FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

Evaluación de herramientas informáticas para el tratamiento de riesgos en la norma NTP-ISO/IEC 27001 2014 en una facultad de ingeniería del sistema universitario peruano

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

Autor(es):

Bach. Apari Valenzuela Oscar

ORCID: https://orcid.org/0000-0003-2009-4094

Asesor(a):

Mg. Jaime Arturo Bravo Ruiz

ORCID: https://orcid.org/0000-0003-1929-3969

Línea de Investigación:

Infraestructura, Tecnología y Medio Ambiente

Pimentel – Perú

2023

Evaluación de herramientas informáticas para el tratamiento de riesgos en la norma NTP-ISO/IEC 27001 2014 en una facultad de ingeniería del sistema universitario peruano

Aprobación del Jurado

MG. MEJIA CABRERA HEBER IVAN

PRESIDENTE DE JURADO

MG. MINGUILLO RUBIO CESAR AUGUSTO

SECRETARIO DE JURADO

MG. TUESTA MONTEZA VICTOR ALEXCI

VOCAL DE JURADO

Universidad
Señor de Sipán

Quien(es) suscribe(n) la DECLARACIÓN JURADA, soy(somos) egresado (s)del Programa de Estudios de **Ingeniería de Sistemas** de la Universidad Señor de Sipán S.A.C, declaro (amos) bajo juramento que soy (somos) autor(es) del trabajo titulado:

EVALUACIÓN DE HERRAMIENTAS INFORMÁTICAS PARA EL TRATAMIENTO DE RIESGOS EN LA NORMA NTP-ISO/IEC 27001 2014 EN UNA FACULTAD DE INGENIERÍA DEL SISTEMA UNIVERSITARIO PERUANO

El texto de mi trabajo de investigación responde y respeta lo indicado en el Código de Ética del Comité Institucional de Ética en Investigación de la Universidad Señor de Sipán, conforme a los principios y lineamientos detallados en dicho documento, en relación con las citas y referencias bibliográficas, respetando el derecho de propiedad intelectual, por lo cual informo que la investigación cumple con ser inédito, original y autentico.

En virtud de lo antes mencionado, firman:

Apari Valenzuela Oscar	DNI: 10708435	

Pimentel, 06 de junio de 2023.

Dedicatorias

A Dios, a mis padres y a mi familia por brindarme siempre su apoyo constante, que ha sido un factor importante para ayudar a cumplir mis metas.

Agradecimientos

Quiero agradecer especialmente a la Mg. Ana María Guerrero y al Dr. Mario Ramos, por su paciencia y asesoría, quienes me brindaron las facilidades para la realización del trabajo de tesis, también a todas las personas que de forma indirecta ayudaron a contribuir con su realización.

Resumen

El presente trabajo de investigación ofrece una visión general sobre el uso de las principales herramientas de seguridad informática para el tratamiento de riesgos en la norma NTP-ISO/IEC 27001 2014, el cual tiene como objetivo principal el gestionar adecuadamente la seguridad de la información. Por ello, se ha procedido a evaluar algunas de las mejores herramientas de seguridad informática que se ofrecen en la actualidad para analizar e identificar niveles de riesgo en los sistemas informáticos y redes de datos a través del uso de diferentes técnicas y métodos. Por otro lado, se ha procedido a analizar dichas herramientas realizando pruebas de uso con sus diferentes parámetros observando su comportamiento y tratando de discernir qué datos son útiles para obtener información acerca de los riesgos existentes en los sistemas informáticos y redes de datos, logrando obtener resultados que demuestran que el uso de herramientas de seguridad informática permiten identificar los niveles de riesgo por parte de un administrador de sistemas, permitiendo a una empresa o institución poder implementar un plan de acción que permita tratar los riesgos según lo indica la norma NTP-ISO/IEC 27001 2014 y de esa manera evitar la pérdida o el robo de la información propiciado por parte de potenciales atacantes. Las pruebas de seguridad informática se realizaron al sitio web de la Facultad de Ingeniería Industrial y de Sistemas de la Universidad Nacional de Ingeniería (UNI), donde se utilizaron herramientas como Owasp Zap, Vega y Arachni.

Palabras Clave: Identificación y Valoración de Riesgos, Seguridad Informática.

Abstract

This research work offers an overview of the use of the main computer security tools for risk treatment in the NTP-ISO/IEC 27001 2014 standard, whose main objective is to adequately manage information security. For this reason, we have proceeded to evaluate some of the best computer security tools currently offered to analyze and identify risk levels in computer systems and data networks through the use of different techniques and methods. On the other hand, these tools have been analyzed by carrying out use tests with their different parameters, observing their behavior and trying to discern which data is useful to obtain information about the risks existing in computer systems and data networks, achieving results. which demonstrate that the use of computer security tools allows a system administrator to identify risk levels, allowing a company or institution to implement an action plan that allows the risks to be treated as indicated by the NTP-ISO/standard. IEC 27001 2014 and thus avoid the loss or theft of information caused by potential attackers. The computer security tests were carried out on the website of the Faculty of Industrial and Systems Engineering of the National University of Engineering (UNI), where tools such as Owasp Zap, Vega and Arachni were used.

Keywords: Identification and Assessment of Risks, Computer Security.

Índice

Índice de Figuras

Índice de Tablas

I. INTRODUCCIÓN

1.1. Realidad Problemática.

Los entes públicos y privados cada día crean información, conocimiento y datos los cuales se reflejan en reportes y material de diversa naturaleza de mucha relevancia para ellos. Esto significa la información necesaria para su funcionar. Para ejecutar estas actividades es imperativo intercambiar información, lo que conlleva a la probabilidad que dentro de esta información que se intercambia, se pueda encontrar algunas vulnerabilidades que se exponga a riesgos de seguridad de información (S.I) de aquí en adelante), que impacten y comprometan la confidencialidad de la información.

Internacional

El año pasado, la empresa FireEye, una de las más grandes de Norte América, difundió que hackers entraron a sus sistemas para sustraerles material, estos estaban relacionados al Gobierno de una nación extranjera. Las dudas se dirigieron a los rusos. [1].

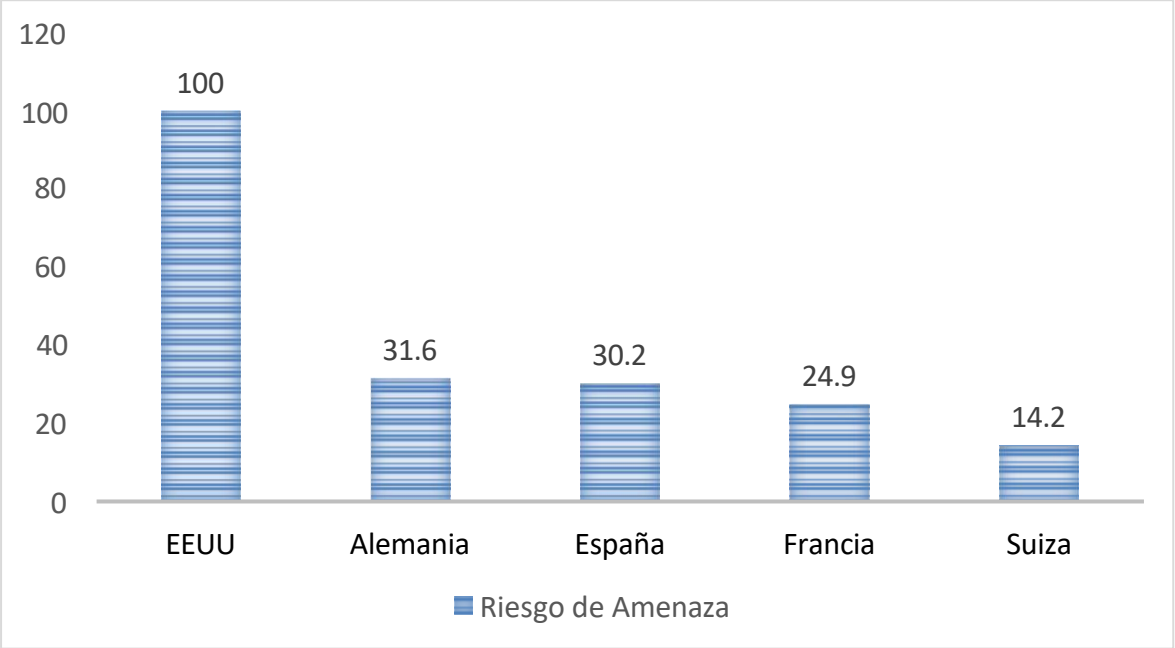


Figura 1. Países más amenazados por los ciberdelincuentes en el 2020

Fuente: IRONHACK, 2020.

Nacional

Nuestro país se encuentra entre los cinco países de Latinoamérica con gran cantidad de ataques cibernéticos, basado en reciente reporte de Check Point Software Technologies. La migración obligada a la plataforma digital por el COVID 19 incrementó los ataques de ciberseguridad. En esta realidad, la información de muchas organizaciones empresariales quedo vulnerable, debido mayormente a que más individuos efectúan el trabajo remoto [2].

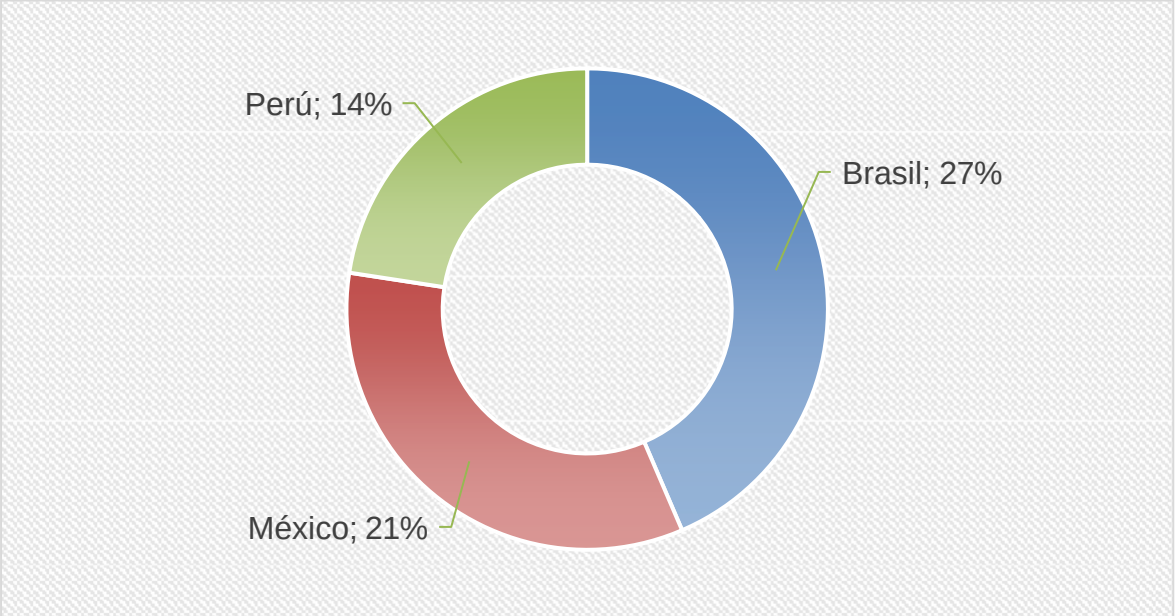


Figura 2. Perú es el tercer país con mas ciberataques en America Latina

Fuente: ElEconomista América, 2019.

Local

A nivel local el BCP con sede principal en Lima, informó que fue objeto de un ataque cibernético en 2018 en el que personas no autorizadas lograron ingresar a la información financiera de un grupo de clientes [3].

En las Pymes los riesgos son más constantes debido a que son pequeñas empresas que están en crecimiento. Por ello su punto débil recae en la ciberseguridad al no contar con personal de TI que se dedique a velar por la S.I [4].

El ingreso no autorizado a la información es cada vez más fácil para el ciberdelincuente, por los diferentes métodos y técnicas existentes para sustraer información, esto ha ocasionado que sea muy difícil salvaguardar la S.I y sus maneras de transmitirlos.

Es por ello que es necesario evaluar el uso de herramientas informáticas que ayuden a identificar los niveles de riesgo en los S.I y redes de datos, y así, según indica la norma NTP-ISO/IEC 27001 2014 elaborar un plan de acción que trate los riesgos.

Trabajos previos.

Los autores [5], en su investigación realizada en Ecuador, describe a las TIC como las tecnologías que hacen facil el adquirir, almacenar, procesar, evaluar, transmitir, distribuir y difundir la información. Son creadas por medio de la concurrencia de la informática, electrónica, telecomunicacion y la microelectrónica. La ISO señala que el riesgo es la probabilidad que la amenaza se realice, aprovechando los puntos vulnerables de un activo o conjunto de activos, originando perjuicios a la empresa. Los riesgos se clasifican según las consecuencias que ocasionan: perjuicios a la parte operativa, al prestigio y daños juridicos de la empresa. Para el análisis de la gestión de riesgos y su posterior ejecución se utiliza el siguiente modelo: planificación, ejecución, verificación y actuación. El enfoque propuesto se basa en el modelo del ciclo PDCA (también conocido como ciclo de Deming), que forma una estrategia de cuatro pasos para la mejora continua de la calidad, también conocida como espiral de mejora continua, y se utiliza ampliamente en varios sistemas utilizados en las organizaciones. Aspectos de gestión como la calidad

(ISO 9000), el medio ambiente (ISO 14000), la seguridad y salud en el trabajo (OHSAS 18000) o la seguridad alimentaria (ISO 22000).

Los autores [6], en su investigación abordaron el tema de S.I. ante los posibles ataques cibernéticos en una realidad globalizada, se revisó la realidad actual en Colombia. El estudio fue cualitativo, documental, teórico y descriptivo. Se efectuó un viaje histórico sobre la ciberseguridad informática, puntualmente en el modulo de S.I. Trabajandose diferentes aspectos (software de gestión, análisis de riesgos, normas de calidad y contextos) a la vez que se exponen los riesgos para las organizaciones, la sociedad y las nacíones, que se hicieron evidentes con la pandemia del COVID-19. Para la realidad colombiana fueron revisados los datos sobre el accionar gubernamental ante las amenazas y se investigo sobre sus estándares de calidad y directrices de seguridad informática.

Los autores [7], en su investigación, buscaron en varias fuentes bibliográficas nacionales e internacionales. De la amplia gama de herramientas disponibles en distribuciones relacionadas con la seguridad informática (Parrot Security, Black Arch y Kali Linux), se seleccionaron las que mejor se ajustan a las características de las redes cubanas.. La investigacion buscó describir algunas herramientas escogidas para la explotación de puntos vulnerables, el escaneo y conceptos basicos relacionados al tema. Este estudio fue de mucho valor para los expertos cubanos en S.I, pues fue util para saber sobre el hacking ético, como también saber cuales son los instrumentos que se podrian usar, considerando los atributos de la red nacional.

Los autores [8], en su investigación realizada en Colombia, desarrollaron un trabajo que consistió en diseñar e implementar Honeypots como un camino complementario al patrón de S.I que existe en una casa de estudios de Caldas. Este estudio analiza y detecta ataques a la seguridad de las redes y otros componentes informáticos en las

organizaciones. Para conseguirlo se utiliza el ciclo PDCA, que mediante una aplicación básica y uso adecuado puede resultar de gran utilidad para realizar con mayor precisión las tareas de producción y gestión. Luego de implementar HoneyPy y Cowrie, fue fácil reconocer diversas modalidades de atacar, direccionando en el servidor IDS la configuración de un script, creando reglas con los registros guardados e implementándolo en Iptables. El diseño de infraestructura con honeypots, implementado permitió hallar brechas de S.I. perteneciente a los servidores de la institución por ataques informáticos.

Los autores [9], en su investigación, mencionaron que, debido al gran número de ciberataques a nivel internacional, se activaron artilugios y protocolos de prevención en las empresas, con el fin de subsanar puntos vulnerables en S.I. El proyecto surgió de la necesidad de proponer a la DIAN (Oficina de S.I), la implementación y control a la táctica de Gobierno en línea de MinTIC en el módulo de S.I. y privacidad, utilizando los lineamientos de la agencia para la S.I. de la institución y gestión del modelo base de conocimiento para la auditoría de servicios web, y que su aplicación se realice a un modelo específico. El diseño para el prototipo de conocimiento base comprende dos etapas, primero se recolecta, procesa y depura la base y la segunda se relaciona al proceso de la temática del modelo del sistema que se propuso. El software free OpenKM se aplicó como el sistema que le da sustento a la base de conocimiento. Para la auditaría, se debe incluir un conjunto de pautas en el enfoque para cada fase del modelo. En el proyecto se utilizaron OWASP, JUnit, ISO27000, OSSTMM y la guía de auditorías y gestión de riesgos difundido por el MinTIC. Se utilizó la técnica OPENUP para desarrollar el prototipo con el WS a exponer. La implementación fue limitada a la creación de dos métodos HTTP: GET y POST para consultar y modificar la información a medida que llega. A través de esta investigación se creó un prototipo base de conocimiento implementado en OpenKM, para realizar auditorías de S.I. de servicios web mediante inyección de SQL en un modelo de organización.

Los autores [10], en su investigación realizada en Colombia, presento la aplicación móvil EVANI, como instrumento informático de soporte a los pueblos, que les facilite en sus zonas identificar los casos de desnutrición en niños con edades inferiores a los 5 años de edad, como también disponer del informe de las coordenadas del caso y la creación de alertas ante el riesgo de mortandad que se derive de esta causa. Luego de desarrollar la aplicación, se efectuó un piloto para la validación del funcionamiento de la app y reconocer el probable impacto, logrando como resultado, su uso en situaciones de alerta preventiva. Esto hizo que se identifique la viabilidad de EVANI como un instrumento que notifique alertas de nutrición, las cuales se convirtieron en un componente de necesidad dentro de los sistemas de alertas preventivas en Seguridad Alimentaria y Nutricional del país, que permitió a las diversas partes de Gobierno ofrecer oportunamente la atención que se necesite para impedir la mortandad por desnutrición.

Los autores [11], en su investigación realizada en Ecuador, dijo que, el avance de la tecnología ha colaborado con el aumento de sucesos inoportunos de diversas índoles en las organizaciones que podrían ocasionar extravió de información; por esta razón, es gravitante efectuar análisis de riesgos de forma adecuada. Teniendo en cuenta que las organizaciones de navegación no se encuentran libres de ataques, amenazas o puntos vulnerables, Se propuso un modelo para los activos de información empresarial que determine la madurez del análisis de riesgo. Esto se logró a través de tres actividades: primero, se analizaron y seleccionaron MEHARI, MAGERIT y OCTAVE como métodos de análisis de riesgos. tomando en consideración que pueda ser utilizada en otras propuestas de creación de prototipos de madurez. Después, se entrevistaron a 7 empresas de navegación con el objeto de saber de su posición de cara a la problemática detectada. Por último, se pudo establecer que la implementación de esta propuesta conllevo a ejecutar un proceso formal de análisis de riesgo, con métodos proactivos de acuerdo a la realidad empresarial definida.

Los autores [12], en su investigación desarrollada en Cuba, analizaron las capacidades para detectar puntos vulnerables en sistemas web que exponen las metodologías principales de pentesting. La finalidad fue establecer la validez de las herramientas, rutinas y pruebas de seguridad planteadas en NIST SP 800-115, PTES, OWASP, OSSTMM e ISSAF para tratar los desafíos de ciberseguridad en la actualidad en la esfera de la creación y mantenimiento de las apps web. Como fundamento comparativo se tomaron los informes de vulnerabilidades de OWASP (2003 – 2017), así como el análisis de los documentos de cada método de pruebas de penetración. Para ello se confeccionó una jerarquía para evaluar las cualidades y su uso, cuyo resultado demostró que la Guía de Pruebas de OWASP llego a ser la más exacta, luego apareció la metodología ISSAF. A pesar de ello, todas las metodologías resultaron no tener la capacidad de proporcionar métodos, pruebas o mecanismos de seguridad para detectar los actuales puntos vulnerables.

Los autores [13], en su investigación realizada en Ecuador, tomaron como base a la metodología OSSTMM con el fin de realizar una auditoría de S.I para la identificación de brechas de seguridad en un centro de estudios superiores, usando para ello el Hacking ético como tipo de prueba. A través de la realización de una investigación de campo se esclareció la situación actual de las políticas de gestión de sistemas de información de las instituciones investigadas. Los medios de información analizados fueron: equipos con software de gestión académica y financiera, áreas administrativas, aulas y laboratorios de cómputo. En función a la auditoría efectuada, se halló que la institución en estudio no controla adecuadamente las políticas de S.I y el uso de estas, alcanzándose como descubrimiento fundamental los valores de evaluación de riesgo (Rav) que equivalen al 72,15% de seguridad. Se llega a la conclusión que la porosidad y las limitaciones facilitan la evaluación del grado de impacto y que tan críticos son las vulnerabilidades halladas. Estas podrían ser mitigadas usando estrategias de gestión de S.I y junto al incremento de

controles de S.I. se optimizaría la puntuación del Rav a un valor del 77,00%; así asegurar la disponibilidad, integridad y confiabilidad de la información.

Los autores [14], en su investigación en México sostuvieron que en un mundo en el que las TIC parecen ser omnipresentes en el día a día, poco se ha meditado sobre los riesgos que implican estas para los humanos. En un lado está la comunidad internacional impulsando que se implementen las TIC para colaborar con el desarrollo de los marginados y vulnerables, pero el otro lado de la moneda es que hay riesgos inminentes que se derivan de la utilización de estas tecnologías. En la actualidad el ciudadano se halla sujeto a circunstancias en la que sus derechos, incluyendo su seguridad personal corren riesgo como consecuencia de la acumulación de la información que se reúnen en softwares informáticos que son el objetivo de los ataques informáticos. Es importante concienciar a la sociedad en general sobre los riesgos permanentes en que se encuentran las personas con el objeto de participar de la prevención de los riesgos.

Los autores [15], en su investigación, realizada en Ecuador, sostienen que las nuevas maneras de desarrollar sistemas informáticos han facilitado la creación de sistemas con diversos fines. Estas implementaciones han aumentado de forma notoria en las últimas décadas, supliendo diversos procesos manuales y agilizando las respuestas en cortos tiempos. Sin embargo, existen diversos protocolos y software diseñados para atacar la privacidad y confidencialidad de la información. El estudio identifica un análisis de evaluación de riesgos basado en lineamientos de la norma ISO 27001. La seguridad se basa en la protección de la información, garantizando la total estabilidad del software y la continuidad del funcionamiento de las computadoras y servidores de los centros de procesamiento de datos. Desarrollándose el sistema de gestión de riesgos de acuerdo con las normas ICREA Std-131-2013 e ISO/IEC 27001.

Los autores [16], en su investigación, consideran a la información como el elemento más valioso para cualquier organización y para muchos de ellos es una herramienta para crear ventaja competitiva. (Vásquez & Gabalán, 2015). No obstante, con el poco conocimiento sobre cómo salvaguardarla de forma adecuada, o a lo complejo de los estándares internacionales que señalan los protocolos para obtener un buen grado de protección, diversos tipos de empresas, específicamente las MPYME, no alcanzan este objetivo. En consecuencia, esta investigación plantea una metodología de S.I para gestionar el riesgo informático que se aplique al ambiente de las empresas y organizaciones del sector MPYME de Ecuador. Para ello, se comparan varias metodologías de gran difusión, como: COBIT 5, Microsoft Risk Guide, OCTAVE-S, COSO III, CRAMM y Magerit. Estas metodologías son usadas a nivel internacional para gestionar el riesgo de la información; tomando como base los estándares de la industria: ISO 27001, 27002, 27005 y 31000.

Los autores [17], en su investigación en Ecuador, sostuvieron que, las nuevas maneras de vivir sobrellevan a la mayor utilización de redes sin conexiones físicas, siendo el teléfono móvil un medio para transmitir datos. Estos están expuestos a las amenazas en los medios que transmiten datos en la red. La S.I cumple un rol muy relevante para asegurar la privacidad, integridad y disponibilidad de la información. Esta tarea se soporta sobre la técnica de la criptografía, cuya base es convertir un mensaje de manera que no se entienda excepto para los que tienen el código para que sea descifrado. El estudio se focalizó en la utilización del algoritmo RSA en los celulares móviles, los datos cifrados son enviados por hilos los cuales son medios de comunicación que, a través de procedimientos y fórmulas que se ejecutan en la Servidora, efectuaran el codificado y decodificado de los datos. Luego, se desarrolló un modelo de intercambio de datos inalámbrico entre dispositivos móviles y pruebas de rendimiento utilizando tres nodos para optimizar la seguridad. Los resultados muestran la efectividad del algoritmo y su funcionamiento; Los

tiempos de codificación y decodificación son más flexibles en comparación con la transferencia de información sin utilizar ningún algoritmo.

Los autores [18], en su investigación, Seguridad en Servicios Web (Argentina), indicaron que, con el apogeo de internet y las diferentes evoluciones de la sociedad actual, ha transformado de gran manera como interactúan los individuos y las organizaciones. Este gran cambio se aprecia en la forma de intercambiar información entre los diversos actores. Pero transformándose en punto a ser atacado por todos los actores que desean alcanzar información de suma utilidad y de valor para sus propios intereses o de otras personas. En este aspecto tiene gran relevancia implementar las medidas y acciones orientadas a impedir los ataques, por esta razón surge lo que se llama Seguridad Informática. El artículo describe una investigación que tiene como finalidad principal desarrollar técnicas, métodos y estrategias dirigidas a incrementar la seguridad de los servicios web.

Los autores [19], en su investigación realizada en Ecuador, efectuaron pruebas de seguridad utilizando el Ethical Hacking como metodología para establecer vulnerabilidades que existen en los S.O de Android y Windows, Utilizando las herramientas del sistema operativo Kali Linux para realizar pruebas de penetración para que los administradores y el personal de TI puedan tomar medidas preventivas contra ataques informáticos. Cada paso del método de Hacking ético utiliza varias herramientas de Kali Linux como Metasploit, Armitage, Nmap, Maltego, Set Toolkit y tácticas como ingeniería social, phishing, etc.; detallando el proceso realizado y demostrando los resultados obtenidos. Se realizaron pruebas de seguridad en entornos virtuales y reales controlados para acceder a dispositivos a través de vulnerabilidades de software, configuraciones predeterminadas o errores humanos en la primera conferencia estudiantil de ciencias realizada en la Universidad Politécnica de Manabí. La investigación efectuada, por medio de la metodología del Ethical Hacking brinda a los Administradores de TI e individuos en general,

un esquema para establecer las áreas vulnerables, facilitando a los individuos ejecutar acciones correctivas e impedir ser víctima de ataques informáticos en el futuro.

Los autores [20], en su investigación desarrollada en Colombia, implementaron un modelo de simulación que permitió la evaluación del nivel óptimo de seguridad con que deben contar las empresas teniendo en cuenta aspectos vinculados con la disminución del riesgo y el logro de beneficios para la empresa. El método usado para construir el prototipo fue la dinámica de sistemas, que hace posible el modelamiento y análisis de cómo se comportan los sistemas de gran complejidad en diferentes plazos de tiempos. Se implementó el modelo con el software “POWERSIM”, que es un entorno fusionado para construir y utilizar prototipos que simulen negocios. En conclusión, si las empresas no disponen de un plan maestro que dirija los trabajos para proteger los activos, nunca lograran alcanzar estándares de seguridad aceptables, por más recursos monetarios que se destinen a la seguridad.

Los autores [21] Realizaron un estudio comparativo sobre mecanismos de S.I. para prevenir ataques informáticos con la finalidad de obtener información de los atacantes y mejorar la seguridad de las bases de datos y servidores web. Se detectaron incidentes de S.I. y se detectó un ataque informático que afectó más al servidor. Al diseñar la red planificada, los investigadores analizaron, diseñaron e implementaron mecanismos de seguridad, el primero de los cuales fue una copia independiente de una red espejo virtual y el segundo fue la implementación del mecanismo Snort en Kali Linux. El impacto del ataque se examinó en el análisis de los resultados. Considerando el tiempo que el servidor estuvo indisponible, el mecanismo Honeynet logró el tiempo más bajo de 0,8 segundos, mientras que Snort logró 1,0 segundos. Como resultado, también se logró el tiempo de respuesta del motor Snort. Su tiempo de respuesta fue de 3,8 segundos, mientras que el tiempo de respuesta de Honeynet fue de 3,6 segundos. En términos del desempeño del mecanismo de seguridad para cada ataque, logró un 97% de especificidad y un 99,2 de

independencia de tercera generación. El mecanismo de seguridad virtual Honeynet tiene una sensibilidad del 97,5%, una precisión del 98,3% y el mecanismo Snort tiene una especificidad del 97,6%, una sensibilidad del 98%, una precisión del 98% y una precisión del 97,9%. A lo largo del estudio se mencionó la realidad problemática y las vulnerabilidades halladas en determinados servidores.

Estado del Arte

Los autores [22], en su investigación, implementaron un catálogo que filtrara líneas de logs de servidores web en formato CLF que señalen un desenvolvimiento anormal. Por ello se codificaron los logs de ingreso en forma de vectores, a continuación, fue usado el algoritmo de ponderación de aprendizaje automático K-NN para filtrar los logs. Los datos de ingreso fueron proporcionados por el CERTuy (Equipo que da respuestas ante Emergencias Informáticas) y el Centro de Operaciones de Seguridad. Las pruebas efectuadas en el servicio de catalogación detectaron 82% de ataques de ciberseguridad de un grupo de datos asociados, se alcanzó filtrar el 80% de logs que señalaban comportamientos normales y se aminoró el tiempo para detectar logs que evidenciaron comportamiento anormal de 13 horas a ¼ de hora.

Los autores [23], en su investigación construyeron un escenario basado en datos proporcionados del análisis de campo, donde se apreciaron los riegos que existen en los ámbitos privados y públicos, mezclando lo mejor de ambos, adicionalmente los parches de seguridad para sitios ASP, JSP y PHP, generándose, una solución solida ante intrusiones y ataques. Al encontrase algunos de los errores (clonación de sitio, sensibilidad a ataques remotos de inyección de información en la base de datos, vulnerabilidades del servidor o límite de solicitudes al servidor), las escuelas pueden ser atacadas por terceros y presentar cambios que signifiquen un peligro, como alteraciones de notas de alumnos, inserción de individuos en actividades o cursos, eliminación de información, entre otros; es así que se presentó una solución para determinados errores informáticos que suceden en

las instituciones de nivel superior, utilizando una aplicación informática la cual fue creada para esta investigación.

Los autores [24], en su investigación, Análisis, clasificación y evaluación basados en métricas CVSS de amenazas y vulnerabilidades de redes informáticas, proporcionan una técnica basada en métricas del Common Vulnerability Scoring System (CVSS) para clasificar y analizar las vulnerabilidades y amenazas de seguridad de redes informáticas predominantes (CNSVT). El problema que se aborda en este documento es que, al momento de escribir este documento, no existían enfoques efectivos para analizar y clasificar CNSVT para propósitos de evaluaciones basadas en métricas CVSS. Los autores de este artículo han logrado esto mediante la generación de un criterio de Contramedida de Clasificación de Análisis de Vulnerabilidad Dinámico (VACC) basado en métricas CVSS que es capaz de clasificar las vulnerabilidades. El VACC basado en métricas CVSS ha permitido el cálculo de la Medida de similitud de vulnerabilidad (VSM) utilizando las funciones métricas de distancia de Hamming y Euclidean. Sin embargo, la métrica CVSS basada en VACC también permitió la medición aleatoria del VSM para un número seleccionado de vulnerabilidades basadas en el puntaje de la clasificación. Esta es una técnica que tiene como objetivo permitir que los expertos en seguridad puedan realizar una detección y evaluación de vulnerabilidades adecuadas en redes basadas en computadoras en función de la ocurrencia percibida al verificar la probabilidad de que se produzcan o no amenazas determinadas. Los autores también han propuesto contramedidas de alto nivel de las vulnerabilidades que se han enumerado. Los autores han evaluado el VACC basado en métricas CVSS y los resultados son prometedores. Con base en esta técnica, vale la pena señalar que estas propuestas pueden ayudar en el desarrollo de herramientas de seguridad informática y de redes más sólidas.

Justificación e importancia del estudio.

Social

Al evolucionar la tecnología este ha sido un proceso que ha permitido que el ser humano cada día se involucre más con los medios de comunicación e información. Los avances de nuevos proyectos tecnológicos ayudan a que hoy en día se cuente con nuevas y mejores herramientas informáticas para combatir ataques informáticos. La presente investigación permitirá a los gestores de red evaluar la S.I empleando diferentes herramientas y técnicas que faciliten tener un mejor control de la seguridad de la red y evitar quedar expuestos a futuros ataques informáticos.

Académica

Añadir un nuevo proyecto de investigación que aporte al crecimiento del conocimiento sobre la utilización de herramientas de seguridad informática, ampliando el conocimiento en el uso de técnicas y métodos empleados por delincuentes informáticos.

Económica

Una incidencia de seguridad podría ocasionar que el servicio se interrumpa de manera parcial o de forma permanente ocasionando daños y/o pérdidas a la institución. Es por ello que será importante la evaluación del uso de herramientas informáticas que ayuden a identificar los riesgos en el software de información, para luego implementar el plan de tratamiento de riesgos y ello permita disminuir la pérdida o sustracción de la información.

1.2. Formulación del Problema.

¿Qué herramientas informáticas se deben evaluar en la etapa de planificación de la norma NTP-ISO/IEC 27001 2014?

1.3. Hipótesis.

La evaluación de herramientas informáticas permitirá saber qué herramientas son las más adecuadas para identificar riesgos en la fase de planificación de la norma NTP-ISO/IEC 27001 2014.

1.4. Objetivos.

Objetivo general.

Evaluar herramientas informáticas que permitan identificar los riesgos de acuerdo a la etapa de planificación de la norma NTP-ISO/IEC 27001 2014 en una facultad de ingeniería del sistema universitario peruano.

Objetivos específicos.

a) Caracterizar la identificación de riesgos en la etapa de planificación de la norma NTP-ISO/IEC 27001 2014.
b) Evaluar las herramientas informáticas apropiadas para la identificación de riesgos.
c) Realizar la medición de las herramientas informáticas seleccionadas.

1.5. Teorías relacionadas al tema.

Evaluación de Herramientas Informáticas

Según [25], los recursos informáticos se transformaron de ser complicados eslabones de programación para analizar y gestionar la información a entornos completamente amigables y con fácil acceso para los usuarios con instrucción básica en el uso de software. En la actualidad muchos paquetes permiten un tratamiento ágil de los datos de tal modo que su análisis y la emisión de conclusiones sobre ellos se realizan más rápido y con más confiabilidad que tiempos atrás.

OWASP ZAP

El programa OWASP tiene una herramienta muy potente el cual es ZAP. Es un entorno que se diseñó básicamente para controlar cuan seguras son las aplicaciones web. Es una aplicación con mucha actividad en relación a las auditorías de seguridad [26].

VEGA

Dispone de dos maneras de operar: escáner automático y proxy de interceptación. El primero es un componente usado para el análisis de base de datos el cual rastrea de forma automática páginas web, obtiene enlaces, procesa formularios y ejecuta componentes en los probables puntos de inyección que detecta. Estos componentes pueden efectuar tareas como probar inyección de SQL o scripts de sitios cruzados (XSS) [Vega] [27].

ARACHNI

Tiene un elevado rendimiento que ayuda a los administradores de red a realizar la evaluación de la S.I. en las aplicaciones web. Esta liberada de pago y es código de fuente abierto (Open Source), también multiplataforma, permite todos los S.O relevantes (Linux, Mac OS X y MS Windows) [27].

Tratamiento de Riesgos

Según [28], el tratamiento de riesgos es entendida como la disciplina existente para enfrentar las amenazas no especulativas, que son aquellos riesgos de los que solo puede suceder un perjuicio para la empresa. La gestión de riesgos tiene objetivos relacionados: desaparecer los riesgos, disminuir a niveles “aceptables” los riesgos que no pueden ser eliminados y en consecuencia, convivir con ellos, aceptándolos ejerciendo de manera cuidadosa los controles que los mantienen en niveles “aceptables” o transferirlos, a través de aseguradoras.

Definición de Términos

Todas las definiciones mostradas en esta investigación, se utilizan según los términos brindados en la ISO/IEC 27000.

ISO/IEC 27001

Norma elaborada por ISO con la finalidad de asistir la gestión de la S.I en una organización [29].

Mejora Continua

Es un proceso utilizado para lograr la calidad total, la excelencia de las empresas de forma progresiva, para así lograr resultados eficaces y eficientes [30].

Auditoría

Proceso documentado, independiente y sistemático, que obtiene evidencia de auditoría con el fin de realizar la evaluación de forma objetiva para establecer hasta qué instancia se da cumplimiento a los fundamentos para auditar [29].

Ataque

Intentar destruir, deshabilitar, robar, alterar, exponer o lograr acceso sin autorización o realizar la utilización no autorizada de un activo [29].

Vulnerabilidad

Punto débil de un control o activo que podría ser aprovechado por una o más amenazas. Dentro del marco de la S.I. de sistemas de información podría ser una falla en un sistema que puede dejarlo expuesto a los atacantes [29].

Amenaza

Causa potencial de un incidente que no se espera, que podría generar perjuicios a una organización o sistema [29].

Riesgo

Impacto de la incertidumbre sobre los objetivos. Se relaciona con la probabilidad de que las amenazas aprovechen los puntos vulnerables de activo(s) de información o grupos de estos y, por ende, ocasionen perjuicios a una empresa [29].

Nivel de Riesgo

Magnitud de un riesgo que se expresa en función de cómo se combinan las consecuencias y sus probabilidades [29].

Identificación de Riesgo

Proceso de búsqueda, reconocimiento y descripción de riesgos [29].

Análisis de Riesgo

Proceso para entender como es la naturaleza del riesgo y para establecer el nivel de riesgo [29].

Evaluación de Riesgo

Proceso integral para identificar riesgos, analizar y evaluar riesgos [29].

Gestión de Riesgo

Actividades que son coordinadas para direccionar y supervisar una empresa con relación al riesgo [29].

Tratamiento de Riesgo

Proceso para modificar riesgo [29].

Indicador

Medida que brinda una evaluación o estimación [29].

Normativa Técnica

Ley Nº 30096 de Delitos Informáticos, tiene como finalidad realizar la prevención y sancionar la ciberdelincuencia, vale decir, son las conductas que causan afectación a los softwares, datos, información y otros bienes jurídicos de importancia penal, ejecutados a través de la utilización de TIC.

II. MATERIAL Y MÉTODO

2.1. Tipo y Diseño de Investigación.

El tipo de esta investigación es aplicativo con diseño cuasi experimental bajo un enfoque cuantitativo.

Aplicativo: la investigación es de tipo aplicativo debido a que se medirá cada herramienta para identificar las vulnerabilidades en sistemas informáticos, y luego anotar sus características.

Cuasi Experimental: inicialmente se hará un análisis acerca de las principales herramientas de seguridad informática, luego de ello se hará el levantamiento de información de procesos críticos con la finalidad de reconocer posibles amenazas y vulnerabilidades. Después y de acuerdo a la información recaudada de dicho análisis hacer la evaluación de riesgos.

Cuantitativo: debido a que tiene una aplicación inmediata, donde se busca medir los resultados y luego a través de resultados estadísticos serán interpretados de manera objetiva. En este punto se aplica la norma en estudio en referencia al numeral 6.1.2, que expresa que los riesgos de S.I deben tener una valoración. Es decir, deben ser cuantificados para luego ser comparados.

2.2. Variables, Operacionalización.

Tabla 1. Variables, Operacionalización.

Variable de estudio	Definición conceptual	Definición operacional	Dimensiones	Ítems	Instrumento	Indicadores	Valores finales	Tipo de variable	Escala de medición
Herramientas Informáticas	Las herramientas informáticas cambiaron de ser complicados eslabones de programación para la gestión y análisis de la información a	Las herramientas informáticas permitirán medir los indicadores de la variable.	Tabla de herramienta informática	1 2 3	Guía de Análisis documental Guía de Observación	Tiempo de Detección	Alto Medio Bajo	Cuantitativa	Ordinal
				1 2 3		Uso de Memoria RAM	Alto Medio Bajo	Cuantitativa	
				1 2		Uso de CPU	Alto Medio		

	entornos completamente amigables y de fácil ingreso a usuarios con formación básica en el manejo de software [25].			3			Bajo	Cuantitativa	
				1 2 3		Uso de Disco Duro	Alto Medio Bajo	Cuantitativa	

Variable de estudio	Definición conceptual	Definición operacional	Dimensiones	Ítems	Instrumento	Indicadores	Valores finales	Tipo de variable	Escala de medición
Identificación y valoración de riesgos	Proceso de búsqueda, reconocimiento, descripción y evaluación de riesgos [29]	Primero se identifica el riesgo, se le categoriza y luego se le asigna un valor o puntuación numérica.	Identificación de Riesgos	1 2 3 4	Guía de Análisis documental Guía de Observación	Nivel de Clasificación de Riesgo	Alto Medio Bajo Informativo	Cuantitativa	Ordinal

2.3. Población de estudio, muestra, muestreo y criterios de selección.

La población en estudio se dio de acuerdo a las 10 principales herramientas de seguridad informática que están disponibles en los momentos actuales. La muestra se realizó con la evaluación de 03 herramientas informáticas que sirvieron para la identificación de riesgos, no se hizo uso de ningún cálculo matemático para resolverlo.

2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad

Técnicas

Análisis Documental:

Se revisó material bibliográfico (libros, artículos, informes técnicos, etc.), para la revisión de las diferentes técnicas utilizadas para identificar riesgos en sistemas informáticos.

Observación:

La observación fue la técnica que se usó para recolectar los datos en base a los escenarios de pruebas que se realizaron para revisar las diferentes técnicas que utilizan las herramientas informáticas.

Instrumentos de recolección de datos

Se utilizaron los siguientes instrumentos:

Guía de Análisis documental:

Se analizaron diversas fuentes bibliográficas como: informes, tesis, artículos científicos, etc., que guardan relación con el uso de métodos y técnicas utilizados para la identificación de riesgos informáticos. Ver Anexo 3.

Guía de Observación:

Se elaboró 01 guía de observación para valuar cada una de las herramientas para la identificación de riesgos, donde se registraron de forma sistemática y confiable el resultado de cada herramienta. Ver Anexo 4.

Validez

La validez fue determinada por medio de las técnicas para recolectar datos, el uso de métodos y técnicas usados para la identificación de riesgos.

Confiabilidad

Se estableció por medio del análisis de 03 herramientas informáticas para la identificación de riesgo como son: Owasp Zap, Vega y Arachni.

La confiabilidad del instrumento usado en esta investigación, hace referencia al nivel en que su uso repetido al mismo elemento y/o individuo genera similares resultados.

Materiales

Herramienta Owasp Zap

La herramienta con más potencia del programa Owasp es Zap que es un entorno que fue diseñado básicamente para controlar la S.I. en las aplicaciones web. Esta aplicación cuenta con mucha más actividad en relación a las auditorías de seguridad [7].

Instalación de la herramienta Owasp Zap

Figura 3. Iniciando la instalación de la herramienta Owasp Zap

Fuente: Elaboración propia.

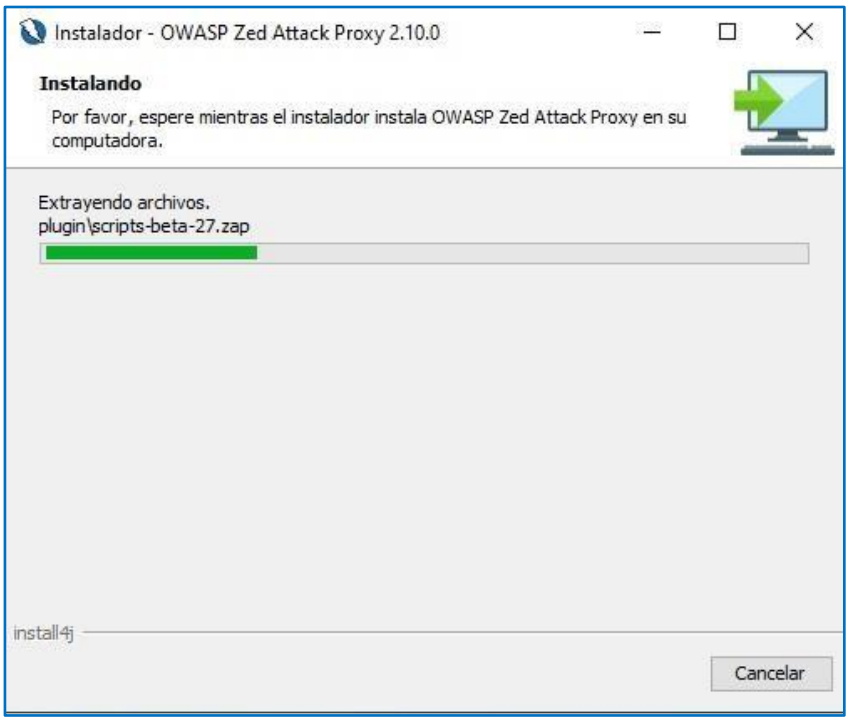


Figura 4. Progreso de instalación de Owasp Zap

Fuente: Elaboración propia.

Figura 5. Finalizando la instalación de Owasp Zap

Fuente: Elaboración propia.

Iniciando la herramienta Owasp Zap

Figura 6. Iniciando Owasp Zap

Fuente: Elaboración propia.

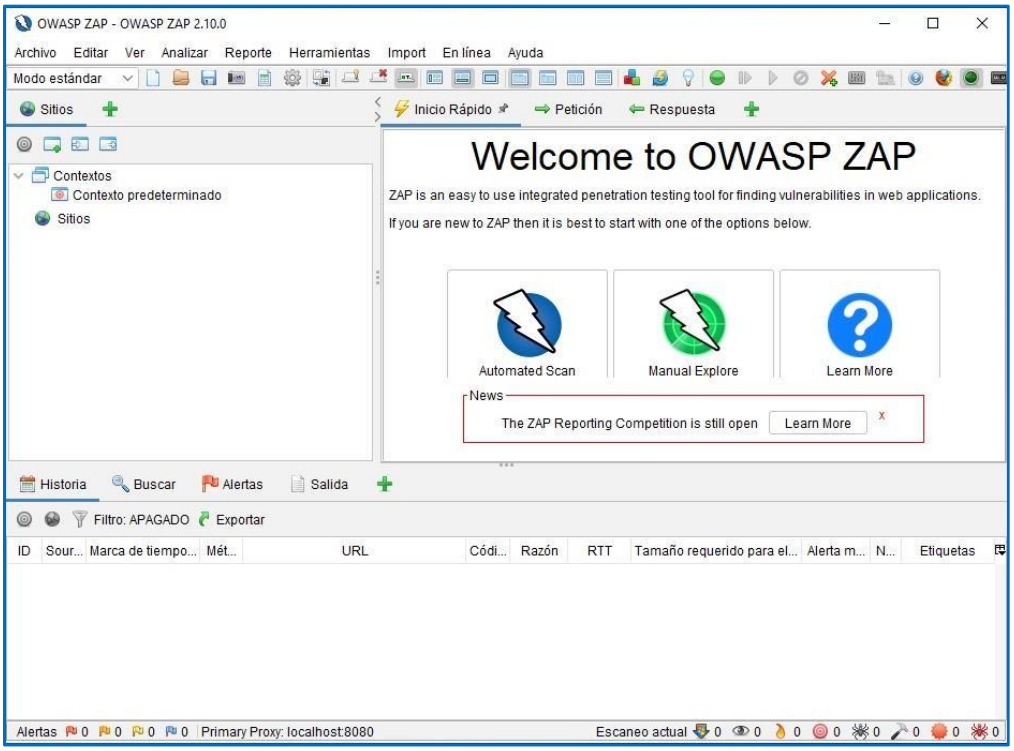


Figura 7. Ventana principal de Owasp Zap

Fuente: Elaboración propia.

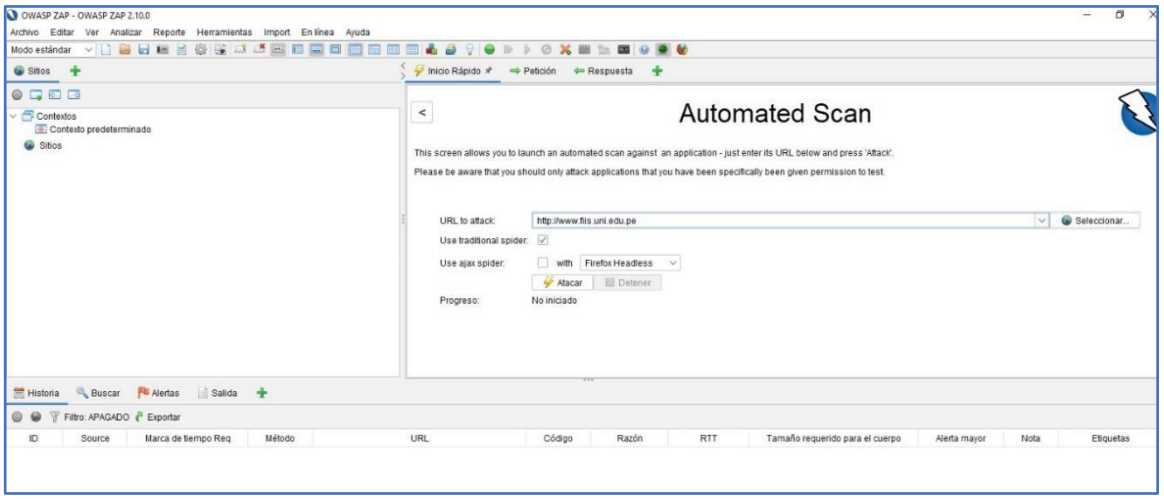


Figura 8. Iniciando el análisis de riesgo con Owasp Zap

Fuente: Elaboración propia.

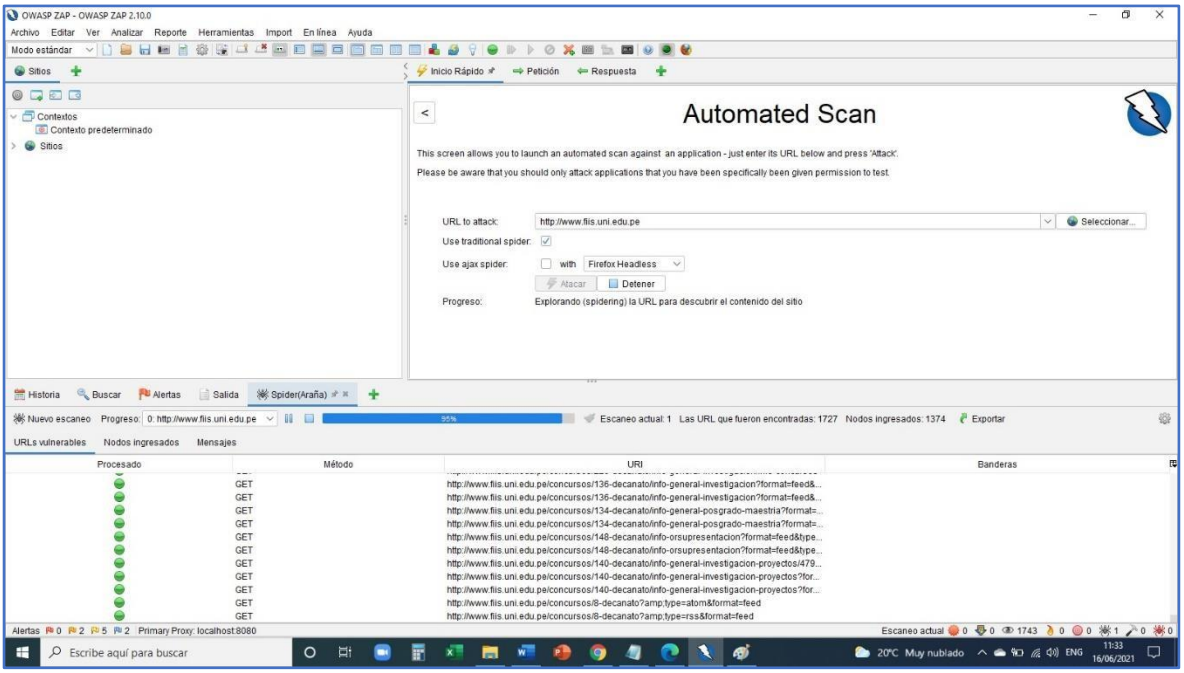


Figura 9. Progreso del análisis de riesgo con Owasp Zap

Fuente: Elaboración propia.

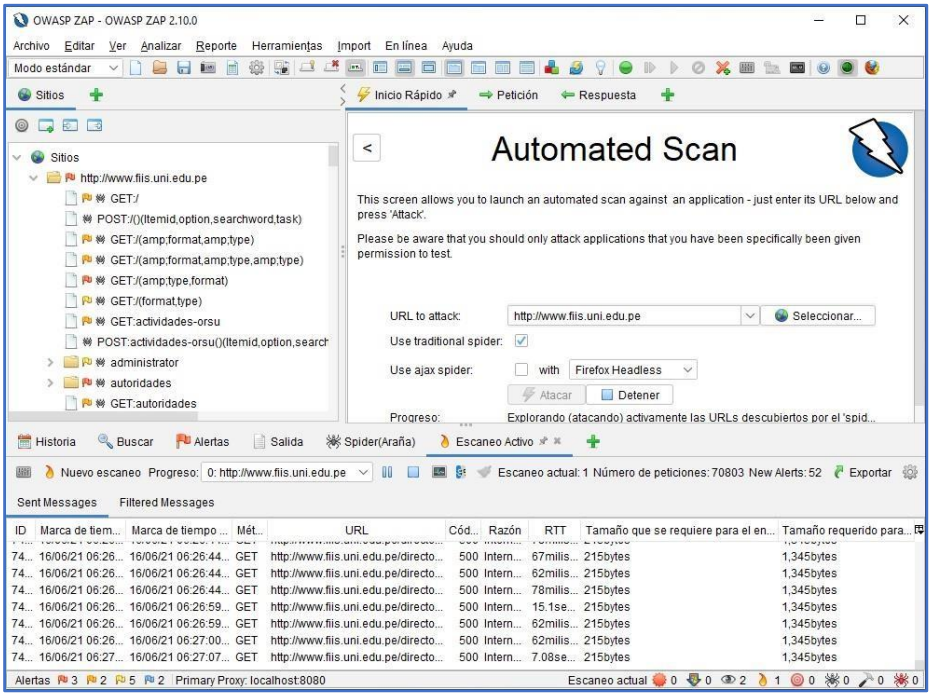


Figura 10. Identificación de niveles de riesgo con Owasp Zap

Fuente: Elaboración propia.

Herramienta Vega

Vega dispone de dos métodos de operación: proxy de interceptación y escáner automático. El escáner automático es el componente usado al analizar el SGD, este hace el rastreamiento de modo automático de sitios web, obtiene enlaces, realiza el procesamiento de formularios y ejecuta componentes en las posibles brechas de inyección que detecta. Estos componentes realizan tareas como inyección de SQL o probar scripts de sitios cruzados (XSS) [27].

Instalación de la herramienta Vega

Figura 11. Iniciando la instalación de la herramienta Vega

Fuente: Elaboración propia.

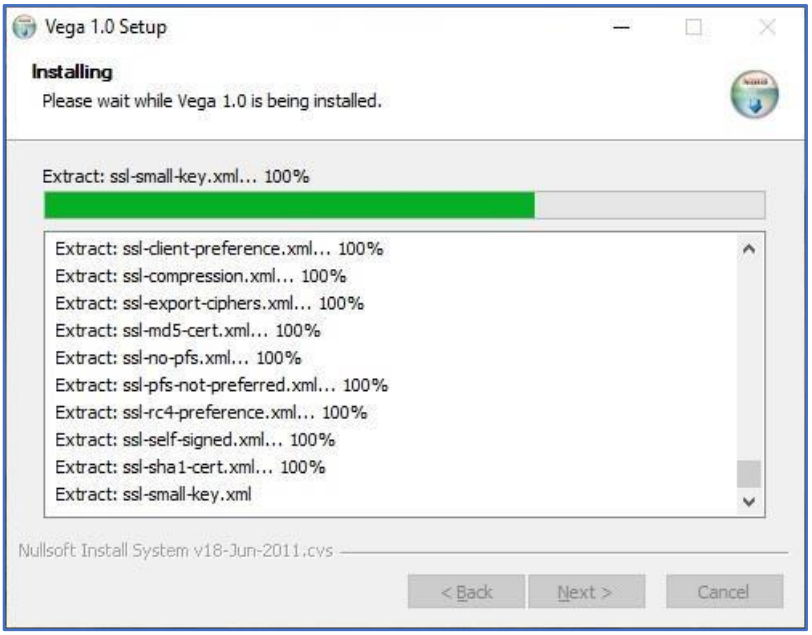


Figura 12. Progreso de instalación de la herramienta Vega

Elaboración propia.

Figura 13. Finalizando la instalación de la herramienta Vega

Fuente: Elaboración propia.

Iniciando la herramienta Vega

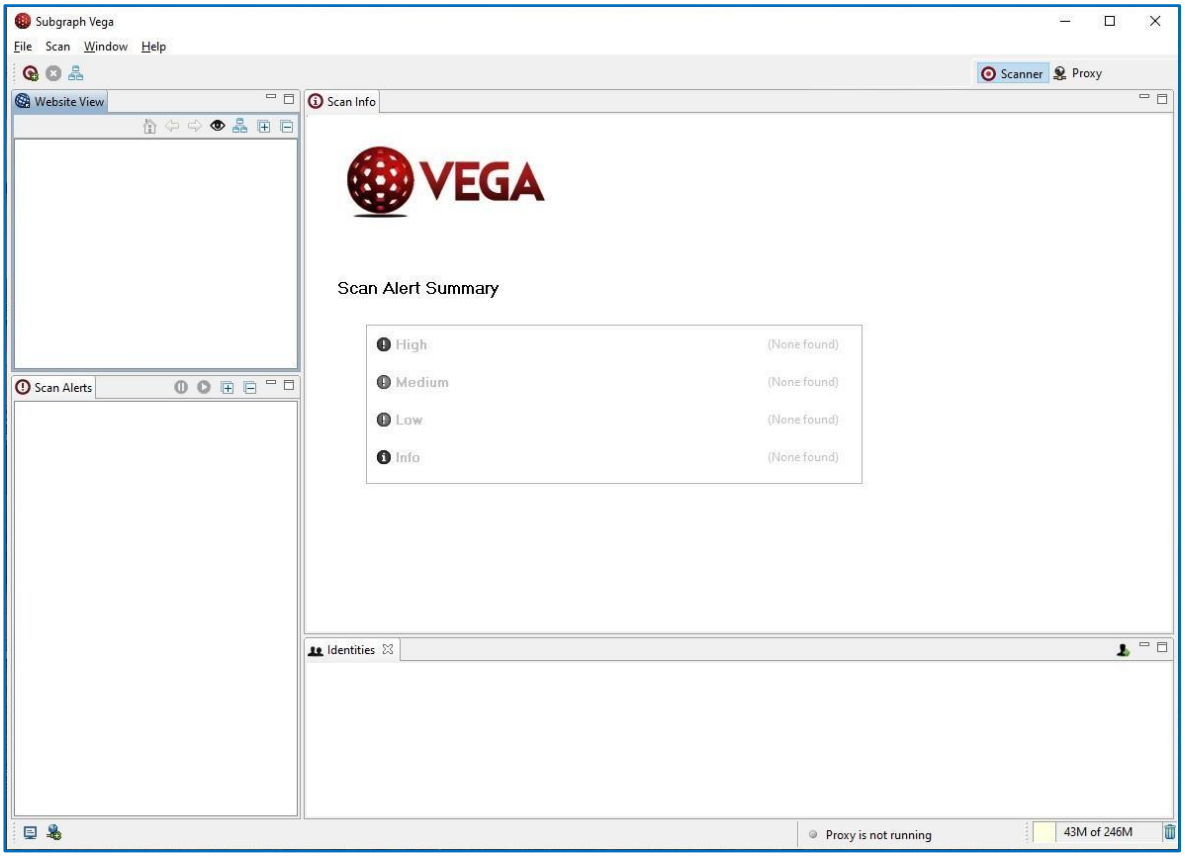


Figura 14. Ventana principal de la herramienta Vega

Fuente: Elaboración propia.

Identificación de Vulnerabilidades con Vega

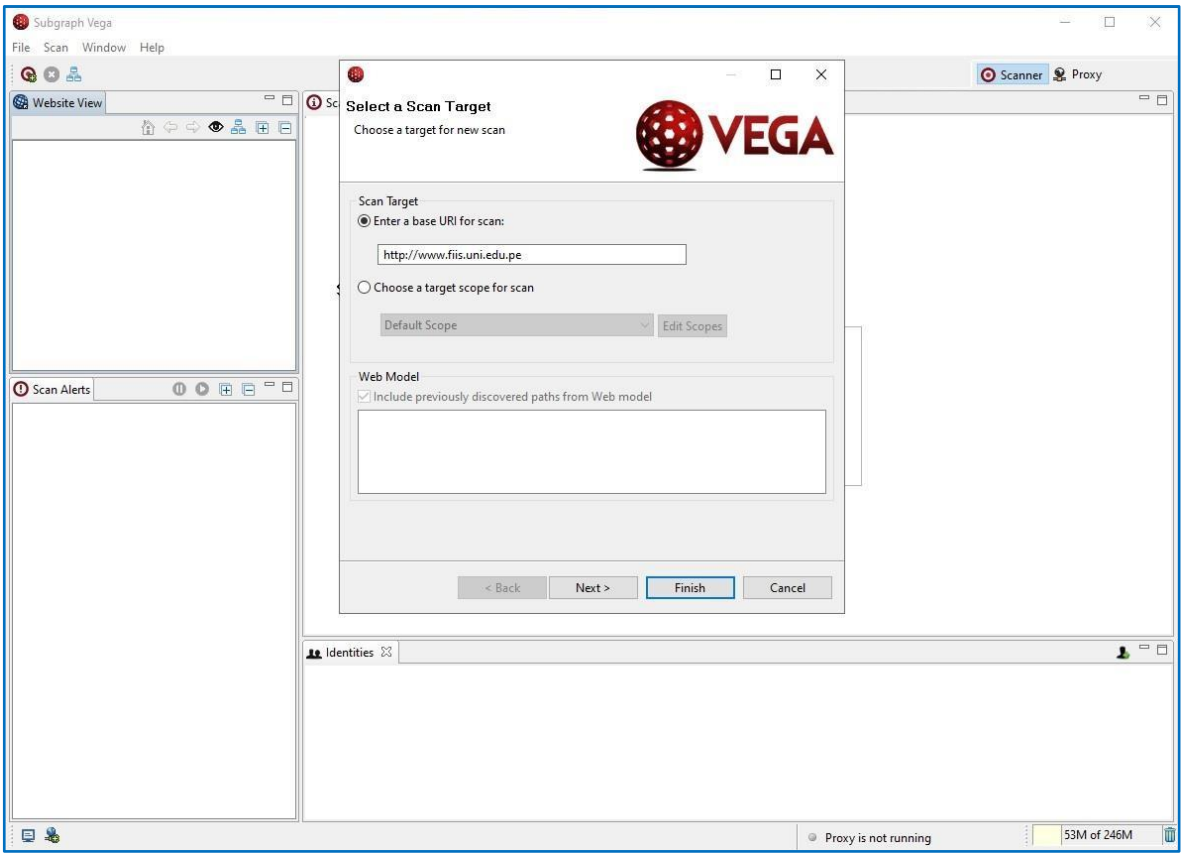


Figura 15. Iniciando la identificación de riesgo con Vega

Fuente: Elaboración Propia.

Herramienta Arachni

Es una herramienta de elevado rendimiento que ayuda a los administradores de red a realizar evaluaciones de S.I. en las aplicaciones web. Es gratis y de código fuente abierta (Open Source), también multiplataforma, permite todos los sistemas operativos relevantes [27].

Instalación de la herramienta Arachni

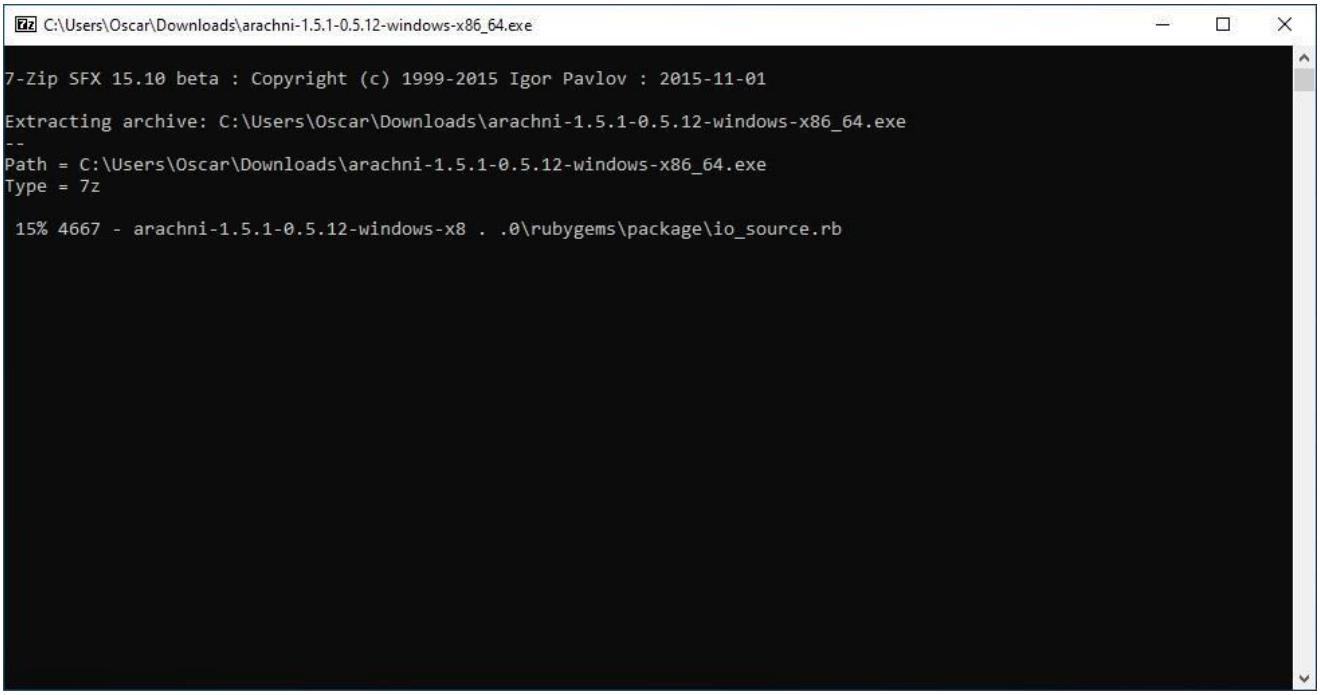


Figura 16. Iniciando la instalación de la herramienta Arachni

Fuente: Elaboración propia.

Iniciando la herramienta Arachni

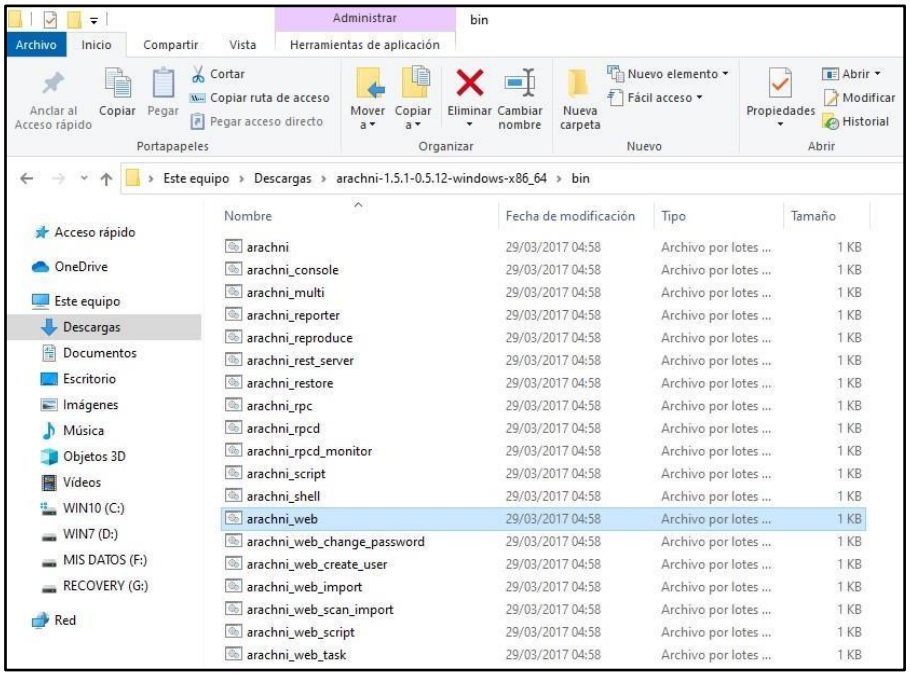


Figura 17. Iniciando la herramienta Arachni

Fuente: Elaboración propia.

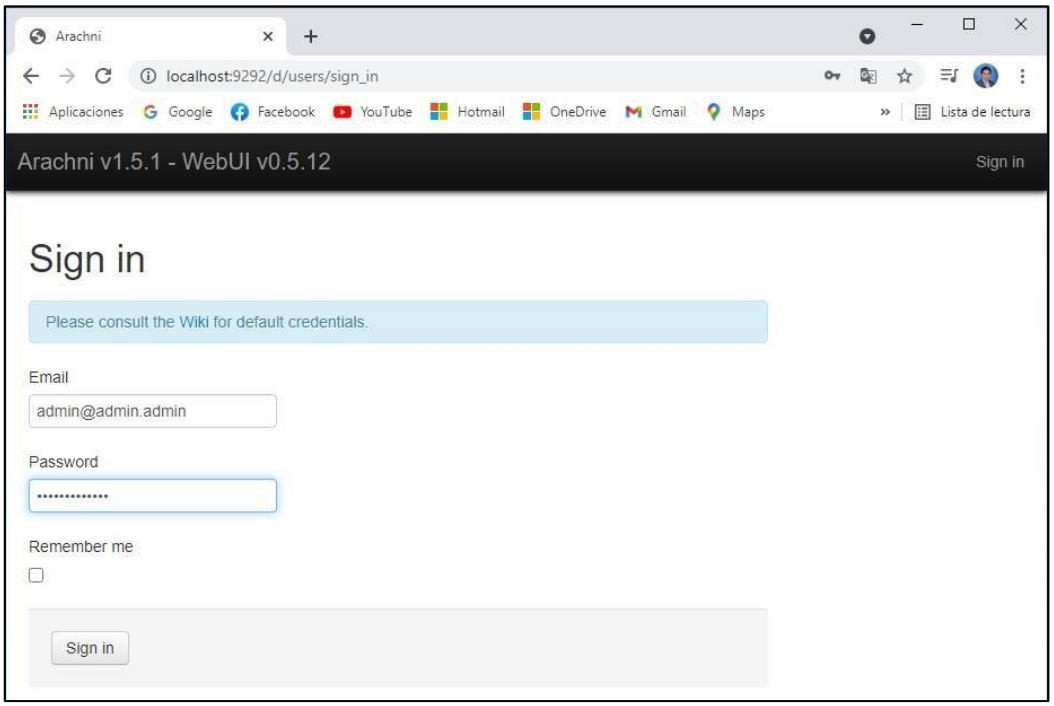


Figura 18. Iniciando sesión con Arachni.

Fuente: Elaboración propia

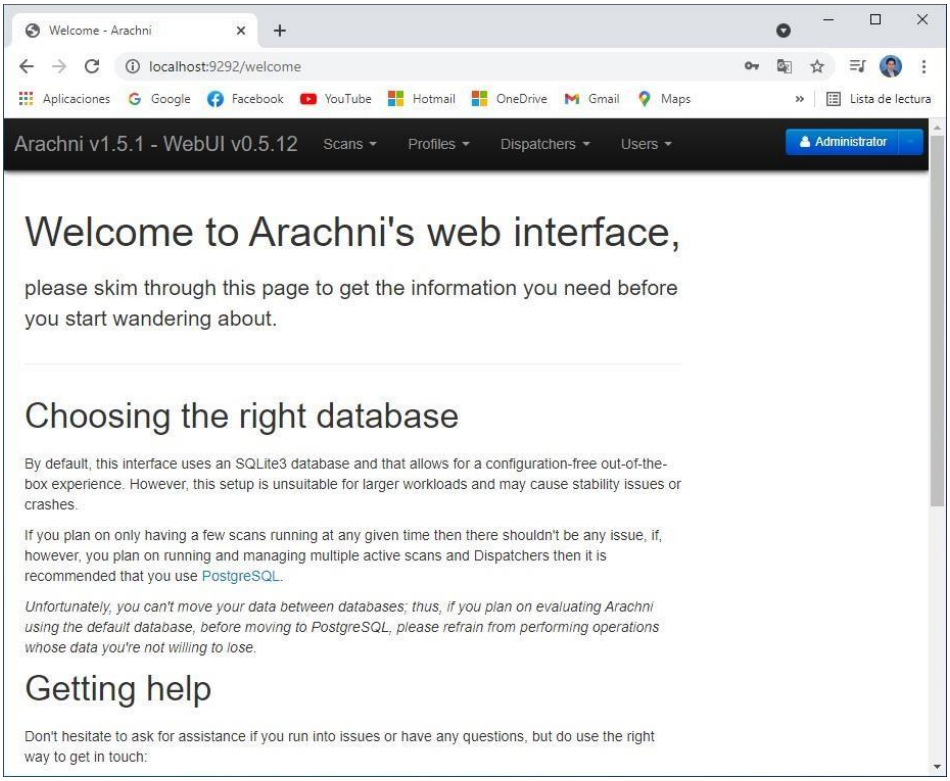


Figura 19. Ventana principal de la herramienta Arachni

Fuente: Elaboración propia.

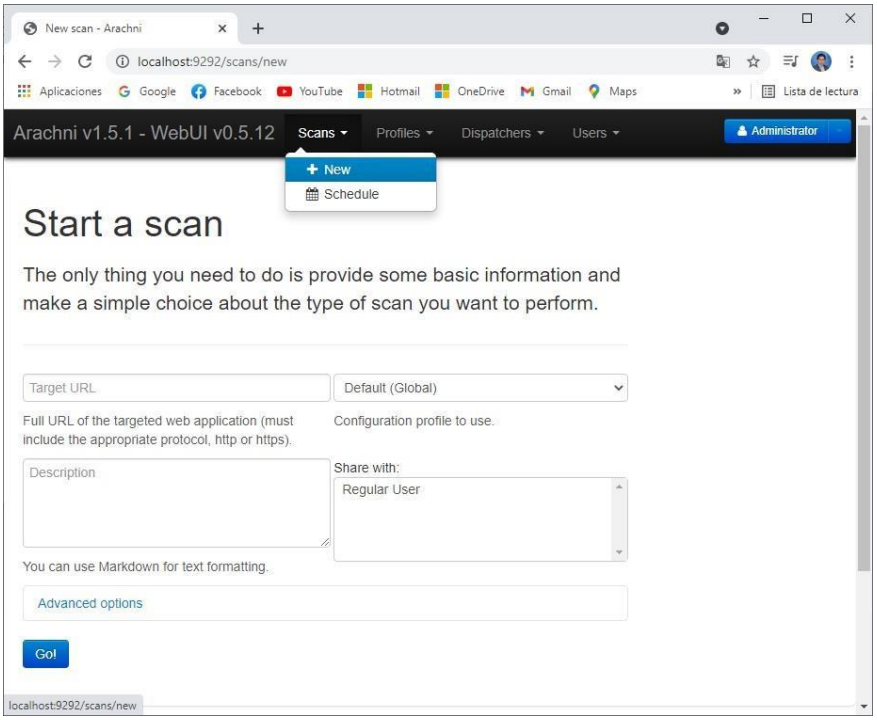


Figura 20. Iniciando una nueva tarea con Arachni

Fuente: Elaboración propia.

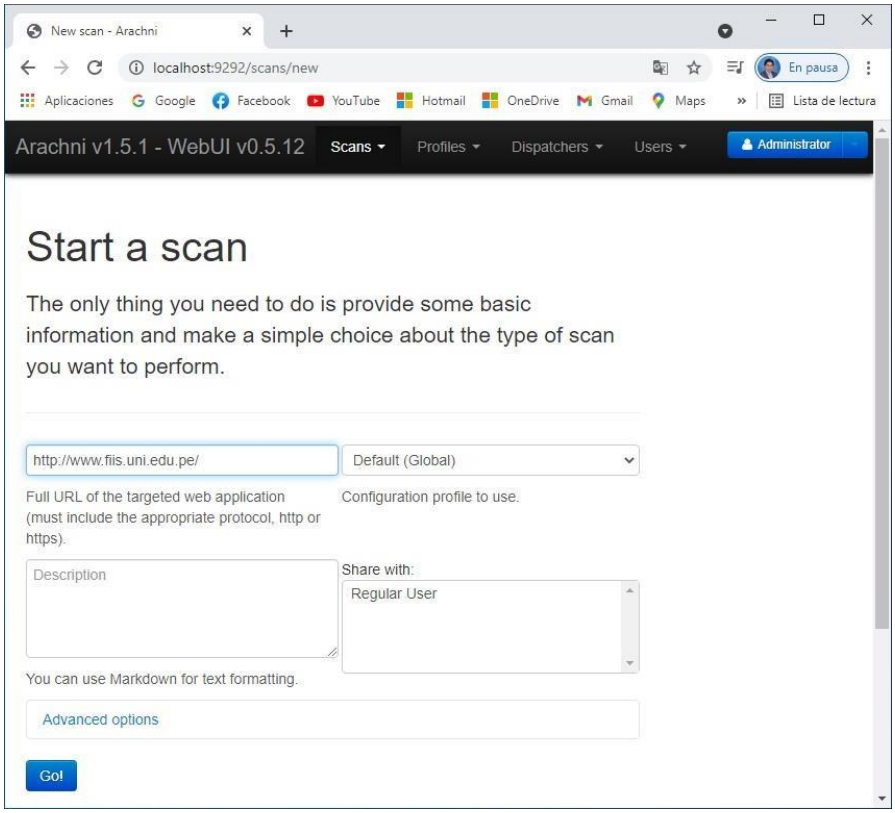


Figura 21. Iniciando la identificación de riesgo con Arachni

Fuente: Elaboración propia.

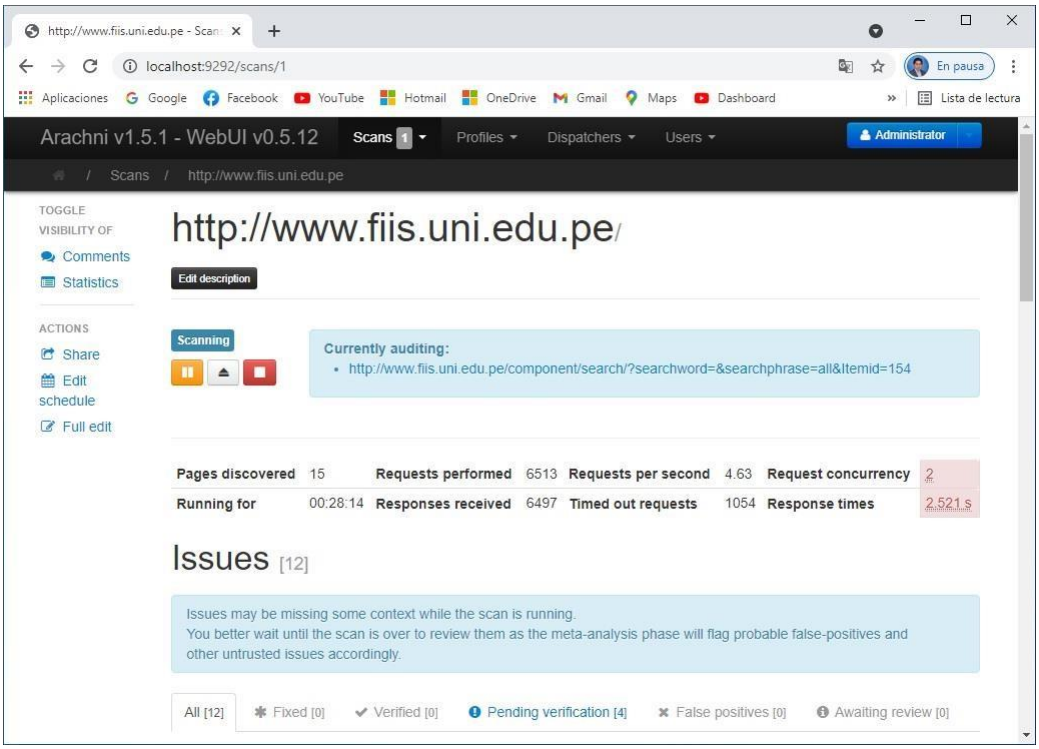


Figura 22. Progreso de la identificación de riesgos con Arachni

Fuente: Elaboración propia.

2.5. Procedimiento de análisis de datos.

Paras el análisis de datos se realizaron las siguientes actividades:

a) Se realizó la revisión del numeral 6.1 que comprende la etapa de planificación de la norma NTP ISO/IEC 27001 2014 correspondientes a las acciones que se deben realizar para tratar los riesgos y las oportunidades dentro de una organización.

b) Se realizó el análisis de la identificación de niveles de riesgo en los servidores de la organización usando las herramientas informáticas como Owasp Zap, Vega y Arachni con la utilización de sus técnicas y métodos para la identificación de riesgos. Esto se realizó con la finalidad de identificar los niveles de riesgo de S.I. Por ello se invoca al numeral 6.1.2 c) de la norma en estudio, que expresa que es necesario identificar los riesgos de seguridad de la información en la organización.

c) La medición de cada herramienta se realizó a través de los indicadores, anotando los resultados del análisis en la guía de observación. En este punto se invoca a la norma 6.1.1 b) en la que se menciona que toda organización en este caso la UNI debe prevenir y planificar los probables riesgos y vulnerabilidades que perjudicarían a sus servidores e infraestructura de TI en la cual reside la información. La finalidad es que la organización reduzca los impactos de estas vulnerabilidades y pueda de forma progresiva alcanzar la mejora continua a través del tiempo.

d) Los resultados fueron evaluados, clasificados y graficados para representar de manera objetiva la realidad encontrada en los sistemas de información. Esto se correlaciona con el numeral 6.1.2 d) que menciona que se deben analizar los riesgos de S.I. La herramienta informática identifica los niveles de riesgo y muestra los recursos que consume al identificar el riesgo. Por ejemplo, cuanto demanda el uso de la memoria RAM o uso de CPU, los cuales son dos recursos muy relevantes en la administración de la información en la UNI.

2.6. Criterios éticos.

La participación del investigador exige una actitud ética por las consecuencias y efectos que se podrían derivar de la iteración establecida con los objetos o sujetos de la investigación.

Veracidad:

La información mostrada será según al ambiente donde se realizaron las pruebas, donde los resultados concordaron con lo definido.

Confidencialidad:

El trabajo de investigación mantuvo una ética profesional al realizar las diferentes pruebas, donde se guardó en privacidad la información que residía en las computadoras y servidores de la empresa.

Originalidad:

Se citarán las fuentes bibliográficas de la información mostrada.

Criterios de Rigor Científico.

Validez:

Al operacionalizar las variables y sus dimensiones fueron evaluadas a través de los indicadores fijados y haciendo uso de los métodos para recolectar datos.

Fiabilidad:

Las pruebas efectuadas, la configuración de las herramientas y los resultados logrados se utilizaron referencialmente.

Replicabilidad:

La investigación puede volver a repetirse sin que los resultados se contradigan.

III. RESULTADOS Y DISCUSIÓN.

3.1. Resultados

Tabla 2. *Nivel de riesgo identificado con la herramienta Owasp Zap.*

Nivel de Riesgo	Cantidad	Porcentaje
Alto	0	0.0%
Medio	2	22.2%
Bajo	5	55.6%
Informativo	2	22.2%
Total	9	100.0%

Fuente: Elaboración propia.

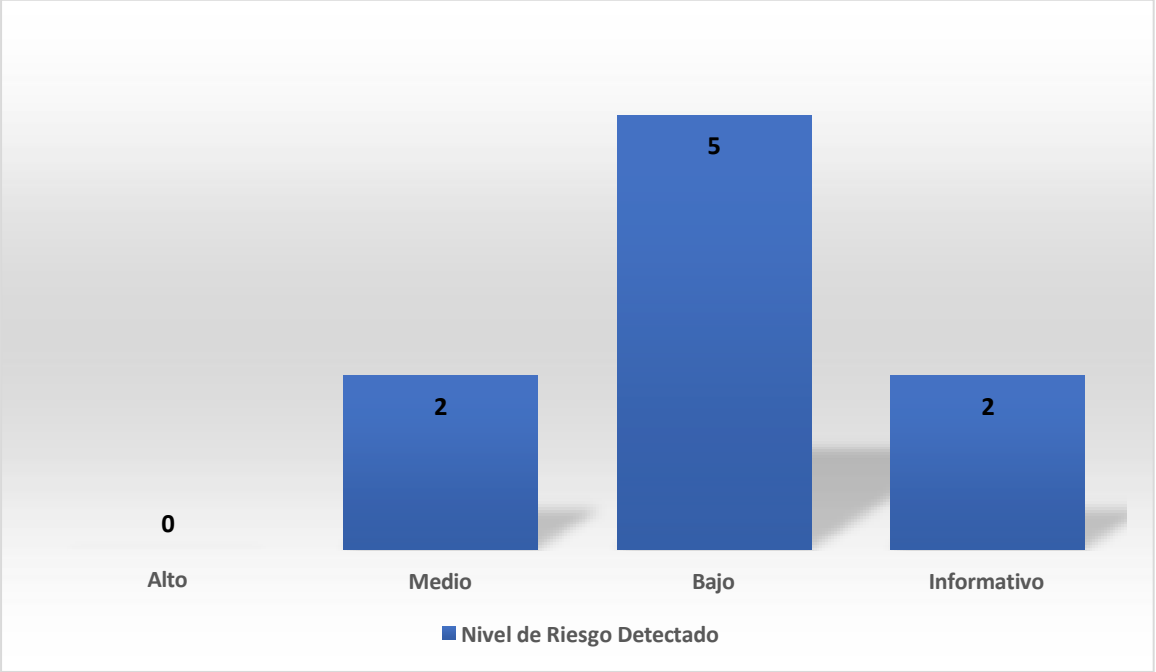


Figura 23. Niveles de riesgo identificado con Owasp Zap

Fuente: Elaboración propia.

De la tabla 2 luego de probar la herramienta Owasp Zap el nivel de riesgo alto tiene la probabilidad que sucedan ataques en un 0%, el nivel de riesgo medio en un 22.2%, el nivel de riesgo bajo en un 55.6% y el nivel de riesgo informativo tiene la probabilidad de

que puedan ocurrir ataques en un 22.2% con referencia a los indicadores mencionados en el párrafo anterior.

En este punto se invoca al numeral 6.1.2 de la norma en estudio que menciona que deben identificarse los niveles de riesgo, por ello el nivel de riesgo alto implica que el sitio web tiene altas probabilidades de sufrir ataques y ser vulnerable a la penetración de código abierto y afectar el sitio web, el nivel de riesgo medio comprende que el sitio web tiene probabilidades medias de sufrir ataques y ser vulnerable a la penetración de código abierto y afectar el sitio web. De manera similar se hace mención del nivel de riesgo bajo en el cual la probabilidad es mínima. Por último, el nivel de riesgo informativo solo tiene carácter de informar de los posibles riesgos y sus efectos, y cuáles serían las medidas a tomar.

Tabla 3*. Nivel de riesgo identificado con la herramienta Vega.*

Nivel de Riesgo	**Cantidad**	**Porcentaje**
Alto	0	0.0%
Medio	2	22.2%
Bajo	3	33.3%
Informativo	4	44.4%
Total	9	100.0%

Fuente: Elaboración propia.

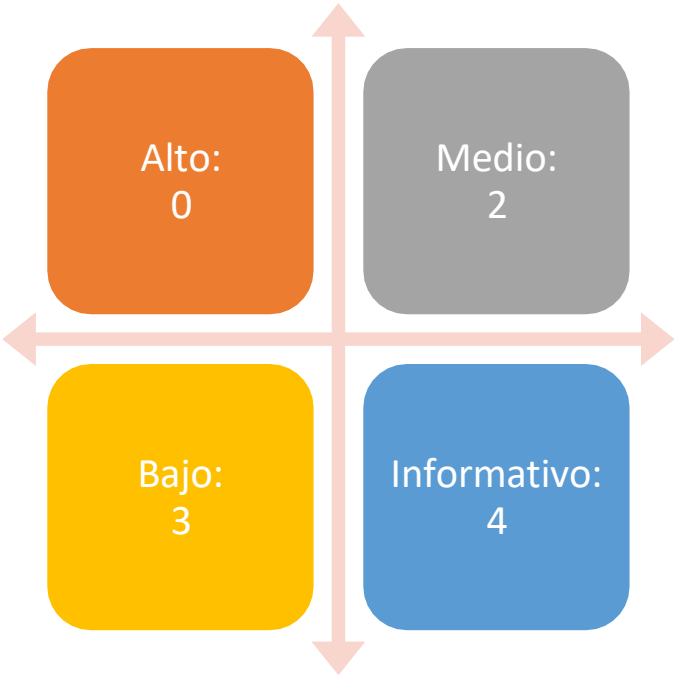


Figura 24. Niveles de riesgo identificado con Vega

Fuente: Elaboración propia.

De la tabla 3 luego de probar la herramienta Vega el nivel de riesgo alto tiene la probabilidad de que ocurran ataques en un 0%, el nivel de riesgo medio en un 22.2%, el nivel de riesgo bajo en un 33.3% y el nivel de riesgo informativo tiene la probabilidad de que ocurran ataques en un 44.4% afectando el normal funcionamiento del sitio web.

En este punto se invoca al numeral 6.1.2 de la norma en estudio que menciona que deben identificarse los niveles de riesgo, en este caso el nivel de riesgo alto implica que el sitio web tiene altas probabilidades de sufrir ataques y ser vulnerable al crawling el cual es un método que recopila información que es utilizado para identificar todos los subdirectorios que tienen relación con un sitio web de código abierto perjudicando en este caso el funcionamiento del sitio web. El nivel de riesgo medio indica que el sitio web tiene probabilidades medias de sufrir ataques y ser vulnerable al crawling, el nivel de riesgo bajo se refiere a que hay probabilidades mínimas de que el sitio web sufra ataques por crawling.

Por último, el nivel de riesgo informativo solo tiene carácter de informar de los posibles ataques y sus efectos, y cuáles serían las medidas a tomar.

Tabla 4. *Nivel de riesgo identificado con la herramienta Arachni.*

Nivel de Riesgo	Cantidad	Porcentaje
Alto	0	0.0%
Medio	2	50.0%
Bajo	1	25.0%
Informativo	1	25.0%
Total	4	100.0%

Fuente: Elaboración propia.

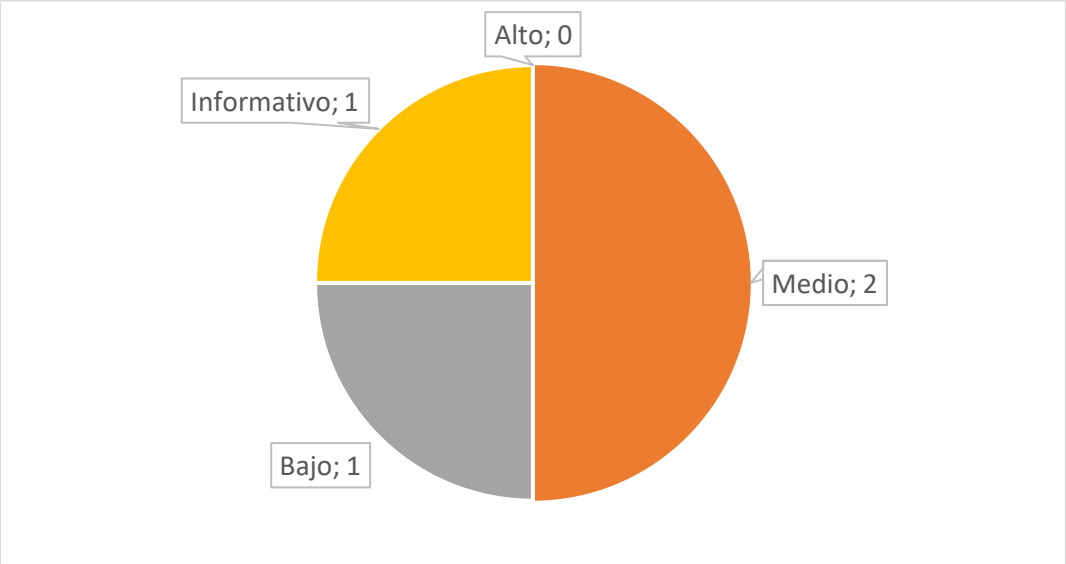


Figura 25. Niveles de riesgo identificado con Arachni

Fuente: Elaboración propia.

De la tabla 4 luego de probar la herramienta Arachni el nivel de riesgo alto tiene la probabilidad de que puedan ocurrir ataques en un 0%, el nivel de riesgo medio un 50%, el nivel de riesgo bajo un 25% y el nivel de riesgo informativo tiene la probabilidad de que puedan ocurrir ataques en un 25%.

Así se invoca al numeral 6.1.2 de la norma en estudio que menciona que se deben identificar los niveles de riesgo, es así que el nivel de riesgo alto implica que el sitio web tiene altas probabilidades de sufrir ataques de tipo SQL Injection y XSS (Cross Site Scripting), el nivel de riesgo medio indica que el sitio web tiene probabilidades medias de sufrir ataques y ser vulnerable al SQL Injection y XSS. Así mismo se referencia del nivel de riesgo bajo en la cual la probabilidad es mínima. Por último, el nivel de riesgo informativo solo tiene carácter de informar de las posibles amenazas y sus efectos, y cuáles serían las medidas a ejecutar.

Tabla 5. *Recursos del sistema utilizados con las herramientas seleccionadas.*

Recurso del sistema	Owasp Zap	Vega	Arachni
Uso de CPU	20.7%	56.7%	1.6%
Uso de RAM	471.9 MB	338.7 MB	26.3 MB
Uso de Disco Duro	0.1 MB/s	0.1 MB/s	0.1 MB/s

Fuente: Elaboración propia.

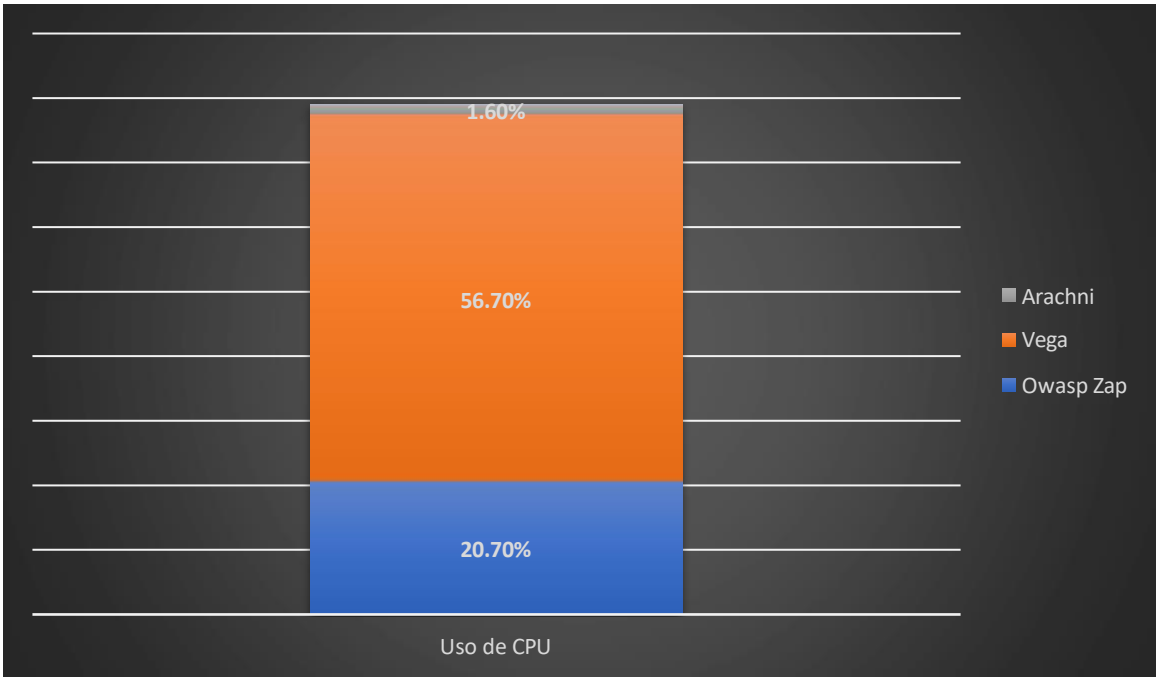


Figura 26. Recurso del sistema utilizado con las herramientas seleccionadas

De la Tabla 5 se puede apreciar los recursos del sistema o indicadores en que se sustenta la presente investigación y que son: el uso de CPU, el uso de memoria RAM y el uso de Disco Duro. Por otro lado, en el eje horizontal se aprecian las tres herramientas informáticas que fueron utilizadas para medir las vulnerabilidades a las que podía estar afectando al sitio web de la Facultad de Ingeniería y de Sistemas de la UNI.

. En la parte central se aprecian los resultados de la medición. Todo esto está sustentado en el numeral 6.2 b) que dice que los objetivos de la S.I se puedan medir y c) tener en cuenta requisitos que se puedan aplicar a la S.I y los resultados que resulten de identificar los niveles de riesgos.

Respecto al uso de CPU, la herramienta Arachni resulto ser la que menos consumo hizo de este recurso con el 1.6% de la CPU para realizar su trabajo de identificar los niveles de riesgo, seguido de la herramienta Owasp Zap que usa el 20.7% de CPU y en tercer lugar la herramienta Vega que utiliza el 56.7% de CPU. Esto significó que la herramienta Arachni resulto ser más eficiente que las otras herramientas debido a que solo utilizo el 1.6% del uso de CPU para poder correr y realizar su análisis para identificar niveles de riesgo a profundidad y emitir un reporte. En el otro extremo se encuentra Vega, resultando ser una herramienta muy pesada que llega a consumir más del 50% del uso de CPU para realizar su trabajo de carga y detección de niveles de riesgo.

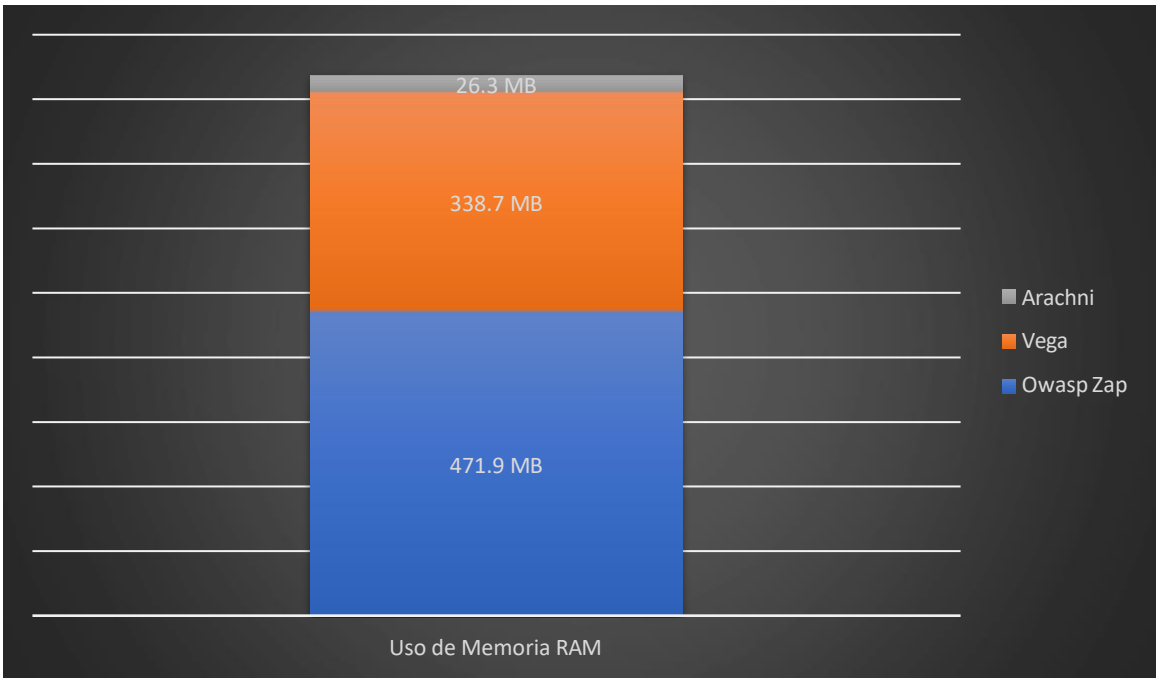


Figura 27. Recurso del sistema utilizado con las herramientas seleccionadas

Con relación al uso de memoria RAM, Arachni fue la que menos recurso consumió con un 26.3 MB de RAM del sistema para realizar su rutina de identificar los niveles de riesgo, esta clase de memoria se encarga de guardar la información que requiere la herramienta Arachni mientras se ejecuta. Por otro lado, la herramienta Vega utilizó 338.7 MB de memoria RAM un consumo considerable al ejecutar sus operaciones de detección de niveles de riesgo y en tercer lugar Owasp Zap fue la herramienta menos eficiente, ya que utiliza el 471.9 MB de la memoria RAM del sistema.

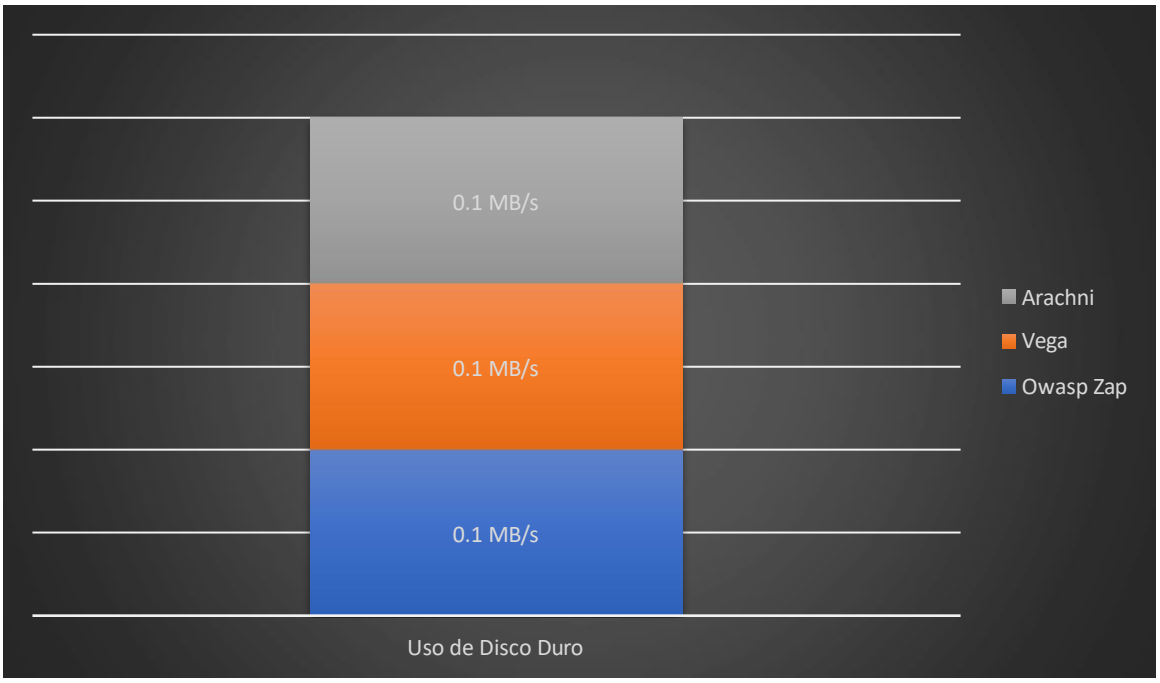


Figura 28. Recurso del sistema utilizado con las herramientas seleccionadas

Por último, con respecto al uso de Disco Duro, las 03 herramientas utilizaron el 0.1 MB/s de Disco Duro para identificar los niveles de riesgo. Es decir, estas herramientas no ocuparon muchos procesos en el disco duro al ser ejecutados obteniendo una velocidad óptima de 0.1 MB/s en el Disco Duro para efectuar el análisis de identificación de niveles de riesgo del sitio web analizado. Es un consumo mínimo del disco duro el utilizado por estas herramientas.

Tabla 6. *Niveles de riesgo identificados con las herramientas seleccionadas.*

Nivel de Riesgo	Owasp Zap	Vega	Arachni
Alto	0	0	0
Medio	2	2	2
Bajo	5	3	1
Informativo	2	4	1
Total	9	9	4

Fuente: Elaboración propia.

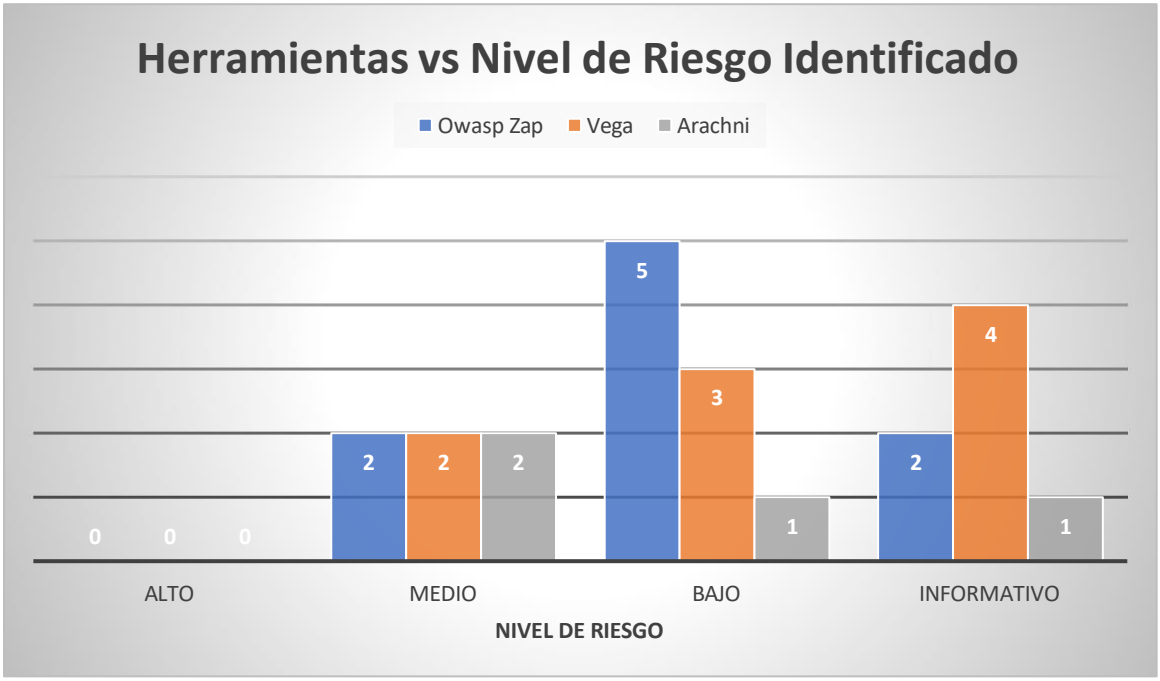


Figura 29. Niveles de riesgo identificado con las herramientas seleccionadas

Fuente: Elaboración propia.

De la Tabla 6 se puede apreciar que la herramienta Owasp Zap identificó un total de 9 vulnerabilidades al igual que la herramienta Vega seguido de la herramienta Arachni que detectó un total de 4 vulnerabilidades clasificando cada vulnerabilidad según el nivel de riesgo. Así mismo haciendo un análisis más profundo y detallado las tres herramientas no

detectaron ninguna vulnerabilidad a nivel de riesgo alto, en la detección a nivel de riesgo medio Owasp Zap, Vega y Arachni solo detectaron 2 tipos de vulnerabilidades, a nivel de riesgo bajo Owasp Zap fue la más eficiente, puesto que detecto 5 tipos de vulnerabilidades, seguido de Vega que detecto 3 tipos de vulnerabilidades y la menos eficiente fue Arachni que solo detecto 1 vulnerabilidad. Con referencia al nivel de riesgo informativo la más eficiente fue Vega que detecto 4 tipos de vulnerabilidades, seguido de Owasp Zap que detecto solo 2 tipos de vulnerabilidades, siendo la menos eficiente Arachni que solo detecto 1 vulnerabilidad.

3.2. Discusión

Objetivo 1:

Caracterización de la identificación de riesgos en la etapa de planificación de la norma NTP-ISO/IEC 27001 2014.

El numeral 6.1 de la norma NTP-ISO/IEC 27001 2014, determinan que las empresas deben planear acciones que afronten los riesgos y las oportunidades. El numeral 6.1.2 indica que la organización debe definir y aplicar un proceso de valoración del riesgo de S.I. El numeral 6.1.3, establece que la empresa debe determinar y aplicar un proceso que trate a los riesgos de S.I. seleccionando alternativas para tratar los riesgos de forma apropiada tomando en consideración el efecto o consecuencia de valorar los riesgos, así como establecer todos los controles que se necesiten al implementar las alternativas elegidas de tratamientos de riesgos de S.I.

Los resultados al ser comparado con el estudio realizado por (Susana Patiño & Franyelit Suárez, 2017) denominado Evaluación de seguridad informática basada en ICREA E ISO27001 (Ecuador), esta investigación concluye que, de acuerdo al análisis realizado de la realidad por la que atraviesan las empresas y organizaciones de estar expuestas a protocolos y softwares que generen vulnerabilidades y ataques que atenten

contra su seguridad y confidencialidad de datos e información, se vieron en la necesidad de realizar un análisis de evaluación de riesgos en base a los lineamientos de la norma ISO 27001 y como consecuencia se creó un sistema de gestión de riesgos de acuerdo a las normas ICREA Std-131-2013 e ISO/IEC 27001.

Objetivo 2:

Evaluar las herramientas informáticas apropiadas para la identificación de riesgos.

Las herramientas seleccionadas para la identificación de riesgos (Owasp Zap, Vega y Arachni) utilizaron las técnicas de pruebas de penetración, identificación de servicios y SQL Injection, los cuales permitieron identificar los riesgos existentes dentro de la organización, como se visualiza en los resultados de la Tabla 2, 3 y 4.

Esta etapa se contrasta con lo que explica Leguizamón et al., (2020) en su investigación, realizada en Colombia. En esta investigación los autores implementaron Cowrie y HoneyPy, una herramienta para detectar diversos modelos y modalidades de ataque, orientando un script mediante la configuración de en el servidor IDS (Intrusion Detection System). El diseño de infraestructura con la herramienta informática creada honeypots, hizo posible detectar riesgos de seguridad en los servidores de la universidad como consecuencia de ataques informáticos.

Objetivo 3:

Realizar la medición de las herramientas informáticas seleccionadas.

Se realizó la identificación de riesgos con las 03 herramientas seleccionadas, primero con la herramienta Owasp Zap utilizando las técnicas de pruebas de penetración e inyección SQL, obteniendo los siguientes resultados de niveles de riesgo: Alto con el 0%, Medio con el 22.2%, Bajo con el 55.6% y de Información con el 22.2%. Después se realizó

la identificación de riesgos con la herramienta Vega utilizando las técnicas de pruebas de penetración e inyección SQL, obteniendo los siguientes resultados de niveles de riesgo: Alto con el 0%, Medio con el 22.2%, Bajo con el 33.3% y de Información con el 44.4%. Finalmente se realizó la identificación de riesgos a través de la herramienta Arachni utilizando las técnicas de pruebas de penetración e inyección SQL, obteniendo los siguientes resultados de niveles de riesgo: Alto con el 0%, Medio con el 50%, Bajo con el 25% y de Información con el 25%. En todos los casos se consideran los niveles de riesgo alto como vulnerabilidades potenciales.

Estos resultados al ser comparados con el estudio realizado por Rodríguez Llerena (2020), en su trabajo de investigación titulado Herramientas fundamentales para el hacking ético (Cuba), en su investigación concluyó que, existen diversos recursos que sirven para la detección para diversos fines, entre estos figuran escaneo de puntos vulnerables en aplicaciones web, así como en dispositivos móviles. Entre estas destacan las herramientas informáticas Kali Linux, Black Arch y Parrot Security. Se concluye que existe una diversidad de herramientas para la identificación de riesgos y ataques informáticos, pero en el caso de Cuba fue importante para saber cuáles son estas herramientas a usar, considerando las cualidades de las redes del Estado en el país socialista.

3.3. Aporte de la investigación.

En la investigación, se realizó la revisión del capítulo 6 de la norma NTP-ISO/IEC 27001 2014, que comprende la etapa de planificación de la norma, donde se indican las acciones que se deben de realizar para tratar los riesgos y las oportunidades dentro de la organización, la norma se encuentra en el Anexo 5.

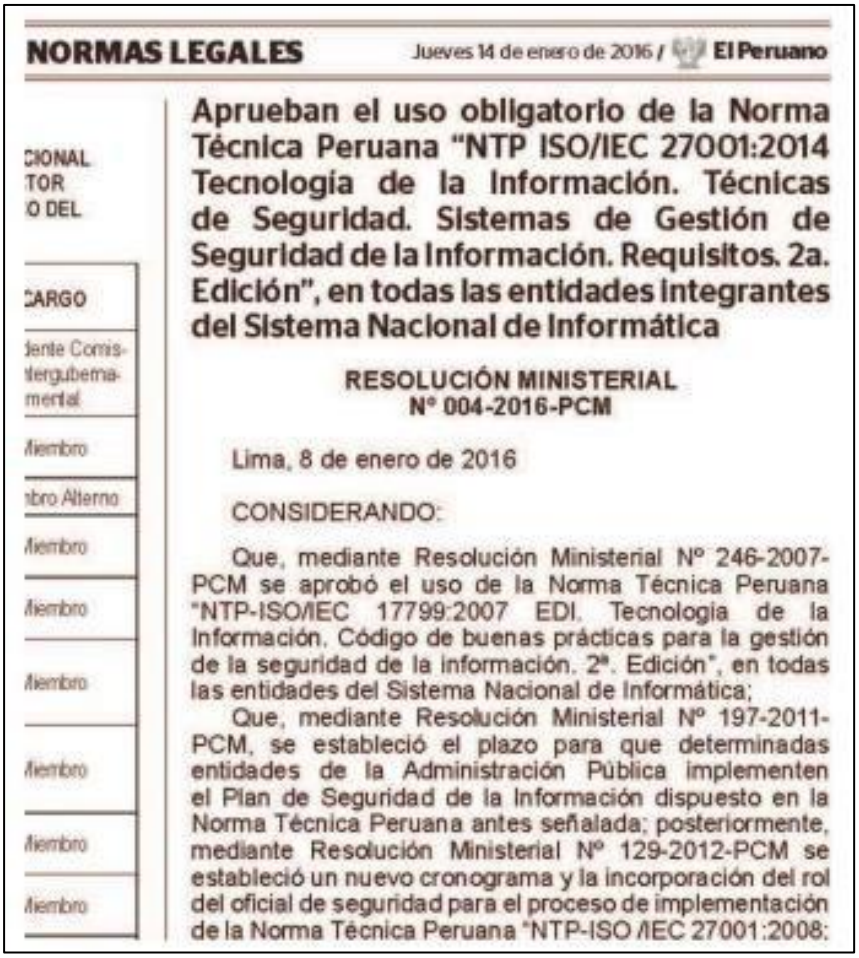
Se seleccionaron 03 de las mejores herramientas para la identificación de riesgos en aplicaciones web como son la herramienta Owasp Zap, Vega y Arachni, la descripción

de las herramientas seleccionadas se puede visualizar en la guía de análisis documental que se encuentra en el Anexo 3.

Se realizó la medición de las herramientas en el portal web de la FIIS UNI a través de los indicadores anotando los resultados en la guía de observación, la guía de observación se encuentra en el Anexo 4.

Los resultados fueron evaluados, clasificados y graficados para ser representados de manera objetiva, como se pueden visualizar en las tablas 2, 3 y 4.

La evaluación de herramientas informáticas para el tratamiento de riesgos se sustentó en la norma NTP-ISO/IEC 27001 2014, que fue aprobado con R.M. N° 004-2016-PCM el 8 de enero de 2016.



NORMAS LEGALES Jueves 14 de enero de 2016 / El Peruano

CIONAL
TOR
O DEL

CARGO

dente Comis-
tergubema-
mental

Miembro

bro Alterno

Miembro

Miembro

Miembro

Miembro

Miembro

Miembro

Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática

RESOLUCIÓN MINISTERIAL
N° 004-2016-PCM

Lima, 8 de enero de 2016

CONSIDERANDO:

Que, mediante Resolución Ministerial Nº 246-2007-PCM se aprobó el uso de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª. Edición", en todas las entidades del Sistema Nacional de Informática;

Que, mediante Resolución Ministerial Nº 197-2011-PCM, se estableció el plazo para que determinadas entidades de la Administración Pública implementen el Plan de Seguridad de la Información dispuesto en la Norma Técnica Peruana antes señalada; posteriormente, mediante Resolución Ministerial Nº 129-2012-PCM se estableció un nuevo cronograma y la incorporación del rol del oficial de seguridad para el proceso de implementación de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008:

Figura 30. Publicación de la Norma NTP-ISO/IEC 27001 2014.

Fuente: Diario Oficial del Peruano.

De la Norma NTP-ISO/IEC 27001 2014, se usaron de forma práctica los siguientes Numerales indicados en la norma:

6.1. Acciones para tratar los riesgos y oportunidades (A nivel de planificación).

8.2. Evaluación de riesgos de S.I (A nivel de operación).

8.3. Tratamiento de riesgos de S.I (A nivel de operación).

Descripción de la Empresa

La FIIS de la UNI se distingue por su gran sentido innovador y constante actualización científica y tecnológica, lo cual le facilita formar profesionales de gran nivel en sus respectivas especialidades, que tienen sólidos principios culturales, morales, éticos y de protección ambiental para encarar con éxito las exigencias del mundo globalizado y contribuyendo con el desarrollo del Perú.

La FIIS de la UNI brinda una gran variedad de información y de accesos a sus diferentes áreas de servicios a través de su portal web sobre el cual fueron probadas las herramientas informáticas para la identificación de riesgos.

IV. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones.

a) La investigación se sustentó en la Norma NTP-ISO/IEC 27001 2014, adaptado a la realidad peruana. Se aplicó a la FIIS de la UNI.

b) En la investigación, se evaluaron 03 herramientas de S.I para la identificación de niveles de riesgo en el portal web de la FIIS de la UNI, donde se utilizaron las técnicas como pruebas de penetración, identificación de servicios e inyección SQL.

c) Las 03 herramientas de seguridad informática identificaron niveles de riesgos las cuales se compararon tomando en cuenta los parámetros: nivel de riesgo detectado, uso de memoria RAM, uso de CPU y uso de Disco Duro. Cada parámetro se cuantificó con números para hacer las comparaciones respectivas y determinar la herramienta más idónea para realizar la identificación de riesgos. Resultando la herramienta Owasp Zap la más eficaz y eficiente para la identificación de riesgos.

d) La situación actual de la S.I. de la FIIS de la UNI no es óptima, dado que presenta falencias y brechas de S.I en muchos de los servicios que ofrece, quedando expuesto a futuros ataques y brechas que hacen que se produzcan ataques de terceros a los servidores de la FIIS de la UNI.

e) Se encontraron diferentes tipos de niveles de riesgo: medio, bajo y de información, el cual permitiría a posibles atacantes realizar ataques sin restricciones.

f) Todo el estudio se centró en la etapa de planificación de la norma NTP-ISO/IEC 27001 2014.

4.2. Recomendaciones.

a) Se recomienda el uso de las herramientas informáticas evaluadas en la presente investigación que, mediante la utilización de las técnicas de pruebas de penetración, identificación de servicios e inyección SQL, permiten identificar los niveles de riesgo que presenta el portal web de la FIIS de la UNI.

b) Se recomienda realizar periódicamente actualizaciones de licencias, firewalls, versiones, etc., de cada uno de los servicios para evitar ataques informáticos que vulneren la S.I que reside en los servidores de la FIIS de la UNI.

c) Se recomienda aplicar estrategias que concienticen al personal en temas de S.I, así como de la implementación de planes preventivos y correctivos para tratar los riesgos encontrados. Esto es materia de trabajos futuros es decir el tratamiento de cómo se abordarán y solucionarán los problemas de riesgo y S.I en la mencionada universidad en estudio.

d) Se debe asignar un presupuesto adecuado y suficiente para gestionar adecuadamente los recursos de S.I, de acuerdo a lo dispuesto en la norma NTP ISO/IEC 27001:2014 que permitan garantizar la integridad, veracidad y disponibilidad de la información y datos almacenados en los servidores web de la FIIS de la UNI.

REFERENCIAS.

[1] «ElEconomista América,» 23 Octubre 2019. [En línea]. Available: https://www.eleconomistaamerica.pe/telecomunicacion-tecnologia-pe/noticias/10157538/10/19/Peru-es-el-tercer-pais-con-mas-ciberataques-en-America-Latina.html.

[2] C. Lengua, «El Comercio,» 16 Noviembre 2020. [En línea]. Available: https://elcomercio.pe/economia/empresas-peruanas-en-riesgo-de-ciberataques-que-opciones-ofrece-el-mercado-ncze-noticia/?ref=ecr.

[3] «RPP Noticias,» 3 Diciembre 2019. [En línea]. Available: https://rpp.pe/economia/economia/bcp-revela-que-en-ataque-cibernetico-del-2018-hackers-accedieron-a-datos-de-clientes-noticia-1232964?ref=rpp.

[4] C. Farro Flores, «Ciberdelincuencia: Amenaza Latente,» *Cargo Security,* p. 12, 2019.

[5] C. A. Pasmiño Zabala, A. K. Serrano Castro y M. M. González Rivera, «Las Tics como herramienta para la gestión de riesgos,» Guaranda, 2020.

[6] M. R. Ospina Díaz y P. E. Sanabria Rangel, «Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia,» Bogotá, 2020.

[7] A. E. Rodriguez Llerena, «Herramientas fundamentales para el hacking ético,» La Habana, 2020.

[8] M. Leguizamón Páez, M. Bonilla Díaz y C. León Cuervo, «Análisis de ataques informáticos mediante Honeypots en la Universidad Distrital francisco José de Caldas,» Bogotá, 2020.

[9] J. E. Moreno Marín y P. C. Coronado Sánchez, «Modelo base de conocimiento para auditorías de seguridad en Servicios Web con SQL Injection,» Bogotá, 2020.

[10] A. Vera Buitrago y J. Camargo Mendoza, «Herramienta informática para notificación comunitaria como insumo para la generación de alertas en seguridad alimentaria y nutricional,» Bogotá, 2019.

[11] F. Y. Holguín García y L. M. Lema Moreta, «Modelo para Medir la Madurez del Análisis de Riesgo de los Activos de Información en el contexto de las Empresas Navieras,» Samborondón, 2019.

[12] H. R. González Brito y R. Montesino Perurena, «Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades frecuentes en aplicaciones web,» La Lisa, 2018.

[13] D. S. Gordón Revelo y R. Pacheco Villamar, «Análisis de Estrategias de Gestión de Seguridad Informática con Base en la Metodología Open Source Security Testing Methodology Manual (OSSTMM) para la Intranet de una Institución de educación Superior,» Guayaquil, 2018.

[14] E. Téllez Carvajal, «TECNOLOGÍAS, SEGURIDAD INFORMÁTICA Y DERECHOS HUMANOS,» México, 2018.

[15] C. M. Susana Patiño y R. N. Franyelit Suárez, «EVALUACIÓN DE SEGURIDAD INFORMÁTICA BASADA EN ICREA E ISO27001,» Quito, 2017.

[16] E. Crespo Martinez, «Ecu@Risk, Una metodología para la gestión de Riesgos aplicada a las MPYMEs,» Cuenca, 2017.

[17] F. Solís, D. Pinto y S. Solís, «Seguridad de la información en el intercambio de datos entre dispositivos móviles con sistema Android utilizando el método de encriptación RSA,» Sangolquí, 2017.

[18] E. Bernardis, H. Bernardis, M. Berón y G. Montejano, «Seguridad en Servicios Web,» San Luis, 2017.

[19] J. Veloz, A. Alcivar, G. Salvatierra y C. Silva, «Ethical hacking, una metodología para descubrir fallas de seguridad en sistemas informáticos mediante la herramienta KALI-LINUX,» Portoviejo, 2017.

[20] V. D. Gil Vera y J. C. Gil Vera, «Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas,» Bogotá, 2017.

[21] J. Izquierdo Cabrera y T. E. Tafur Callirgos, «MECANISMOS DE SEGURIDAD PARA CONTRARRESTAR ATAQUES INFORMATICOS EN SERVIDORES WEB Y BASE DE DATOS,» Pimentel, 2017.

[22] M. Pérez del Castillo, G. Rial, R. Sotelo y M. Gurméndez, «Clasificador de logs de acceso para detección de incidentes de Ciberseguridad,» Montevideo, 2020.

[23] I. A. Rodríguez, F. A. Majul Ramírez, R. A. Gurrola y M. A. Cussin Delgado, «GESTIÓN INTEGRADA EN RIESGOS EN EL PROCESAMIENTO DE INFORMACIÓN EN EL SECTOR EDUCATIVO,» Durango, 2018.

[24] V. R. Kebande, I. Kigwana, H. S. Venter, N. M. Karie y R. D. Wario, «Análisis, clasificación y evaluación basados en métricas CVSS de amenazas y vulnerabilidades de redes informáticas,» Durban, 2018.

[25] M. Restrepo Gallego, «Aplicación de las herramientas Informáticas en el tratamiento de la información científica,» Revista Lasallista de Investigación, Medellin, 2005.

[26] A. E. Rodriguez Llerena, «Herramientas fundamentales para el hacking ético,» La Habana, 2020.

[27] R. Ahumada Matuz, «ANÁLISIS DE LA SEGURIDAD DENTRO DEL DESARROLLO WEB E IMPLEMENTACION DE TESTING,» Veracruz, 2018.

[28] F. M. Arévalo, I. P. Cedillo y S. A. Moscoso, «Metodología Agil para la Gestión de Riesgos Informáticos,» Cuenca, 2017.

[29] ISO 27001.

[30] D. X. Proaño Villavicencio, V. Gisbert Soler y E. Pérez Bernabeu, «3 Ciencias,» 2017.

ANEXOS

Anexo 1. Resolución de aprobación del trabajo de investigación

SE RESUELVE:

ARTÍCULO 1°: MODIFICAR, el tema de la Tesis denominada **EVALUACIÓN DE HERRAMIENTAS INFORMÁTICAS QUE DAN SOPORTE A LA NORMA ISO 27001 EN UNA FACULTAD DE INGENIERÍA DEL SISTEMA UNIVERSITARIO PERUANO"** por **"EVALUACIÓN DE HERRAMIENTAS INFORMÁTICAS PARA EL TRATAMIENTO DE RIESGOS EN LA NORMA NTP-ISO/IEC 27001 2014 EN UNA FACULTAD DE INGENIERÍA DEL SISTEMA UNIVERSITARIO PERUANO"** perteneciente a la linea de investigación de **INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE**, a cargo de **APARI VALENZUELA OSCAR** en condición de egresado, del Programa de estudios **INGENIERÍA DE SISTEMAS**.

USS | UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
RESOLUCIÓN N°0434-2021/FIAU-USS

Pimentel, 24 de mayo de 2021

ARTÍCULO 2°: MODIFICAR, la Resolución de Facultad con la que se asignó Asesor especialista y la Resolución de Facultad con la que se asignó Jurado evaluador, en el extremo del tema de la tesis quedando tal como se indica en el artículo 1° de la presente Resolución.

ARTÍCULO 3°: DEJAR SIN EFECTO, toda Resolución emitida por la Facultad que se oponga a la presente Resolución.

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE

Dr. Mario Fernando Ramos Moscol
Decano - Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

MBA. Maria Noelia Sialer Rivera
Secretaria Académica / Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

Anexo 2. Matriz de consistencia

TÍTULO	PREGUNTA GENERAL	OBJETIVO GENERAL	VARIABLES	POBLACIÓN	TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS
Evaluación de Herramientas Informáticas para el Tratamiento de Riesgos en la Norma NTP-ISO/IEC 27001 2014 en una Facultad de Ingeniería del Sistema Universitario Peruano	¿Qué herramientas informáticas son adecuadas evaluar para el tratamiento de riesgos en la etapa de implementación de la norma NTP-ISO/IEC 27001 2014?	Evaluar herramientas informáticas que permitan identificar los riesgos de acuerdo a la etapa de planificación de la norma NTP-ISO/IEC 27001 2014 en una facultad de ingeniería del sistema universitario peruano.	Variable Independiente: Herramientas Informáticas	La población en estudio se da de acuerdo a las 10 principales herramientas de seguridad informática disponibles en el medio	Análisis Documental / Guía de Análisis Documental Observación / Guía de Observación

	PREGUNTAS ESPECÍFICAS	**OBJETIVOS ESPECÍFICOS**			
	¿Cuáles son los requisitos de la norma NTP-ISO/IEC 27001 2014 para tratamiento de riesgos?	Caracterizar la identificación de riesgos en la etapa de planificación de la norma NTP-ISO/IEC 27001 2014.	Variable Dependiente: Identificación y valoración de Riesgos		
	¿Qué técnica y herramienta se utilizará para el tratamiento de riesgos?	Evaluar las herramientas informáticas apropiadas para la identificación de riesgos.			
	¿Cómo se probará la eficacia de la	Realizar la medición de las herramientas			

	herramienta seleccionada?	informáticas seleccionadas			

Fuente: Elaboración propia.

Anexo 3. Guía de análisis documental

Herramienta Owasp Zap	
Nombre del documento	Revista Cubana de Informática Médica
Autor	Rodríguez LAE.
Referencia bibliográfica	Herramientas fundamentales para el hacking ético. Revista Cubana de Informática Médica. 2020;12(1):116-131.
Palabras clave de búsqueda	hacking ético, vulnerabilidades, escaneo, seguridad informática
Ubicación	https://www.medigraphic.com/cgi-bin/new/resumen.cgi?IDARTICULO=94154
Descripción del aporte al tema seleccionado	El aporte del autor a la investigación es describir algunas de las herramientas seleccionadas para el escaneo y explotación de vulnerabilidades, y conceptos fundamentales sobre el tema.

Herramienta Vega	
Nombre del documento	Aplicaciones web vulnerables a propósito
Autor	Román Muñoz, Fernando Sabido Cortes, Iván Israel García Villalba, Luis Javier
Referencia bibliográfica	Repositorio Institucional - UIGV
Palabras clave de búsqueda	hacking ético, vulnerabilidades, escaneo, seguridad informática

Ubicación	http://hdl.handle.net/20.500.11818/660
Descripción del aporte al tema seleccionado	En el presente trabajo se hace un análisis y valoración de las aplicaciones vulnerables a propósito existentes, con el objetivo de seleccionar y probar las que más tipos de vulnerabilidades incluyan y que mejor se puedan ampliar con nuevas

Herramienta Arachni	
Nombre del documento	Integración de nuevas herramientas de pruebas de seguridad en la Plataforma de Seguridad en las Tecnologías de la Información (PlatSI)
Autor	Medina Aguilera, Carlos Miguel Méndez Denis, Carlos Alejandro
Referencia bibliográfica	https://repositorio.uci.cu/jspui/handle/123456789/7698
Palabras clave de búsqueda	hacking ético, vulnerabilidades, escaneo, seguridad informática
Ubicación	https://repositorio.uci.cu/jspui/handle/123456789/7698
Descripción del aporte al tema seleccionado	El autor realiza un estudio sobre las herramientas de pruebas de seguridad a aplicaciones web existentes en la actualidad, con la finalidad de seleccionar las posibles a integrar a PlatSI. La Plataforma para la realización de auditorías tiene integradas cinco herramientas de pruebas de seguridad, ellas son: “Acunetix”, “Nikto”, “Arachni”, “ZAP” y “W3af”’

Anexo 4. Guía de observación

Objetivo: Observar y evaluar el uso de herramientas informáticas para la identificación de niveles de riesgos y el uso de recursos del sistema.

Observador: Apari Valenzuela Oscar.

Fecha: 18/06/2021

Duración: 2 horas por cada herramienta.

Lugar: Domicilio personal.

Sujetos observados: Herramienta informática Owasp Zap, Vega y Arachni.

Elementos observables: Diferentes niveles de riesgo que podrían vulnerar la seguridad del sitio web analizado.

Criterios de evaluación: Son los niveles de riesgo Alto, Medio, Bajo e Informativo.

Indicadores de efectividad de la herramienta informática: Nivel de Riesgo Identificado, Uso de CPU, Uso de Memoria RAM y Uso de Disco Duro.

Evaluación de la Herramienta Owasp Zap

Indicadores	**Criterios de Evaluación**			
	Alto	Medio	Bajo	Informativo
Nivel de Riesgo Identificado		x	x	x
Uso de CPU			x	
Uso de Memoria RAM			x	
Uso de Disco Duro			x	

Fuente: Elaboración propia.

Evaluación de la Herramienta Vega

Indicadores	Criterios de Evaluación			
	Alto	Medio	Bajo	Informativo
Nivel de Riesgo Identificado		x	x	x
Uso de CPU		x		
Uso de Memoria RAM			x	
Uso de Disco Duro			x	

Fuente: Elaboración propia.

Evaluación de la Herramienta Arachni

Indicadores	Criterios de Evaluación			
	Alto	Medio	Bajo	Informativo
Nivel de Riesgo Identificado		x	x	x
Uso de CPU			x	
Uso de Memoria RAM			x	
Uso de Disco Duro			x	

Fuente: Elaboración propia.

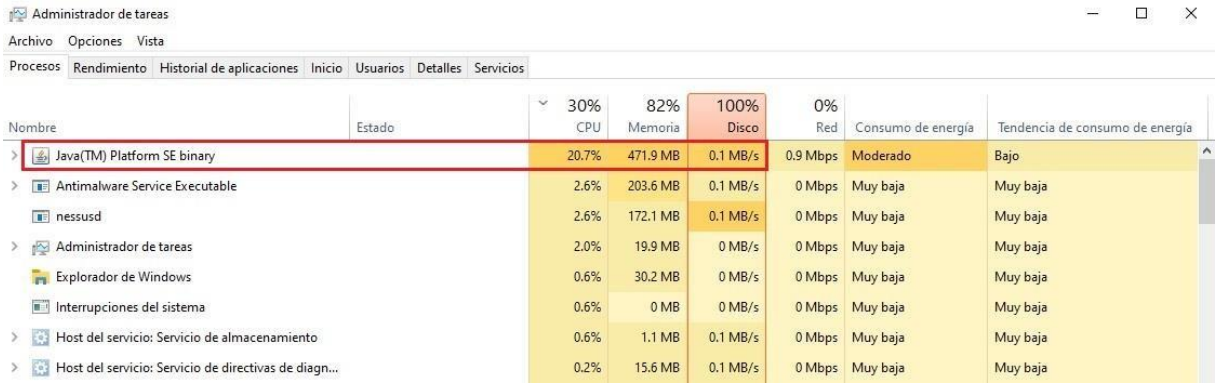


Figura 31. Recursos del sistema utilizados con la herramienta Owasp Zap

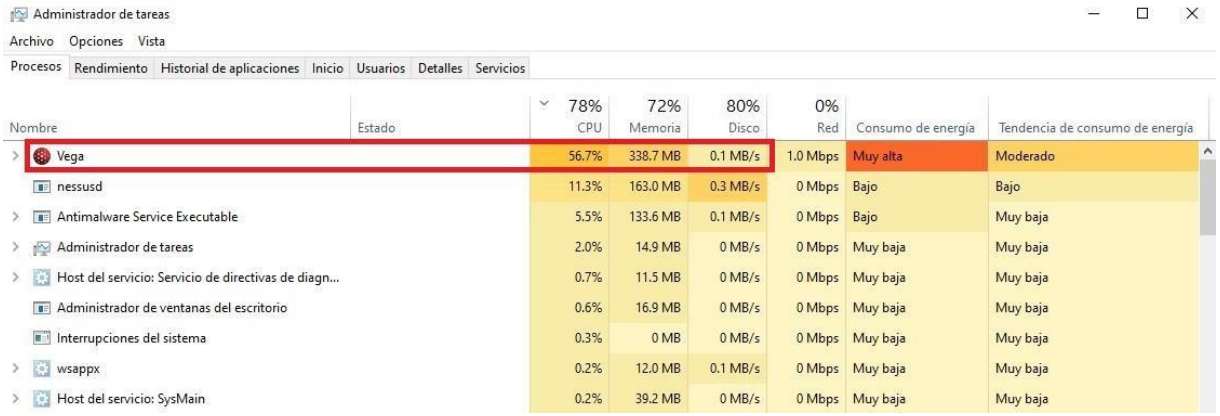


Figura 32. Recursos del sistema utilizados con la herramienta Vega

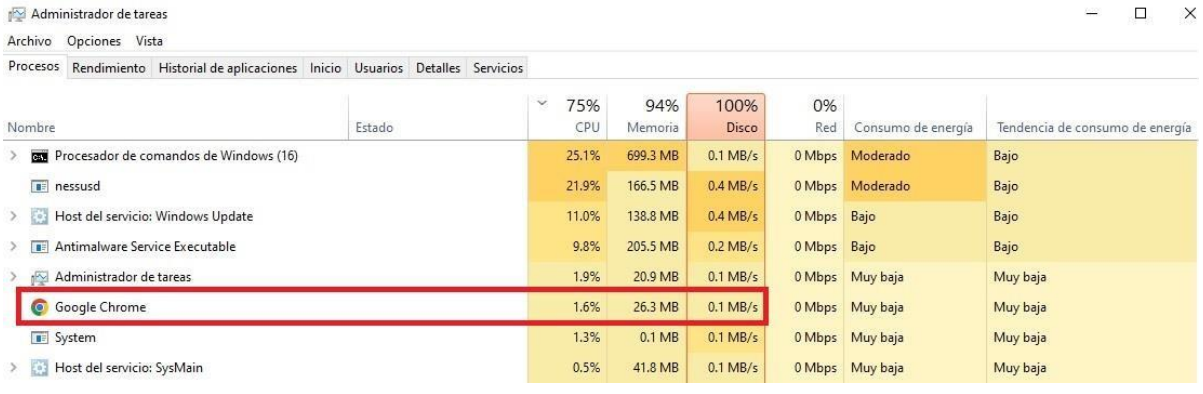


Figura 33. Recursos del sistema utilizados con la herramienta Arachni

Anexo 5. Norma Técnica Peruana NTP-ISO/IEC 27001 2014

NORMA TÉCNICA PERUANA | NTP-ISO/IEC 27001 2014

Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias - INDECOPI
Calle de La Prosa 104, San Borja (Lima 41) Apartado 145 Lima, Perú

TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos

INFORMATION TECHNOLOGY. Security techniques. Information security management systems — Requirements

(EQV. ISO/IEC 27001:2013+ISO/IEC 27001:2013/COR 1 Information technology -- Security techniques – Information security management systems – Requirements)

2014-11-20
2ª Edición

R.0129-2014/CNB-INDECOPI. Publicada el 2014-12-01 Precio basado en 36 páginas
I.C.S.: 35.040 ESTA NORMA ES RECOMENDABLE
Descriptores: Tecnología, información, técnicas, seguridad, sistema de gestión, requisitos

© ISO/IEC 2013 - © INDECOPI 2014

© ISO/IEC 2013
Todos los derechos son reservados. A menos que se especifique lo contrario, ninguna parte de esta publicación podrá ser reproducida o utilizada por cualquier medio, electrónico o mecánico, incluyendo fotocopia o publicándolo en el Internet o intranet, sin permiso por escrito del INDECOPI, único representante de la ISO/IEC en territorio peruano.

© INDECOPI 2014
Todos los derechos son reservados. A menos que se especifique lo contrario, ninguna parte de esta publicación podrá ser reproducida o utilizada por cualquier medio, electrónico o mecánico, incluyendo fotocopia o publicándolo en el Internet o intranet, sin permiso por escrito del INDECOPI.

INDECOPI

Calle de La Prosa 104, San Borja
Lima- Perú
Tel.: +51 1 224-7777
Fax.: +51 1 224-1715
sacreclamo@indecopi.gob.pe
www.indecopi.gob.pe

PREFACIO

A. RESEÑA HISTÓRICA

A.1 La presente Norma Técnica Peruana ha sido elaborada por el Comité Técnico de Normalización de Codificación e intercambio electrónico de datos, mediante el Sistema 1 o de Adopción, durante los meses de abril a junio del 2014, utilizando como antecedente a la norma ISO/IEC 27001:2013 Information Technology – Security techniques – Information security management systems – Requirements y la ISO/IEC 27001:2013/COR 1 2013 Information Technology – Security techniques – Information security management systems – Requirements

A.2 El Comité Técnico de Normalización de Codificación e intercambio electrónico de datos presentó a la Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias -CNB-, con fecha 2014-08-19, el PNTP-ISO/IEC 27001:2014, para su revisión y aprobación, siendo sometido a la etapa de discusión pública el 2014-10-18. No habiéndose presentado observaciones fue oficializada como Norma Técnica Peruana **NTP-ISO/IEC 27001:2014 TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos**, 2ª Edición, el 01 de diciembre de 2014.

A.3 Esta Norma Técnica Peruana reemplaza a la NTP-ISO/IEC 27001:2008 (revisada el 2013) y es una adopción de la norma ISO/IEC 27001:2013 y de la ISO/IEC 27001:2013/COR 1 . La presente Norma Técnica Peruana presenta cambios editoriales referidos principalmente a terminología empleada propia del idioma español y ha sido estructurada en concordancia a las Guías Peruanas GP 001:1995 y GP 002:1995.

B. INSTITUCIONES QUE PARTICIPARON EN LA ELABORACIÓN DE LA NORMA TÉCNICA PERUANA

Secretaría	GS1 PERU
Presidente	Roberto Puyó
Secretaria	Mary Wong

© ISO/IEC 2013 - © INDECOPI 2014 - Todos los derechos son reservados

ENTIDAD	REPRESENTANTE
B2IMPROVE S.A.C.	Belén Alvarado
CONSULTOR	Carlos Horna
DELOITTE & TOUCHE S.R.L.	Diana Lagos
DMS Perú S.A.C.	Adela Bárcenas Walter Equizabal
INDECOPI	Ivan Ancco
NSF INASSA SAC.	Raúl Miranda
SUPERINTENDENCIA DE ADMINISTRACION TRIBUTARIA – SUNAT	Daniel Llanos
GS1 PERU	Sara Carrión
CONTRALORÍA GENERAL DE LA REPÚBLICA	Marco Bermúdez Joel Mercado
FOLIUM S.A.C.	Roberto Huby
ONGEI	Ricardo Dioses
Facultad de Ciencias e Ingeniería - PUCP	Viktor Khlebnikov Willy Carrera
ITICSEC S.A.C.	Maurice Frayssinet
Consultora	Judith Blanco Jallurana

© ISO/IEC 2013 - © INDECOPI 2014 - Todos los derechos son reservados

PRÓLOGO
(ISO)

ISO (la Organización Internacional para la Normalización) e IEC (la Comisión Electrotécnica Internacional) forman el sistema especializado para la normalización mundial. Los órganos nacionales que son miembros de ISO o de IEC participan en el desarrollo de las Normas Internacionales a través de comités técnicos establecidos por la respectiva organización para ocuparse de campos particulares de actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en enlace con ISO y con IEC, también participan en el trabajo. En el campo de la tecnología de la información, ISO e IEC han establecido un comité técnico conjunto, ISO/IEC JTC 1.

Se redactan las Normas Internacionales en concordancia con las reglas proporcionadas en las Directivas ISO/IEC, Parte 2.

La tarea principal del comité técnico conjunto es preparar las normas internacionales adoptadas por el comité técnico conjunto, se circulan a los órganos nacionales para su votación. La publicación como una Norma Internacional requiere la aprobación de al menos 75 % de los órganos nacionales que emiten un voto.

Se señala la posibilidad de que alguno de los elementos de este documento pueda estar sujeto a derechos de patentes. No se hará responsable a ISO e IEC de identificar cualquiera o todos los mencionados derechos de patentes.

ISO/IEC 27001 fue preparada por el Comité Técnico conjunto ISO/IEC JTC 1, Tecnología de la información, Sub-comité SC 27, Técnicas de seguridad de la TI.

Esta segunda edición cancela y reemplaza la primera edición (NTP-ISO/IEC 27001:2008), la cual se ha revisado técnicamente.

© ISO/IEC 2013 - © INDECOPI 2014 - Todos los derechos son reservados

6. PLANIFICACIÓN

6.1 Acciones para tratar los riesgos y las oportunidades

6.1.1 Generalidades

Cuando se planifica para el sistema de gestión de seguridad de la información, la organización debe considerar los asuntos referidos en el numeral 4.1 y los requisitos referidos en el numeral 4.2 y determinar los riesgos y oportunidades que necesitan ser tratados para:

a) asegurar que el sistema de gestión de seguridad de la información pueda lograr su(s) resultado(s) esperado(s);

b) prevenir, o reducir, efectos indeseados; y

c) lograr la mejora continua.

La organización debe planificar:

d) acciones que traten estos riesgos y oportunidades; y

e) como

1) integrar e implementar estas acciones en sus procesos del sistema de gestión de seguridad de la información; y

2) evaluar la efectividad de estas acciones.

© ISO/IEC 2013 - © INDECOPI 2014 - Todos los derechos son reservados

6.1.2 Valoración del riesgo de seguridad de la información

La organización debe definir y aplicar un proceso de valoración del riesgo de seguridad de la información que:

a) establezca y mantenga criterios de riesgo de seguridad de la información que incluyan;

1) los criterios de aceptación de los riesgos; y

2) los criterios para realizar valoraciones de riesgo de seguridad de la información;

b) asegure que las valoraciones repetidas de riesgos de seguridad de la información produzcan resultados consistentes, válidos y comparables;

c) identifique los riesgos de seguridad de la información

1) aplicando el proceso de valoración de riesgos de seguridad de la información para identificar riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad para la información dentro del alcance del sistema de gestión de seguridad de la información; e

2) identificando a los propietarios de riesgos;

d) analice los riesgos de seguridad de la información:

1) valorando las consecuencias potenciales que resultarían si los riesgos identificados en 6.1.2 c) 1) fueran a materializarse;

2) valorando la probabilidad realista de la ocurrencia de los riesgos identificados en 6.1.2 c) 1); y

3) determinando los niveles de riesgo;

e) evalúe los riesgos de seguridad de la información:

1) comparando los resultados del análisis de riesgo con los criterios de riesgo establecidos en 6.1.2 a); y

2) priorizando los riesgos analizados para el tratamiento de riesgos.

© ISO/IEC 2013 - © INDECOPI 2014 - Todos los derechos son reservados

La organización debe retener información documentada sobre el proceso de valoración de riesgos de seguridad de la información.

6.1.3 Tratamiento de riesgos de seguridad de la información.

La organización debe definir y aplicar un proceso de tratamiento de riesgos de seguridad de la información para:

a) seleccionar opciones de tratamiento de riesgos de seguridad de la información apropiadas, tomando en cuenta los resultados de la valoración de riesgos;

b) determinar todos los controles que son necesarios para implementar la(s) opción(es) elegida(s) de tratamiento de riesgos de seguridad de la información;

NOTA: Las organizaciones pueden diseñar controles según se requiera, o identificarlos de cualquier fuente.

c) Comparar los controles determinados en 6.1.3 b) con aquellos del Anexo A y verificar que no se ha omitido ningún control necesario;

NOTA 1: El Anexo A contiene una lista integral de objetivos de control y controles. Los usuarios de esta Norma Técnica Peruana pueden dirigirse al Anexo A para asegurar que no se deje de lado ningún control necesario.

NOTA 2: Los objetivos de control están incluidos implícitamente en los controles escogidos. Los objetivos de control y los controles listados en el Anexo A no son exhaustivos y pueden ser necesarios objetivos de control y controles adicionales.

d) producir una Declaración de Aplicabilidad que contenga los controles necesarios (véase 6.1.3 b) y c)) y la justificación de las inclusiones ya sea que se implementen o no, así como la justificación de excluir controles del Anexo A;

e) formular un plan de tratamiento de riesgos de seguridad de la información; y

f) obtener la aprobación, por parte de los propietarios de riesgos, del plan de tratamiento de riesgos de la seguridad de la información y la aceptación de los riesgos residuales de la seguridad de la información.

La organización debe retener información documentada sobre el proceso de tratamiento de riesgos de seguridad de la información.

© ISO/IEC 2013 - © INDECOPI 2014 - Todos los derechos son reservados

NOTA: El proceso de valoración y tratamiento de riesgos de seguridad de la información en esta Norma Técnica Peruana se alinea con los principios y lineamientos genéricos proporcionados en ISO 31000[5]

6.2 Objetivos de seguridad de la información y planificación para conseguirlos

La organización debe establecer objetivos de seguridad de la información a niveles y funciones relevantes.

Los objetivos de seguridad de la información deben:

a) ser consistentes con la política de seguridad de la información;

b) ser medibles (si es práctico);

c) tomar en cuenta requisitos aplicables de seguridad de la información y resultados de la valoración y tratamiento de riesgos;

d) ser comunicados; y

e) ser actualizados según sea apropiado.

La organización debe retener información documentada sobre los objetivos de seguridad de la información.

Cuando planifique cómo lograr sus objetivos de seguridad de la información, la organización debe determinar:

f) qué se hará;

g) qué recursos serán requeridos;

h) quién será responsable;

i) cuándo se culminará;

j) cómo los resultados serán evaluados.

© ISO/IEC 2013 - © INDECOPI 2014 - Todos los derechos son reservados

Anexo 6. Carta de Aceptación

UNIVERSIDAD NACIONAL DE INGENIERIA

Oficina de Tecnologías de la Información

Lima, 08 de marzo 2024

CARTA N°026//CTIC-UNI/Jefatura-2024

Señor
OSCAR APARI VALENZUELA
Presente. –

Asunto. – Autorización para realizar pruebas de detención de vulnerabilidades informáticas en un portal WEB de nuestra entidad.

De mi consideración:

Sírvase la presente para expresarle mi cordal saludo y al mismo tiempo, dar respuesta al documento de la referencia para informar a su persona, que se AUTORIZA a realizar las pruebas de detección de vulnerabilidades informáticas en un portal web de nuestra entidad, utilizando las herramientas Owasp Zap. Vega y Arachni.

Sin otro particular me suscribo de Usted.

Atentamente,

MAG. ING. RUBÉN ARTURO BORJA ROSALES
JFE – OTI

Av. Túpac Amaru 210, Lima 15333, Perú
Teléfonos: 481-2559 / 481-1070 Anexo 7002
email: oti@uni.edu.pe

Reporte de similitud

NOMBRE DEL TRABAJO

Evaluación de herramientas informáticas para el tratamiento de riesgos en la norma NTP-ISO_IEC 27001

AUTOR

Oscar Apari Valenzuela

RECUENTO DE PALABRAS

10635 Words

RECUENTO DE CARACTERES

58568 Characters

RECUENTO DE PÁGINAS

78 Pages

TAMAÑO DEL ARCHIVO

4.0MB

FECHA DE ENTREGA

Jul 2, 2024 9:02 AM GMT-5

FECHA DEL INFORME

Jul 2, 2024 9:03 AM GMT-5

13% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 10% Base de datos de Internet
- 2% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 8% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Coincidencia baja (menos de 8 palabras)