PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

ESMERALDAS

ESCUELA DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

TESIS DE GRADO

GESTIÓN DE IDENTIDAD DIGITAL DE USUARIOS EN SERVICIOS WEB PARA LA PROTECCIÓN DE LA PRIVACIDAD DE LA INFORMACIÓN

LÍNEA DE INVESTIGACIÓN:

GOBIERNO Y ADMINISTRACIÓN DE TECNOLOGÍA DE INFORMACIÓN

Previo a la obtención del título de Ingeniero de Sistemas y Computación

AUTORA:

PAOLA UTRERAS

ASESORA: Susana Patiño

ESMERALDAS – ECUADOR, 2021

Tesis de grado aprobada luego de haber dado cumplimiento a los requisitos exigidos por el reglamento de grado de la PUCE Esmeraldas, previo a la obtención del título de INGENIERA DE SISTEMAS Y COMPUTACIÓN.

TRIBUNAL DE GRADUACIÓN

Mgt. Susana Patiño f.- ……

Asesor

Mgt. Kléber Vera f.- ……

Lector 1

Mgt. Evelin Flores f.- ……

Lector 2

Mgt. Susana Patiño f.- ……

Director de Escuela

Mgt. David Guashpa f.- ……

Secretario/a PUCESE

Esmeraldas, Ecuador, 2021

DECLARACIÓN DE AUTORÍA

Yo, **Paola Lissette Utreras Logacho**, con cedula de identidad No. **172417022-8** declaro mediante la presente que los resultados en la investigación que presento como tesis de grado, previo a la obtención del título “Ingeniera de Sistemas y Computación” son absolutamente originales, auténticos y personales.

En tal virtud, declaro que todo el contenido, comprendiendo resultados, conclusiones, los efectos legales y académicos que se desprenden de esta investigación son y será de exclusiva responsabilidad académica y legal.

AGRADECIMIENTOS

Agradezco primeramente a mis padres por siempre haberme apoyado y porque a pesar de los momentos difíciles siempre han sido mi ejemplo a seguir, a mis hermanos por brindarme el apoyo en mis metas. A toda mi familia y amigos que de una u otra manera colaboraron para en esta culminación de carrera universitaria haya podido llegar a su mejor final.

Y sobre todo a Dios.

DEDICATORIA

El presente trabajo de investigación esta

completamente dedicado a mis padres

que me han brindado todo su apoyo y

comprensión a lo largo del camino,

especialmente a mi madre que siempre ha

sido mi más grande motivación y mis

fuerzas para seguir adelante para poder

cumplir todas las metas que me he trazado.

RESUMEN

Actualmente, el riesgo de los sistemas informáticos ha incrementado el nivel de complejidad en las tecnologías de la información. Así mismo, las computadoras que se encuentran conectadas a internet están en peligro por distintas amenazas. Una posible consecuencia de todo eso es el incremento en el número de ataques informáticos. Una manera de evitar que esto suceda es identificando las vulnerabilidades potenciales que pueden ser aprovechadas por los atacantes.

La presente investigación fue desarrollada con el propósito de proteger la información del usuario evaluando las amenazas de los principales servicios web de la PUCESE, identificando cuáles son las posibles vulnerabilidades en el proceso de autenticación utilizando lineamentos basados en OWASP y de un modelo de identidad digital basado en el Instituto Nacional de Estándar y Tecnologías (NIST) SP – 800-63.

Se utilizó el lineamiento de seguridad informática QualysGuard que permite realizar un escaneo a los servicios web, generando un reporte con las vulnerabilidades, amenazas, impacto, el nivel de gravedad de esa vulnerabilidad y una posible solución a ese problema.

Se detectaron vulnerabilidades como el clickjacking en el que un atacante puede engañar al usuario para que haga clic en un marco invisible de la página, haciéndole tomar una acción que no quería tomar. También los atacantes pueden utilizar las cabeceras para tomar huellas digitales y lanzar ataques que son específicos para tecnologías y versiones usadas por la aplicación web.

Palabras clave: servicios web, OWASP, NIST SP – 800-63, seguridad informática, herramientas de detección de vulnerabilidades.

ABSTRACT

Currently, the risk of computer systems has increased due to the difficulty in information technologies. Likewise, the computers that are connected to the internet are in danger due to different threats. A possible consequence of all this is the increase in the number of computer attacks. One way to prevent this from happening is to identify potential vulnerabilities that can be exploited by attackers.

This research was developed with the purpose of protecting user information by evaluating the threats of the main PUCESE web services, identifying which are the possible vulnerabilities in the authentication process using OWASP-based lines and a digital identity based model at the National Institute of Standard and Technologies (NIST) SP - 800-63.

The QualysGuard computer security guideline is used, which allows you to scan web services, generate a report with vulnerabilities, threats, impact, the level of severity of that vulnerability and a possible solution to that problem.

Vulnerabilities such as clickjacking were detected in which an attacker can trick the user into clicking on an invisible frame on the page, causing him to take an action he did not want to take. Attackers can also use headers to take fingerprints and launch attacks that are specific to technologies and versions used by the web application.

Keywords: web services, OWASP, NIST SP - 800-63, informatic security, vulnerability detection tools.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

GLOSARIO DE TÉRMINOS

- **Amenazas. –** Se puede definir como amenaza a todo elemento o acción capaz de atentar contra la seguridad de la información[1].
- **Ataques XSS**. - Los ataques XSS son un tipo de inyección en la cual un atacante logra ejecutar código en los navegadores de los usuarios que acceden a un sitio web legítimo[2].
- **Autenticación. –** Es el proceso que debe seguir un usuario para tener acceso a los recursos de un sistema o de una red de computadores[3].
- **Base de datos. –** Una base de datos es una colección de información organizada de forma que un programa de ordenador pueda seleccionar rápidamente los fragmentos de datos que necesite[4].
- **Browsers. –** Un browser (que es también navegador web) es un programa mediante el cual se accede a internet cuya función es interpretar la información que recibe de manera tal que los usuarios puedan verla y utilizarla para realizar ciertas tareas mediante uno de los distintos tipos de browsers, como por ejemplo Internet Explorer[5].
- **Cláusulas de confidencialidad. –** Un acuerdo de confidencialidad (ADC), acuerdo de no divulgación (en inglés non-disclosure agreement), también referidos como contratos o convenios de confidencialidad, es un contrato legal entre al menos dos entidades para compartir material confidencial o conocimiento para ciertos propósitos, pero restringiendo su uso público[1].
- **Clickjacking**. - Es cuando un atacante usa varias capas transparentes u opacas para engañar a un usuario para que haga clic en un botón o enlace en otra página cuando intenta hacer clic en la página del nivel superior[2].
- **Cookies. –** Cookie" es un término informático que se refiere a un archivo de texto pequeño que los sitios web almacenarán en la computadora[6].
- **Criptografía. –** Básicamente, a criptografía es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet[6].

- **Cross-Site Scripting**. - También llamada ejecución de comandos en sitios cruzados es un tipo de vulnerabilidad informática o agujero de seguridad típico de las aplicaciones Web, que puede permitir a una tercera persona inyectar en páginas web visitadas por el usuario código JavaScript o en otro lenguaje similar[6].
- **Encriptada. –** Encriptar es una manera de codificar la información para protegerla frente a terceros. Por lo tanto, la encriptación informática sería la codificación la información de archivos o de un correo electrónico para que no pueda ser descifrado en caso de ser interceptado por alguien mientras esta información viaja por la red[7].
- **Fraude online. –** El fraude cibernético e informático se refiere al fraude realizado a través del uso de una computadora o del internet[1].
- **Gestión de identidad. –** Es una amplia área administrativa que se ocupa de la identificación de individuos en un sistema (por ejemplo, un país, una red o una empresa) así como de controlar su acceso a los recursos dentro de ese sistema mediante la asociación de derechos de usuario y restricciones conforme a la identidad establecida[1].
- **Hacker. –** Hacker es una voz del inglés para referirse a una persona o a una comunidad que posee conocimientos en el área de informática y se dedica a acceder a sistemas informáticos para realizar modificaciones en el mismo. Los hackers también son conocidos como “piratas informáticos[8].
- **Handshake SSL/TLS.** - En un protocolo de enlace TLS / SSL, los clientes y servidores intercambian certificados SSL, requisitos de conjuntos de cifrado y datos generados aleatoriamente para crear claves de sesión[9].
- **Huella digital. –** La huella digital es el rastro que dejamos al navegar por internet. La huella digital es la suma de lo que nosotros publicamos en internet, lo que compartimos y lo que publican otros sobre nosotros[6].
- **Identidad digital. –** Todos tenemos identidad digital. Es el rastro que cada usuario de internet deja en la red como resultado de su interrelación con otros usuarios o con la generación de contenidos[3].
- **IP. –** Una dirección IP es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo

(computadora, tableta, portátil, smartphone) que utilice el protocolo IP o (internet Protocol), que corresponde al nivel de red del modelo TCP/IP[6].

- **Llave criptográfica. –** La llave Criptográfica asocia la identidad de una persona o de un equipo informático a un documento[10].
- **Malware. –** Malware es la abreviatura de Malicious software y este término engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento[6].
- **Man-in-the-middle(MITM)**.- Un ataque Man in the Middle (en adelante MitM) o ataque de intermediario es el método por el cual un hacker interviene en el tráfico de datos de dos partes vinculadas entre sí en una comunicación haciéndose pasar por cualquiera de ellas, haciéndoles creer que se están comunicando entre ellos cuando en realidad es el intermediario quien recibe la comunicación[1].
- **Nodos o mixes. –** Conjunto de nodos interconectados. Un nodo es el punto en el que una curva se interseca consigo mismo. Lo que un nodo es concretamente, depende del tipo de redes a que nos refiramos[6].
- **Online. –** Online es una palabra inglesa que significa "en línea". El concepto se utiliza en el ámbito de la informática para nombrar a algo que está conectado o a alguien que está haciendo uso de una red (generalmente, internet)[1].
- **Página web. –** Una página web, o página electrónica, página digital, o ciberpágina es un documento o información electrónica capaz de contener texto, sonido, vídeo, programas, enlaces, imágenes y muchas otras cosas, adaptada para la llamada World Wide Web (WWW) y que puede ser accedida mediante un navegador web[1].
- **Perfiles de usuario**. – En informática se entiende por perfil de usuario, el conjunto de características o preferencias que la persona tiene sobre sus búsquedas de Internet o en los sitios Web que frecuenta[6].
- **Pharming. –** Un perfil es el conjunto de información que contiene su configuración, preferencias, mensajes de correo, contraseñas, libretas de direcciones y certificados[1].
- **Phishing. –** El phishing es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario,

contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima[1].

- **Plataformas colaborativas. –** Una plataforma de trabajo colaborativo es un espacio virtual de trabajo, o sea, una herramienta informática (con frecuencia un sitio digital en internet), que centraliza todas las funcionalidades ligadas a la conducción de un proyecto[1].
- **Políticas de seguridad. –** La política de seguridad es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información. Contiene la definición de la seguridad de la información desde el punto de vista de cierta entidad[6].
- **Privacidad. –** La protección de datos, también llamada privacidad de información es el aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartidos con terceros[6].
- **Pseudónimo. –** Es un nombre utilizado, normalmente por un autor un artista que reemplaza al nombre auténtico[11].
- **Redes. –** Se trata del conjunto de equipos (computadoras, periféricos, entre otros) que están interconectados y que comparten diversos recursos[12].
- **Reputación online. –** La reputación online es la imagen de una empresa, persona o institución en internet. Más allá de la imagen que proyecta la propia marca, la reputación online está también compuesta por las noticias, comentarios y opiniones expresadas por terceros en redes sociales, foros, blogs y medios online[1].
- **Router. –** Un router es un dispositivo de hardware que permite la interconexión de ordenadores en red[6].
- **Selfies. –** Selfie es un término inglés que se emplea como sinónimo de autofoto o autorretrato[11].
- **Servicios web. –** Un servicio web (en inglés, web service o web services) es una tecnología que utiliza un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones[10].
- **Sistemas biométricos. –** Entenderemos por sistema biométrico a un sistema automatizado que realiza labores de biometría. Es decir, un sistema que fundamenta

sus decisiones de reconocimiento mediante una característica personal que puede ser reconocida o verificada de manera automatizada[10].

- **SSL Striping. -** Eliminar el cifrado ofrecido por HTTPS, llamado SSL Strip, es una seria amenaza cibernética para muchas corporaciones, ya que sus empleados están constantemente en movimiento y requieren acceso a Internet[9].
- **Software. –** Se conoce como software al soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas[2].
- **Suplantación de identidad. –** Se entiende por suplantación de identidad aquella acción por la que una persona se hace pasar por otra para llevar a cabo actividades de carácter ilegal, como pueden ser pedir un crédito o préstamo hipotecario, contratar nuevas líneas telefónicas o realizar ataques contra terceras personas[1].
- **Token. –** Un token de seguridad (también token de autenticación o token criptográfico) es un aparato electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación[10].
- **Viral. –** Viral es un adjetivo que se emplea para nombrar a lo que está vinculado a los virus. Este concepto (virus) se emplea en la biología para nombrar a un tipo de organismo y en la informática con referencia a un software dañino[3].
- **Vulnerabilidad. –** Hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones[12].
- **Web caching. –** Almacena documentos web (es decir, páginas, imágenes, etcétera) para reducir el ancho de banda consumido[6].
- **Wifi. -** permite conectar a internet equipos electrónicos, como computadoras, tablets, smartphones o celulares, entre otros[6].

INTRODUCCIÓN

Presentación del Tema de Investigación

La presente investigación se refiere al tema de la identidad digital que se puede definir en cómo el usuario deja un rastro por la red o aquellos comentarios, fotos, búsquedas, información personal que se sube a internet y que van formando parte de esta. La característica principal de la identidad digital es cómo los usuarios interactúan entre sí, de manera que muchas personas aportan a la identidad digital del usuario sin la aprobación de este.

Para realizar el análisis es necesario mencionar sus causas, una de ellas es la inseguridad. Se entiende por inseguridad al riesgo que corre el usuario con toda la información personal que se coloca en internet debido a que puede ser usada por terceras personas de manera mal intencionada. Es decir, los usuarios que han sido víctimas de suplantación de identidad o robo de información, así como los fallos de equipamiento e infraestructura que se pueden producir por cortes de energía, caídas de vínculos de internet, entre otros.

El usuario cuando usa distintas plataformas y recursos virtuales hace que quede expuesta su identidad[13]. La manera en que se comunica, consulta y se relaciona con otros influye en gran medida debido a que internet va ganando popularidad y es cada vez más común usarse.

El alcance del presente proyecto es evaluar la identidad digital de los usuarios en los servicios web para mejorar la forma en que los usuarios gestionan la identidad y así poder realizar el respectivo análisis para proteger la información personal del usuario para obtener datos mediante la utilización de OWASP que es una guía de autoevaluación de seguridad de aplicaciones web, con el interés de conocer la pérdida de autenticación al momento en que el usuario ingresa en los servicios web de la PUCESE.

Planteamiento del Problema

El entorno en el que se desenvuelven las personas es cada día más digital, adquiriendo información de diferentes fuentes incluyendo sus propios datos, de esta manera no se trata solo de estar conectado o no en la red, teniendo en las redes sociales los perfiles abiertos. Las diferentes actividades que se hacen en internet generan una huella que permiten identificar al usuario.

Otro problema que se evidencia en la seguridad de la identidad se refiere a las técnicas de programación que se usa en el sitio web, debido a que no son las más adecuadas para asegurar la información en el proceso de autenticación, ataques de vulnerabilidad en la seguridad de la información, cookies instalados en software piratas para registrar la navegación de un usuario incluyendo credenciales de acceso. Estar expuestos en la red ya sea de manera consciente al momento de subir información o inconsciente por la información que suben los demás, se ha vuelto un problema al momento de proteger la intimidad del usuario. Un ejemplo de esto es la cantidad de correos electrónicos que es posible crear bajo un seudónimo cualquiera, sin embargo, es importante recordar que todo se guarda y registra en internet, dejando un rastro almacenado como datos en los servidores.

Otro riesgo es la suplantación de identidad, es decir, que otra persona se haga pasar por el usuario. En un principio puede no parecer importante, pero esto perjudica la reputación del usuario por el robo de información que podría generar por culpa de usuarios malintencionados o hackers.

La falta de control de los usuarios en el internet ocasiona que se vea amenazada la seguridad de la información personal (nombre, dirección, teléfono, entre otros), intereses personales, comentarios, amigos y rutas de lugares que frecuenta. Este problema es más visible en los servicios web al momento de autenticarse el usuario. Por ejemplo, cuando dos personas se comunican entre sí, una persona malintencionada (atacante) interviene dicha comunicación, haciendo creer que se habla con la otra persona cuando en realidad es con el atacante.

Justificación

En la actualidad, el riesgo que corren los sistemas informáticos ha ido en aumento por la creciente complejidad en las tecnologías de la información. También está el hecho de que cualquier computadora conectada a internet está en peligro a diferentes amenazas. Todo esto pudiéndose evitar anticipándose a los riesgos, detectando las posibles vulnerabilidades que son aprovechadas por distintos atacantes.

La importancia que tiene proteger la información de los usuarios es que se puede disminuir la probabilidad del éxito por parte de los atacantes para vulnerar la seguridad de dichos datos. Para ello, se puede utilizar distintas técnicas o herramientas para la detección de las vulnerabilidades, analizando el impacto que ocasionan y la mejor forma de mitigarlos. La falta de los controles adecuados al momento de autenticarse en un servicio web en el que solicitan al usuario información personal es una posible vulnerabilidad que puede ser utilizada para obtener información.

El beneficio que traerá a los usuarios que utilizan los servicios web de la página de la PUCESE es debido a que muestra las vulnerabilidades de los mismos y, por lo tanto, reduce amenazas como la suplantación de identidad, así como asegurar la información de los usuarios al disminuir la pérdida de información.

Objetivos

Objetivo General

- Evaluar las vulnerabilidades de los servicios web que utiliza la gestión de identidad digital de los usuarios de la Pontificia Universidad Católica del Ecuador en la ciudad de Esmeraldas, aplicando la guía de seguridad para aplicaciones web OWASP y herramientas informáticas.

Objetivos Específicos

- Identificar los lineamientos de un modelo de identidad digital basado en el Instituto Nacional de Estándar y Tecnologías (NIST) SP – 800-63.
- Seleccionar una herramienta informática que aplique la metodología de prueba de penetración para detectar la pérdida de autenticación en aplicaciones web.
- Analizar las vulnerabilidades de los principales servicios web utilizados por los usuarios externos de la Pontificia Universidad Católica del Ecuador de Esmeraldas.

CAPÍTULO 1: MARCO TEÓRICO

1.1. Antecedentes

La identidad permite poder diferenciarse de los demás y esto también es verdad en el mundo digital. Cobra importancia en este ambiente algunas características de la comunicación, en exclusiva las relativas a: la inmediatez, visibilidad, credibilidad, influencia y permanencia de la información [1]. Es considerable la identidad digital para que el usuario pueda comunicarse y sea usado en entornos colaborativos en internet.

Autenticación es el verificar la identidad de un usuario, entidad o dispositivo que desee utilizar la información personal, recursos o aplicaciones, la validación de esta entidad establece una relación de confianza para futuras interacciones con la base de datos. Hace posible el vincular el acceso y las acciones a identidades especificas permitiendo la rendición de cuentas, después de la autenticación se puede permitir o limitar los niveles de acceso y acción permitidos a esta entidad gracias a los procesos de autorización [14].

Tener presencia en internet por medio de una página o portal web es una necesidad para la mayoría de las empresas. Esto permite ofrecer servicios de manera global como una comunicación más estrecha con el cliente, ahorro de recursos, constante publicidad, posibilidad de venta online, entre otros [15].

Para el usuario la huella digital hace mucho más que identificar como individuo en la Red. A través de la identidad digital, con la huella que se va dejando con lo que se realiza en internet se puede llegar a comprender mucho más que en la vida real porque cada labor que se hace en la red deja huella. La identidad digital se va comprobando con todas las actividades que va realizando el usuario [1].

La memoria tan duradera que tiene internet es la causa principal de preocupación cuando se habla de reputación online y de redes sociales. Sin embargo, existen otros elementos que pueden engañar a los usuarios como los spambots que hacen a los usuarios de Twitter clicar enlaces de cuentas hackeadas, pudiendo afectar la imagen digital [11].

La mayoría de las empresas públicas y privadas emplean sitios web y aplicativos móviles como instrumentos esenciales para informar sus labores o para automatizar algunos de sus procesos administrativos y operativos; en vista de que los percances de seguridad en este caso involucrarían la confidencialidad, integridad o disponibilidad de todos los datos asociados al aplicativo web, así como también a los usuarios de este[16].

Una vulnerabilidad se da en el punto o centro de ataque a la seguridad informática, sin embargo, esto causa daño en sí, debido a que es inevitable que exista una amenaza. A partir de la presencia de vulnerabilidades surgen las amenazas, es decir que solo es posible una amenaza si se encuentra una vulnerabilidad y es utilizada, aún si en un sistema informático se pueda comprometer la seguridad o no[7].

El riesgo para los sistemas informáticos ha aumentado debido a un crecimiento en la complejidad en las tecnologías de la información. Cualquier computadora conectada a internet está expuesta a diversas amenazas. Una consecuencia es el aumento en el número de ataques informáticos [15].

En dos tipos las amenazas se pueden distribuir: Intencionales al momento de pretender realizar un daño, por ejemplo, el robo de información, o no intencionales, en el cual existen acciones u omisiones de acciones que aun si no busca estallar una vulnerabilidad, colocando en peligro los activos de información y pueden realizar un daño, por ejemplo, las amenazas relacionadas con fenómenos naturales[7].

La forma de intercambiar información entre diferentes usuarios se vuelve de especifico interés para las personas que quieren información valiosa siendo por esto el blanco de ataques

por parte de todos aquellos que quieren obtener información útil y valiosa a sus propios intereses o de terceros. Aquí es en donde cobra exclusiva importancia implementar todo tipo de medidas y acciones pendientes a evitar estos ataques[7].

Son muchos los países del mundo que regulan la protección de datos personales para poder proteger los derechos de los ciudadanos, y fomentar el desarrollo de empresas de servicios, cuyo objeto de negocios es la información. Así mismo, la protección de datos personales es fundamental para tener un enfoque transnacional en donde el lenguaje jurídico debe estar a la par del desarrollo tecnológico para de esta manera establecer políticas coherentes de gobierno electrónico[17].

La empresa israelí de seguridad informática vpnMentor corroboró a la agencia de noticias internacional EFE que se ha producido una filtración con información confidencial que contiene datos personales y financieros de millones de ciudadanos de Ecuador [1]. Los informáticos de vpnMentor Noam Rotem y Ran Lokar han logrado descubrir la presencia de una base de datos que abarca detalles privados de millones de personas de Ecuador. En la filtración se incluiría gran cantidad de informaciones sensibles sobre la situación financiera, los salarios percibidos, los puestos de trabajo e incluso las relaciones familiares de muchos ciudadanos, exponiendo a las víctimas a ciberataques, espionaje o robos de dinero por parte de piratas informáticos. De acuerdo con los expertos israelíes, han quedado expuestas decenas de millones de datos de ciudadanos ecuatorianos que podrían ser utilizados para “el robo de dinero y para el robo de identidad”. El caché de información fue encontrado en un servidor no seguro de Amazon en Miami, Estados Unidos. Los 18 gigabytes de datos filtrados son administrados por la empresa ecuatoriana Novaestrat [2].

Los usuarios con la facilidad del intercambio de información usando distintas formas entre las cuales se encuentran las diferentes redes sociales, los correos electrónicos, pagos de manera online, juegos, entre otros. Las distintas formas en que interactúan las personas y las empresas han cambiado en gran medida con el aumento del internet y con diversas dinámicas en la sociedad actual. Es este intercambio que es blanco de ataque por el interés de personas que desean conseguir información importante y preciada para sus propios intereses o de

terceros. El implementar todo tipo de medidas y acciones para eludir estos ataques cobra particular relevancia, surgiendo lo que se denomina Seguridad Informática[7]. El aumento de la interacción entre varios usuarios ha traído la atención de distintos individuos que buscan aprovecharse de la falta de medidas de seguridad e ingenuidad de los usuarios que piensan que la información que intercambian no será víctima de algún ataque o robo.

Las diferentes maneras en que se entiende la seguridad informática dependen del punto de vista que tenga el usuario, pero de manera general ayuda a preservar la confidencialidad, integridad y disponibilidad de la información en la red. La información es un conjunto organizado de datos, que dependiendo el ámbito en que se utilice intercambia su enfoque y su estado de conocimiento. Por ejemplo, si la información se encuentra en el punto de vista de la ingeniería se entiende como un estudio de las características y estadísticas del lenguaje que permite su análisis desde un enfoque matemático, científico y técnico. En cambio, si es desde el punto de vista de una empresa viene siendo el conjunto de datos propios que se gestionan y mensajes que se intercambian personas o máquinas[7].

La seguridad es importante porque la información se ve afectada de diferentes maneras. Por este motivo seguridad de la información es una disciplina, con un objetivo que es mantener el conocimiento y datos libres de eventos indeseables como el robo, espionaje, amenazas y otros peligros. Incluye todas las acciones tomadas con anticipación, para evitar eventos no deseados[7]. El tener la tranquilidad de que dicha información este protegida o al menos tenga un nivel de seguridad que les dificulte a los atacantes obtener información ajena es importante para reducir el número de ataques que tienen los usuarios.

De esta manera garantizar la integridad, confidencialidad y disponibilidad de la información son los pilares fundamentales para asegurar la información. En una aplicación web serían aplicados de la siguiente forma: la confidencialidad que es una propiedad que asegura que solo los que están autorizados tendrán acceso a la información, la integridad que asegura la no alteración de la información, la autenticación que hace referencia a la identificación siendo el nexo de unión entre la información y su emisor, disponibilidad de la información en cualquier momento solo a usuarios autorizados, evitando la divulgación [6].

1.2. Bases Teórico – Científicas

1.2.1. Identidad Digital

El usuario cuando usa distintas plataformas y recursos virtuales hace que quede expuesta su identidad [13]. La manera en que se comunica, consulta y se relaciona con otros influye en gran medida debido a que internet va ganando popularidad y es cada vez más común usarse.

Por esto el conjunto de información expuesta en internet como datos, imágenes, registros, noticias, comentarios, conforma una descripción de la identidad del usuario en el plano digital[1]. Al momento en el que se registra en el correo electrónico o una red social usualmente pide datos, dirección, fecha de nacimiento, contraseñas que forma parte de la identidad en internet.

La identidad digital del usuario está compuesta de categorías de información/datos: Los elementos de autenticación como el nombre y apellido del usuario, contraseña, dirección de correo electrónico, pseudónimo, IP, dirección, entre otros. Los datos administrativos, profesionales, personales, bancarios, sociales, entre otros. Identificadores como el logo, imagen, fotografía, avatar, entre otros. Trazas digitales que contribuyen a sistemas de gestión de contenidos públicos como Wikipedia, Twitter, YouTube, entre otros [11].

Según M. Pérez [18] las características sobre la identidad digital son: social debido a que se construye navegando por las redes sociales a partir del reconocimiento de los demás sin ni siquiera llegar a comprobar si esa identidad es real o no, subjetiva dependiendo de cómo los demás perciban a esa persona a través de las informaciones que genera, valiosa cuando a veces personas y empresas navegan por las redes sociales para investigar la identidad digital de un candidato o una candidata y tomar decisiones sobre él o ella, indirecta al no permitir conocer a la persona directamente sino las referencias publicadas de esa persona, compuesta debido a que la identidad digital se construye por las aportaciones de la misma persona y también por otras personas sin la participación o consentimiento de esa persona real, cuando

la información de la identidad digital puede producir efectos positivos y negativos en el mundo real y dinámica porque la identidad digital no es una foto instantánea, sino que está en constante cambio o modificación.

Figura 1. Identidad personal digital [18]

1.2.2. Modelo de Identidad Digital basado en NIST SP - 800-63

La identidad digital es la representación única de un sujeto involucrado en una transacción en línea. El proceso que utiliza para confirmar la asociación de un sujeto con su identidad del mundo real se llama prueba de identidad. En estas pautas, la parte a ser probada se llama solicitante. Cuando el solicitante completa con éxito el proceso de revisión, se le conoce como suscriptor[3].

Ciertos procesos de inscripción, prueba de identidad y emisión realizada por los proveedores de servicios de credenciales (CSP) a veces se delegan a una entidad conocida como autoridad de registro (RA) o administrador de identidad (IM). Los CSP es una entidad confiable que emite tokens de seguridad o credenciales electrónicas a los suscriptores, formando parte de un sistema de autenticación identificado generalmente como una entidad separada en un sistema de autenticación federado. Un relying party (RP o parte confiable) es un servicio,

sitio o entidad que depende de un proveedor de identidad externo para identificar y autenticar a un usuario que solicita acceso a un recurso digital [3].

Asimismo, la parte a autenticar se llama reclamante y la parte que verifica esa identidad se llama verificador. Cuando un reclamante demuestra con éxito la posesión y el control de uno o más autenticadores a un verificador a través de un protocolo de autenticación, el verificador puede verificar que el reclamante es un suscriptor válido. El verificador pasa al RP una afirmación sobre el suscriptor, que puede ser seudónimo o no seudónimo. Esa afirmación incluye un identificador y puede incluir información de identidad sobre el suscriptor, como el nombre u otros atributos que se recopilaron en el proceso de inscripción (sujeto a las políticas del CSP, las necesidades del RP y el consentimiento para la divulgación de los atributos dados por el tema). Donde el verificador es también el RP, la afirmación puede ser implícita. El RP puede usar la información autenticada proporcionada por el verificador para tomar decisiones de autorización[3].

La autenticación establece la confianza de que el reclamante tiene posesión de uno o más autenticadores vinculados a la credencial y en los valores de atributo del suscriptor (por ejemplo, si el suscriptor es ciudadano de los EE. UU., es estudiante de una universidad en particular, o se le asigna un número o código particular por una agencia u organización). La autenticación no determina las autorizaciones o privilegios de acceso del reclamante; esta es una decisión separada. Los RP pueden usar la identidad y los atributos autenticados de un suscriptor con otros factores para tomar decisiones de autorización. [3].

En la autenticación digital, el reclamante posee y controla uno o más autenticadores que se han registrado con el CSP y se utilizan para probar la identidad del reclamante. El (los) autenticador (es) contiene secretos que el reclamante puede usar para demostrar que él o ella es un suscriptor válido, el reclamante se autentica en un sistema o aplicación a través de una red al demostrar que tiene la posesión y el control de uno o más autenticadores[3].

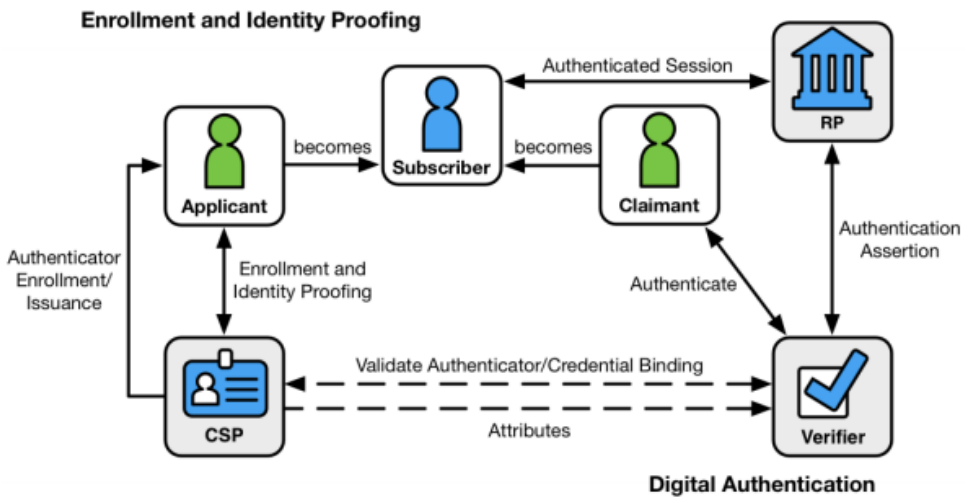

Figura 2. Modelo de identidad digital [3]

En la Figura 2, el lado izquierdo del diagrama muestra la inscripción, la emisión de credenciales, las actividades de gestión del ciclo de vida y varios estados de un proceso de prueba de identidad y autenticación. La secuencia habitual de interacciones es la siguiente[3]: Un solicitante aplica a un CSP a través de un proceso de inscripción, la identidad del CSP prueba a el solicitante que tras una prueba exitosa el solicitante se convierte en suscriptor, el autenticador y una credencial correspondiente se establecen entre el CSP y el suscriptor, el CSP mantiene la credencial, su estado y los datos de inscripción recopilados durante la vigencia de la credencial (como mínimo) y el suscriptor mantiene su autenticador.

Un suscriptor se denomina reclamante cuando necesita autenticarse en un verificador. Las interacciones son las siguientes[3]: El reclamante demuestra la posesión y el control de los autenticadores al verificador a través de un protocolo de autenticación, el verificador interactúa con el CSP para validar la credencial que vincula la identidad del suscriptor a su autenticador y de manera opcional obtener los atributos del reclamante, el CSP o verificador proporciona una afirmación sobre el suscriptor del RP que puede usar la información en la afirmación para tomar una decisión de autorización, se establece una sesión autenticada entre el suscriptor y el RP.

El verificador no necesita comunicarse en tiempo real con el CSP para completar la actividad de autenticación (por ejemplo, algunos usos de certificados digitales). Por lo tanto, la línea discontinua entre el verificador y el CSP representa un enlace lógico entre las dos entidades. En algunas implementaciones, las funciones de verificador, RP y CSP pueden distribuirse y separarse como se muestra en la figura anterior. Sin embargo, si estas funciones residen en la misma plataforma, las interacciones entre los componentes son mensajes locales entre aplicaciones que se ejecutan en el mismo sistema en lugar de protocolos sobre redes compartidas y no confiables[3].

Como se señaló anteriormente, un CSP mantiene información de estado sobre las credenciales que emite. Los CSP generalmente asignarán una vida útil limitada al emitir credenciales para limitar el período de mantenimiento. Cuando el estado cambia, o cuando las credenciales están a punto de caducar, las credenciales pueden renovarse o volver a emitirse; o, la credencial puede ser revocada y destruida. Por lo general, el suscriptor se autentica en el CSP utilizando su autenticador y credencial existentes y no vencidos para solicitar la emisión de un nuevo autenticador y credencial. Si el suscriptor no solicita la autentificación y la reemisión de credenciales antes de su vencimiento o revocación, es posible que deba repetir el proceso de inscripción para obtener un nuevo autenticador y credencial. Alternativamente, el CSP puede optar por aceptar una solicitud durante un período de gracia después del vencimiento[3].

1.2.2.1. Inscripción y prueba de identidad

Un individuo, conocido como solicitante en esta etapa, opta por una prueba de identidad al CSP. Si el solicitante pasa la prueba con éxito, el individuo se denomina suscriptor de ese CSP. El CSP establece un mecanismo para identificar de manera única a cada suscriptor, registrar las credenciales del suscriptor y rastrear los autenticadores emitidos a ese suscriptor. Al suscriptor se le pueden dar autenticadores en el momento de la inscripción, el CSP puede vincular a los autenticadores que el suscriptor tiene. Los suscriptores tienen el deber de mantener el control de sus autenticadores y cumplir con las políticas de CSP para mantener

autenticadores activos. El CSP mantiene registros de inscripción para cada suscriptor para permitir la recuperación de autenticadores, por ejemplo, cuando se pierden o son robados[3].

1.2.2.2. Autenticación y gestión del ciclo de vida

Sobre los tipos de autenticadores se indica otros métodos de autenticación además de la autenticación tradicional, distribuidos según su clase. En esta ocasión hace la división según el modo: Basados en algo conocido como son las contraseñas, los sistemas de autenticación más utilizados son aquellos basados en conocimiento, por ejemplo, aquellos que usan un ID de usuario y una contraseña, o una llave criptográfica. Basados en algo poseído como son usb, tarjeta de identidad, token que son sistemas de autenticación basados únicamente en algo que el usuario posee, estos métodos se fundamentan en que el usuario tiene en su dominio un token, los cuales podemos distribuir en tokens de memoria y tokens inteligentes. Basados en características físicas como huellas, voz, ojos de manera que para lograr la autenticación estos sistemas se utilizan las características o atributos, fisiológicos y de comportamiento, propios de cada individuo que lo hacen único. Estos sistemas son notables también como sistemas biométricos[10].

La fortaleza de los sistemas de autenticación está determinada en gran medida por el número de factores incorporados por el sistema: cuantos más factores se empleen, más robusto será el sistema de autenticación. Aunque se considera el uso de dos factores como adecuado para concluir con los requisitos de seguridad más alto[3].

Los secretos contenidos en los autenticadores se basan en pares de claves públicas (claves asimétricas) o secretos compartidos (claves simétricas). Una clave pública y una clave privada relacionada comprenden un par de claves públicas. La clave privada se almacena en el autenticador y el reclamante la utiliza para demostrar la posesión y el control de autenticador. Un verificador, que conoce la clave pública del reclamante a través de alguna credencial (generalmente un certificado de clave pública), puede usar un protocolo de

autenticación para verificar la identidad del reclamante al demostrar que el reclamante posee y controla el autenticador de clave privada asociado[3].

Al almacenar los secretos compartidos en los autenticadores, estos pueden ser claves simétricas o secretos memorizados (por ejemplo, contraseñas y PIN), a diferencia de las claves asimétricas descritas anteriormente, que los suscriptores no necesitan compartir con el verificador. Si bien ambas claves y contraseñas se pueden usar en protocolos similares, una diferencia importante entre los dos es cómo se relacionan con el suscriptor. Si bien las claves simétricas generalmente se almacenan en hardware o software que controla el suscriptor, las contraseñas están destinadas a ser memorizadas por el suscriptor. Dado que la mayoría de los usuarios eligen contraseñas cortas para facilitar la memorización y la facilidad de entrada, las contraseñas suelen tener menos caracteres que las claves criptográficas. Además, mientras que los sistemas eligen claves al azar, los usuarios que intentan elegir contraseñas memorables a menudo seleccionan de un subconjunto muy pequeño de las posibles contraseñas de una longitud determinada, y muchos elegirán valores muy similares. Como tal, mientras que las claves criptográficas suelen ser lo suficientemente largas como para hacer insostenibles los ataques de adivinanzas basados en la red, las contraseñas elegidas por el usuario pueden ser vulnerables, especialmente si no hay controles establecidos[3].

Algunos de los factores de autenticación clásicos no se aplican directamente a la autenticación digital. Por ejemplo, una licencia de conducir física es algo que tiene y puede ser útil cuando se autentica a un humano (por ejemplo, un guardia de seguridad), pero no es en sí mismo un autenticador para la autenticación digital. Los factores de autenticación clasificados como algo que se conoce tampoco son necesariamente secretos. La autenticación basada en el conocimiento, donde se solicita al reclamante que responda preguntas que supuestamente solo conoce el reclamante, tampoco constituye un secreto aceptable para la autenticación digital. Un biométrico tampoco constituye un secreto. En consecuencia, estas pautas solo permiten el uso de datos biométricos para la autenticación cuando están fuertemente vinculados a un autenticador físico[3].

Un sistema de autenticación digital puede incorporar múltiples factores. Por ejemplo, puede satisfacerse combinando un secreto memorizado (lo que sabe) con un dispositivo (lo que tiene). Ambas se presentan al verificador para autenticar al reclamante. Por otro lado, se considera una pieza de hardware (el autenticador) que contiene una clave criptográfica (el secreto del autenticador) donde el acceso está protegido con una huella digital. Cuando se usa con la biométrica, la clave criptográfica. Se emplea como un factor único de autenticación. Las características biométricas son atributos personales únicos que se pueden usar para comprobar la identidad de un individuo que está físicamente presente en el punto de verificación. Incluyen rasgos faciales, huellas digitales, patrones de iris, huellas de voz y muchas otras características[3].

1.2.2.3. Credenciales

Una credencial vincula un autenticador al suscriptor, a través de un identificador, como parte del proceso de emisión. El CSP almacena y mantiene una credencial, aunque el reclamante puede poseerla. El reclamante posee un autenticador, pero no necesariamente posee la credencial. [3].

El proceso de autenticación comienza cuando el reclamante demuestra al verificador la posesión y el control de un autenticador que está vinculado a la identidad afirmada a través de un protocolo de autenticación. Una vez que se ha demostrado la posesión y el control, el verificador verifica que la credencial sigue siendo válida, generalmente al interactuar con el CSP. La naturaleza exacta de la interacción entre el verificador y el reclamante durante el protocolo de autenticación es extremadamente importante para determinar la seguridad general del sistema. Los protocolos bien diseñados pueden proteger la integridad y la confidencialidad de la comunicación entre el reclamante y el verificador durante y después de la autenticación, y pueden ayudar a limitar el daño que puede hacer un atacante disfrazado de verificador legítimo. Además, los mecanismos ubicados en el verificador pueden mitigar los ataques de adivinanzas en línea contra los secretos de entropía más bajos, como las contraseñas y los PIN, al limitar la velocidad a la que un atacante puede realizar intentos de autenticación o retrasar los intentos incorrectos. En general, se realiza al limitar el número

de intentos fallidos, ya que la premisa de un ataque es que la mayoría de los intentos fallarán. El verificador es un rol funcional, pero con frecuencia se implementa en combinación con el CSP, el RP o ambos. Si el verificador es una entidad separada del CSP, a menudo es deseable asegurarse de que el verificador no aprenda el secreto del autenticador del suscriptor en el proceso de autenticación, o al menos asegurarse de que el verificador no tenga acceso ilimitado a los secretos almacenados por el CSP[3].

1.2.2.4. Amenazas en la gestión de la identidad

Un atacante que puede obtener el control de un autenticador a menudo podrá hacerse pasar por el propietario del autenticador. Las amenazas a los autenticadores se pueden clasificar en función de los ataques a los tipos de factores de autenticación que componen el autenticador[5]:

- Algo que sabes puede ser revelado a un atacante. El atacante podría adivinar un secreto memorizado. Cuando el autenticador es un secreto compartido, el atacante podría obtener acceso al CSP o verificador y obtener el valor secreto o realizar un ataque de diccionario en un hash de ese valor. Un atacante puede observar la entrada de un PIN o código de acceso, encontrar un registro escrito o entrada en el diario de un PIN o código de acceso, o puede instalar un software malicioso (por ejemplo, un registrador de teclado) para capturar el secreto. Además, un atacante puede determinar el secreto a través de ataques fuera de línea en una base de datos de contraseñas mantenida por el verificador.
- Algo que tenga puede ser perdido, dañado, robado del propietario o clonado por un atacante. Por ejemplo, un atacante que obtiene acceso a la computadora del propietario podría copiar un autenticador de software. Un autenticador de hardware puede ser robado, manipulado o duplicado. Los secretos fuera de banda pueden ser interceptados por un atacante y utilizados para autenticar su propia sesión.
- Algo que eres puede ser replicado. Por ejemplo, un atacante puede obtener una copia de la huella digital del suscriptor y construir una réplica.

Asumiendo que el suscriptor no está asociado con un atacante que intenta autenticar falsamente al verificador, las amenazas a los autenticadores utilizados para la autenticación digital se enumeran en la Tabla, junto con algunos ejemplos[5].

Tabla 1. Amenazas de autenticador [5]

Autenticador Amenaza / Ataque	**Descripción**	**Ejemplo**
Fabricación o modificación de aserciones	El atacante genera una afirmación falsa.	El CSP comprometido afirma la identidad de un reclamante que no se ha autenticado adecuadamente
	El atacante modifica una afirmación existente.	Proxy comprometido que cambia AAL de una aserción de autenticación
Robo	Un atacante roba un autenticador físico	Se roba un dispositivo criptográfico de hardware
		Un teléfono celular es robado
Duplicación	El autenticador del suscriptor se ha copiado con o sin su conocimiento.	Se revelan las contraseñas escritas en papel.
		Las contraseñas almacenadas en un archivo electrónico se copian.
		Software PKI autenticator (clave privada) copiado.
		Autenticación secreta de búsqueda copiada.
		Autenticador biométrico falsificado.
Espionaje	El autenticador secreto se revela al atacante cuando el suscriptor se está autenticando.	Los secretos de la memorización se obtienen mirando la entrada del teclado.
		Los secretos de la memorización o las salidas del autenticador son interceptados por el software de registro de pulsaciones de teclas.
		Se captura un PIN desde un dispositivo de teclado PIN.
		Un atacante obtiene y utiliza una contraseña hash para otra autenticación (ataque pass-thehash).
	El atacante intercepta un autenticador secreto fuera de	Un secreto fuera de banda se transmite a través de WiFi

	banda al comprometer el canal de comunicación.	sin cifrar y el atacante lo recibe.
Agrietamiento fuera de línea	El autenticador se expone utilizando métodos analíticos fuera del mecanismo de autenticación.	Un autenticador de PKI de software está sujeto a un ataque de diccionario para identificar la contraseña correcta para descifrar la clave privada.
Ataque de canal lateral	El autenticador secreto se expone utilizando las características físicas del autenticador.	Una clave se extrae mediante análisis de potencia diferencial en un autenticador criptográfico de hardware.
		Un secreto de autenticador criptográfico se extrae mediante el análisis del tiempo de respuesta del autenticador durante varios intentos.
Phishing o Pharming	La salida del autenticador se captura engañando al suscriptor para que piense que el atacante es un verificador o RP.	El suscriptor revela una contraseña a un sitio web que se hace pasar por el verificador.
		Un suscriptor bancario revela una respuesta secreta a una consulta por correo electrónico de un phisher que pretende representar al banco.
		El suscriptor revela una respuesta secreta en un sitio web falso del verificador alcanzado a través de la falsificación de DNS.
Ingeniería social	El atacante establece un nivel de confianza con un suscriptor para convencerlo de que revele sus respuestas secretas	El suscriptor revela una respuesta secreta a un compañero de oficina que solicita la contraseña en nombre del jefe del suscriptor.
		Un suscriptor revela un secreto memorizado en una consulta telefónica de un atacante disfrazado de administrador del sistema.
		Un atacante recibe la respuesta secreta enviado por mensaje de texto que ha convencido al operador móvil para que redirija el

		teléfono móvil de la víctima al atacante.
Adivinanzas en línea	El atacante se conecta al verificador en línea e intenta adivinar una salida de autenticador válida en el contexto de ese verificador	Los ataques de diccionario en línea se utilizan para adivinar secretos memorizados.
		Las conjeturas en línea se utilizan para adivinar las salidas del autenticador para un dispositivo OTP registrado a un reclamante legítimo.
Compromiso de punto final	El código malicioso en el punto final representa el acceso remoto a un autenticador conectado sin el consentimiento del suscriptor.	Se utiliza un autenticador criptográfico conectado al punto final para autenticar a los atacantes remotos.
	El código malicioso en el punto final hace que la autenticación sea distinta del verificador previsto.	La autenticación se realiza en nombre de un atacante en lugar del suscriptor.
		Una aplicación maliciosa en el punto final lee un secreto fuera de banda enviado por SMS y el atacante usa el secreto para autenticarse.
	El código malicioso en el punto final compromete un autenticador criptográfico de software multifactor.	El código malicioso representa la autenticación o exporta claves de autenticación desde el punto final.
Unión no autorizada	Un atacante puede hacer que un autenticador bajo su control esté vinculado a la cuenta de un suscriptor.	Un atacante intercepta un autenticador o una clave de aprovisionamiento en ruta hacia el suscriptor.

Debido al distinto nivel de gravedad que tienen algunas amenazas a diferencia de otras, se mencionan las que tienen mayor índice de probabilidad que ocurra. Entre estas tenemos la suplantación de identidad es la usurpación de perfiles de usuarios en internet por personas malintencionadas, actuando en nombre de este. Dentro de este riesgo está la forma en cómo se crea o accede a un perfil no autorizado de un usuario o entidad en un medio social y como se lo utiliza como si se tratara de la persona suplantada. Para esto existe distintas técnicas: El estafador o phisher se apodera de la identidad ya sea un correo electrónico o un perfil en redes sociales de una empresa o institución de confianza para que el receptor dé una comunicación electrónica supuestamente oficial haciendo esto por vía email, redes sociales

o un SMS para que crea que es verídico y se pueda facilitar los datos privados como credenciales o cuentas que son de interés para el estafador. Para dar credibilidad a la usurpación se usan imágenes de marca originales o direcciones de sitios web parecidos al oficial. A través de las redes sociales son más frecuentes los casos de phishing.

Con el pharming el atacante modifica los mecanismos de resolución de nombres en donde el usuario accede a diferentes páginas web por medio de un navegador. Esto ocasiona que al momento en que el usuario desee ingresar en un sitio web oficial, automáticamente es enviado en dirección a una página web engañosa que esté suplantando a la original. Los efectos de la suplantación de identidad es la confusión con la identidad original, fraude online, robo de información, extorsión, entre otros.

Así es cómo permite llegar a realizar usos engañosos como el phishing, una modalidad de estafa por correo electrónico planteada para consentir de manera fraudulenta a cuentas bancarias. El phishing y las técnicas para obtener tarjetas de crédito o claves de sistemas informáticos se introducen dentro de las prácticas de ingeniería social, las cuales tienen como finalidad obtener información confidencial haciendo uso del engaño y la manipulación de las personas legítimas [18].

La fuga de información en donde una buena imagen y prestigio de una entidad puede ser afectada por una publicación en internet con información confidencial como los datos personales de trabajadores y clientes, datos bancarios, información estratégica de la organización, entre otros. Esto ocurre por obtener lucro debido a que, al tener la información bancaria de la empresa y los clientes, se chantajea al propietario de los datos a cambio de una recompensa, aunque también es por espionaje industrial o dar desprestigio a la organización. Se distinguen dos posibles orígenes de la fuga de información. La primera puede ocurrir desde el interior de la organización por un accidente de los empleados o por una acción consciente e intencionada. En el primer caso el que se pierda un pendrive o un dispositivo móvil son causas de pérdida de información. En el segundo caso, un empleado que esté descontento o que sea despedido tome represalias contra la empresa difundiendo documentos o datos a los que ha tenido acceso. La segunda puede ocurrir desde el exterior, utilizando diferentes

técnicas para robar información de los equipos y sistemas de la entidad atacada, por ejemplo, al infectar con malware para robar datos, estando una vez instalado en el equipo de la víctima se dedica a reunir información y pasarla al atacante, sin que el usuario se entere. También puede ser por los ataques de la persona ubicada en el medio, en donde el atacante se ubica entre el servidor web de la entidad y el equipo que solicita la conexión a dicho servidor, pudiendo leer, filtrar e incluso modificar información que se está transfiriendo sin dejar ningún rastro.

De acuerdo a la investigación del Instituto Nacional de Ciberseguridad indica que algunos aspectos relevantes sobre la privacidad [1]: conocer y poder configurar detalladamente las opciones de privacidad para proteger los datos personales identificando los efectos y funciones de cada acción, proteger la información personal teniendo en cuenta que cada usuario es el primer filtro y evaluar qué condiciones de privacidad tienen los contactos que tiene cada usuario, mantener una actitud dinámica en defender los datos del usuario informando a los demás sobre el criterio que se tiene al respecto y supervisando lo que se publica.

1.2.2.5. Estrategias de mitigación de amenazas

Estrategias de mitigación de amenazas: Los mecanismos relacionados que ayudan a mitigar las amenazas identificadas anteriormente se resumen en la Tabla[5].

Tabla 2. Mitigar las amenazas del autenticador

Autenticador **Amenaza / Ataque**	**Mitigación de amenazas**
Robo	Utilice autenticadores de múltiples factores que deben activarse a través de un secreto memorizado o biométrico.
	Use una combinación de autenticadores que incluya un secreto memorizado o biométrico.
Duplicación	Utilice autenticadores de los que es difícil extraer y duplicar secretos de autenticación a largo plazo.

Espionaje	Garantice la seguridad del punto final, especialmente con respecto a la ausencia de malware, como los registradores de claves, antes de su uso.
	Evite el uso de redes inalámbricas no confiables como canales secundarios de autenticación fuera de banda no cifrados.
	Autentíquese a través de canales protegidos autenticados (por ejemplo, observe el icono de candado en la ventana del navegador).
	Utilice protocolos de autenticación que sean resistentes a los ataques de repetición, como pasar el hash
	Use puntos finales de autenticación que empleen entrada confiable y capacidades de visualización confiables.
Agrietamiento fuera de línea	Utilice un autenticador con un secreto de autenticador de alta entropía.
	Almacene los secretos de la memorización en forma de hash, incluyendo un hash con clave.
Ataque de canal lateral	Utilice algoritmos de autenticación diseñados para mantener un consumo de energía y un tiempo constantes independientemente de los valores secretos.
Phishing o Pharming	Utilice autenticadores que proporcionen resistencia de suplantación de verificador.
Ingeniería social	Evite el uso de autenticadores que presenten un riesgo de ingeniería social de terceros, como los agentes de servicio al cliente.
Adivinanzas en línea	Utilice autenticadores que generen un alto rendimiento de entropía.
	Use un autenticador que se bloquee después de varios intentos de activación fallidos repetidos
Compromiso de punto final	Utilice autenticadores de hardware que requieran una acción física por parte del suscriptor.
	Mantener claves basadas en software en almacenamiento de acceso restringido
Unión no autorizada	Utilice protocolos resistentes al ataque del “hombre del medio” (man-in-the-middle attack MitM) para el aprovisionamiento de autenticadores y claves asociadas. MitM es un ataque en el que el atacante transmite en secreto y posiblemente altera las comunicaciones entre dos partes que creen que se están comunicando directamente entre sí.

Se pueden aplicar varias estrategias para mitigar las amenazas descritas en la Tabla 1 de Amenazas de autenticador [5]:

- Múltiples factores hacen que los ataques exitosos sean más difíciles de lograr. Si un atacante necesita robar un autentificador criptográfico y adivinar un secreto

memorizado, entonces el trabajo para descubrir ambos factores puede ser demasiado alto.

- Se pueden emplear mecanismos de seguridad física para proteger un autenticador robado de la duplicación. Los mecanismos de seguridad física pueden proporcionar evidencia de manipulación, detección y respuesta.
- Requerir el uso de largos secretos memorizados que no aparecen en los diccionarios comunes puede obligar a los atacantes a probar todos los valores posibles.
- Se pueden emplear controles de seguridad del sistema y de la red para evitar que un atacante obtenga acceso a un sistema o instale software malicioso.
- Se puede realizar una capacitación periódica para garantizar que los suscriptores entiendan cuándo y cómo informar si consideran comprometidas sus credenciales, o reconocer patrones de comportamiento que pueden significar que un atacante intenta comprometer el proceso de autenticación.
- Se pueden emplear técnicas fuera de banda para verificar la prueba de posesión de dispositivos registrados (por ejemplo, teléfonos celulares).

1.2.2.6. Recuperación de autenticador

El punto débil de muchos mecanismos de autenticación es el proceso seguido cuando un suscriptor pierde el control de uno o más autenticadores y necesita reemplazarlos. En muchos casos, las opciones que quedan disponibles para autenticar al suscriptor son limitadas, y las preocupaciones económicas (por ejemplo, el costo de mantener los centros de llamadas) motivan el uso de métodos de autenticación de respaldo económicos y, a menudo, menos seguros. En la medida en que la recuperación del autenticador sea asistida por humanos, también existe el riesgo de ataques de ingeniería social. Para mantener la integridad de los factores de autenticación, es esencial que no sea posible aprovechar una autenticación que involucre un factor para obtener un autenticador de un factor diferente. Por ejemplo, un secreto de la memorización no debe ser utilizado para obtener una nueva lista de búsqueda de secretos [5].

Los ataques de secuestro en la sesión después de un evento de autenticación pueden tener impactos de seguridad similares. Las pautas de administración son esenciales para mantener la integridad de la sesión contra ataques, como XSS. Además, es importante desinfectar toda la información que se mostrará [prevención OWASPXSS] para garantizar que no contenga contenido ejecutable. Estas pautas también recomiendan que los inicios de sesión sean inaccesibles para el código móvil con el fin de proporcionar protección adicional contra la filtración de secretos de sesión. Otra amenaza posterior a la autenticación, la falsificación de solicitudes entre sitios (CSRF), aprovecha la tendencia de los usuarios de tener varias sesiones activas al mismo tiempo. Es importante incrustar y verificar un identificador de sesión en las solicitudes web para evitar la posibilidad de que una URL o solicitud válida se active de forma involuntaria o malintencionada[5].

1.2.2.6.1. Autenticación

1.2.2.6.2. Atributos de los perfiles de usuario

Entre los distintos componentes que permite formar un perfil de usuario se puede encontrar atributos personales que están conformados por datos personales típicos como el nombre, edad, sexo, dirección, entre otros, intereses del usuario o temas preferidos, como el futbol, coches, entre otros, opiniones que tenga un usuario acerca de determinados argumentos, como la música, cine, entre otros, topología de amistades que lo conforman, las identificaciones de los amigos del usuario, identidades, ubicación de sitios que visita el usuario, las rutas normales para ir al trabajo, a casa, entre otros [6].

1.2.2.7. Gestión de Riesgos de identidad digital

En los servicios digitales de hoy en día, la combinación de pruebas, autenticación y requisitos de federación en un solo paquete a veces tiene consecuencias no deseadas y puede poner una carga de implementación innecesaria en la organización implementadora. Es muy posible que una agencia pueda brindar el conjunto más eficaz de servicios de identidad al evaluar el

riesgo y los impactos de las fallas para cada componente individual de la autenticación digital, en lugar de como una LOA única y global. Se detalla los requisitos para ayudar a las agencias a evitar: Errores de prueba de identidad (es decir, un solicitante falso que reclama una identidad que no es legítimamente suya); Errores de autenticación (es decir, un reclamante falso que utiliza una credencial que no es legítimamente suya); y Errores de federación (es decir, una aserción de identidad está comprometida)[3].

Desde la perspectiva de una falla de prueba de identidad, hay dos dimensiones de falla potencial[3]: El impacto de proporcionar un servicio al sujeto equivocado (por ejemplo, un atacante prueba con éxito como otra persona); El impacto de la prueba de identidad excesiva (es decir, recopilar y almacenar de forma segura más información sobre una persona de la que se requiere para proporcionar con éxito el servicio digital).

Las evaluaciones de riesgos determinan en qué medida los riesgos deben ser mitigados por los procesos de prueba de identidad, autenticación y federación. Estas determinaciones impulsan las elecciones relevantes de las tecnologías aplicables y las estrategias de mitigación, en lugar del deseo de cualquier tecnología determinada que impulse las determinaciones de riesgo [3].

1.2.2.8. Huella Digital

Cuando se habla de la huella digital en internet se refiere al rastro que se deja al navegar e interactuar con la red. Alternativamente al avance de las tecnologías de la información y la comunicación, cualquier persona realiza cualquier actividad por medio del internet, dejado un rastro en aquellos lugares por los que se va visitando, es lo que se conoce como huella digital [3]. Muchas veces se contribuye sin ser consciente de ello a un retrato en línea que puede tener acceso una gran cantidad de personas, no se trata de no dejar una huella digital, sino que tipo de información vas a compartir.

La huella digital de un usuario puede crearse de manera activa o pasiva. La diferencia entre ambas se basa en el rastro se deja de forma consciente o inconsciente. La creación activa de una huella digital se basa con tareas que intencionalmente realiza el usuario. Con la aparición de la Web 2.0, las aplicaciones sociales en la red donde los usuarios originan un perfil con opiniones, fotos y datos personales como el número de teléfono, situación civil, trabajo, entre otros, se desarrolló significativamente. La huella digital creada de manera activa es compromiso del mismo usuario y consigue instruirse a dominarla para un beneficio propio. La creación pasiva de una huella digital se basa en componentes prácticamente imperceptibles para el usuario como el web caching o las cookies. Debido a que el usuario no conoce su existencia al ser estos elementos trasparentes, es peligroso desde el punto de vista de la privacidad [6].

Pese a que se puede borrar información personal que se ha compartido en internet, esta permanece en la red por estar subida unos segundos, haciendo difícil que pueda ser eliminada la huella digital, además no se garantiza que la información que se desea eliminar desaparezca por completo [3]. Información que un usuario decide compartir en línea puede volverse viral en cuestión de segundos, haciendo que sea complicado eliminarla cuando el mismo usuario lo desee.

Empleadas las cookies como mecanismo de comunicación que se encuentra incesante en sitios web donde se las originan y los browsers de los visitantes. Identificar al usuario al almacenar el historial de actividad de un sitio web específico, ofreciendo contenido más apropiado según sus hábitos La persistencia de las cookies se interpreta como un sencillo trozo de texto, acumulándose en el disco duro del ordenador del usuario permitiendo al servidor web identificar al usuario cada vez que se conecta, conociendo y guardando las preferencias de usuario y cualquier actividad que pueda [6].

La forma más fácil de identificar a un usuario es por medio del sistema de identificación por cookies que retorna a un sitio web debido a que el habitual uso de direcciones IP dinámicas desecha este método para dicho cometido, y el pedirle al usuario que ingrese un login/password puede ser una contrariedad para la persona.

1.2.2.9. Técnicas para protección de información

Los mecanismos que se usan para verificar el contenido de la huella digital cambian delicadamente en manejo de la técnica de creación donde se aplican. Se distinguen las medidas planteadas para manejar la creación activa de la huella digital que entrega con la utilización de aplicaciones sociales y las medidas que eluden la creación pasiva de la huella que se basa especialmente en la identificación del browser del usuario y el estudio de su conducta. Los mecanismos para resguardar la privacidad de los usuarios, que de manera activa difunden recursos y datos personales en internet, se basan en tres modelos básicos: el sentido común, las medidas de control de acceso y criptografía[6]:

El sentido común se basa en no crear contenido dispuesto a ser explotado por terceros. Prosiguiendo con la idea, Consumer Reports muestra recomendaciones básicas para librar a los usuarios de problemas posteriores de privacidad y seguridad. Estas recomendaciones se enlistan a continuación: el usar passwords sencillos o débiles debe evitarse, los perfiles de usuario no deben contener fechas de nacimiento completas, deben usarse los mecanismos de privacidad proporcionados por las aplicaciones basadas en la Web 2.0 como, por ejemplo, redes sociales.

Es fundamental las medidas de control de acceso en el desarrollo de la creación activa de la huella digital. De forma más precisa, son usadas comúnmente en aplicaciones Web 2.0 como las redes sociales. Se recalca que, al ser medidas trabajadas prudentemente por el usuario, no se permiten usarse en el proceso de creación pasiva de la huella digital. Las medidas de control de acceso se basan en tres tecnologías diferentes: Configuración individual de privacidad, este mecanismo es el más sencillo de implementar y sucede que es usado por defecto en las redes sociales estándar y aplicaciones vinculadas. Se fundamenta en elegir entre diversas alternativas de privacidad facilitadas por la propia aplicación y la configuración idónea para cada persona.

La criptografía cuando se está utilizando puede ser tanto simétrica como asimétrica. Esta medida de privacidad puede aplicarse a contenidos que son autosuficientes de la aplicación

web, en consecuencia, se facilita más seguridad a comparación del caso anterior. Asimismo, en el sistema la dificultad está fundamentada en seleccionar acceso a cierto recurso, en consecuencia, básicamente no es notable la dificultad en la configuración. Como grave problema de este tipo de medidas logran señalar que no todas las aplicaciones Web 2.0 las soportan y, en consecuencia, estrechamente limitada esta su instauración.

El acceso a los requerimientos se logra mediante el análisis de la calidad de la relación entre el usuario que publica el recurso y la entidad que pretende conseguir dicho elemento. Dependiendo de la calidad de dicha relación, acceder podría denegarse o aceptarse. Esta solución se fundamenta en el uso de un sistema de análisis y contabilización de confianzas. Su meta es automatizar el proceso de configuración de la privacidad.

Las medidas fundamentadas en la alteración se concentrar en cambiar los datos personales a fin de incrementar su ambigüedad y, en consecuencia, la privacidad de los usuarios que los han producido. Este proceso se conoce como generalización.

La generación pasiva de la huella digital de un usuario depende especialmente del talento de reconocer correctamente las diferentes interacciones mediante la utilización de cookies u otros métodos. En consecuencia, las medidas para esquivar o controlar este proceso se fundamentan en imposibilitar la identificación adecuada por parte de la entidad que ejecuta la búsqueda del usuario.

Los sistemas de identificación manifiestan que medidas fáciles, de acuerdo con utilizar seudónimos por parte de los usuarios, son completamente inútiles debido a que la identificación y análisis del rastro del usuario por lo común sucede sin que la víctima se percate de la situación. La misma máquina del usuario manifiesta la identidad real a pesar de que la persona se oculte posterior a un seudónimo [6].

1.2.3. Metodologías de pruebas de penetración

Existen diferentes metodologías y guías para que se realice pruebas de penetración. A continuación se describe algunas metodologías desde la perspectiva en aplicativos webs[12]:

1.2.3.1. OWASP

OWASP es un proyecto de código abierto destinado a la de seguridad en aplicaciones Web, esta comunidad está dedicada a habilitar a las organizaciones para desarrollar, comprar y mantener aplicaciones confiables.

El software inestable hace perder fuerza en las finanzas, salud, defensa, energía, entre otros. A medida que el software se transforma en algo decisivo, complicado e interconectado, el aumento del problema para conseguir seguridad en las aplicaciones crece de forma acelerada. El ritmo acelerado de los procesos de desarrollo de software modernos aumenta aún más el peligro de no mostrar vulnerabilidades de manera diligente y esencial. Aunque inicialmente el objetivo de OWASP fue concientizar a desarrolladores y gerentes, se ha transformado en un standard de seguridad de factor [2].

1.2.3.2. OSSTMM

OSSTMM (Open Source Security Testing Methodology Manual) en la versión 3 difundida en el 2010 por ISECOM (Institute for Security and Open Methodologies). En el caso por las aplicaciones web, no abarca etapas, canales o módulos determinados para su valoración, se compone de cuatro etapas o fases [12]:

- Fase de Inducción: Decreta la importancia, requisitos y limitaciones de la auditoría.
- Fase de Interacción: Se trata de manifestar vínculos entre el alcance, los objetivos y los activos involucrados.
- Fase de requerimientos: Ejecutan comprobaciones de procesos, de configuraciones, capacitaciones, propiedad intelectual, información expuesta y otros.
- Fase de Intervención: Se orienta en la implantación de los objetivos y su afectación.

1.2.3.3. PTES

El Estándar para la Ejecución de Pruebas de Penetración o PTES (Penetration Testing Execution Standard), es un plan establecido por distintas organizaciones y empresas. Algunas secciones de la metodología escasean de descripción y no cubre todo el alcance que se necesita en el campo de aplicaciones web. Se compone por siete fases [12]:

- Preacuerdo: Determinan la importancia y objetivos de la prueba de penetración.
- Recopilación de inteligencia: Se realiza la recopilación de información de inteligencia desde fuentes abiertas.
- Modelado de amenazas: Se declaran las favorables estrategias de penetración.
- Análisis de vulnerabilidades: Revelan vulnerabilidades que podrían ser explotadas.
- Explotación: Pretende explotar las vulnerabilidades reconocidas.
- Post explotación: Los especialistas de seguridad pueden continuar escalando el proceso de explotación.
- Reporte: Se comunica al cliente la información que le permita solucionar las vulnerabilidades localizadas.

1.2.3.4. ISSAF

El ISSAF (Information System Security Assessment Framework) o Marco de Evaluación de Seguridad de Sistemas de Información, fue desarrollada por OISSG (Open Information Systems Security Group). El proceso de pruebas de penetración se desarrolla a través de tres fases[12]:

- Fase I. Planificación y Preparación: Entiende los pasos para la reciprocidad de informaciones iniciales, planificación y preparación para las pruebas de seguridad.
- Fase II. Evaluación: Adaptan las pruebas de seguridad de la metodología de penetración de ISSAF.
- Fase III. Reportes, Limpieza y Destrucción de Artefactos: Toda la información creada y acumulada en los sistemas como parte de las pruebas de seguridad se descartan.

1.2.3.5. Análisis comparativo de las principales metodologías

En el estudio realizado por Henry Raúl González Brito y Raydel Montesino Perurena titulado "Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades frecuentes en aplicaciones web" describen el análisis cualitativo realizado a los principales requerimientos de seguridad en las aplicaciones web. Para indagar dicho análisis, ellos crearon una escala de evaluación cualitativa como en la Tabla 3 para poder analizar cómo se aproximan las vulnerabilidades más usuales en aplicaciones web. Los resultados de aplicar la escala de evaluación se encuentran en la Tabla 4.

Tabla 3. Escala de evaluación de las metodologías respecto a las principales vulnerabilidades de seguridad en las aplicaciones web[12].

Valor	Descripción
0	No se hace ninguna alusión a la vulnerabilidad ni a pruebas de seguridad o comprobación relacionada con esta.
1	Se hace mención a la vulnerabilidad, pero no se describe como hacer la prueba de seguridad para su detección.
2	Se describe como realizar la prueba de seguridad, pero el contenido presentado no es suficiente para realizar una prueba de seguridad real.
3	Se describe como realizar la prueba de seguridad con suficientes detalles para ser aplicada directamente en una prueba de seguridad real.

Tabla 4. Presencia de pruebas de seguridad asociadas a aplicaciones web [12]

Principales Vulnerabilidades	**OSSTMM**	**PTES**	**ISSAF**	**OWASP**
Inyección de código	1	2	2	2
Pérdida de autenticación y gestión de sesiones	2	1	1	3
Secuencia de comandos en sitios cruzados (XSS)	0	1	3	3
Control de acceso interrumpido	1	1	1	3
Referencia directa insegura a objetos	1	1	2	3
Ausencia de control de acceso a funciones	1	1	2	3
Configuración de seguridad incorrecta	1	1	2	2
Exposición de datos sensibles	1	1	2	2
Falsificación de peticiones en sitios cruzados (CSRF)	0	1	0	3
Utilización de componentes con vulnerabilidades conocidas	1	1	1	3
Entidades externas de XML (XXE)	1	1	0	3
Deserialización insegura	0	0	0	0
Registro y monitoreo insuficiente	0	0	0	0
Totales	**10**	**12**	**16**	**30**

Como se muestra en la Tabla 4, La Guía de pruebas de OWASP es la que muestra un nivel de aplicación mayor (76%), siguiéndole ISSAF (41%), PTES (31%) y finalmente OSSTMM (26%).

La Guía de Pruebas de OWASP es más apropiada para ser elegida fundamento en una prueba de penetración en aplicaciones web, inyección de código y pérdida de autenticación y gestión de sesiones. La semejanza con las vulnerabilidades más reiteradas en aplicaciones web, enseñan que sus grandes privaciones en el caso de la Guía de Pruebas de OWASP está en la obligación de narrar con pruebas de seguridad que admitan valorar la deserialización insegura, el registro y monitoreo de la aplicación web [12].

1.2.4. Metodología de prueba de penetración OWASP

El software inestable hace perder fuerza en las finanzas, salud, defensa, energía, entre otros. A medida que el software se transforma en algo decisivo, difícil e interconectado, el aumento del impedimento para conseguir seguridad en las aplicaciones crece gradualmente. El ritmo acelerado de los procesos de desarrollo de software modernos aumenta aún más el peligro de

no revelar vulnerabilidades de forma ágil y determinada. Aunque inicialmente el objetivo de OWASP fue concienciar a desarrolladores y gerentes, se ha transformado en un standard de seguridad de factor [2].

El desfavorecer el negocio u organización el algo que los agresores logren realizar si usan distintas rutas a través de una aplicación. Cada camino significa un peligro que puede merecer atención o no. Muchas veces estos caminos son sencillos de hallar y reconocer, mientras que a veces son mucho más complicados. De igual manera, el deterioro causado puede no tener efecto, o puede dejarlo en ruina. Con el fin de definir el peligro para una organización para llegar a una resolución, se puede valorar la posibilidad relacionada a cada agente de amenaza, vector de ataque, debilidad de seguridad y acoplarlo con una consideración de la colisión técnica y de negocio para su organización. Juntos, estos factores definen su riesgo general[2].

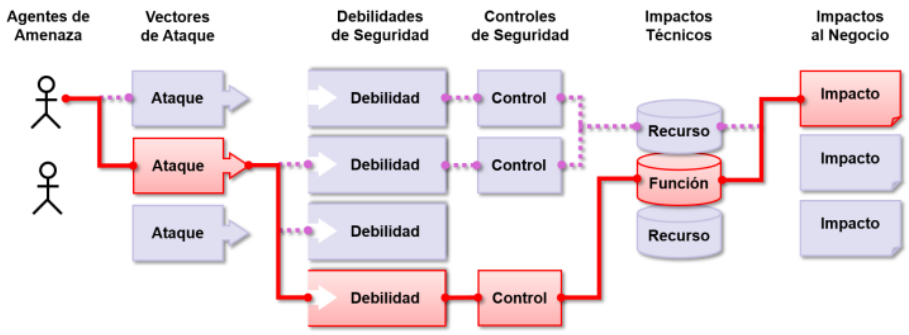

Figura 3. Ruta a través de una aplicación [2]

OWASP se orienta en distinguir los riesgos más culminantes para un abundante tipo de organizaciones. A cada uno de estos riesgos, se provee información genérica sobre la probabilidad y el impacto técnico, usando el siguiente esquema de evaluación, fundamentado en la Metodología de Evaluación de Riesgos de OWASP. Como cada organización, los agentes de amenaza son únicos para la organización, con objetivos y la impresión de cualquier brecha. Es importante saber que el riesgo para la organización en función de los agentes de amenaza aplicables a su negocio y los impactos comerciales[2].

Agente de Amenaza	Explotabilidad	Prevalencia de Vulnerabilidad	Detección de Vulnerabilidad	Impacto Técnico	Impacto de Negocio
Específico de la Aplicación	Fácil 3	Difundido 3	Fácil 3	Severo 3	Específico del Negocio
	Promedio 2	Común 2	Promedio 2	Moderado 2	
	Difícil 1	Poco Común 1	Difícil 1	Mínimo 1	

Figura 4. Esquema de evaluación, basado en la Metodología de Evaluación de Riesgos de OWASP[2].

A continuación, se mencionan los riesgos en seguridad de aplicaciones[2]:

- Inyección

Al momento de mandar datos que no son verídicos a un intérprete sucede una falla de inyección como SQL o NoSQL, como parte de un comando o consulta. El intérprete puede ser burlado por datos dañinos de un atacante para llevar a cabo comandos involuntarios o ingrese a los datos sin la debida autorización.

Un vector de inyección puede ser cualquier fuente de datos como variables de entorno, parámetros, servicios web externos e internos, y todo tipo de usuarios. Sin embargo, una inyección también causa divulgación, pérdida o corrupción de la información, así como también la negación de acceso. Los defectos de inyección pueden ser bastantes comunes, más si con de código heredado, ocurre cuando a un intérprete puede enviársele información dañina por parte del atacante. Los errores de inyección son sencillos de revelar al comprobar el código y los escáneres y fuzzers ayudan a encontrarlos.

- Pérdida de Autenticación

Los atacantes ayudados por la equivocada implementación de las funciones de la aplicación relacionadas a autenticación y gestión de sesiones, favoreciendo el exponer las contraseñas

y usuarios, token de sesiones, o aprovechar otros errores de implementación para aceptar la identidad de otros usuarios (temporal o permanentemente).

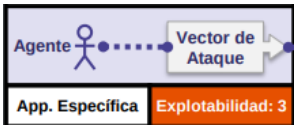

Figura 5. Vector de ataque [2]

En vista de la fuga de información los atacantes tienen entrada a millones de combinaciones de pares de usuario y contraseña conocidas, además de cuentas administrativas por defecto. Utilizando herramientas de fuerza bruta o diccionarios se puede realizar ataques para quebrantar los hashes de las contraseñas.

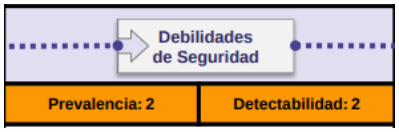

Figura 6. Debilidades de seguridad [2]

En el diseño y en la puesta en funcionamiento de la mayor cantidad de los controles de acceso son frecuentes que existan los errores de pérdida de autenticación. La gestión de sesiones es la piedra angular de los controles de autenticación y está presente en las aplicaciones. Con el uso de medios manuales los atacantes tienen la facilidad de descubrir si la autenticación es deficiente y usando herramientas automatizadas puede exportarlos con listas de contraseñas y ataques de diccionario.

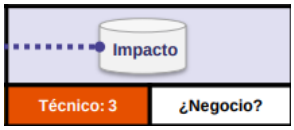

Figura 7. Impacto [2]

Adquiriendo el acceso a una reducida cantidad de cuentas o a una cuenta administrador para involucrar al sistema. El robo de identidad, lavado de dinero y la difusión de información susceptible resguardada regularmente depende del dominio de la aplicación.

La confirmación de la identidad y la gestión de sesiones del usuario son fundamentales para resguardarse contra ataques relacionados con la autenticación. Pueden econtrarse debilidades de autenticación si la aplicación[2]:

- Permite ataques automatizados como la reutilización de credenciales conocidas, teniendo en cuenta que el atacante ya tiene una lista de pares de usuario y contraseña válidos.
- Permite ataques de fuerza bruta o ataques automatizados.
- Permite contraseñas por defecto, débiles o muy conocidas, como “Password1”, “Contraseña1” o “admin/admin”.
- Posee procesos débiles o inefectivos en el proceso de recuperación de credenciales, como “respuestas basadas en el conocimiento”, las cuales no se pueden implementar de forma segura.
- Almacena las contraseñas en texto claro o cifradas con métodos de hashing débiles.
- No posee autenticación multi-factor o fue implementada de forma ineficaz.
- Expone SessionIDs en las URL, no la invalida correctamente o no la rota satisfactoriamente luego del cierre de sesión o de un periodo de tiempo determinado.

Para prevenir que existan debilidades y resguardarse frente a ataques vinculados en la autenticación[2]:

- Implemente autenticación multi-factor para evitar ataques automatizados, de fuerza bruta o reúso de credenciales robadas.
- No se utiliza credenciales por defecto en el software, particularmente en el caso de administradores.

- Se debe implementar controles contra contraseñas débiles. Cuando el usuario ingrese una nueva clave, la misma puede verificarse contra la lista del Top 10.000 de peores contraseñas.
- Alinear la política de longitud, complejidad y rotación de contraseñas u otras políticas de contraseñas modernas, basadas en evidencias.
- Mediante la utilización de los mensajes genéricos iguales en todas las salidas, se debe asegurar que el registro, la recuperación de credenciales y el uso de APIs, no permiten ataques de enumeración de usuarios.
- Limita o incrementa el tiempo de respuesta de cada intento fallido de inicio de sesión. Registre todos los fallos y avise a los administradores cuando se detecten ataques de fuerza bruta.
- Utilice un gestor de sesión en el servidor, integrado, seguro y que genere un nuevo ID de sesión aleatorio con alta entropía después del inicio de sesión. El Session-ID no debe incluirse en la URL, debe almacenarse de forma segura y ser invalidado después del cierre de sesión o de un tiempo de inactividad determinado por la criticidad del negocio.

Un ejemplo de una posible escena de ataque es el relleno automático y el uso de listas de contraseñas. El no utilizar protecciones automáticas en la aplicación, puede usarse para definir si son válidas las credenciales. Un segundo ejemplo de una posible escena de un ataque de autenticación es el utilizar únicamente contraseñas como factor. Se requiere la rotación y dificultad de las contraseñas, desalentando el utilizar claves débiles por de los usuarios. Se recomienda a las organizaciones utilizar las prácticas recomendadas en la Guía NIST 800-63 y el uso de autenticación multi-factor (2FA). Un tercer ejemplo de un escenario similar es el no tener de manera adecuada la configuración de la aplicación durante el tiempo de vida de las sesiones. El usuario al usar una computadora, publica para ingresar a la aplicación y en lugar de elegir “logout” sencillamente cierra la pestaña del navegador. El atacante al momento de utilizar el mismo navegador momentos más tarde, encuentra la sesión activa y el usuario esta autenticado[2].

- Pérdida de Control de Acceso

Las limitaciones hacia los usuarios sobre lo que pueden hacer no es exactamente aprovechado. Aprovechando estos fallos para acceder de manera no autorizada para poder explotar por parte de los atacantes, a datos o funcionalidades, cuentas de usuarios, ver archivos sensibles, modificar datos, cambiar derechos de acceso y permisos por parte de los atacantes. Una de las capacidades que tiene los atacantes es el explotar el control de acceso. Las herramientas SAST y DAST pueden detectar la ausencia de controles de acceso, sin embargo, no permiten saber si son correctos en caso de estar presentes. Se puede detectar cuando se utiliza los medios manuales o de manera automática en varios frameworks que no tienen un control de acceso[2].

El decaimiento en el control de acceso es habitual por la falta de detección automática y pruebas funcionales que sean seguras por parte de los que desarrollan las aplicaciones. Las pruebas automatizadas tanto estéticas como dinámicas, no suelen cubrir la detección de fallas en el control de acceso. Los atacantes anónimos que se hacen pasar por usuarios o administradores son incluidos en el impacto técnico, son usuarios que utilizan funciones privilegiadas o crean, acceden, actualizan o eliminan cualquier registro[2].

- Configuración de Seguridad Incorrecta

Debido a la forma errónea de la configuración de seguridad se ha convertido en un problema muy habitual y esto ocurre en parte por establecer de manera manual la configuración. Se puede poner de ejemplo a: cabeceras HTTP configuradas de forma incorrecta, mensajes de error con contenido sensible, falta de parches y actualizaciones, frameworks, dependencias y componentes desactualizados, entre otros. [2]

Es muy común que los atacantes intenten explotar las vulnerabilidades que no estén parchadas o intenten acceder a las cuentas por defecto, páginas no utilizadas, archivos y directorios desprotegidos, entre otros. para así tener acceso o conocimiento del sistema o del

negocio. En cualquier nivel del stack tecnológico (cualquier combinación de lenguajes de programación y tecnologías, o una combinación de productos de software, también llamado stack de soluciones o ecosistema de datos) puede existir configuraciones erróneas en la seguridad, incorporados servicios de red, la plataforma, el servidor web, el servidor de aplicaciones, la base de datos, frameworks, el código personalizado y máquinas virtuales preinstaladas, contenedores, entre otros. Para localizar configuraciones erróneas son apropiados los escáneres automatizados, el uso de cuentas o configuraciones predeterminadas, servicios innecesarios, opciones heredadas, entre otros. Los atacantes a través de los desperfectos obtienen acceso no autorizado a determinado número de datos o funciones del sistema, eventualmente esos errores dan como consecuencia un completo compromiso del sistema[2].

La presente investigación se basó en los lineamientos del proyecto OWASP que ubica las vulnerabilidades por niveles:

Vulnerabilidades confirmadas

Las vulnerabilidades (QID) son fallas de diseño, errores de programación o malas configuraciones que hacen que la aplicación web y su plataforma de aplicación web sean susceptibles de ataques maliciosos. Dependiendo del nivel de riesgo de seguridad, la explotación exitosa de una vulnerabilidad puede variar desde la divulgación de información hasta un compromiso completo de la aplicación web y/o la plataforma de aplicación web. Incluso si la aplicación web no está completamente comprometida, una vulnerabilidad explotada podría llevar a que la aplicación web sea utilizada para lanzar ataques contra los usuarios del sitio.

Tabla 5. Vulnerabilidades Confirmadas

Gravedad	Nivel	Descripción
	Mínimo	La divulgación de información básica (por ejemplo, el tipo de servidor web, el lenguaje de programación) podría permitir a los intrusos descubrir otras vulnerabilidades, pero la falta de esta información no hace que la vulnerabilidad sea más difícil de encontrar.
	Medio	Los intrusos pueden ser capaces de recopilar información sensible sobre la plataforma de la aplicación, como la versión exacta del software utilizado. Con esta información, los intrusos pueden explotar fácilmente las vulnerabilidades conocidas específicas de las versiones de software. Otros tipos de información sensible pueden revelar unas pocas líneas de código fuente o directorios ocultos.
	Serio	Las vulnerabilidades de este nivel suelen revelar información relacionada con la seguridad que podría dar lugar a un uso indebido o a una explotación. Los ejemplos incluyen la divulgación del código fuente o la transmisión de credenciales de autenticación a través de canales no cifrados.
	Crítico	Los intrusos pueden explotar la vulnerabilidad para obtener contenido altamente sensible o afectar a otros usuarios de la aplicación web. Los ejemplos incluyen ciertos tipos de scripts de sitios cruzados y ataques de inyección SQL.
	Urgente	Los intrusos pueden explotar la vulnerabilidad para comprometer el almacén de datos de la aplicación web, obtener información de las cuentas de otros usuarios u obtener la ejecución de comandos en un host en la arquitectura de la aplicación web.

Vulnerabilidades Potenciales

Las vulnerabilidades potenciales indican que el escáner observó una debilidad o un error que se utiliza comúnmente para atacar una aplicación web, y el escáner no pudo confirmar si la debilidad o el error podía ser explotado. Siempre que sea posible, la sección de descripción y resultados del QID incluye información y consejos para el seguimiento del análisis manual. Por ejemplo, la explotabilidad de un QID puede estar influenciada por características que el escáner no puede confirmar, como la arquitectura de red de la aplicación web, o la prueba

para confirmar la explotabilidad requiere pruebas más intrusivas de las que el escáner está diseñado para realizar.

Tabla 6 Vulnerabilidades Potenciales

Gravedad	Nivel	Descripción
	Mínimo	La presencia de esta vulnerabilidad es indicativa de la divulgación de información básica (por ejemplo, el tipo de servidor web, el lenguaje de programación) y podría permitir a los intrusos descubrir otras vulnerabilidades. Por ejemplo, en este escenario, se puede revelar información como el tipo de servidor web, el lenguaje de programación, las contraseñas o las referencias de la ruta de los archivos.
	Medio	La presencia de esta vulnerabilidad es indicativa de la divulgación de información básica (por ejemplo, el tipo de servidor web, el lenguaje de programación) y podría permitir a los intrusos descubrir otras vulnerabilidades. Por ejemplo, se puede revelar la versión del software o los datos de la sesión, que podrían utilizarse para su explotación.
	Serio	La presencia de esta vulnerabilidad podría dar acceso a la información relacionada con la seguridad a los intrusos que están obligados a hacer un mal uso o explotar. Ejemplos de lo que podría suceder si se explotara esta vulnerabilidad son: hacer caer el servidor o causar un obstáculo al servicio regular.
	Crítico	La presencia de esta vulnerabilidad podría dar a los intrusos la posibilidad de obtener contenido altamente sensible o afectar a otros usuarios de la aplicación web.
	Urgente	La presencia de esta vulnerabilidad podría permitir a los intrusos comprometer el almacén de datos de la aplicación web, obtener información de las cuentas de otros usuarios u obtener la ejecución de comandos en un host de la arquitectura de la aplicación web. Por ejemplo, en este escenario, los usuarios de la aplicación web pueden ser potencialmente el objetivo si la aplicación es explotada.

Información Recopilada

Los problemas de Información Recopilada (QID) incluyen información visible sobre la plataforma, el código o la arquitectura de la aplicación web. También puede incluir información sobre los usuarios de la aplicación web.

Tabla 7 Información Recopilada

Gravedad	Nivel	Descripción
	Mínimo	Los intrusos pueden ser capaces de recuperar información sensible relacionada con la plataforma de la aplicación web.
	Medio	Los intrusos pueden ser capaces de recuperar información sensible relacionada con la funcionalidad interna o la lógica de negocio de la aplicación web.
	Serio	Los intrusos pueden ser capaces de detectar datos altamente sensibles, como la información de identificación personal (PII) sobre otros usuarios de la aplicación web.

Una herramienta que aplica el OWASP y se utiliza para hacer proceso de autenticación es QualysGuard Web Application Scanning WAS**, e**s un servicio basado en la nube que proporciona rastreo y pruebas automáticas de aplicaciones web personalizadas para identificar vulnerabilidades, incluidas las secuencias de comandos entre sitios (XSS) y la inyección de SQL. El servicio automatizado permite pruebas regulares que producen resultados consistentes, reducen los falsos positivos y se escalan fácilmente para cubrir miles de sitios web. Incluye una tecnología de escaneo adicional para monitorear proactivamente los sitios web en busca de infecciones de malware, enviando alertas a los propietarios de sitios web para ayudar a prevenir las listas negras y el daño a la reputación de la marca.

Al momento de ingresar el usuario y contraseña, la herramienta cuenta con características como: Dashboard, Aplicaciones Web, Escaneos, Reportes y Configuraciones. Cada una de estas características cuentan con un menú de opciones a configurar para realizar de mejor forma el escaneo a un sitio web usando la URL de la página. En Option Profiles se configura

para que realizar un escaneo bajo OWASP usando el parámetro de “Initial Parameters”, como se observa en la figura 9.

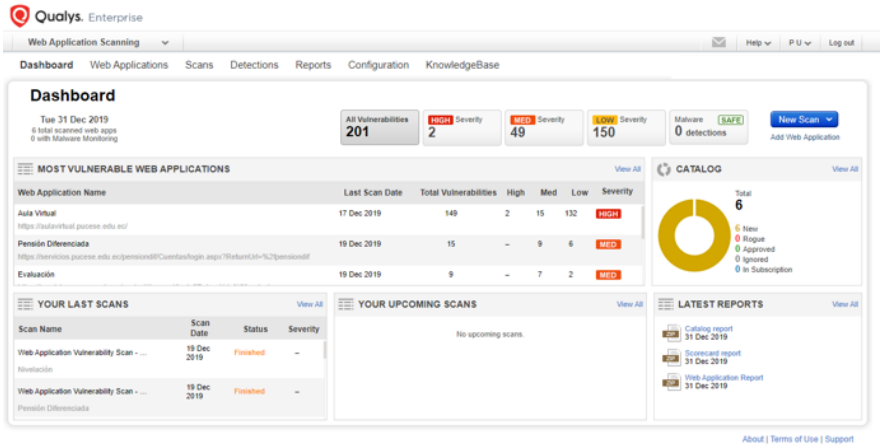

Figura 8. Pagina inicial de la herramienta QualysGuard

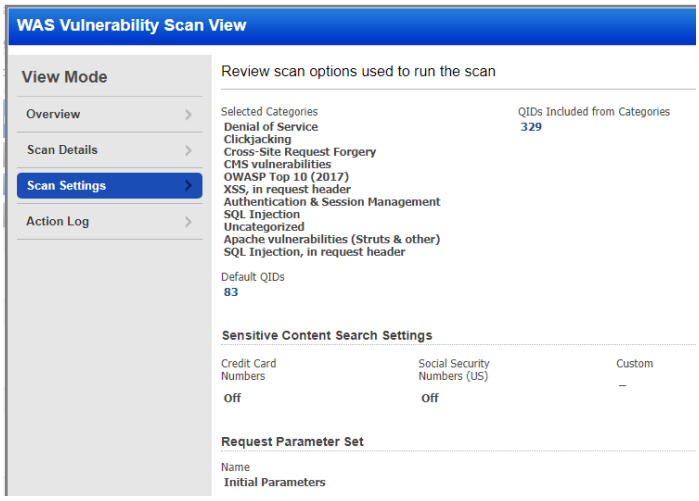

Figura 9. Categorías seleccionadas para realizar el escaneo en Initial Parameters

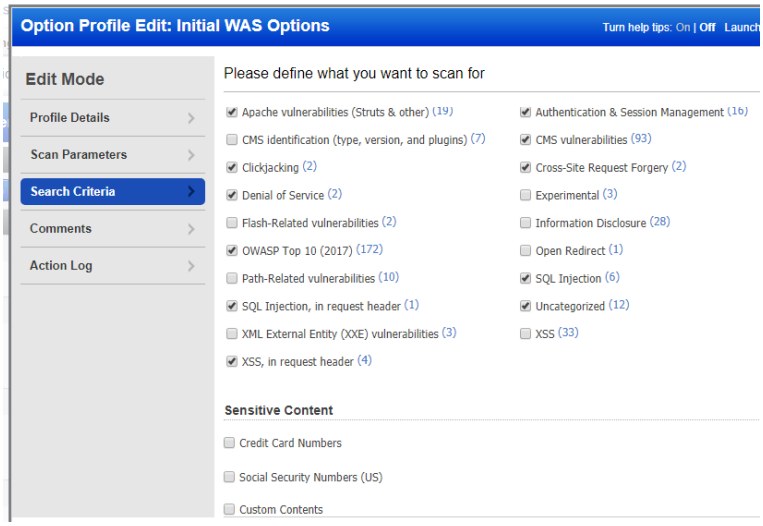

Figura 10. Initial Parameters configurando para realizar el escaneo bajo OWASP

Vulnerabilidades

Las vulnerabilidades que se encuentran en QualysGuard aplicando OWASP son:

El clickjacking es utilizado por el atacante para engañar al usuario para que este haga clic en un marco invisible de la página web, provocando así que el realice una acción que no quería tomar. Con frecuencia esto da a los atacantes acceso no autorizado a algunos datos del sistema o funcionalidad.

El encabezado de opciones de X-Frame no está configurado en la respuesta HTTP, lo que puede llevar a que el atacante engañe al usuario para que hagan clic en un enlace malicioso que este en la página principal y muestre una capa encima de ella con botones de aspecto legítimo.

Error de conexión ocurrido durante el escaneo de la aplicación web, siendo estos posibles errores de conexión causados por una alteración ocurrido en la conectividad de red entre el escáner y la aplicación web, el servidor de aplicaciones que alberga la aplicación se ha caído en medio de un escaneo, sobrecarga ocurrido posiblemente debido a la carga generada por el escaneo, un error en el handshake SSL/TLS que se aplica sólo a las aplicaciones web HTTPS,

un dispositivo de seguridad como un IDS/IPS o un firewall de aplicaciones web (WAF) comenzó a eliminar o rechazar las conexiones HTTP del escáner.

En las formas rastreadas consiste en los formularios únicos enviados por el Escáner de aplicaciones Web. La lista de formularios reportados no contiene formularios de autenticación (es decir, formularios de login)

En el diagnóstico por escáner proporciona varios detalles del rendimiento y el comportamiento del escaneo. En algunos casos, esta comprobación se puede usar para identificar problemas que el escáner encontró al rastrear la aplicación Web de destino.

La lista de enlaces únicos rastreados y formularios HTML puede contener menos enlaces que el umbral máximo definido al iniciar el escaneo. También incluye todos los enlaces redundantes/rutas URL rastreadas y no rastreadas, Formularios rastreados, todos los Formulario de autenticación encontrado y Ciertas solicitudes rastreadas.

La divulgación de información a través del encabezado de respuesta como los encabezados de respuesta HTTP podrían revelar información sobre la plataforma y las tecnologías utilizadas por el sitio web. Pueden utilizarse las cabeceras por los atacantes para tomar huellas digitales y lanzar ataques específicos a las tecnologías y versiones utilizadas por la aplicación web.

Falta el encabezado política de características cuya cabecera de respuesta de la política no está presente. Permite a los desarrolladores web habilitar, deshabilitar y modificar selectivamente el comportamiento de ciertas API y características web como "geolocalización", "cámara", "usb", "pantalla completa", "animaciones", entre otros. en el navegador. Estas políticas restringen las API a las que el sitio puede acceder o modificar el comportamiento predeterminado del navegador para determinadas funciones.

El encabezado de Política de referencia controla cuánta información de referencia se envía a un sitio cuando se navega por él. La ausencia de un encabezado de política de referencia puede provocar una fuga de información sensible a través del encabezado de referencia.

La Política de Seguridad de Contenidos es un mecanismo de defensa que puede reducir significativamente el riesgo y el impacto de los ataques XSS en los navegadores modernos. La especificación de CSP proporciona un conjunto de restricciones de contenido para los recursos web y un mecanismo para transmitir la política desde un servidor a un cliente donde se aplica la política. Cuando se especifica una política de seguridad de contenidos, se cambian una serie de comportamientos predeterminados en los agentes de usuario; específicamente el contenido en línea y las construcciones de evaluación de JavaScript no se interpretan sin directivas adicionales. En resumen, CSP permite crear una lista blanca de fuentes de contenido confiable. La política de CSP instruye al navegador para que sólo muestre los recursos de esas fuentes de la lista blanca. Aunque un atacante pueda encontrar una vulnerabilidad de seguridad en la aplicación a través de la cual inyectar el script, éste no coincidirá con las fuentes de la lista blanca definida en la política de CSP, y por lo tanto no se ejecutará.

La ausencia de una Política de Seguridad de Contenidos en la respuesta permitirá al atacante explotar las vulnerabilidades, ya que la protección proporcionada por el navegador no es en absoluto aprovechada por la aplicación Web. Si no se implementa una configuración segura de CSP, los navegadores no podrán bloquear los ataques de inyección de contenido como Cross-Site Scripting y Clickjacking.

El encabezado de respuesta de las opciones de tipo X-Contenido no está presente. Todos los navegadores web emplean un algoritmo de rastreo de contenido que inspecciona el contenido de las respuestas HTTP y también ocasionalmente anula el tipo MIME proporcionado por el servidor. Si el encabezado X-Content-Type-Options no está presente, los navegadores pueden ser potencialmente engañados para tratar las respuestas no HTML como HTML. Un atacante puede entonces aprovechar la funcionalidad para realizar un ataque de cross-site scripting (XSS).

El encabezado de respuesta X-XSS-Protection proporciona una capa de protección contra los ataques de XSS (Cross Site Scripting) reflejados. Esta es una medida de defensa de segunda línea de mejor esfuerzo que ayuda a evitar que un atacante utilice técnicas de evasión para evitar los mecanismos de neutralización que los filtros utilizan de forma predeterminada. Cuando se configuran adecuadamente, los filtros XSS a nivel de navegador pueden proporcionar capas adicionales de defensa contra los ataques a las aplicaciones web.

Se encontró que faltaba el encabezado HTTP Strict Transport Security (HSTS) o que estaba mal configurado. El encabezado HSTS dicta a un navegador conforme que las conexiones actuales y todas las subsiguientes (durante un período de tiempo configurable) al sitio web en cuestión sólo deben realizarse sobre una capa de transporte segura. Además, los usuarios no pueden evitar los errores de los certificados SSL/TLS, lo que impide que el navegador haga clic en los certificados que han caducado o que no son fiables. Si el encabezado HSTS no es configurado por las aplicaciones Web que utilizan TLS, los usuarios son potencialmente vulnerables a los ataques activos Man-in-the-middle(MITM) y SSL Striping.

1.3. Marco Legal

Los usuarios tienen derecho a saber que las múltiples visitas que se realiza en internet dejan un rastro que puede ser aprovechado por terceras personas con fines negativos. La privacidad y las posibles consecuencias que se puede tener al incumplir consta en el Código Orgánico Integral Penal (COIP) con leyes se sancionan en el Ecuador.

Existen numerosos artículos en el COIP que sancionan a las personas con prisión para quienes cometan delitos que afecten a la identidad digital del usuario. Entre estos artículos se puede mencionar el artículo 178 que castiga con prisión de uno a tres años a las personas que violen la intimidad del usuario publicando datos o información personal del usuario sin su consentimiento. En el artículo 186 se sanciona con prisión de cinco a siete años a las personas que buscando beneficio patrimonial utilice información de otra persona o utilice información falsa.

En el artículo 212 se sanciona la suplantación de identidad. El castigo con prisión de uno a tres años si alguna persona intenta suplantar la identidad de otra persona para obtener algún beneficio para el mismo o para un tercero. El artículo 230 sanciona la interceptación ilegal de datos. El castigo es de tres a cinco años si alguien diseña, desarrolla, programa o envía mensajes, enlaces o ventanas con los dominios de servicios financieros ilegales a la gente con la finalidad de extraer información financiera de las víctimas. En el artículo 229 se sanciona la revelación ilegal de base de datos con prisión de uno a tres años a la persona que intentando sacar algún beneficio revele información que esté contenida en alguna base de datos o medios semejantes violando la intimidad y privacidad el usuario.

En la ley orgánica de gestión de la identidad y datos civiles, en el artículo 1 garantiza el derecho a la identidad de las personas y regular la gestión y el registro de los hechos y actos relativos al estado civil de las personas y su identificación. En el artículo 6 se promueve en conjunto con el ente rector de la ciencia, tecnología e innovación y otras instituciones públicas o privadas, la investigación científica y tecnológica para el fortalecimiento de la gestión de la identidad y registro de datos civiles.

CAPÍTULO 2: METODOLOGÍA

La presente investigación estuvo orientada hacia la evaluación de la gestión de identidad digital de usuarios de servicios web, es decir, amenazas que afectan a la privacidad de la información, considerando referente la pérdida de autenticación en servicios web y las vulnerabilidades encontradas en los resultados obtenidos.

El diseño de investigación usado es de tipo no experimental, puesto que, no se han manipulado las variables obtenidas, sino que, se utilizaron tal y como se las obtuvo. La variable con las que se trabajó es identidad digital de usuarios en servicios web.

2.1. Tipo de Estudio

El presente estudio se desarrolló bajo el paradigma de investigación cuantitativa, puesto que se aplicó un escaneo a los diferentes servicios web y se realizó un análisis estadístico de los datos obtenidos. Los aspectos que se tuvieron en cuenta es la seguridad de autenticación de los servicios web de la página de la Pontificia Universidad Católica del Ecuador – Esmeraldas. Se realizó un escaneo a los servicios web tales como el Sistema de Notas, Aula Virtual, Intranet, Pensión Diferenciada y el Sistema de Evaluación de Académica para Estudiantes.

De acuerdo con el alcance de investigación, de tipo descriptivo, considerando que se indicaron las características de los procesos de autenticación que utilizan los servicios web de sitios de la Pontificia Universidad Católica del Ecuador – Esmeraldas.

2.2. Definición conceptual y operacionalización de las variables

Para medir la variable del estudio, se realizó un escaneo a los servicios web que son utilizados por los usuarios de la PUCESE, el análisis de estas variables permite evaluar la gestión de

identidad digital de usuarios en los servicios web de la Pontificia Universidad Católica del Ecuador – Esmeraldas.

Tabla 8. Variables

Variable	**Definición conceptual**	**Definición operacional**	**Dimensiones**	**Indicadores**
Vulnerabilidades de los servicios web de la PUCESE	Debilidades que ponen en riesgo la seguridad de la información.	Analizar autenticación	Autenticación Medidas de Seguridad	Se basará en el estándar de OWASP

2.3.Métodos

En relación con la forma en que se trataron y manejaron los datos, la presente investigación utilizó el método deductivo y analítico-sintético, ya que busca ir desde lo más general hacia lo especifico, siendo que esto conlleva al cumplimiento de los objetivos propuestos, se realizó un análisis de los procesos y datos durante la autenticación en sitios de servicios web de la PUCESE.

2.4.Técnicas e instrumentos

OWASP es una guía de seguridad para aplicaciones web implementada en el lineamiento sobre los bienes prácticos de seguridad informática, siendo el instrumento utilizado el lineamiento basado en OWASP llamada QualysGuard. La técnica que se utiliza es la observación por medio del lineamiento, que tendrá posteriormente el análisis para la obtención de datos. Para poder determinar el nivel de calidad se analizó utilizando como técnica OWASP, cuyos indicadores permitieron evaluar los aspectos principales de los servicios web de las PUCESE.

La herramienta que se utilizó para realizar el escaneo a los servicios web es QualysGuard Web Application Scanning WAS que es una herramienta en la nube que proporciona rastreo y pruebas automáticas de aplicaciones web personalizadas para identificar vulnerabilidades, además de pruebas de penetración y permite encontrar vulnerabilidades del top 10 de OWASP.

2.5. Análisis de datos

La técnica del análisis constó en describir los resultados mostrados en la herramienta QualysGuard, donde se pueden identificar cada uno de los servicios web que se han escaneado y comprender los niveles de vulnerabilidad que genera la misma. Se realizó el análisis de los datos mediante procedimientos estadísticos con la información obtenida.

QualysGuard es el punto de entrada para generar el análisis de los datos. Se procede a ingresar al sitio web para configurar las dimensiones de identidad digital seleccionadas para la exploración y el software genera un reporte de vulnerabilidades por niveles del sitio web basado en OWASP.

CAPÍTULO 3: RESULTADOS

Para poder determinar el grado en el que se cumplieron los objetivos propuestos en esta investigación, se han analizado los resultados mediante la realización del escaneo a los servicios web de la PUCESE por medio de lineamientos basados en el proyecto OWASP utilizando la herramienta informática QualysGuard, que ha permitido obtener varios reportes en base a las configuraciones que se realizaron, para medir su nivel de gravedad.

Vulnerabilidades obtenidas en el escaneo del servicio web de intranet

En cuanto a los resultados obtenidos realizando el escaneo se puede señalar que: Son dos las vulnerabilidades obtenidas con un nivel de gravedad de 3, seguida de 6 vulnerabilidades con un nivel de gravedad de 2 y el resto teniendo un nivel de 1.

En el gráfico correspondiente a la figura 12 se muestran las vulnerabilidades del servicio web de Intranet de la PUCESE ubicado por el nivel de gravedad.

Figura 11. Vulnerabilidades obtenidas en el escaneo del servicio web Intranet

Vulnerabilidades obtenidas en el escaneo del servicio web de la Pensión Diferenciada

En relación con los resultados obtenidos durante el escaneo se pudo obtener que: son 6 las vulnerabilidades con un nivel de gravedad de 3, seguida de 7 vulnerabilidades de nivel 2 y el resto teniendo un nivel de gravedad de 1.

En el gráfico correspondiente a la figura 15 se muestran las vulnerabilidades del servicio web de la Pensión Diferenciada de la PUCESE ubicado por el nivel de gravedad.

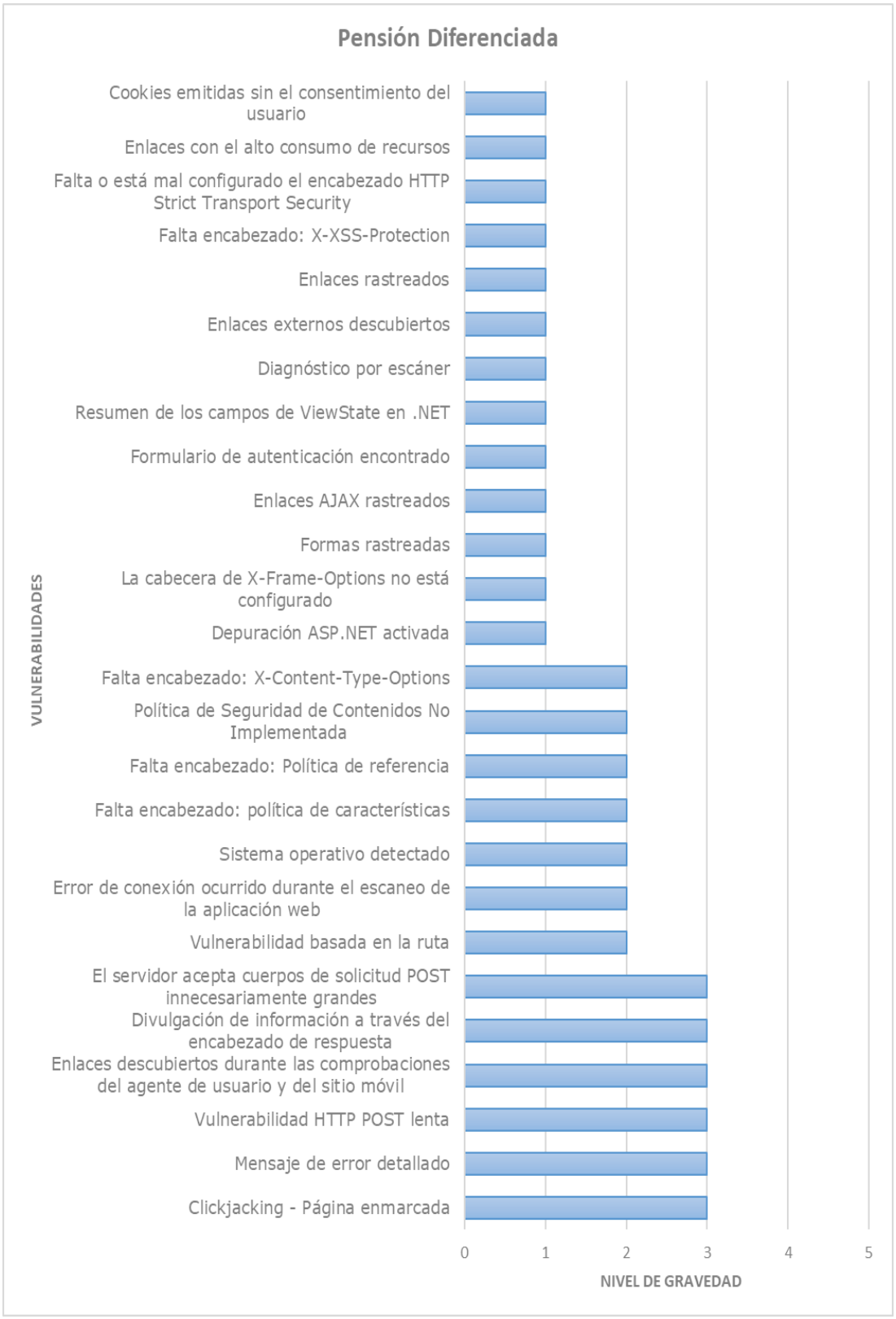

Figura 12. Vulnerabilidades obtenidas en el escaneo del servicio web de la Pensión Diferenciada

Vulnerabilidades obtenidas en el escaneo del servicio web del Sistema de Evaluación Académica para Estudiantes

Se expone a continuación los resultados obtenidos en relación con el escaneo realizado donde se obtuvo que 7 vulnerabilidades con el nivel de gravedad de 3, seguido de 7 vulnerabilidades con un nivel 2 y el resto 1.

En el gráfico correspondiente a la figura 16 se muestran las vulnerabilidades del servicio web del Sistema de Evaluación Académica para Estudiantes de la PUCESE ubicado por el nivel de gravedad.

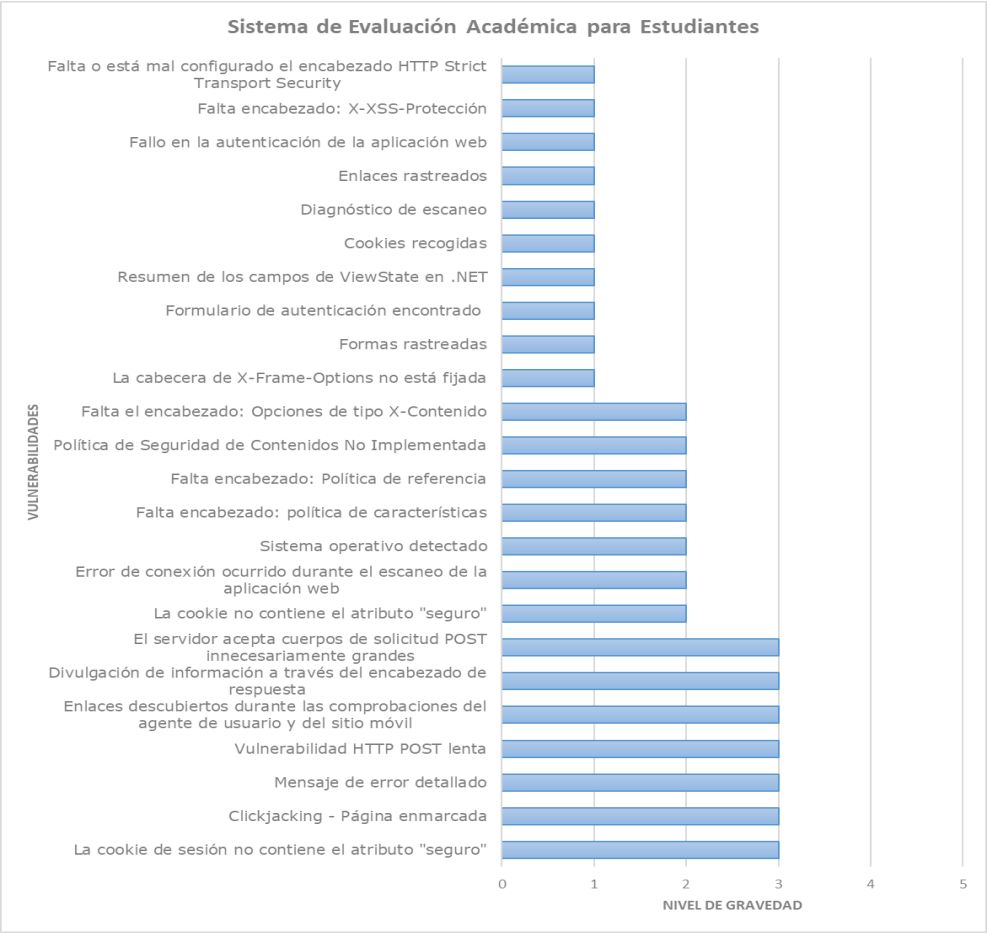

Figura 13. Vulnerabilidades obtenidas en el escaneo del servicio web Sistema de Evaluación Académica para Estudiantes

Vulnerabilidades obtenidas en el escaneo del servicio web del Sistema de Notas

En relación con los resultados obtenidos durante el escaneo se pudo obtener que 6 de las vulnerabilidades con más alto nivel de gravedad es 3, seguido de 6 vulnerabilidades de nivel 2, y el resto de nivel 1.

En el gráfico correspondiente a la figura 17 se muestran las vulnerabilidades del servicio web del Sistema de Notas de la PUCESE ubicado por el nivel de gravedad.

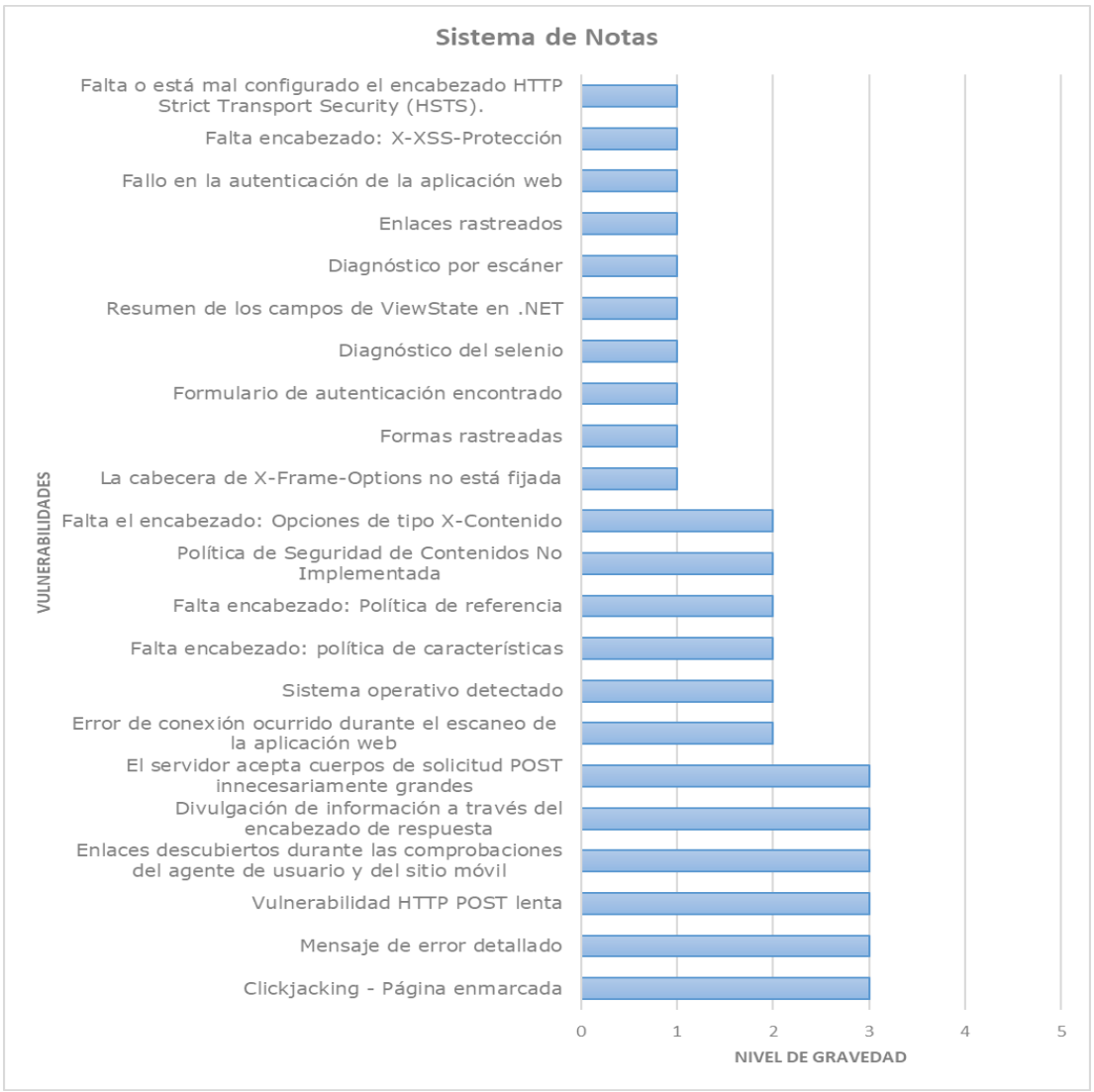

Figura 14.Vulnerabilidades obtenidas del servicio web Sistema de Notas

Vulnerabilidades obtenidas en el escaneo del servicio web del Aula Virtual

En cuanto a los resultados obtenidos realizando el escaneo se puede señalar que: existe una vulnerabilidad de nivel de gravedad 5, seguida de 7 vulnerabilidades de nivel 3, 10 vulnerabilidades de nivel de gravedad 2, y el resto de nivel de gravedad 1.

En el gráfico correspondiente a la figura 18 se muestran las vulnerabilidades del servicio web del Aula Virtual de la PUCESE ubicado por el nivel de gravedad.

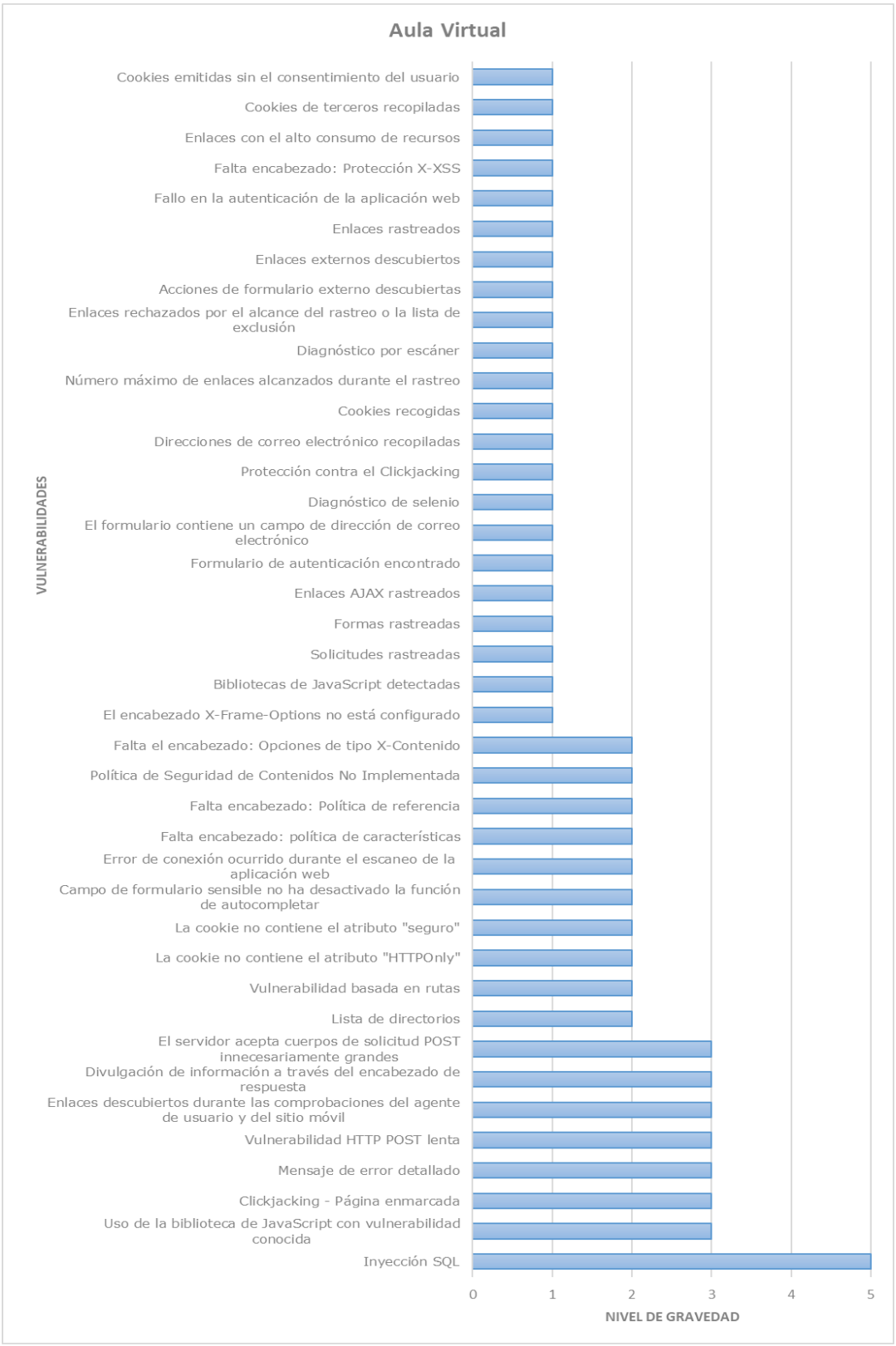

Figura 15. Vulnerabilidades obtenidas en el escaneo del servicio web Aula Virtual

Resumen de las vulnerabilidades en los servicios web

En cuanto al resumen de las vulnerabilidades se puede señalar que: el servicio web con más vulnerabilidades es el Aula virtual con 40 vulnerabilidades, seguida del Intranet con 27 vulnerabilidades, la Pensión Diferenciada con 26 vulnerabilidades, el Sistema de evaluación académica para estudiantes con 24 vulnerabilidades y el Sistema de Notas con 22 vulnerabilidades.

Tabla 9. Resumen de las vulnerabilidades de los servicios web

Nivel de gravedad	**Intranet**	**Pensión Diferenciada**	**Sistema de Evaluación Académica para Estudiantes**	**Sistema de Notas**	**Aula Virtual**
1	19	13	10	10	22
2	6	7	7	6	10
3	2	6	7	6	7
4	-	-	-	-	-
5	-	-	-	-	1

En la tabla 9 podemos observar un resumen de los servicios web y el número de vulnerabilidades encontradas en cada nivel.

Entre las vulnerabilidades más comunes en los servicios web de Intranet, Pensión Diferenciada, Sistema de Evaluación Académica para Estudiantes, Sistema de Notas y Aula virtual está el clickjacking donde el atacante puede engañar al usuario para que haga clic en un marco invisible de la página, haciéndole tomar una acción que no quería tomar. También podría engañar al usuario para que hagan clic en un enlace malicioso que este en la página principal y muestre una capa encima de ella con botones de aspecto legítimo al encabezado de opciones de X-Frame no estar configurado en la respuesta HTTP.

La falta del encabezado política de características cuya cabecera de respuesta de la política no está presente, permite a los desarrolladores web habilitar, deshabilitar y modificar selectivamente el comportamiento de ciertas API. Estas políticas restringen las API a las que

el sitio puede acceder o modificar el comportamiento predeterminado del navegador para determinadas funciones.

La ausencia de un encabezado de política de referencia puede provocar una fuga de información sensible a través del encabezado de referencia. La ausencia de una Política de Seguridad de Contenidos en la respuesta permitirá al atacante explotar las vulnerabilidades, ya que la protección proporcionada por el navegador no es en absoluto aprovechada por la aplicación Web y el navegador no podrán bloquear los ataques de inyección de contenido como Cross-Site Scripting y Clickjacking.

Un atacante puede entonces aprovechar que el encabezado X-Content-Type-Options no está presente para realizar un ataque de cross-site scripting (XSS) y los navegadores pueden ser potencialmente engañados para tratar las respuestas no HTML como HTML. Este caso específico es conocido como un ataque XSS de "Content-Sniffing". Al no configurar el encabezado HSTS en las aplicaciones Web que utilizan TLS, los usuarios son vulnerables a ataques activos como Man-in-the-middle(MITM), SSL Striping.

Entre las vulnerabilidades menos comunes entre los servicios web está el formulario que contiene un campo de dirección de correo electrónico, formulario que recoge direcciones de correo electrónico generando mensajes a los sistemas back-end. Al no aplicar ninguna limitación de tasa o CAPTCHA a los envíos de formularios, las pruebas de vulnerabilidad contra este formulario pueden producir una cantidad significativa de mensajes y si se generan demasiados mensajes, entonces puede producir una situación de Denegación de Servicio.

Las direcciones de correo electrónico pueden ayudar a un usuario malicioso con los ataques de fuerza bruta y de phishing. También las cookies pueden contener información sensible sobre el usuario y las que son enviadas a través de HTTP pueden ser encontradas. Es posible que no se detecten las vulnerabilidades que requieren la autenticación de la aplicación Web, siendo esta vulnerabilidad el fallo en la autenticación de la aplicación web.

Los enlaces con alto consumo de recursos podrían ser utilizados para realizar DOS en el servidor con sólo realizar GET Flooding. Los atacantes podrían derribar el servidor más fácilmente si hay grandes acaparamientos de recursos en él, realizando menos peticiones

Para los servicios web de Intranet, Evaluación Académica para Estudiantes y Sistema de Notas pueden utilizarse las cabeceras por los atacantes para tomar huellas digitales y lanzar ataques específicos a las tecnologías y versiones utilizadas por la aplicación web.

En los servicios web de Pensión Diferenciada, Sistema de Evaluación Académica para Estudiantes y Sistema de Notas se encontró que los atacantes pueden utilizar mensajes de error detallados que les permiten obtener detalles técnicos y aprender información interna sobre la aplicación, permitiéndoles usarla de manera más efectiva. También es vulnerable a un ataque de Denegación de Servicio (DoS) de "HTTP POST lento" que consume los recursos del servidor al mantener las conexiones abiertas durante un periodo de tiempo prolongado enviando lentamente el tráfico al servidor, provocando que no sea capaz de responder a conexiones nuevas y legítimas.

En el servicio web del Sistema de Evaluación Académica para Estudiantes se encontró que las cookies de sesión con atributo "seguro" sólo se pueden enviar a través de HTTPS debido a que las que son enviadas a través de HTTP exponen a los usuarios a ataques de "sniffing" que pueden llevar a la suplantación de la identidad del usuario o al compromiso de la cuenta.

La vulnerabilidad con el nivel de gravedad más alto en el servicio web del Aula Virtual se refiere a la inyección SQL que permite a un atacante modificar la sintaxis de una consulta SQL con el fin de recuperar, corromper o eliminar datos. Esto se logra manipulando los criterios de la consulta de manera que se afecte la lógica de esta. Las causas típicas de esta vulnerabilidad son la falta de validación de entrada y la construcción insegura de la consulta SQL. Las consultas creadas mediante la concatenación de cadenas con la sintaxis SQL y los datos suministrados por el usuario son propensas a esta vulnerabilidad. Si se puede modificar cualquier parte de la concatenación de cadenas, entonces se puede cambiar el significado de

la consulta. Se puede evitar los riesgos al momento de que el usuario ingrese su nombre y contraseña con un captcha o mecanismos de validación para evitar los ataques simultáneos.

En base a las vulnerabilidades que se encontraron en los servicios web de Intranet, Sistema de Evaluación Académica para Estudiantes y el Sistema de Notas se debería determinar el siguientes control y cambio en la configuración: utilizar la Opción X-Frame que permite especificar si el navegador debería permitir o no que muestre una página con la etiquta de <frame>, <iframe> u <object>. Con las vulnerabilidades encontradas en el servicio web Intranet, se puede instalar complementos que sean capaces de determinar si los dominios son confiables o no.

Con las vulnerabilidades que se encontraron en los servicios web de Pensión Diferenciada, Sistema de Evaluación Académica para Estudiantes y el Sistema de Notas se debería garantizar que solo se muestre mensajes de error genéricos implementando un manejo de excepciones y errores fuertes.

En las vulnerabilidades que se encontraron en los servicios web de la Pensión Diferenciada y el Sistema de Notas se debe aplicar medidas de seguridad consistentes independientemente de la plataforma del navegador, el tipo o la versión utilizada para acceder, si no se realiza controles de seguridad a representaciones alternativas del sitio, entonces puede estar expuesta a vulnerabilidades como cross-site scripting, inyección SQL o ataques basados en la autorización que son utilizados por sitios web para validar la identidad de un usuario junto con la contraseña. Para evitar esto, se debería tener un captcha o mecanismos de validación para evitar los ataques simultáneos.

Con las vulnerabilidades encontradas en el servicio web de Pensión Diferenciada se deberían determinar los siguientes cambios en la configuración: implementar una rigurosa validación de los datos de entrada y restringir los datos suministrados por el usuario para que consistan en un conjunto mínimo de caracteres necesarios para el campo de entrada y valide los datos para garantizar que se ajustan al formato esperado.

Se deberían determinar los siguientes cambios en la configuración en base a las vulnerabilidades encontradas en el servicio web del Sistema de Evaluación Académica para Estudiantes: aplicar el atributo "seguro" a las cookies de sesión para asegurarse de que se enviarán sólo a través de HTTPS, garantizar que solo se muestre mensajes de error genéricos implementando un manejo de excepciones y errores fuertes.

Con las vulnerabilidades que se encontraron en el servicio web del Aula Virtual se deberían determinar los siguientes controles y cambios de configuración: las vulnerabilidades de la inyección SQL se pueden abordar en tres áreas: validación de entrada, creación de consultas y seguridad de la base de datos.

Todas las entradas recibidas del cliente Web deben ser validadas para que el contenido sea correcto. Si se conoce de antemano el tipo o el rango de contenido de un valor, se deben aplicar filtros más estrictos. Por ejemplo, una dirección de correo electrónico debe tener un formato específico y sólo contener caracteres que la conviertan en una dirección válida; o los campos numéricos, como un código postal de Ecuador., deben limitarse a valores de seis dígitos. Las vulnerabilidades de inyección SQL se pueden mitigar mediante el uso de listas de control de acceso o acceso basado en roles dentro de la base de datos. Por ejemplo, una cuenta de solo lectura evitará que un atacante modifique datos, pero no evitará que el usuario vea datos no autorizados. Los controles de acceso basados en tablas y filas potencialmente minimizan el alcance de un compromiso, pero no evitan las vulnerabilidades.

CAPÍTULO 4: DISCUSIÓN

Esta investigación tuvo como propósito identificar y describir aquellas vulnerabilidades del proceso de autenticación presente en los sitios web. Sobre todo, se pretendió examinar cuáles son los servicios web más vulnerables, qué nivel de vulnerabilidad presentan y qué amenaza provoca.

Desde hace tiempo se sabe que la seguridad de la contraseña de los usuarios es generalmente terrible, en el año 2019 Carlos Castro concluyó en su artículo "Pruebas de penetración e intrusión" sobre la importancia de la explotación de las vulnerabilidades junto con las recomendaciones adecuadas para cerrar esas brechas de seguridad que ponen en riesgo al usuario. También mencionan el reconocimiento que ha tenido la seguridad informática en empresas con información como su mayor activo, siendo este un impulso para asegurar la información del sistema y evitar ataques como en la compañía Facebook, ocurrido en septiembre del 2018 donde los atacantes filtraron datos, robando tokens de acceso (claves que permiten iniciar la sesión de Facebook de manera automática y no tener que volver a escribir una contraseña cada vez que se quiere acceder) [19]. Mientras tanto en nuestra investigación se determinó que ciertas aplicaciones son vulnerables a la inyección SQL, esto provoca que las contraseñas no tengan un formato o regla de creación.

En el artículo del año 2019 "Frecuencia de contraseñas comprometidas utilizadas por estudiantes y personal de Asia Pacific College" también descubrieron que los usuarios escriben un promedio de 8 contraseñas por día, no siendo de extrañar que prefieran reutilizar las contraseñas (y usar muy fácil de recordar y escribir, es decir, contraseñas inseguras) [20]. En los resultados obtenidos dentro del análisis de los servicios web realizados en esta investigación, todos tienen la vulnerabilidad de utilizar la misma contraseña.

De malera similar, Juan Carlos Guerrero Ortega, Robinson Andrés Jiménez Toledo, en su artículo científico "Aspectos fundamentales en la construcción de páginas web seguras basados en OWASP" en el año 2017, describen cinco principales ataques relacionado con la

seguridad en aplicaciones web, OWASP. Entre estos ataques se encuentran la Inyección, Secuencia de Comandos en Sitios Cruzados, Configuración de Seguridad Incorrecta, Exposición de datos sensibles, Falsificación de Petición en Sitios Cruzados (CSRF), concluyendo que las vulnerabilidades que ocurren en los sistemas muchas veces son producidos por un incorrecto mantenimiento y fortalecimiento en la seguridad, haciendo el sistema vulnerable frente a amenazas[21]. En el estudio se identificó en los servicios web las vulnerabilidades de inyección SQL que permite a un atacante modificar la sintaxis de una consulta SQL con el fin de recuperar, corromper o eliminar datos.

Ortegón Serna, Carlos Andrés en el año 2019 con su trabajo "Amenazas, vulnerabilidades, factores de riesgo y defensa en profundidad en aplicaciones web", describen el beneficio de tener varios niveles de defensa en caso de que alguno se vea comprometido en una aplicación web, siendo importante planificar todas las acciones a realizar, concluyendo su trabajo lo valioso de la implementación de la seguridad en aplicaciones web, primero teniendo que aceptar las organizaciones que su seguridad puede ser vulnerada. De los resultados obtenidos en esta investigación, se puede deducir que los principales factores de riesgo de los servicios web es engañar al usuario para que haga clic en una parte de la página, realizando una acción que no quería tomar. También se puede engañar a los usuarios para que hagan clic en un enlace malicioso y mostrando sobre la página original una capa con botones de aspecto legítimo[22]. Del análisis de los resultados de este estudio se puede afirmar que la probabilidad de que un usuario sea víctima de un ataque por parte de personas malintencionadas es alta por la falta de mecanismos necesarios para la mitigación de este tipo de ataques.

CAPÍTULO 5: CONCLUSIONES

Los lineamientos de un modelo de identidad digital basado en NIST SP – 800-63 influyen al momento de implementar servicios de identidad digital, así como su verificación y autenticación de usuarios, mitigando los impactos negativos de un error de autenticación. Dentro de las técnicas utilizadas para el escaneo de las vulnerabilidades de los servicios web destaca QualysGuard, el cual permite encontrar las vulnerabilidades basadas en OWASP en conjunto con el impacto y la posible solución, además aplicándolo sobre los servicios web se logró generar reportes sobre los resultados encontrados, así como sus amenazas y el nivel de gravedad que tienen.

Para realizar el escaneo correspondiente a los servicios web se utilizó la herramienta QualysGuard debido a que permite detectar la perdida de autenticación y manejo de sesión existente, con el fin de encontrar la mejor técnica para mitigar dicha vulnerabilidad. Debido a que la herramienta se basa en Owasp demostró que es la más indicada para la investigación porque abarca la evaluación más completa para las principales vulnerabilidades en aplicaciones web.

Una de las principales vulnerabilidades presentes en los sitios web fueron encontradas en esta investigación, como el clickjacking donde un atacante puede engañar al usuario para que haga clic en un marco invisible de la página, haciéndole tomar una acción que no quería tomar. También se encontró que puede ser víctima de un ataque de cross-site scripting (XSS) que permite al atacante ejecutar un script malicioso en el navegador de la víctima, secuestrando sesiones de usuario, contraseñas, o cualquier información sensible almacenada en el navegador. Otra opción es el ataque de XSS reflejado que permite el atacante hacer uso de correos engañosos logra que las victimas hagan clic en un enlace disfrazado para producir un robo de las cookies y luego la identidad del usuario. De las 5 aplicaciones, en todas se presentó estas amenazas.

CAPÍTULO 6: RECOMENDACIONES

Al gestionar una enorme cantidad de datos personales, se recomienda disponer de un adecuado sistema de protección de dicha información para así evitar riesgos. El tener controles adecuados ayudara a asegurar la disponibilidad, confidencialidad e integridad de toda la información personal que manejan, dándose a conocer a todo el personal de acuerdo con sus funciones y nivel de acceso a la información.

Se recomienda realizar un análisis de vulnerabilidades por cada sitio web determinando el riesgo inicial, las medidas recomendadas y el impacto que provoca, esto de manera anual por el personal junto con las herramientas y software que se requieren. Cuando de este análisis resulte un riesgo elevado se recomienda tomar las medidas de seguridad idóneas para mitigar este riesgo.

La necesidad de publicar información con los datos personales de los estudiantes como el nombre, el número de cedula o matricula se considera excesivo ya que con solo el número de matrícula puede identificarse al estudiante. Recomendamos regular y controlar el manejo de información y la manera en cómo se trata, procesa, conserva los datos personales de los usuarios.

Debido a que esta es una de las vulnerabilidades que se encontraron y considerando la sensibilidad de la información del aplicativo web de notas, es fácil vulnerar esta página de autentificación por medio de inyección SQL, asiendo ingeniería social o buscando información de los estudiantes en la web se podría ya acceder a este servicio, por tanto, se recomienda que este sea el cambio inmediato que se haga.

.

CAPÍTULO 7: REFERENCIAS

[1] "Ciberseguridad en la identidad digital y la reputación online Una guía de aproximación para el empresario índice," 2016.

[2] Comunidad OWASP, "OWASP Top 10 - 2017 Los diez riesgos más críticos en Aplicaciones Web," pp. 1–24, 2017.

[3] P. A. Grassi, M. E. Garcia, and J. L. Fenton, "Digital Identity Guidelines. NIST Special Publication 800-63-3," p. 34, 2017.

[4] R. Salas and D. Andrea, "INYECCIONES SQL," *Rev. Tecnol. e Innovación*, 2019.

[5] J. L. Fenton *et al.*, "Digital Identity Guidelines," *NIST Spec. Publ. 800-63B*, pp. 2–79, 2017.

[6] A. V. Galicia and J. Castellà-roca, "Privacidad."

[7] E. Bernardis, H. Bernardis, M. Berón, and G. A. Montejano, "Seguridad en servicios web," pp. 1094–1098, 2017.

[8] A. V. Fernández, J. Manuel, and C. Rodríguez, "Capítulo tercero Análisis de las ciberamenazas.," pp. 97–138.

[9] M. E. Cueva Hurtado and D. J. Alvarado Sarango, "Análisis de Certificados SSL / TLS gratuitos y su implementación como Mecanismo de seguridad en Servidores de Aplicación . (Analysis of free SSL / TLS Certificates and their implementation as Security Mechanism in Application Servers .)," *Enfoque UTE*, vol. v.7, pp. 273–286, 2017.

[10] M. Jones, J. Bradley, and N. Sakimura, "JSON Web Token (JWT)," *Ietf*, vol. 84, pp. 487–492, 2015.

[11] Sáinz Peña Rosa Maria, "Identidad_Digital," *Fund. Telef.*, no. la identidad digital, p. 140, 2016.

[12] H. R. González Brito and R. Montesino Perurena, "Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades frecuentes en aplicaciones

web," *Rev. Cuba. Ciencias Informáticas*, vol. 12, no. 4, pp. 52–65, 2018.

[13] R. Telem, M. Valentina, P. Mondrag, and E. P. Guill, "Servicios De Autenticación Y Autorización Orientados a Internet De Las Cosas Autentication and Autorization Services To the Internet of Things," vol. 17, no. 2, pp. 42–51, 2020.

[14] D. C. Bogotá, "Julian Camilo Alvarado Carlos Universidad Libre Facultad de Ingeniería Ingeniería de Sistemas," 2017.

[15] Tatsuyoshi Minobe, "Protección de la página web," p. 456、453、603, 2017.

[16] C. Flores Urgilés, B. Zhinin Aguayza, A. Segovia Cantos, M. Mayancela Zhinin, and J. Marlene García, "Evaluación de seguridad de la información en las páginas web pertenecientes a los municipios de la provincia del Cañar," *Kill. Técnica*, vol. 2, no. 1, p. 13, 2018.

[17] L. Álvarez, "Paradignas de la protección de datos personales en Ecuador," *Análisis del pryecto Ley Orgánica Protección a los Derechos a la Intimidad y Privacidad dobre atos Pers.*, no. 27, p. 19, 2017.

[18] M. Pérez, "Identidad Digital," *Telos*, vol. 28, no. La Identidad Digital., p. 4, 2012.

[19] "Pruebas de Penetración e Intrusión," pp. 1–11, 2019.

[20] J. V. Roig *et al.*, "Frequency of compromised passwords used by students and staff of Asia Pacific College: An analysis using NIST SP 800-63B and pwned passwords," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 482, no. 1, pp. 0–6, 2019.

[21] J. C. Guerrero, R. A. Jiménez, J. A. Muñoz, A. M. Zambrano, and G. A. Ojeda, "Aspectos fundamentales en la construcción de páginas web seguras basados en OWASP," *Univ. Marian. - Boletín Inf. CEI*, vol. 4, no. 2, pp. 1–45, 2017.

[22] F. D. E. Riesgo and Y. D. En, "PROFUNDIDAD EN APLICACIONES WEB," pp. 1–10, 2019.

[23] Primicias, «Empresa ecuatoriana protagoniza filtración de millones de datos,» *Primicias,* 2019.

[24] N. Mundo, «Filtración de datos en Ecuador,» *News Mundo,* 2019.

[25] P. Rochina, «Revista Digital,» 2018. [En línea]. Available: https://revistadigital.inesem.es/informatica-y-tics/huella-digital-internet/.