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3167

CVE (2021). *CVE - CVE-2017-7679*. Recuperado de https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7679

CVE (2021). *CVE - CVE-2019-0217*. Recuperado de https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0217

Daragon, F. (2021). *Comb: The Big Password Leak*. Recuperado de https://www.syhunt.com/en/?n=Articles.COMBPasswordLeak2021

Diazgranados, H. (2021). *47% de empresas latinas usa tecnología obsoleta dentro de su infraestructura de TI*. Recuperado de https://latam.kaspersky.com/blog/47-de-empresas-latinas-usa-tecnologia-obsoleta-dentro-de-su-infraestructura-de-ti/21321/

Edureka (2020). *Important Benefits Of Ethical Hacking*. Recuperado de https://www.edureka.co/blog/benefits-of-ethical-hacking/

El Peruano (2000). *Ley N° 27309 – Ley que incorpora los Delitos Informáticos al Código Penal*. Recuperado de https://cdn.www.gob.pe/uploads/document/file/356824/NORMA_1887_Ley_27309.pdf

El Peruano (2013). *Ley N° 30096 – Delitos Informáticos*. Recuperado de https://busquedas.elperuano.pe/normaslegales/ley-de-delitos-informaticos-ley-n-30096-1003117-1/

Espinosa, O. (2019). *Qué es y para qué sirve Whois*. Recuperado de https://www.redeszone.net/tutoriales/internet/que-es-whois/

Fortiguard (2021). *SMB.Login.Brute.Force*. Recuperado de https://www.fortiguard.com/encyclopedia/ips/12090/smb-login-brute-force

Fortiguard (2021). *SSH.Connection.Brute.Force*. Recuperado de https://www.fortiguard.com/encyclopedia/ips/35662/ssh-connection-brute-force

Fortiguard (2021). *W32/Bancos.CFR!tr*. Recuperado de https://www.fortiguard.com/encyclopedia/virus/537825

Fortiguard (2021). *W32/Generic_PUA_MC.FXK*. Recuperado de http://www.fortiguard.com.geo.fortinet.net/encyclopedia/virus/7615109

Fortinet (2021). *Threat Intelligence Insider*. Recuperado de https://www.fortiguardthreatinsider.com/es/bulletin/Q3-2021

Gestión (2020). *Los cinco ciberataques más frecuentes en el Perú*. Recuperado de https://gestion.pe/tecnologia/los-cinco-ciberataques-mas-frecuentes-en-el-peru-hackers-noticia/

GreyCampus (2021). *What is Ethical Hacking?*. Recuperado de https://www.greycampus.com/opencampus/ethical-hacking/what-is-ethical-hacking

Grupo Electrodata (2020). *Ciberdelincuentes hackearon el sistema del bono universal y robaron casi un millón de soles*. Recuperado de https://www.electrodata.com.pe/2020/06/09/6719/?fbclid=IwAR1DkpD7uWZs_nfomlg_-aUI_lX6zLXhh4B1gLmA6rFRipbpN7Zv1UYTmUE

HackerTarget (2019). *DNSdumpster*. Recuperado de https://dnsdumpster.com/

Harán, J. (2020). *El 42% de las empresas no estaba preparada para teletrabajar de forma segura*. Recuperado de https://www.welivesecurity.com/la-es/2020/06/23/teletrabajo-seguro-empresas-no-estaban-preparadas/

Hareesh, E. (2017). *Analyzing, Implementing and Monitoring Critical Security Controls: A Case Implemented in J & B Group* (Tesis para optar la Maestría en Ciencias en Aseguramiento de la Información). Universidad Estatal St. Cloud. Recuperado de https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1060&context=msia_etds

Hernández-Sampieri, R. (2014). *Metodología de la Investigación (6ta ed.)*.

Herrera, J. (2021). *Impacto ocupacional del trabajo remoto en docentes durante la emergencia sanitaria en una institución educativa. Chota - Cajamarca 2020* (Tesis para optar el Título Profesional de Licenciada en Tecnología Médica en el área de Terapia Ocupacional). Universidad Nacional Mayor de San Marcos. Recuperado de https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/16401/Herrera_fj.pdf?sequence=1&isAllowed=y

Incibe-Cert (2021). *Vulnerabilidad en Apache httpd (CVE-2017-3167)*. Recuperado de https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2017-3167

Incibe-Cert (2021). *Vulnerabilidad en Apache httpd (CVE-2017-7679)*. Recuperado de https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2017-7679

Incibe-Cert (2021). *Vulnerabilidad en Apache HTTP Server (CVE-2019-0217)*. Recuperado de https://www.incibe-cert.es/alerta-temprana/vulnerabilidades/cve-2019-0217

Infobae (2020). *Anonymous hackeó la web del Congreso de Perú tras la fuerte represión a las protestas por la destitución del presidente Vizcarra*. Recuperado de https://www.infobae.com/america/america-latina/2020/11/15/anonymous-hackeo-la-web-del-congreso-de-peru-tras-la-fuerte-represion-a-las-protestas-por-la-destitucion-del-presidente-vizcarra/

ISOTools (2021). *Software ISO 27001 Sistemas de Gestión de Riesgos y Seguridad*. Recuperado de https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

Jara, H. & Pacheco, F. (2012). *Ethical Hacking 2.0*. Recuperado de https://kupdf.net/downloadFile/5995f22fdc0d605539300d17

Kaspersky (2021). *¿Qué es una brecha de seguridad?*. Recuperado de https://www.kaspersky.es/resource-center/threats/what-is-a-security-breach

Kaspersky (2021). *Black hat, White hat, and Gray hat hackers – Definition and Explanation*. Recuperado de https://www.kaspersky.com/resource-center/definitions/hacker-hat-types

López, E. (2011). *Google Hacking para Pentesters*. Recuperado de http://index-of.co.uk/Google/Google-Hacking-para-Pentesters.pdf

Meyer, B. (2021). *COMB: largest breach of all time leaked online with 3.2 billion records*. Recuperado de https://cybernews.com/news/largest-compilation-of-emails-and-passwords-leaked-free/

Microsoft (2020). *Aislamiento de servidor y dominio mediante IPsec y Directiva de grupo*. Recuperado de http://exa.unne.edu.ar/informatica/redes-ap/apuntesAlumnos/ms-Dise%F1o%20y%20planificaci%F3n%20de%20grupos%20de%20aislamiento.pdf

Palomino, O. (2018). *Curso Ethical Hacking Básico*.

Paredes, J. (2015). *Modelo de seguridad de informática perimetral para reducir los riesgos de ataque al RENIEC* (Tesis para optar el Título de Ingeniero de Sistemas Empresariales). Universidad Científica del Sur. Recuperado de https://repositorio.cientifica.edu.pe/handle/20.500.12805/321

Pontiroli, S. (2020). *Kaspersky: América Latina registra 5 mil ataques de ransomware por día*. Recuperado de https://latam.kaspersky.com/about/press-releases/2020_kaspersky-america-latina-registra-5-mil-ataques-de-ransomware-por-dia

Poston, H. (2020). *What are black box, grey box, and white box penetration testing?*. Recuperado de https://resources.infosecinstitute.com/topic/what-are-black-box-grey-box-and-white-box-penetration-testing/

PricewaterhouseCoopers (2018). *Encuesta Global Sobre Delitos Económicos y Fraude 2018*. Recuperado de https://www.pwc.pe/es/publicaciones/assets/brochures/GECS2018_2.pdf

Redscan (2021). *NIST NVD ANALYSIS 2020*. Recuperado de https://www.redscan.com/media/Redscan_NIST-Vulnerability-Analysis-2020_v1.0.pdf

Rojas, K. (2019). *Sistemas biométricos, el nuevo blanco de los ataques a instituciones financieras*. Recuperado de https://gestion.pe/tecnologia/sistemas-biometricos-nuevo-blanco-ataques-instituciones-financieras-263895-noticia/

Romero, G. (2019). *Hacking ético, 1*. Recuperado de https://cronicaseguridad.com/2019/02/05/hacking-etico-1/

RPP (2020). *Anonymous hizo caer las páginas web del Congreso y varios sitios del gobierno*. Recuperado de https://rpp.pe/tecnologia/redes-sociales/anonymous-paginas-web-del-congreso-y-varios-sitios-del-gobierno-se-restablecen-tras-caida-noticia-1304238

Rus, E. (2021). *Investigación aplicada*. Recuperado de https://economipedia.com/definiciones/investigacion-aplicada.html

Shamma, B. (2018). *Implementing CIS Critical Security Controls for Organizations on a low-budget* (Tesis para optar la Maestría en Ciencias de la Seguridad del Sistema de Información). Universidad de Houston. Recuperado de https://uh-ir.tdl.org/bitstream/handle/10657/4048/SHAMMA-THESIS-2018.pdf

Sigwadi, W. (2014). *The Adoption and Use of Ethical Hacking to Secure Information in Small Companies* (Tesis para optar la licenciatura en Tecnología en TI:

Redes de comunicación). Universidad Walter Sisulu. Recuperado de https://www.academia.edu/29496652/THE_ADOPTION_AND_USE_OF_ETHICAL_HACKING_TO_SECURE_INFORMATION_IN_SMALL_COMPANIES

The Apache Software Foundation (2020). *Httpd 2.4 vulnerabilities*. Recuperado de https://httpd.apache.org/security/vulnerabilities_24.html

Tyas, A. (2021). *What is Information Security?*. Recuperado de https://www.upguard.com/blog/information-security

U.S. DOI (2021). *Penetration Testing*. Recuperado de https://www.doi.gov/ocio/customers/penetration-testing

Velasco, R. (2019). *Obtén toda la información de un dominio en segundos con DNSdumpster*. Recuperado de https://www.redeszone.net/2019/01/19/dnsdumpster-informacion-dominio/

Vishwas, V. (2018). *Implementing CIS Cybersecurity Controls for the Department of Residence, Iowa State University* (Tesis para optar la Maestría en Ciencias en Sistemas de Información). Universidad del Estado de Iowa. Recuperado de https://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=1130&context=creativecomponents

Vuldb (2021). *Vulnerability Database*. Recuperado de https://vuldb.com/es/

QuestionPro (2021). *¿Qué es la investigación descriptiva?*. Recuperado de https://www.questionpro.com/blog/es/investigacion-descriptiva/

QuestionPro (2021). *¿Qué es la investigación no experimental?*. Recuperado de https://www.questionpro.com/blog/es/investigacion-no-experimental/

QuestionPro (2021). *¿Qué es una encuesta?*. Recuperado de https://www.questionpro.com/es/una-encuesta.html

QuestionPro (2021). *5 ejemplos de escalas Likert para tu próxima encuesta*. Recuperado de https://www.questionpro.com/blog/es/ejemplos-de-escalas-likert/

Whois (2021). *Whois Domain Lookup*. Recuperado de https://www.whois.com/whois/

Anexos

Anexo N°01: Listado de comandos de búsqueda avanzada de Google Hacking

Tabla 27
Listado de comandos de búsqueda avanzada de Google Hacking

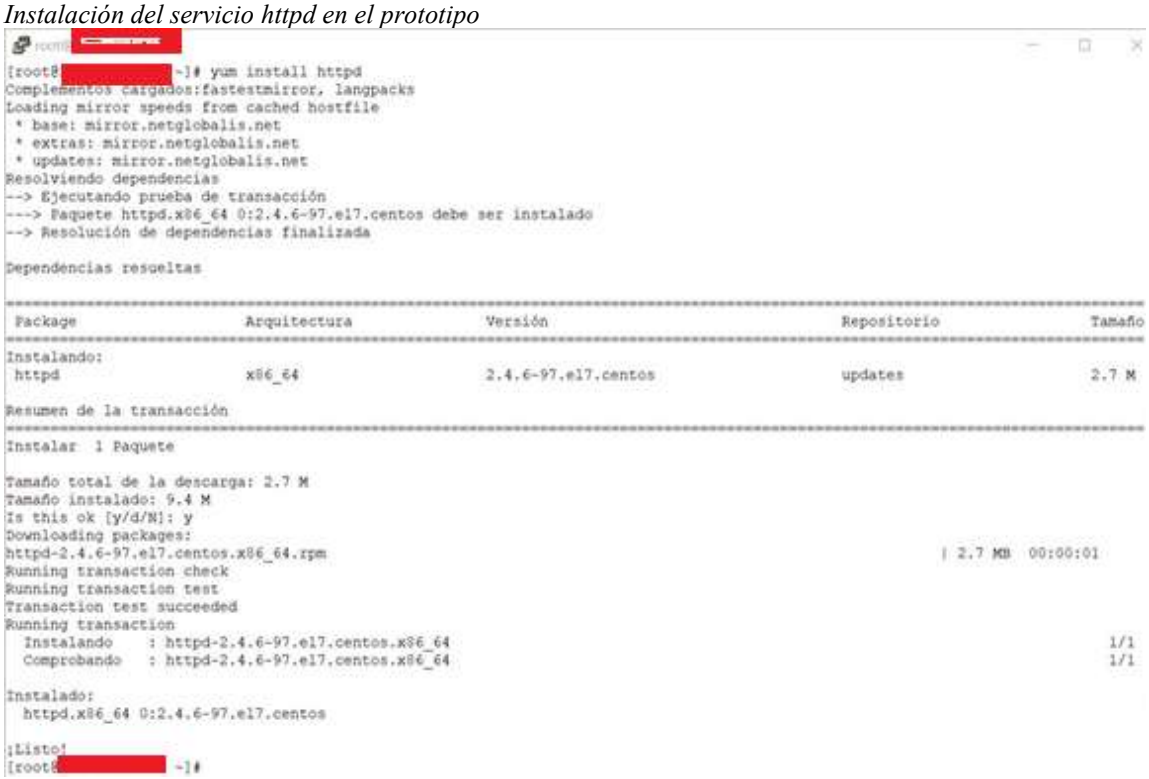
Comandos	Ejemplo de búsqueda en Google	Propósito
site	site:chevrolet.com.pe	Buscar resultados dentro de un sitio específico
intitle	intitle:chevrolet	Buscar en el título de la página
inurl	inurl:chevrolet	Buscar una palabra contenida en una URL
cache	cache:chevrolet.com.pe	Buscar la versión del sitio en caché
define	define:chevrolet	Busca la definición de una palabra que no conozcas
info	info:www.chevrolet.com.pe	Te muestra resultados donde se ofrezca información sobre una página web.
link	link:www.chevrolet.com.pe	Te muestra en los resultados páginas que tienen enlaces a la web que hayas especificado.
inanchor	inanchor:"autos deportivos"	Resultados con páginas donde se incluya un enlace con un texto anclado donde se incluya uno o varios términos especificados.
related	related:chevrolet.com.pe	Buscar sitios relacionados
intext	intext:chevrolet	Buscar en el texto del sitio web solamente
filetype	filetype:pdf	Buscar por tipos de archivo específicos
+	chevrolet + camaro	Buscar más de una palabra clave
–	chevrolet - camaro	Excluir palabras de la búsqueda
*	how to * Chevrolet	Operador de comodín
“”	“Chevrolet”	Buscar palabra por coincidencia exacta
( )	("chevrolet" OR "yaris") -camaro	Te permite combinar operadores.
AND	chevrolet AND camaro	Busca páginas que incluya los dos términos especificados
OR	chevrolet OR yaris	Combinar dos palabras
AROUND	Autos around(8) Chevrolet	Resultados aparecen para dos palabras específicas, pero se determina el número de términos entre ellas.
imagesize	imagesize:320×320	Búsqueda de imágenes por tamaño
@	@wikipedia	Buscar en redes sociales
#	#chevrolet	Buscar hashtags

Fuente: López, E. (2011)

Anexo N°02: Prototipo del uso completo del Hacking Ético en una máquina virtual similar a un servidor del dominio público de una entidad

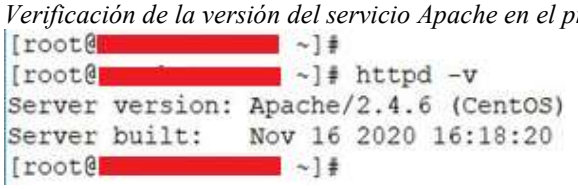
Se realizó un prototipo de manera virtual de un servidor del dominio público de una entidad (ver Figura 16 y 17).

Figura 16
Instalación del servicio httpd en el prototipo



Fuente: Elaboración propia

Figura 17
Verificación de la versión del servicio Apache en el prototipo

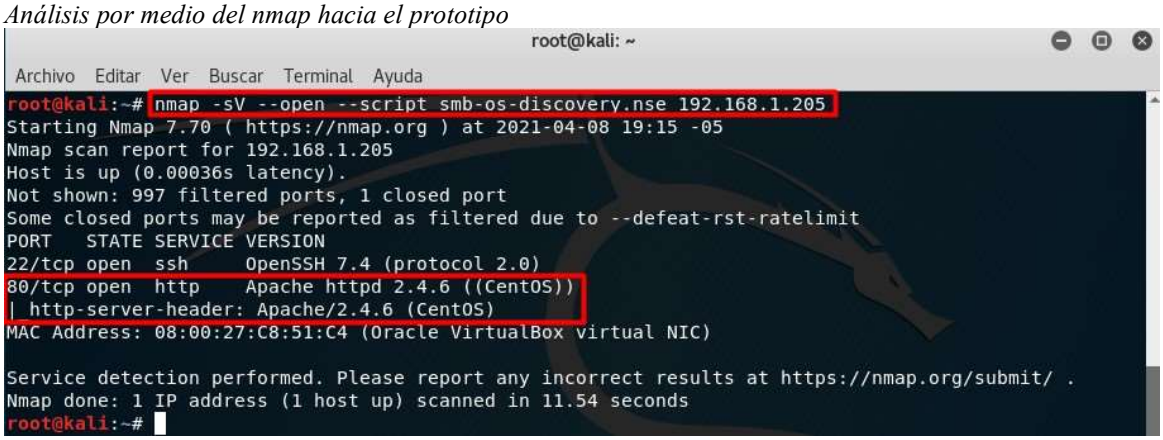


Fuente: Elaboración propia

En base a las Figuras 16 y 17, se instaló un servicio Apache httpd en la versión 2.4.6. Esta información podría ser identificada por la herramienta DNSDumpster, por lo que debería ser validado por la herramienta nmap (ver Figura 18). Nmap (*Network Mapper*) es una

herramienta gratuita de código abierto para el escaneo de redes y para la auditoría de seguridad, ejecutando tareas como detección del inventario de la red, versiones de servicio y sistema operativo, vulnerabilidades, etc.

Figura 18
Análisis por medio del nmap hacia el prototipo

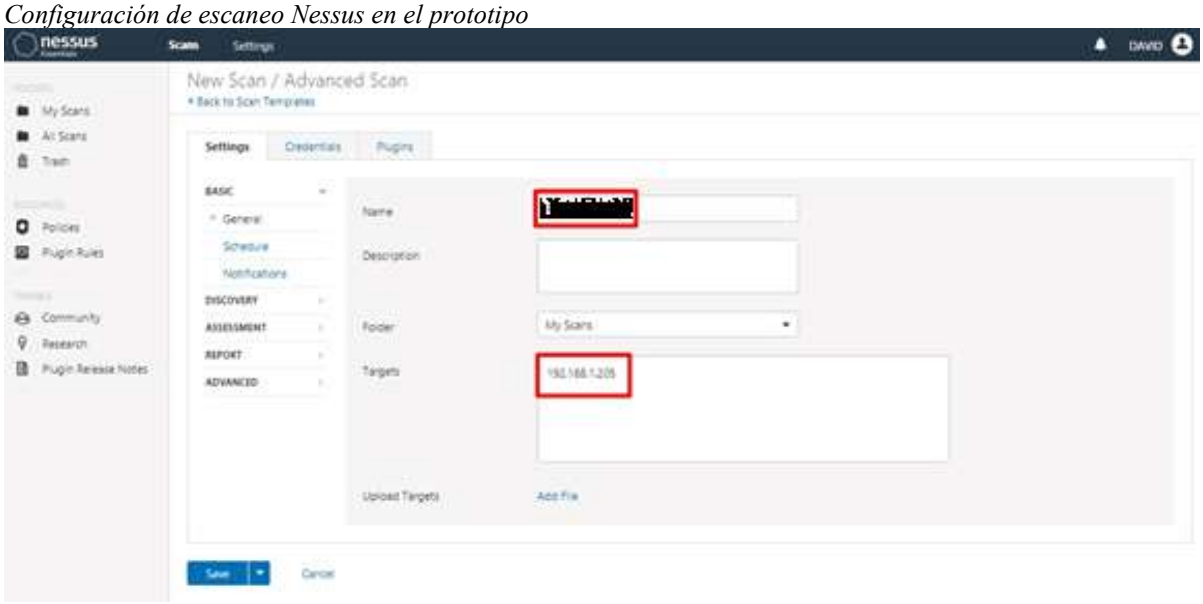


Fuente: Elaboración propia

Otra herramienta para escaneo de puertos y vulnerabilidades es el *software* Nessus en cual valida la información mostrada al igual que el nmap (ver Figura 19, 20, 21, 22 y 23). Nessus es un *software* de escaneo de vulnerabilidades en diversos sistemas operativos. Realiza un escaneo en el sistema objetivo, y muestra e informa de forma gráfica el avance sobre el estado de los escaneos.

Figura 19

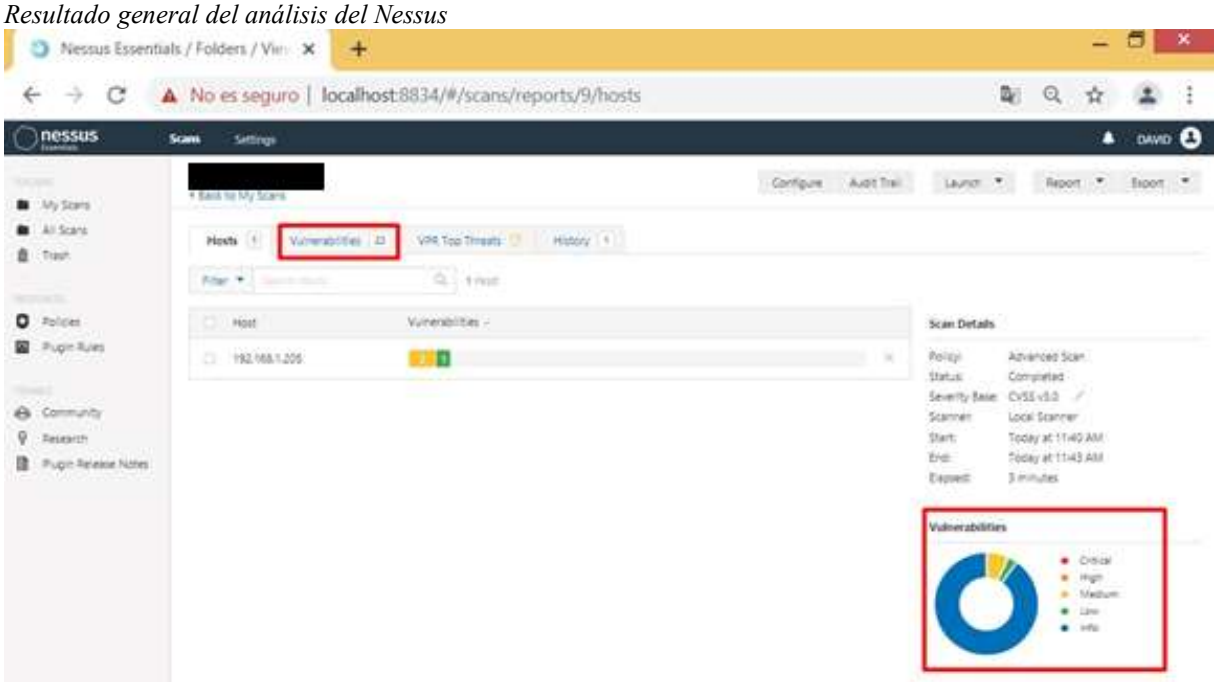
Configuración de escaneo Nessus en el prototipo



Fuente: Elaboración propia mediante la herramienta Nessus

Figura 20

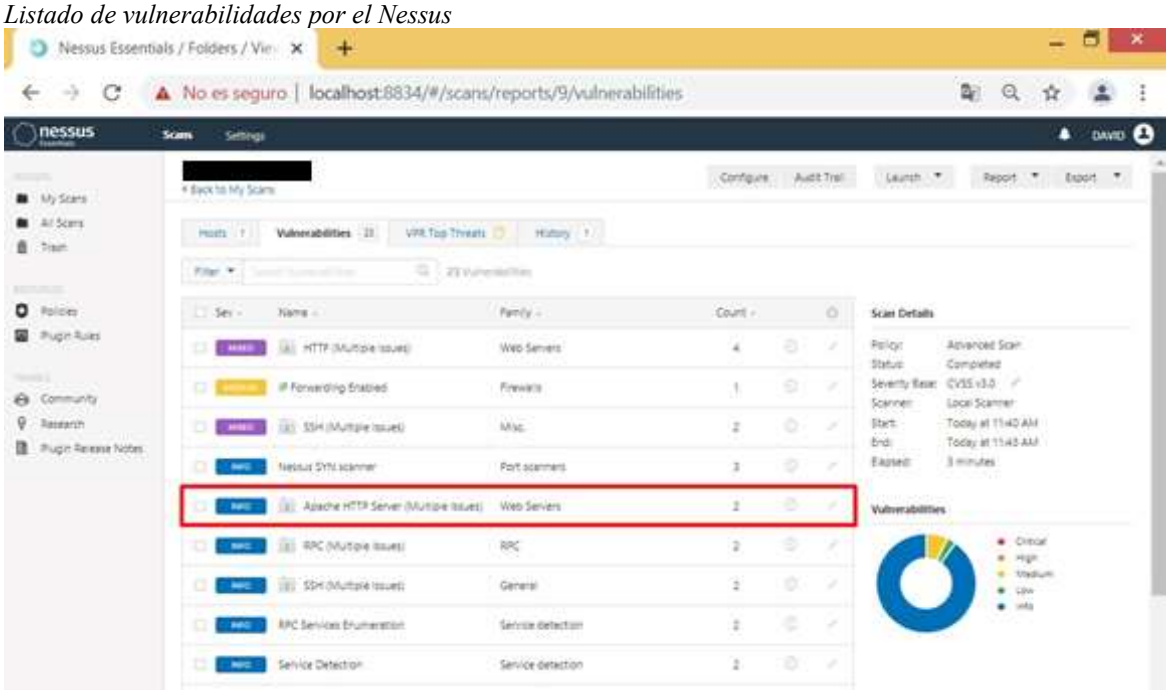
Resultado general del análisis del Nessus



Fuente: Elaboración propia mediante la herramienta Nessus

Figura 21

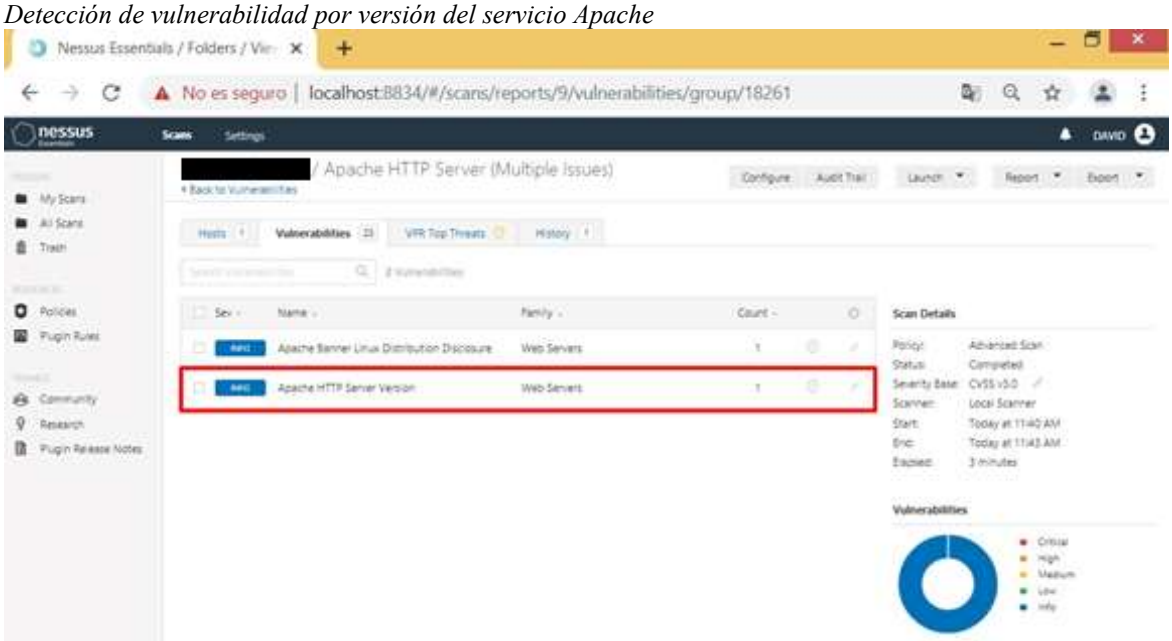
Listado de vulnerabilidades por el Nessus



Fuente: Elaboración propia mediante la herramienta Nessus

Figura 22

Detección de vulnerabilidad por versión del servicio Apache



Fuente: Elaboración propia mediante la herramienta Nessus

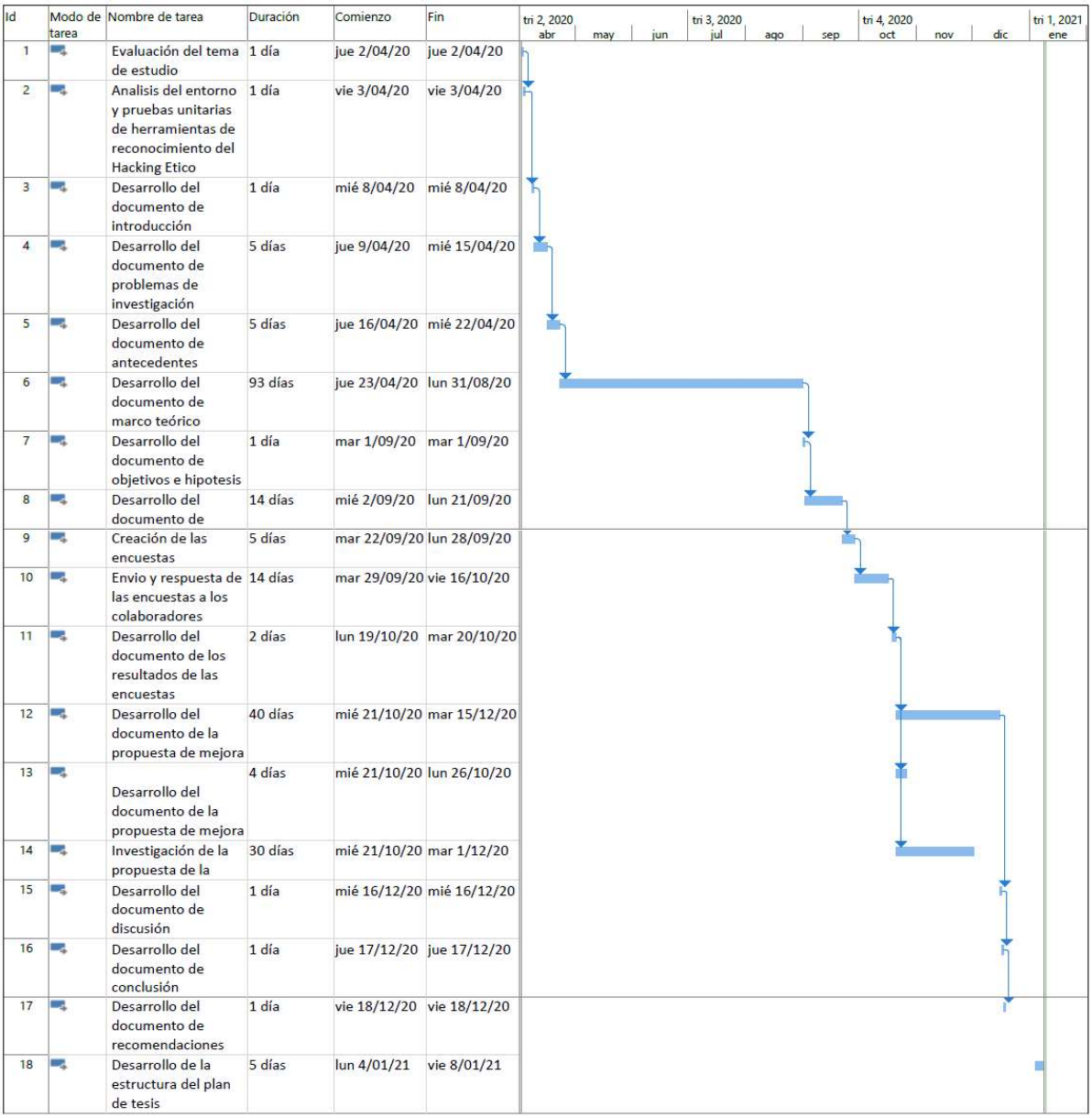
Figura 23

Información de la versión actual del Apache dentro del prototipo

Fuente: Elaboración propia mediante la herramienta Nessus

Anexo N°03: Cronograma de actividades

Figura 24
Cronograma de actividades



Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin
1		Evaluación del tema de estudio	1 día	jue 2/04/20	jue 2/04/20
2		Analisis del entorno y pruebas unitarias de herramientas de reconocimiento del Hacking Etico	1 día	vie 3/04/20	vie 3/04/20
3		Desarrollo del documento de introducción	1 día	mié 8/04/20	mié 8/04/20
4		Desarrollo del documento de problemas de investigación	5 días	jue 9/04/20	mié 15/04/20
5		Desarrollo del documento de antecedentes	5 días	jue 16/04/20	mié 22/04/20
6		Desarrollo del documento de marco teórico	93 días	jue 23/04/20	lun 31/08/20
7		Desarrollo del documento de objetivos e hipotesis	1 día	mar 1/09/20	mar 1/09/20
8		Desarrollo del documento de	14 días	mié 2/09/20	lun 21/09/20
9		Creación de las encuestas	5 días	mar 22/09/20	lun 28/09/20
10		Envio y respuesta de las encuestas a los colaboradores	14 días	mar 29/09/20	vie 16/10/20
11		Desarrollo del documento de los resultados de las encuestas	2 días	lun 19/10/20	mar 20/10/20
12		Desarrollo del documento de la propuesta de mejora	40 días	mié 21/10/20	mar 15/12/20
13		Desarrollo del documento de la propuesta de mejora	4 días	mié 21/10/20	lun 26/10/20
14		Investigación de la propuesta de la	30 días	mié 21/10/20	mar 1/12/20
15		Desarrollo del documento de discusión	1 día	mié 16/12/20	mié 16/12/20
16		Desarrollo del documento de conclusión	1 día	jue 17/12/20	jue 17/12/20
17		Desarrollo del documento de recomendaciones	1 día	vie 18/12/20	vie 18/12/20
18		Desarrollo de la estructura del plan de tesis	5 días	lun 4/01/21	vie 8/01/21

Fuente: Elaboración propia

Anexo N°04: Presupuesto

INVERSIÓN: S/. 1,950.00

Tabla 28
Presupuesto

Descripción	Cantidad	Precio Unidad (S/.)	Monto (S/.)
Computadora	1	1850	1850
Colaboración para los exempleados que nos ayudaron a completar la encuesta	20	5	100
		TOTAL S/.	1950

Fuente: Elaboración propia

Anexo N°05: Respuesta de las encuestas

	Respuesta de los encuestados									
Preguntas	**# 1**	**# 2**	**# 3**	**# 4**	**# 5**	**# 6**	**# 7**	**# 8**	**# 9**	**# 10**
En su área de trabajo, ¿ha sido afectado por algún incidente informático?	5	3	5	1	1	4	3	5	2	2
En su área de trabajo, ¿han recibido correos *phishing* en su correo laboral?	1	1	2	2	1	4	1	3	2	4
En su área de trabajo, ¿se ejecuta alguna herramienta de análisis de vulnerabilidades automática o manualmente por algún especialista de informática?	3	3	5	5	2	5	5	3	4	1
De ejecutarse alguna herramienta de análisis de vulnerabilidades automática o manualmente, ¿se comparan los resultados de escaneo con escaneos pasados?	3	4	2	1	3	3	3	4	3	3
En su área de trabajo, ¿se ejecuta algún programa de aplicación de parches de software y/o sistema operativo?	4	1	2	3	5	1	1	5	3	2
En su área de trabajo, ¿se ejecuta algún sistema de protección de red (firewall, aplicación de filtrado de puertos)?	5	5	2	4	5	5	4	3	2	5
En su área de trabajo, ¿se ejecuta algún sistema de búsqueda y/o denegación de acceso no autorizado?	5	4	4	4	4	5	4	3	3	4
En su área de trabajo, ¿se implementa listas de control de acceso?	5	3	3	2	3	4	4	3	5	1
En su área de trabajo, ¿se actualiza periódicamente las aplicaciones usadas en su estación de trabajo?	2	2	3	3	4	2	2	2	2	5

	Respuesta de los encuestados									
Preguntas	**# 11**	**# 12**	**# 13**	**# 14**	**# 15**	**# 16**	**# 17**	**# 18**	**# 19**	**# 20**
En su área de trabajo, ¿ha sido afectado por algún ıcidente informático?	3	2	5	3	5	2	3	2	4	4
En su área de trabajo, ¿han recibido correos *phishing* en su correo laboral?	1	4	5	4	4	1	3	2	5	4
En su área de trabajo, ¿se ejecuta alguna herramienta de análisis de vulnerabilidades automática o manualmente por algún especialista de informática?	1	3	1	3	3	3	4	4	3	1
De ejecutarse alguna herramienta de análisis de vulnerabilidades automática o manualmente, ¿se comparan los resultados de escaneo con escaneos pasados?	1	3	3	5	2	4	1	2	4	4
En su área de trabajo, ¿se ejecuta algún programa de aplicación de parches de software y/o sistema operativo?	2	1	3	2	1	3	2	1	3	3
En su área de trabajo, ¿se ejecuta algún sistema de protección de red (firewall, aplicación de filtrado de puertos)?	4	5	2	5	3	3	5	5	5	5
En su área de trabajo, ¿se ejecuta algún sistema de búsqueda y/o denegación de acceso no autorizado?	5	5	2	4	3	2	5	5	2	5
En su área de trabajo, ¿se implementa listas de control de acceso?	3	4	2	3	5	4	3	5	1	5
En su área de trabajo, ¿se actualiza periódicamente las aplicaciones usadas en su estación de trabajo?	2	4	1	2	2	1	3	5	2	5